NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

DRAFT Implementation Guidance
Pending Submittal for ERO Enterprise Endorsement

Cyber Security – Communications Between Control Centers

Implementation Guidance for CIP-012-2

~~November 2021~~October 2022

RELIABILITY | RESILIENCE | SECURITY




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

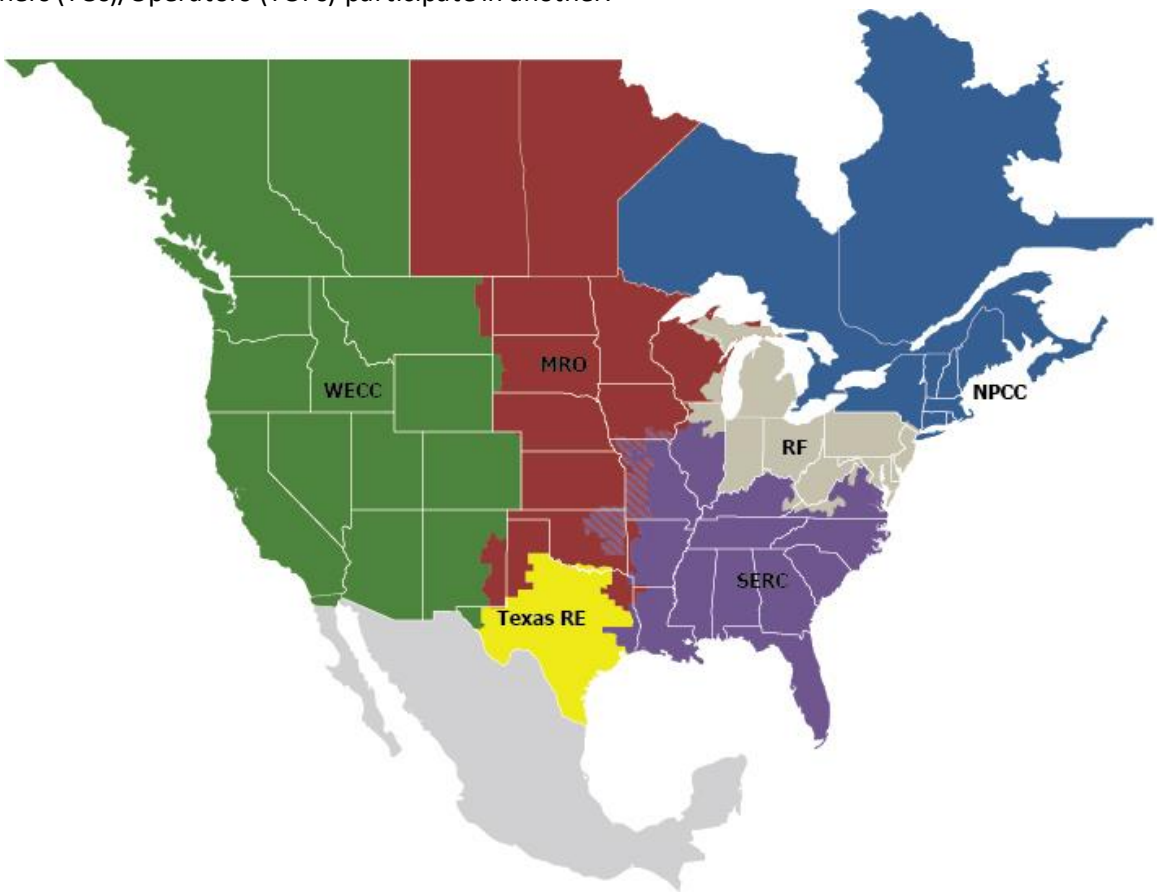
Table of Contents

Preface

Electricity is a key component of the fabric of modern society and the Electric Reliability Organization (ERO) Enterprise serves to strengthen that fabric. The vision for the ERO Enterprise, which is comprised of the North American Electric Reliability Corporation (NERC) and the six Regional Entities (REs), is a highly reliable and secure North American bulk power system (BPS). Our mission is to assure the effective and efficient reduction of risks to the reliability and security of the grid.

Reliability | Resilience | Security
Because nearly 400 million citizens in North America are counting on us

The North American BPS is made up of six RE boundaries as shown in the map and corresponding table below. The multicolored area denotes overlap as some load-serving entities participate in one RE while associated Transmission Owners (TOs)/Operators (TOPs) participate in another.



MRO	Midwest Reliability Organization
NPCC	Northeast Power Coordinating Council
RF	ReliabilityFirst
SERC	SERC Reliability Corporation
Texas RE	Texas Reliability Entity
WECC	WECC

Introduction

The Project 2020-04 Standard Drafting Team (SDT) drafted this Implementation Guidance to provide example approaches for compliance with CIP-012-2. Implementation Guidance does not prescribe the only approach, but highlights one or more approaches that would be effective in achieving compliance with the standard. ~~-~~Because Implementation Guidance only provides examples, entities may choose alternative approaches that better fit their individual situations[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-012-2 document.

This document will be reviewed and updated upon initiation of a standards development project to modify the CIP-012-2 standard.

Background

CIP-012-1

The Commission issued Order No. 822 on January 21, 2016 approving 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~~Bulk Electric System (BES) data communicated between ~~bulk electric system~~BES Control Centers in a manner that is appropriately tailored to address the risks posed to the ~~bulk electric system~~BES 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 one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable 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).

CIP-012-2

On January 23, 2020, the Federal Energy Regulatory Commission (FERC) issued Order No. 866 approving CIP-012-1 and directing NERC to develop modifications to CIP-012-1 to require Responsible Entities to develop one or more plan(s) to implement protections for the availability of communications links and data communicated between the ~~Bulk Electric System (~~BES~~)~~ Control Centers. In response to the directive in Order No. 866, the Project 2020-04 standard drafting team (SDT) developed modifications to CIP-012-2 to include availability requirements.

In Order No. 866, FERC also stated that "maintaining the availability of communication networks and data should include provisions for incident recovery and continuity of operations in a responsible entity's compliance plan." FERC recognized that the redundancy of communication links cannot always be guaranteed and acknowledged there should be plans for both recovery of compromised communication links and use of backup communication capability[2]. The SDT recognized that Responsible Entities may already have plans to address these contingencies in their CIP-008 or CIP-009 plan(s) and these could be referenced as part of their CIP-012 plan(s) to meet the requirement and avoid duplication of effort.

[1] NERC's Compliance Guidance Policy

[2] See Order No. 866 at PP 35-36.

The SDT modified requirements to provide Responsible Entities with the latitude to protect Real-time Assessment and Real-time monitoring data, mitigating against the risks posed by unauthorized disclosure, unauthorized modification and loss of availability both to satisfy the security and availability objectives.

Requirements

R1. The Responsible Entity shall implement, except under CIP Exceptional Circumstances, one or more documented plan(s) to mitigate the risks posed by unauthorized disclosure, unauthorized modification, and loss of availability of data used for Real-time Assessment and Real-time monitoring while such data is being transmitted between any applicable Control Centers. The Responsible Entity is not required to include oral communications in its plan. The plan shall include: *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning]*

1.1. Identification of ~~security and availability protection~~method(s) used to mitigate the risks posed by unauthorized disclosure~~,~~ and unauthorized modification~~, and loss of availability~~ of data used for Real-time Assessment and Real-time monitoring while such data is being transmitted between Control Centers;

1.2. Identification of ~~methods to be~~method(s) used ~~for~~to mitigate the ~~recovery of~~risk posed by loss of Real-time Assessment and Real-time monitoring data while such data is being transmitted between Control Centers;

~~**1.2.**~~**1.3.** Identification of method(s) used to recover communication links used to transmit Real-time Assessment and Real-time monitoring data between Control Centers;

~~**1.3.**~~**1.4.** Identification of where the Responsible Entity ~~applied security and availability protections~~implemented method(s) as required in ~~Part~~Parts 1.1 and 1.2; and

~~**1.4.**~~**1.5.** If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for ~~applying security and availability protection(s) to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers~~implementing method(s) as required in Parts 1.1 and 1.2.

General Considerations

Plan Development

As noted in the Technical Rationale and Justification for CIP-012-2, the focus of requirement R1 is implementing a documented plan to protect information that is critical to the real-time operations of the ~~Bulk Electric System~~BES while in transit between applicable Control Centers. With the approval of CIP-012-1 in Order 866, FERC also directed NERC to address protections regarding the availability of communications links and data communicated between ~~bulk electric system~~BES Control Centers. CIP-012-2 was developed to address these additional needed availability protections for data while in transit motion.

For CIP-012-2, the SDT ~~relied upon a~~modified the definition of availability as defined by National Institute of Standards and Technology (NIST~~):~~) [3]:

- Availability is defined as "Ensuring timely and reliable access to ~~and use of~~ information"[4]

The number of plan(s) and their content may vary depending on a Responsible Entity's management structure and operating conditions. The Responsible Entity may document as many plans as necessary to meet its needs. A Responsible Entity may also reference other CIP or Operations and Planning (O&P) plans within their CIP-012 plan that ~~include~~meet the required elements of the CIP-012 plan. For instance, they may reference within their CIP-012 plan the location within their CIP-009 plan that covers the recovery portion needed to meet the CIP-012 R1.~~2~~3 requirement. A Responsible Entity may choose to document one plan per Control Center or choose an all-inclusive, single plan for its Control Center communication environment. 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~~,~~ through 1.~~2, 1.3 and 1.4~~5 of requirement R1.

Responsible Entities should note that "associated data centers" are included in the Control Center definition. Also, data at rest and oral communication fall outside the scope of CIP-012[5].

Identification of Real-time Assessment and Real-time Monitoring Data

Responsible Entities can expect to receive or have received requests for Operations Planning Analysis, Real-time Assessment and Real-time monitoring data from their RC(s), BA(s) and TOP(s). These data requests, pursuant to the data specification from TOP-003 and IRO-010 requirements, may also include other types of data under the same request. CIP-012 requires protection only for Real-time Assessment and Real-time monitoring data. If the provided data specification does not indicate which data is Real-time Assessment and Real-time monitoring data, Responsible Entities could choose to conduct an assessment to identify this data from among the other data requested or being communicated. Once a data assessment is completed, the Responsible Entity should confirm its findings with the other communicating entity before applying security controls. If the Real-time Assessment and Real-time monitoring data is not clearly identified in the provided data specification, the Responsible Entity should document the methodology used and all actions taken to identify the Real-time Assessment and Real-time monitoring data.

[3] NIST SP 800-59 under Availability from 44 U.S.C., Sec. 3542 (b)(1)(C)

[4] ~~NIST SP 800-59 under Availability from 44 U.S.C., Sec. 3542 (b)(1)(C)~~

[5] NERC Order No. 866 at PP 11.

~~Identification of Security~~Mitigate Risks Associated with Unauthorized Disclosure and ~~Availability Protections~~Modification (R1.1)

Entities have latitude to identify and choose which security protections are used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers.

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 risks posed by unauthorized disclosure and unauthorized modification of applicable data. Physical protection is usually appropriate if two Control Centers are in close physical proximity such that the cabling and connections over which the data travels between them is physically protected between the two. Physical protection may also be appropriate when the equipment that is performing encryption is close to but still outside a Control Center and physical protection is used to protect the cabling and connections between the encryption endpoint and the Control Center itself.

Security protection implementation can be demonstrated in many ways. If a Responsible Entity uses physical protection, it may demonstrate implementation through review of an applicable Control Center floor plan with details subsequently confirmed through visual inspection, which identifies the physical security measures in place protecting the communication link. If the Responsible Entity uses logical protection, it may demonstrate implementation through an export of the device configuration which applies the security protection. Some examples include:

- An export of the configuration of a firewall showing the configuration of a VPN tunnel and the routing that directs applicable data through the VPN
- An export of the configuration of a transport level device that demonstrates encryption is enabled for applicable (or all) data
- Configuration of an application that demonstrates that the applicable data is encrypted from the application to the remote client or application

Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP or where other physical protection is applied.

Responsible Entities also have flexibility in determining how the CIP-012 availability component is implemented. Information identified as Real-time Assessment and Real-time monitoring data has a quality component that must be met via Requirements in IRO-010 and TOP-003. TOP-003 requirement R1.3 and R1.4 specifically represent time constraints regarding a Responsible Entity providing Real-time Assessment and Real-~~Time~~time monitoring data. An inability to access this data in a timely manner may impact a Responsible Entity's ability to provide or utilize this data when needed. A Responsible Entity must identify how the availability objective in CIP-012 is met while data is being transmitted. Availability can be achieved utilizing diversity, redundancy, or a combination of both. Diversity is using heterogeneity to minimize common mode failures[6]. For example, using two or more communication protocols or channels with differing characteristics. Redundancy is providing multiple protected instances of critical resources[7].

For example, having more than one circuit path or method to deliver the data. ~~–~~ A diverse and redundant solution for CIP-012 may use multiple circuit types (e.g., fiber optic and radio) and different ~~protocols~~systems (e.g., ~~DNP3~~a primary and ~~ICCP~~a secondary) to mitigate against multiple failure scenarios associated with data availability.

[6] NIST SP 800-160v2, 11

[7] NIST SP 800-160v2, 11

As noted previously, availability is generally defined as ensuring timely and reliable access to ~~and use of~~ information. The availability of data in transit can be achieved in a number of ways. One example method would be to use redundant circuits traversing discrete paths which would help ensure that, should one circuit path degrade or fail, data can continue to flow. Another discrete path approach is to get the same data points from multiple Control Centers. For example, a Reliability Coordinator may be willing to pass-through the originator's data to your Control Center, enabling a secondary source from a discrete path. ~~–~~This can be demonstrated via network diagrams indicating carrier diversity or discrete pathing.

Another method would be to use multiple ~~protocols~~systems that can aid availability in that one software solution providing data can fail independently of the other while data continues to flow via the alternate software/protocol stack. This can also be demonstrated utilizing network or system diagrams that identify the method(s) by which the protections are afforded by the solution.

~~Identification~~Mitigating Risks Posed by Loss of Data During Transit (R1.2)

Mitigating the risks posed by loss of data consists of taking measures to help protect the continued flow of data. This can be accomplished a variety of ways including redundant links, diverse systems or services designed to protect against loss of data. Real-time Assessment and Real-time monitoring data is required by the Responsible Entity to maintain the functionality and stability of the BES. The methods used to mitigate the loss of data should be agreed upon by both entities when this responsibility is shared between multiple entities.

Methods Used for ~~the~~ Recovery ~~of Communication Links~~ (R1.~~2~~3)

A component of maintaining availability is identifying, as part of the CIP-012 plan, the information needed to recover data communication links should they be interrupted. ~~–~~This objective is consistent with the TOP and IRO ~~O&P~~ Standards. Restoration of communications services can be addressed specifically within the Responsible Entity's CIP-012 plan or within other applicable plans referenced by their CIP-012 plan. ~~-~~When sharing data with other Responsible Entities, support responsibilities and restoration alignments can be documented in a variety of methods such as a joint procedure, a memorandum of understanding, contractual agreements, meeting minutes or other documentation of the defined responsibilities between the two parties.

The SDT also recognizes that the availability components within the plan may or may not be applied to Cyber Assets identified as BES Cyber Assets. When addressing restoration of links or circuits within a CIP-012 plan by referencing another plan (e.g., a CIP-009 recovery plan), the Responsible Entity should address within its CIP-012 plan any components of the availability solution that fall outside of the scope of the referenced plan. This may be achieved by inclusion within the other plan or directly within the CIP-012 plan.

Identification of Where Security and Availability Protections are Applied (R1.~~3~~4)

A Responsible Entity should consider its environment when identifying where security and availability protections should be applied. One approach is to implement the protections within the Control Center itself to ensure that data confidentiality and integrity is protected throughout the transmission. The Responsible Entity can identify where security protection is applied using a logical or physical location. The application of security in accordance with CIP-012 requirements does not add additional assets to the scope of the CIP Reliability Standards. Locations of applied security protection may vary based on many factors such as impact levels of the Control Center, different technologies, or infrastructures. Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP or where other physical protection is applied.

Identification of where a Responsible Entity applies security and availability protections could be demonstrated with a list or a Control Center diagram showing physical or logical security controls and components used to provide availability protections. Physical diagrams may require visual confirmation of these controls. These diagrams or a list could be included within the plan developed for requirement R1. A Responsible Entity could also use labels to identify on-site devices where CIP-012 security and availability protections are applied.

When exchanging data between two entities, if a Responsible Entity only manages one end of a communication link, the Responsible Entity is not responsible for identifying where the security protection is applied by the neighboring entity with which it is exchanging data. However, if a Responsible Entity has taken responsibility for both ends of the communication link (such as by placing a router within the neighboring entity's data center), then the Responsible Entity shall identify where the security protection is applied at both ends of the link. The Responsible Entity on each side of the link must also identify where their availability protections are applied, respectively.

Similarly, if a Responsible Entity owns and operates both Control Centers which are exchanging data (such as in the case of a primary and backup Control Center), then the Responsible Entity shall identify where security and availability protections are applied at both ends of the link.

Identification of Responsibilities when the Control Centers are Owned or Operated by Different Responsible Entities (R1.45)

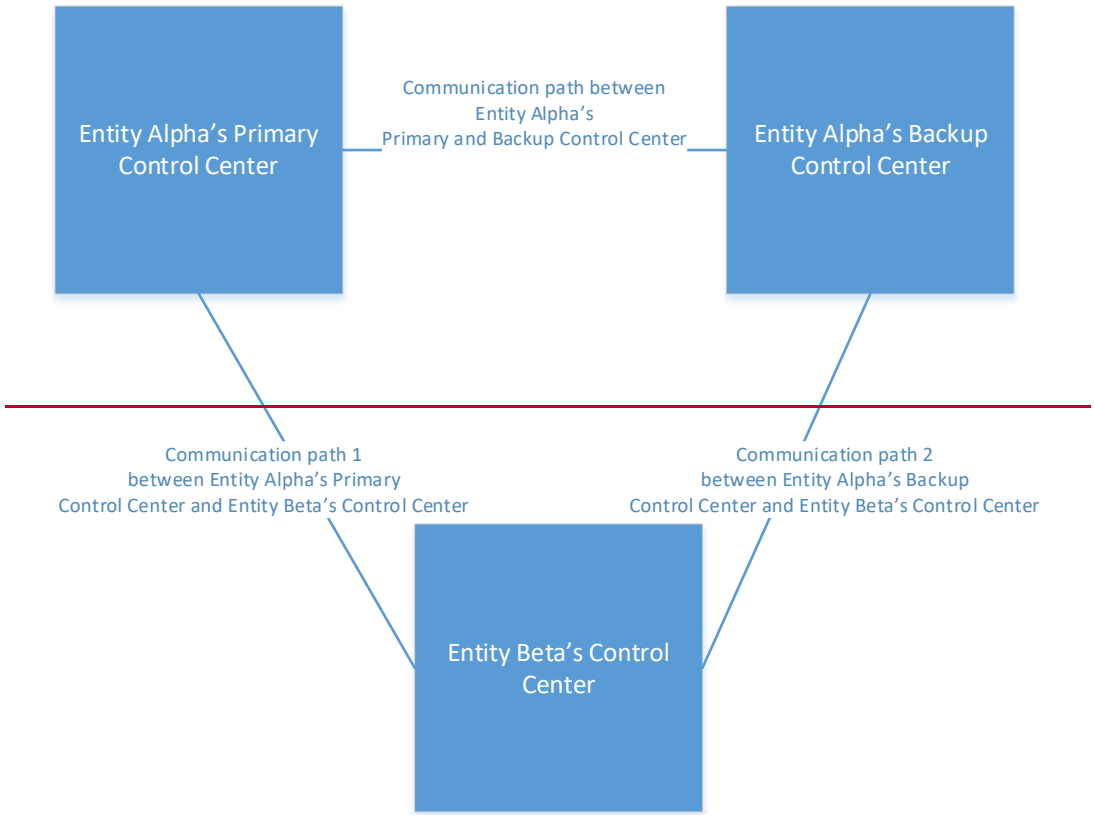
The Technical Rationale and Justification for CIP-012 identifies key considerations in the Control Center Ownership section when the communications are between Control Centers with different owners or operators. Many operational relationships between Responsible Entities are unique. Consequently, there is no single way to identify responsibilities for applying security and availability protections to the transmission of Real-time Assessment and Real-time monitoring data between Control Centers. Discussions between Responsible Entities might identify requirements for after-hours support in situations where data availability is reliant on independent actions such as an ICCP link reset.

The implementation of responsibilities must be documented to clearly identify the responsible parties and the point of demarcation where responsibility of the communications link transfers from one entity to the other. This documentation may include network diagrams, a joint procedure, a memorandum of understanding, or meeting minutes, documenting the defined responsibilities for each party.

Where the operational obligations of an entire communication link, including both endpoints, belong to the Control Center of another Responsible Entity, the Responsible Entity without operational obligations for the communication link may demonstrate compliance by ensuring the communications link endpoint is within its Control Center, which could be limited to including the communication link endpoint within a PSP or where other physical protection is applied.

Reference Model

For this Implementation Guidance, the SDT uses a basic reference model of Primary and Backup Control Centers (Entity Alpha) to illustrate approaches to demonstrating 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 model does 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.



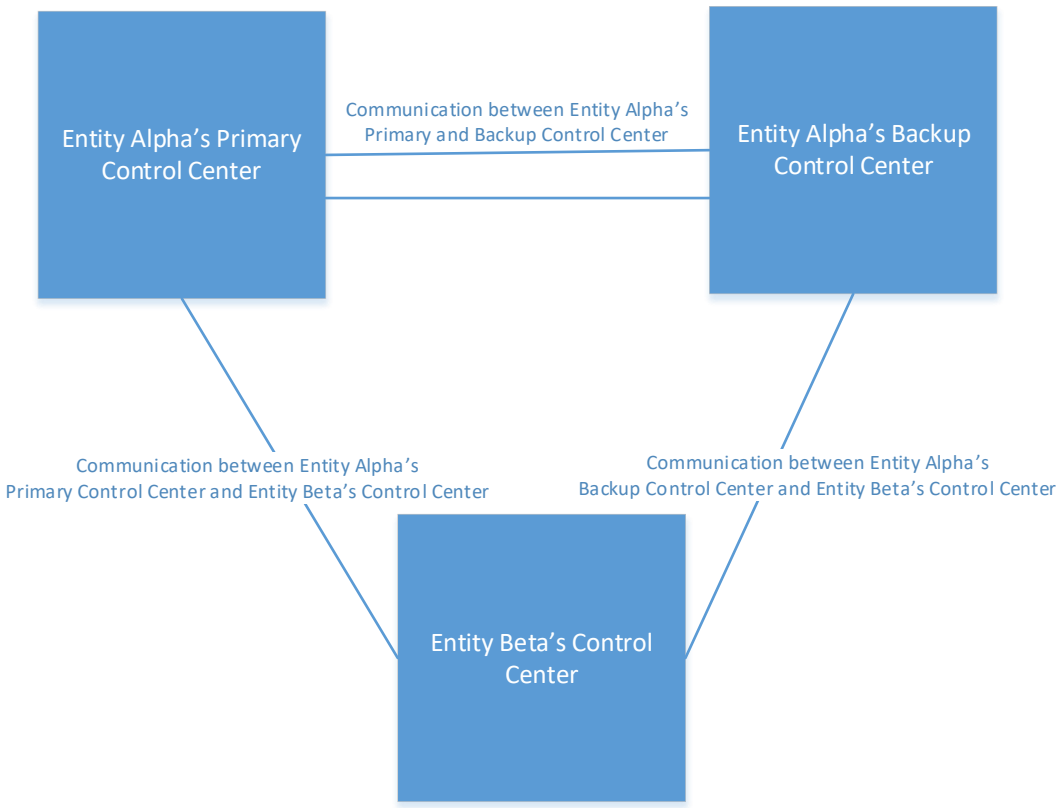


Figure 1: High Level Block Diagram of Reference Model Control Centers

Reference Model Discussion

Requirement R1 requires the implementation of a documented plan. To comply with requirement R1, one approach to a plan is to first determine which communications are in scope of CIP-012. There are multiple ways to identify an entity's scope in requirement 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.

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 data; or (2) communication links which are used to transmit Real-time Assessment and Real-time monitoring data between Control Centers. In either case, Entity Alpha could refer to the data specification for Real-time Assessment and Real-time monitoring data identified in TOP-003 and IRO-010. These ~~O&P Standards~~standards also include the periodicity requirements of the data, to establish the bounds for availability. For this reference model scenario, identifying the communication links used to transmit Real-time Assessment and Real-time monitoring 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 data, Entity Alpha determined that it communicates applicable data between its primary and backup Control Centers across ~~a single~~redundant communication ~~link~~links. 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~~communication links the applicable data traverses, Entity Alpha now considers the ~~four~~five required elements of its required ~~communications~~communication links between Control Centers for its plan.

Identification of Security ~~and Availability~~ Protection

Entity Alpha must ensure that protection is applied where identified in its CIP-012 plan. The protection must also meet the security objectives of mitigating the risks posed by unauthorized disclosure and unauthorized modification of applicable data while in transit between Control Centers. ~~Entity Alpha must also ensure that this protection accounts for a need to ensure appropriate availability of the data. The identification of security protection could be demonstrated by a network diagram similar to that shown in Figure 2 or Figure 3 that identifies one or more communication segments between Control Centers and the protections implemented per segment.~~

In a simple case where the security protection is applied at a point within 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 ~~as long as measures for availability are also addressed.~~. For this case, shown in Figure 2, Entity Alpha implements a Virtual Private Network (VPN) connection across a communication circuit for each of its three in-scope communication links along with data source failover capability. ~~-~~To meet the security objective, Entity Alpha documents that its VPN uses Internet Protocol security (IPsec) with encryption and when failing over to the backup control center, the data traverses an alternate path.

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. ~~-~~In Figure 3, the encryption endpoint is located on transport equipment (WAN router) located outside the Control Center. Entity Alpha then physically protects the cabling and connections over which the data travels until it is within the Control Center (CIP-006 R1.10). ~~-~~The SDT notes that the same technical architecture could exist where the responsibilities of the registered entities are different. ~~-~~Therefore, as shown in Figure 2 & 3, in the scenario where entity Alpha owns and operationally manages the communication link and endpoint equipment, Entity Beta is responsible for ensuring the communication endpoint of the communication link is within a Control Center. ~~-~~Entity Beta ensures Entity Alpha's communication link endpoint equipment is within a Control Center by including the communication endpoint within a Control Center PSP. The physical controls for the PSP are described in CIP-006 documentation and do not need to be repeated for this requirement. This satisfies Entity Beta's obligation for Part 1.1 ~~and 1.2~~.

While these scenarios are all specific to communication links, it is possible that Entity Alpha and Entity Beta achieve the security objective by applying protections to the data rather than directly to 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 risks posed by unauthorized disclosure and unauthorized 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 SSL/TLS or other application layer encryption methods to exchange applicable data. ~~The security objective for availability is achieved via alternate communication link pathing from the backup control center.~~

~~Identification~~

Mitigating the Risk Posed by Loss of ~~Measures~~Data

In Figure 2, Entity Alpha must also ensure that this protection accounts for a need to ensure appropriate availability of the data. Entity Alpha has two circuits going into the communications carrier cloud through which it communicates with its back up control center and Entity Beta. Entity Beta has two communication links going into

the communications carrier cloud through which it communicates with Entity Alpha's primary and secondary Control Centers. This gives each entity at least two paths to each of the Control Centers with which they need to communicate. This could be demonstrated by a network diagram similar to that shown in Figure 2 or Figure 3 that identifies one or more communication segments between Control Centers and the protections implemented per segment.

Methods Used for ~~the~~ Recovery of Communication Links

Entity Alpha has a comprehensive CIP-009 plan for disaster recovery. Within its recovery plan, Entity Alpha has the information needed to not only restore the BES Cyber Systems covered by CIP-009, but also the key network infrastructure needed for Control Center to Control Center communications. To meet the security objective of measures used for the recovery of communications links used for Control Center to Control Center communication, Entity Alpha has referred to the CIP-009 recovery plan within the CIP-012 plan, referencing the applicable area within the plan that describes restoration of the necessary communications paths.

Identification of Where Security and Availability Protection is Applied by the Responsible Entity

Similar to the identification of security protection above, the identification of where security protection is applied can also be demonstrated by a network diagram similar to those found in Figures 2 and 3.

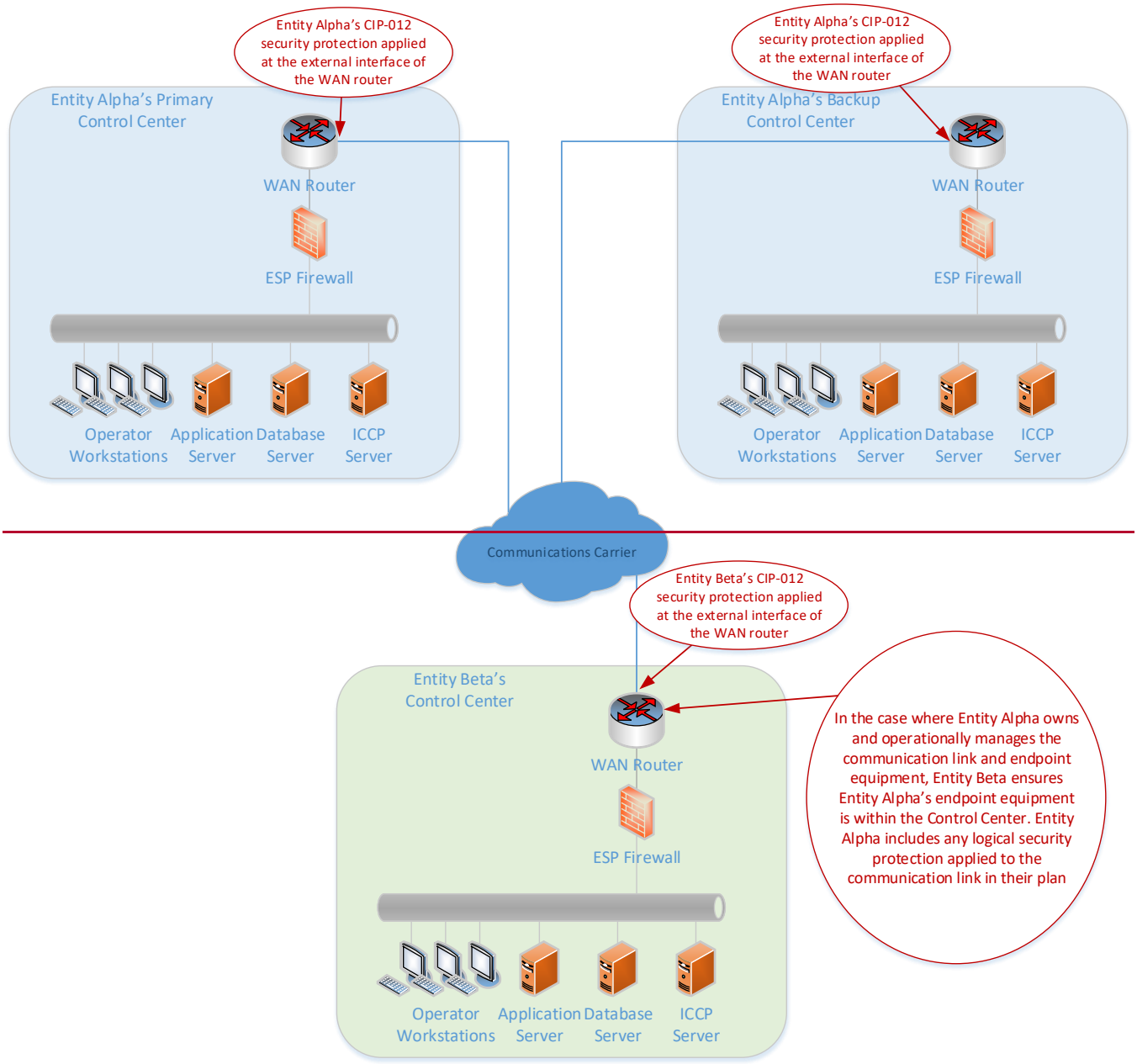
- Figure 2 shows the identification where CIP-012 security protection is applied for the Entity Alpha reference model when a single encrypted tunnel is used to implement the required protection. Entity Alpha has identified that security protection is applied at each of its Control Centers on the external Ethernet interface on the WAN router. Entity Beta, in this example, has redundant communications through communications carriers to both Entity Alpha's primary and secondary Control Centers. While the diagram depicts where Entity Beta has applied security protection for illustrative purposes, Entity Alpha is not responsible for identifying where Entity Beta has applied security protection.
- In order to understand the application of security protection in context of who controls the communication link, it may be helpful to identify both where CIP-012 security protection is applied and the location of the telecommunications carrier (telco) demarcation point. Figure 3 provides such an example where the telco demarcation point may not be within the Control Center and based the facts and circumstances surrounding this scenario, Entity Alpha has implemented a combination of security controls to comply with CIP-012. In this scenario, Entity Alpha identifies that it has applied physical security protection for its PSP and continuing for its WAN router and that it has applied logical security protection (encryption) at the WAN router. 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.
- Figures 2 & 3 provide an example of where the operational obligations of an entire communications link, including both endpoints, belong to Entity Alpha. In this case, Entity Beta may be responsible for ensuring the communications endpoint of the communications link is within their Control Center. Entity Beta ensures Entity Alpha's communication link endpoint equipment is within a Control Center by including the communication endpoint within a Control Center PSP. The documentation provided for Part 1.1 by Entity Beta fulfills this obligation.
- The data-centric scenario described above is less intuitive for identifying where security protection is applied by Entity Alpha. If security protection is applied at the application layer, Entity Alpha could reasonably identify the application or service applying the security as the location of where security protection is applied.
- ~~Availability protection~~Mitigating the risk of the loss of data transmission capability can be shown with network diagrams showing multiple circuits, redundant systems, application details or other documentation describing the protections used.

Identification of 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~~IPsec authentication.

Rather than use a pre-shared key, Entity Alpha and Entity Beta may decide to use digital certificates for the ~~IPSec~~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.

In the example where the communication link and endpoint equipment are owned by Entity Alpha, both entities should include ownership responsibilities in their plans satisfying requirement 1.~~4~~5. Examples include but are not limited to, a letter indicating ownership or responsibility, a copy of a contract indicating ownership or responsibilities, an excerpt from an operational agreement or manual indicating ownership or responsibility. This documentation should also include information regarding roles or responsibilities for maintaining the availability of the circuits, systems, or flow of data.


Entity Alpha's CIP-012 security protection applied at the external interface of the WAN router
Entity Alpha's Primary Control Center
WAN Router
ESP Firewall
Operator Workstations
Application Server
Database Server
ICCP Server
Entity Alpha's CIP-012 security protection applied at the external interface of the WAN router
Entity Alpha's Backup Control Center
WAN Router
ESP Firewall
Operator Workstations
Application Server
Database Server
ICCP Server
Communications Carrier
Entity Beta's CIP-012 security protection applied at the external interface of the WAN router
Entity Beta's Control Center
WAN Router
ESP Firewall
Operator Workstations
Application Server
Database Server
ICCP Server
In the case where Entity Alpha owns and operationally manages the communication link and endpoint equipment, Entity Beta ensures Entity Alpha's endpoint equipment is within the Control Center. Entity Alpha includes any logical security protection applied to the communication link in their plan

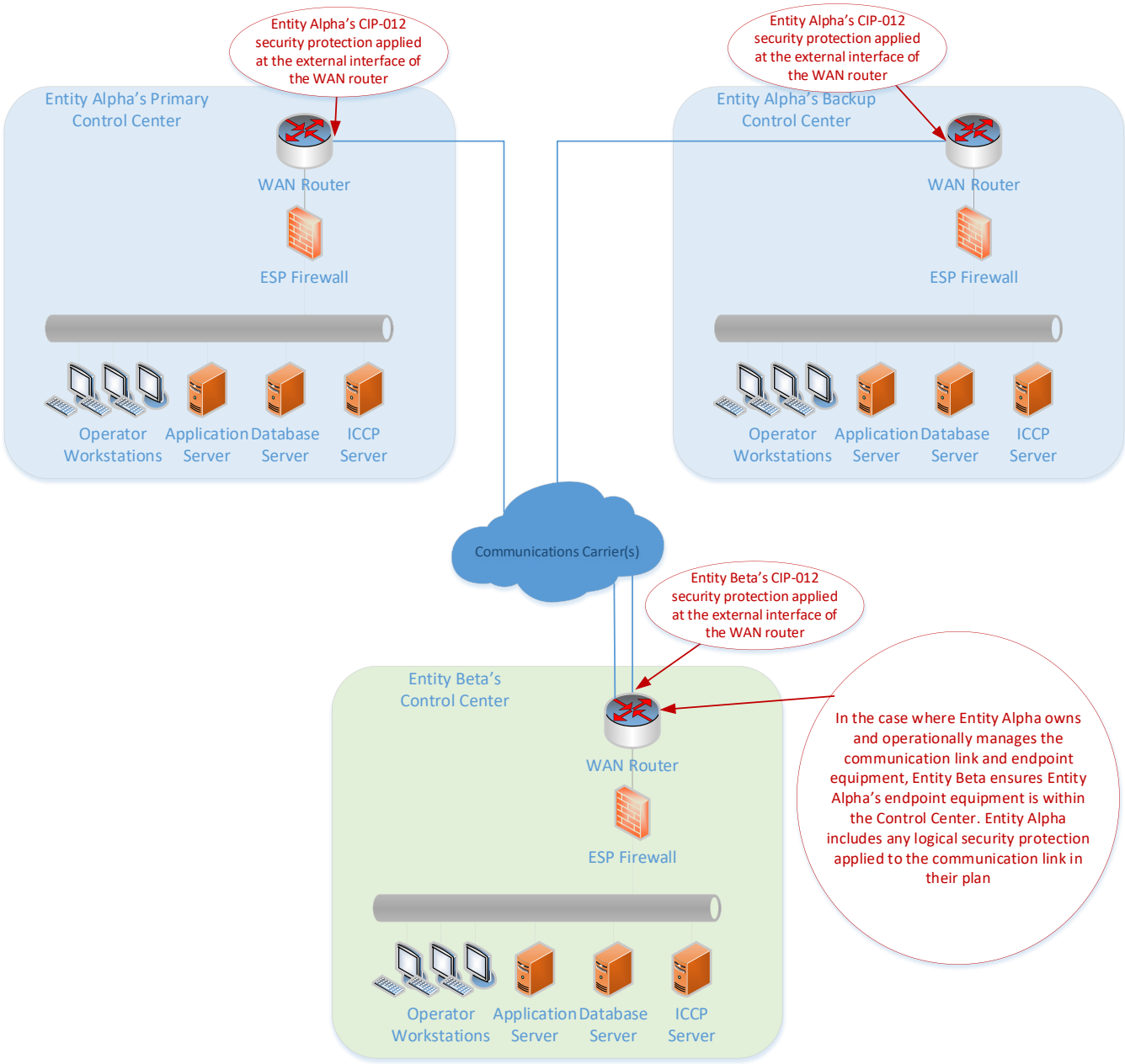
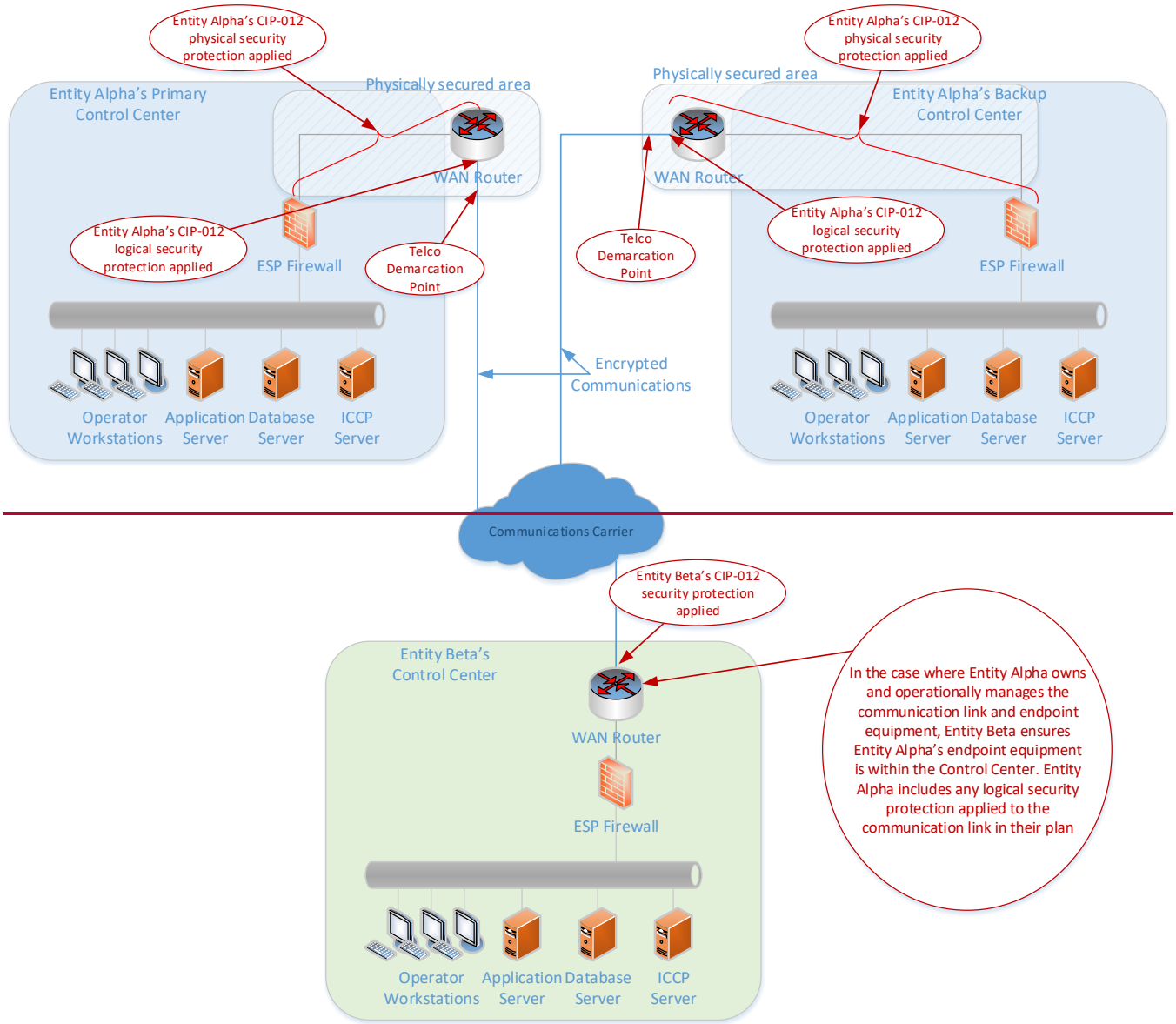


Figure 2: Network diagram and identification of where security protection is applied


Entity Alpha's CIP-012 physical security protection applied
Entity Alpha's Primary Control Center
Physically secured area
WAN Router
Entity Alpha's CIP-012 logical security protection applied
ESP Firewall
Telco Demarcation Point
Operator Workstations
Application Server
Database Server
ICCP Server
Entity Alpha's CIP-012 physical security protection applied
Physically secured area
Entity Alpha's Backup Control Center
WAN Router
Telco Demarcation Point
Entity Alpha's CIP-012 logical security protection applied
ESP Firewall
Operator Workstations
Application Server
Database Server
ICCP Server
Encrypted Communications
Communications Carrier
Entity Beta's CIP-012 security protection applied
Entity Beta's Control Center
WAN Router
ESP Firewall
Operator Workstations
Application Server
Database Server
ICCP Server
In the case where Entity Alpha owns and operationally manages the communication link and endpoint equipment, Entity Beta ensures Entity Alpha's endpoint equipment is within the Control Center. Entity Alpha includes any logical security protection applied to the communication link in their plan

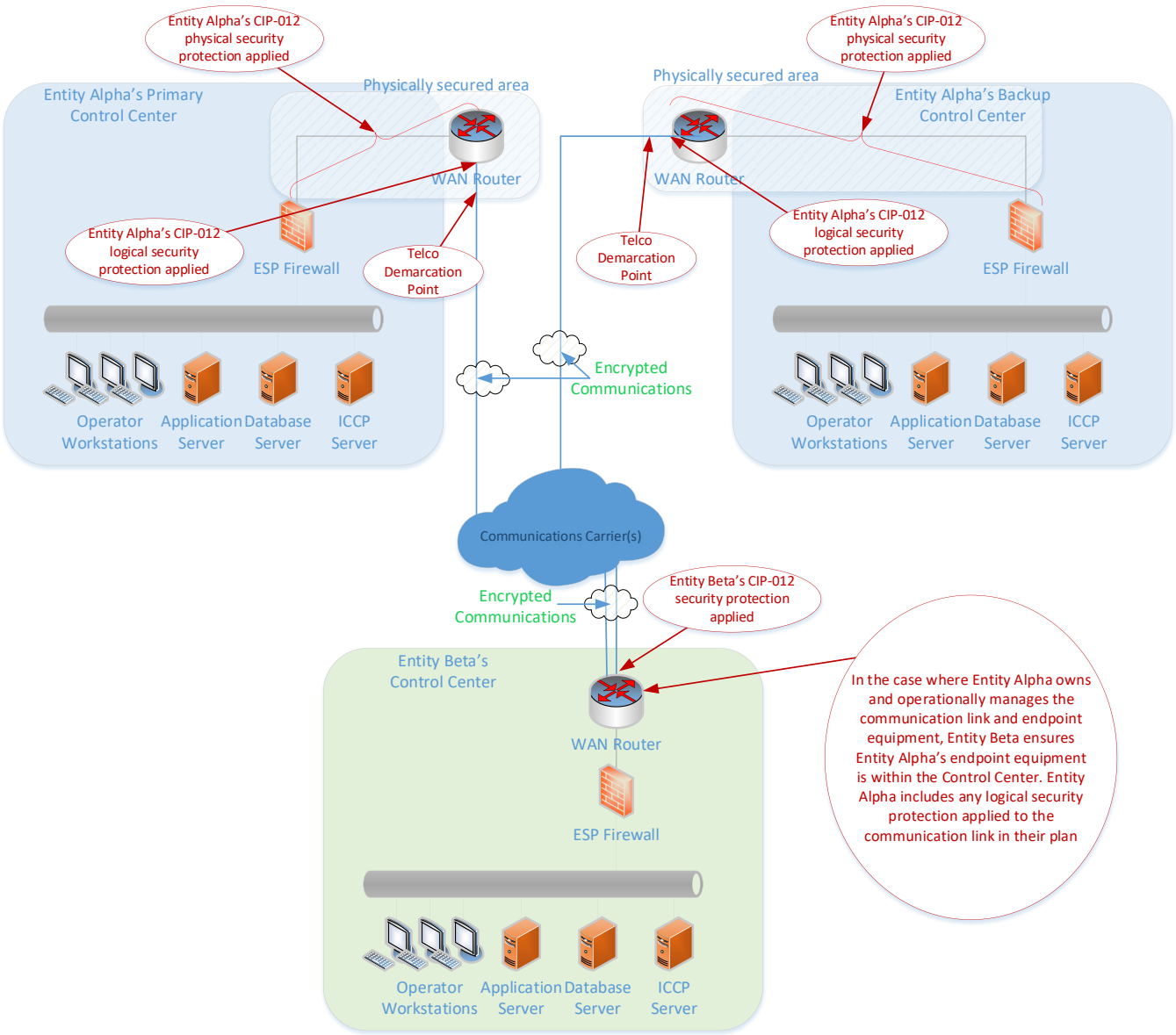


Figure 3: Network diagram using a combination of controls for CIP-012

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