NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Industry Webinar

Project 2020-04 Modifications to CIP-012

October 11, 2023

RELIABILITY | RESILIENCE | SECURITY

Agenda

- Administrative Items
    - Review NERC Antitrust Compliance Guidelines and Public Announcement
- FERC Order 866
- Presenters
    - Standard Drafting Team
        - Chair, Joseph Gatten, Xcel Energy
        - Vice Chair, Pete Rembusch, Duke Energy
    - NERC Staff
        - Ben Wu (Senior Standards Developer)
- Project 2020-04 Status
- Proposed CIP-012 Revisions
- Implementation Plan for CIP-012
- Next Steps
- Questions and Answers

NERC Antitrust

- 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. It is the responsibility of every NERC participant and employee who may in any way affect NERC’s compliance with the antitrust laws to carry out this commitment.

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

NERC Public Disclaimer

- Public Announcement
  - Participants are reminded that this meeting is public. Notice of the meeting was widely distributed. Participants should keep in mind that the audience may include members of the press and representatives of various governmental authorities, in addition to the expected participation by industry stakeholders
- Presentation Material
  - Information used herein is used for presentation purposes and may not reflect the actual work of the official posted materials
- For the official record
  - This presentation is not a part of the official project record
  - Comments must be submitted during the formal posting
- Q&A Session
  - Q/A feature or the raise hand feature

FERC Order 866

- January 23, 2020, the Federal Energy Regulatory Commission (FERC) issued Order No. 866 approving CIP-012-1
- The Order approving CIP-012 also included an additional directive
    - The order directed NERC to develop modifications to the CIP Reliability Standards to require protections regarding the *availability* of communication links and data communicated between bulk electric system Control Centers
    - Order 866 also stated, “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.”

Standard Drafting Team (SDT)

Name	Organization/ Company
Joseph Gatten (Chair)	Xcel Energy
Pete Rembusch (Vice Chair)	Duke Energy
Robert Melis	CAISO
Nicholas Morton	AEP
Matthew Hartung	EDP
Gianfranco Cataudella	ORU
David Pacheco	SRPNET

Project Status

- The third posting started on October 3, 2022 and ended on November 29, 2022 with 57.87% approval while the Implementation Plan got 71.28% approval from the industry.
- On March 22, 2023, Standards Committee appointed additional members to the Project 2020-04 Modifications to CIP-012 Standard Drafting Team (SDT).
- The SDT met 13 times, including a two-day in person meeting, since May, 2023 to review the comments received from the third posting and modifying the Standard based on the feedback received.
- Current posting started on September 19, 2023 and will end on November 2, 2023.

Proposed CIP-012 Revisions

Changes made to the Standard Language of CIP-012-1

- **Parent Requirement R1**:
  - Inclusion of “Availability” into Requirement Language to address FERC Order 866
  - Updated reference to “Real-time Assessment and Real-time monitoring data” to “data used in” and “while such data is”… so not to infer that there is a defined term of Real-time Assessment and Real-time monitoring data

Proposed CIP-012 Revisions

Changes made to the Standard Language of CIP-012-1

- **Sub Requirements:**
  - R1.1
    - ○ Updated language from the identification of "security protections" to the identification of "methods"
  - R1.2
    - ○ Updated Requirement language from "Identification of methods used to mitigate the risks posed by <u>loss of data</u>" to Identification of methods used to mitigate the risks posed by "loss of the <u>ability to communicate</u>"

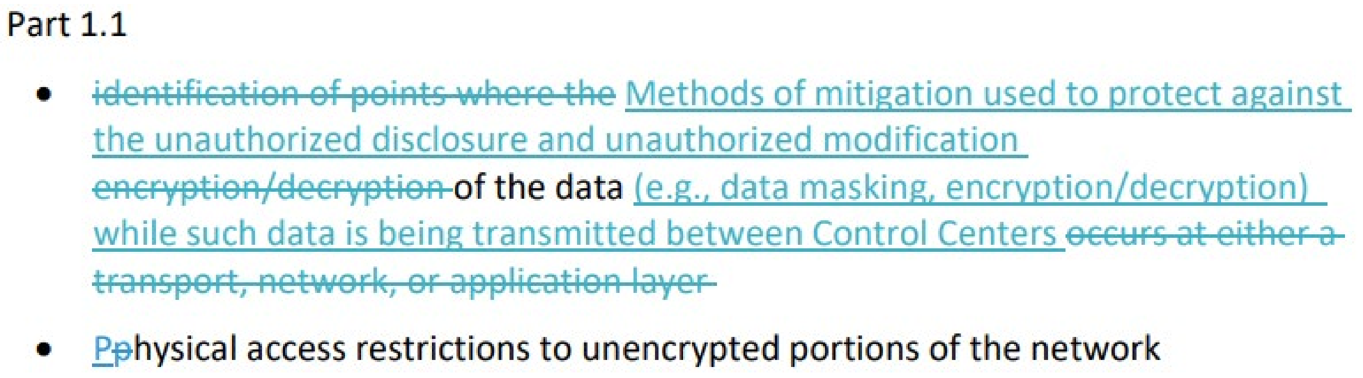
Proposed CIP-012 Revisions

Changes made to the Standard Language of CIP-012-1

- **Sub Requirements:**
  - R1.3
    - Updated language from "the identification of methods used to recover communication links" to the identification of methods used to initiate the recovery of communication links
  - R1.4
    - No updates
  - R1.5
    - Updated language to include new sub-Requirement 1.3 in addition to the previously identified sub-Requirements of R1.1 and R1.2 for the identification of responsibilities for Responsible Entities that own and operate differing Control Centers

Changes made to the Measures Section of CIP-012-1

Proposed CIP-012 Revisions Measures



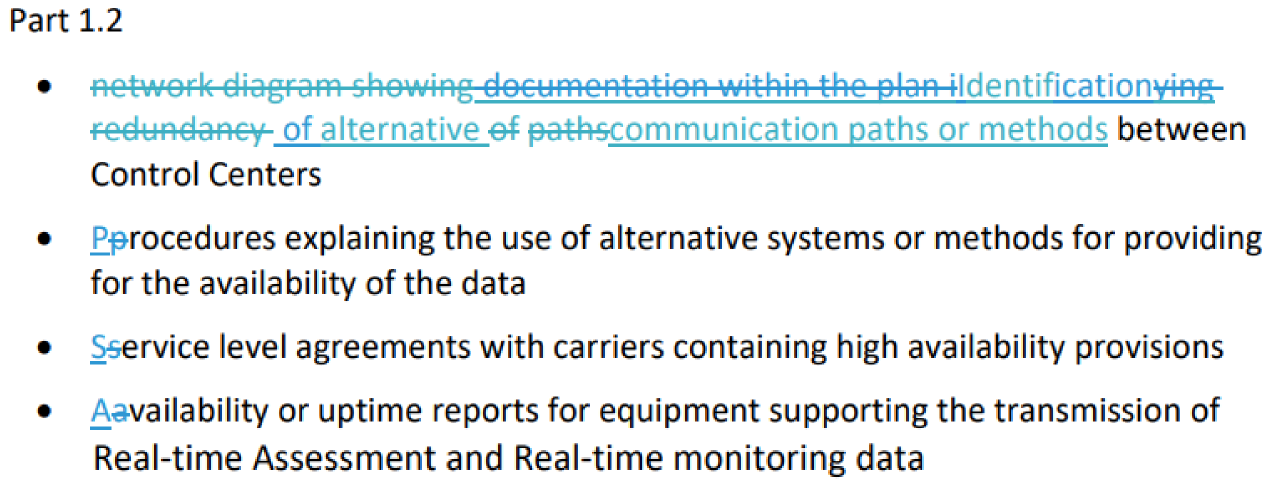
Part 1.1

- ~~identification of points where the~~ Methods of mitigation used to protect against the unauthorized disclosure and unauthorized modification ~~encryption/decryption~~ of the data (e.g., data masking, encryption/decryption) while such data is being transmitted between Control Centers ~~occurs at either a transport, network, or application layer~~
- P~~p~~hysical access restrictions to unencrypted portions of the network

Identification of Methods – *Unauthorized Disclosure & Unauthorized Modification*

- Minor update since previous Draft (Draft 3)
- Logical or physical protections, or a combination of both
- Logical protection (e.g., data masking, encryption), *such as*:
  - Encryption via VPN routers providing IP Security (IPSEC) tunneling
  - Encryption details & key type (e.g., pre-shared)
  - Inventory of end-point Cyber Assets (e.g., DMVPN routers)
- Physical (e.g., PSP and other physical protections), *such as*:
  - Physical Security Perimeters (PSPs) used for protection of in-scope encryption/decryption points and any relevant unencrypted links/path sections
  - Other physical protections such as physical secured area/boundary (e.g., Demarc room), fiber in conduit for unencrypted links to/from PSPs, and badge readers for access to physical boundary area

Proposed CIP-012 Revisions Measures



Part 1.2

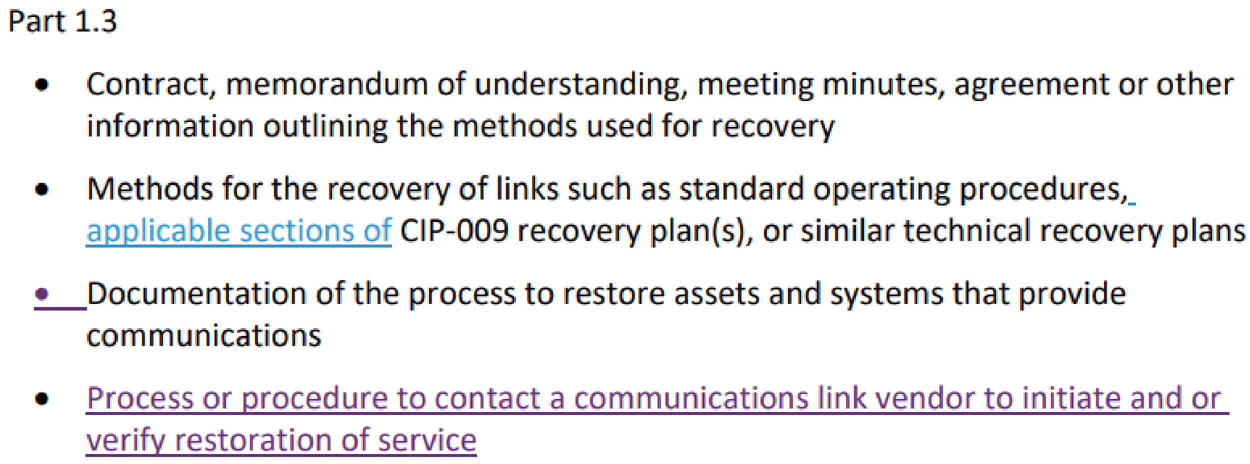
- ~~network diagram showing documentation within the plan i~~Identification~~ying redundancy~~ of alternative ~~of paths~~communication paths or methods between Control Centers
- P~~p~~rocedures explaining the use of alternative systems or methods for providing for the availability of the data
- S~~s~~ervice level agreements with carriers containing high availability provisions
- A~~a~~vailability or uptime reports for equipment supporting the transmission of Real-time Assessment and Real-time monitoring data

Identification of Methods – *Loss of Ability to Communicate*

- Minor update since previous Draft (Draft 3)
- Redundant links/alternative communication paths, *such as*:
  - A pair of routers providing redundant links (i.e., two circuits) into VPN mesh connection between each router and its peers at other facilities
  - Traffic would be managed by redundant router in the event of a Cyber Asset failure
- Use of dual Internet Service Provider (ISPs) for redundancy, *such as*:
  - Admins use two ISP links; one acts as a primary connection and the other acts as a backup connection
- Service Level Agreements (SLAs) with carriers detailing high-availability of network, *such as*:
  - SLA related to the ISP network redundancy as it relates to support of VPN solution

NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Proposed CIP-012 Revisions Measures



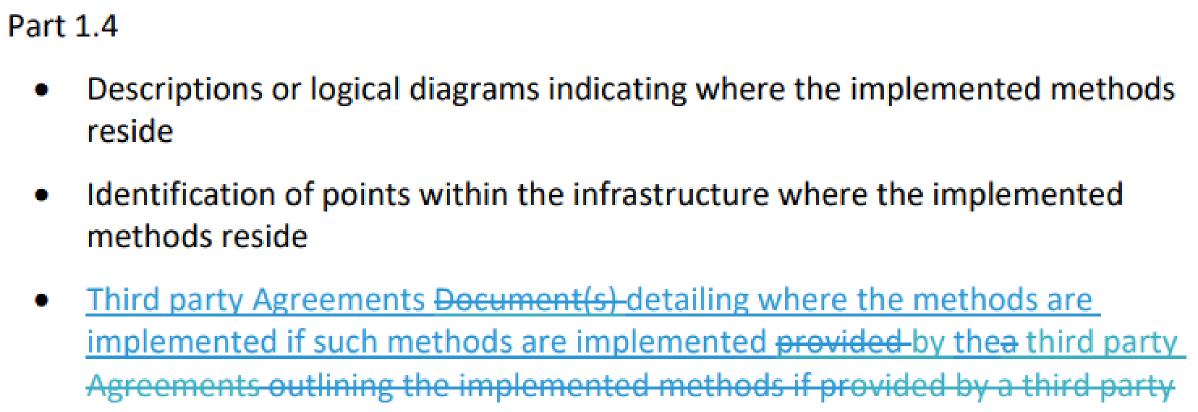
Part 1.3

- Contract, memorandum of understanding, meeting minutes, agreement or other information outlining the methods used for recovery
- Methods for the recovery of links such as standard operating procedures, applicable sections of CIP-009 recovery plan(s), or similar technical recovery plans
- Documentation of the process to restore assets and systems that provide communications
- Process or procedure to contact a communications link vendor to initiate and or verify restoration of service

Identification of Methods – *Used to Initiate Recovery of Communication Links*

- Minor update since previous Draft (Draft 3)
- Procedures/Documentation as primary example measures (process/procedure/methods)
  - Use of CIP-012 procedures to detail the methods used for recovery, which could include the Entities’ stance on declaration of a CIP Exceptional Circumstances (CEC) for protection failures
  - References within CIP-012 procedures/plans to CIP-009 procedures related to recovery plans of systems
  - Standalone technical documentation for restoration of Cyber Assets (e.g., DMVPN routers)
  - Procedures for coordination with third-party vendors/Internet Service Providers (ISPs), etc. for initiating service restoration

Proposed CIP-012 Revisions Measures



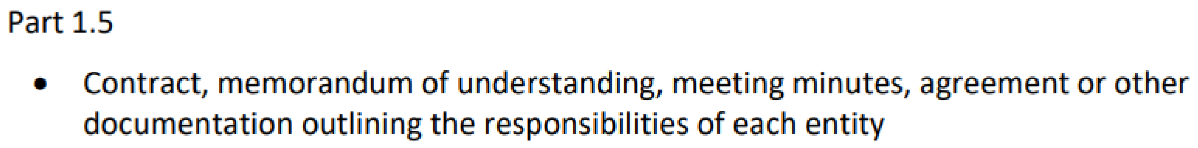
Part 1.4

- Descriptions or logical diagrams indicating where the implemented methods reside
- Identification of points within the infrastructure where the implemented methods reside
- Third party Agreements ~~Document(s)~~ detailing where the methods are implemented if such methods are implemented ~~provided~~ by the~~a~~ third party ~~Agreements outlining the implemented methods if provided by a third party~~

Identification of Where – *Responsible Entity Implemented Methods*

- Minor update since previous Draft (Draft 3)
- Logical diagrams indicating and/or documented records describing where implemented methods reside is still the primary example measure
  - Many Entities using same template as used for documentation of Electronic Security Perimeter(s)
  - Consider supplementing ESP-style diagrams with unique records of each link in scope of CIP-012
- Addition of third-party Agreements if a third-party is used to implement method(s) as required in Parts 1.1 and 1.2

Proposed CIP-012 Revisions Measures



Part 1.5

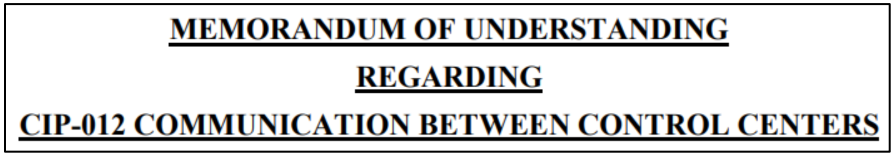
- Contract, memorandum of understanding, meeting minutes, agreement or other documentation outlining the responsibilities of each entity

Identification of Responsibilities – *if CCs owned/operated by different Responsible Entities*

- No changes since previous Draft (Draft 3)
- Contract, Memorandum of Understanding (MOU), meetings minutes, agreement, joint procedure, or other documentation
- Verification letter used to confirm how TOP or IRO data specifications are being used/not used by other Entities
- Some ISOs/RTOs have developed manuals outlining data exchange requirements that may also outline associated responsibilities
- Many entities have developed MOU/Agreement templates for use/re-use for multiple relationships

PJM Manual 01:

Control Center and Data Exchange Requirements



MEMORANDUM OF UNDERSTANDING

REGARDING

CIP-012 COMMUNICATION BETWEEN CONTROL CENTERS

Changes made to Draft 3 of the Rationale of CIP-012-1

- **Updates made to General Considerations for Requirement R1**
  - Identification of Methods in place of Security and Availability Protections
  - Physical Protections (R1.1)
  - Loss of the ability to communicate (R.2)
  - Measures to initiate recovery (R1.3)

- **Updates made in Overview of Confidentiality Integrity, and Availability section**
  - Removed examples of ways to mitigate risk from rationale and identified that examples are in the Measures section of the Standard

- **Conforming and non-substantive changes made throughout the document**

Changes made to the Implementation Guidance of CIP-012-1

Implementation Guidance for CIP-012

- Implementation Guidance
  - Acronym/term cleanup across document
  - R1 –
    - Availability definition clarification
    - Revision to referencing documents outside of the documented plan
    - Enhanced language around the loss of *availability to communicate* data vs. the data itself
  - Identification of Security Protection –
    - Focus on communication protection:
      - Enhanced Figure 2 (logical protection application): Addition of Encrypted Communications Link
      - Enhanced Figure 3 (combination of controls): Clarification of "…where other physical protection is applied."
        - Figure updated to separate PSP and Physically Secured Area should this situation exist

Implementation Guidance for CIP-012 contd.

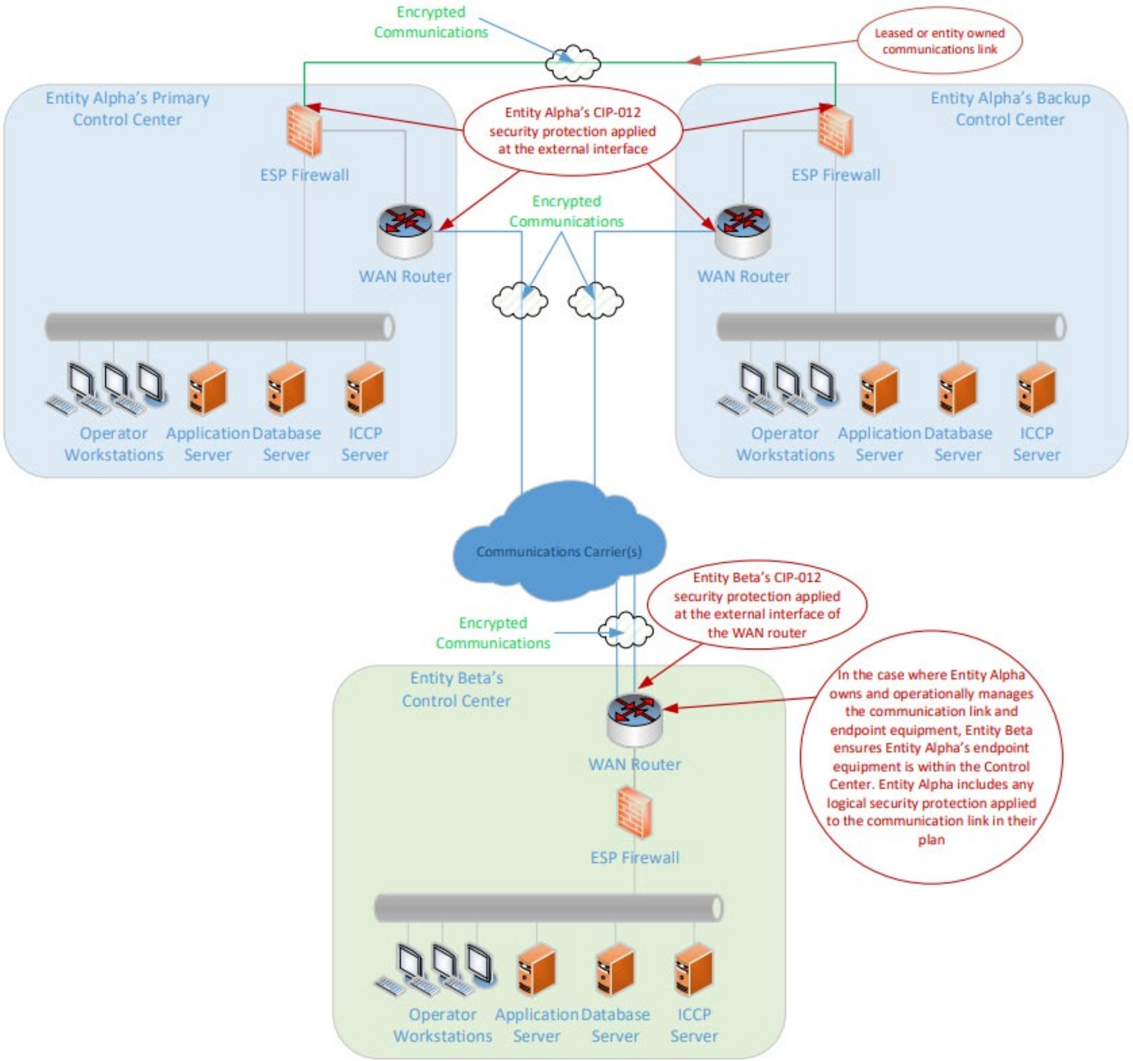
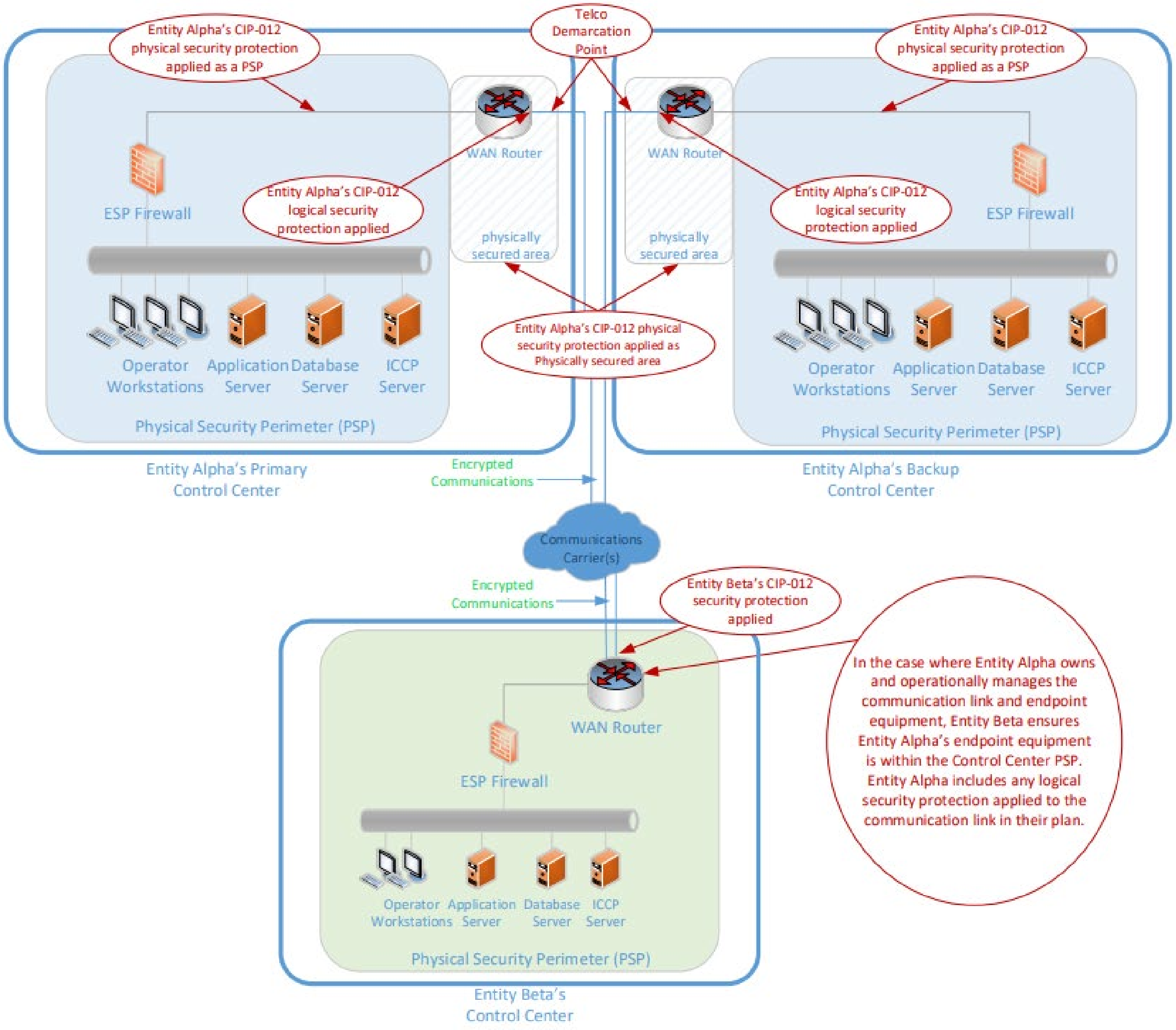

Encrypted Communications
Leased or entity owned communications link
Entity Alpha's Primary Control Center
Entity Alpha's CIP-012 security protection applied at the external interface
Entity Alpha's Backup Control Center
ESP Firewall
ESP Firewall
Encrypted Communications
WAN Router
WAN Router
Operator Workstations
Application Server
Database Server
ICCP Server
Operator Workstations
Application Server
Database Server
ICCP Server
Communications Carrier(s)
Entity Beta's CIP-012 security protection applied at the external interface of the WAN router
Encrypted Communications
Entity Beta's Control Center
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
WAN Router
ESP Firewall
Operator Workstations
Application Server
Database Server
ICCP Server

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

Implementation Guidance for CIP-012 contd.



Entity Alpha's CIP-012 physical security protection applied as a PSP

Entity Alpha's CIP-012 physical security protection applied as a PSP

Entity Alpha's CIP-012 logical security protection applied

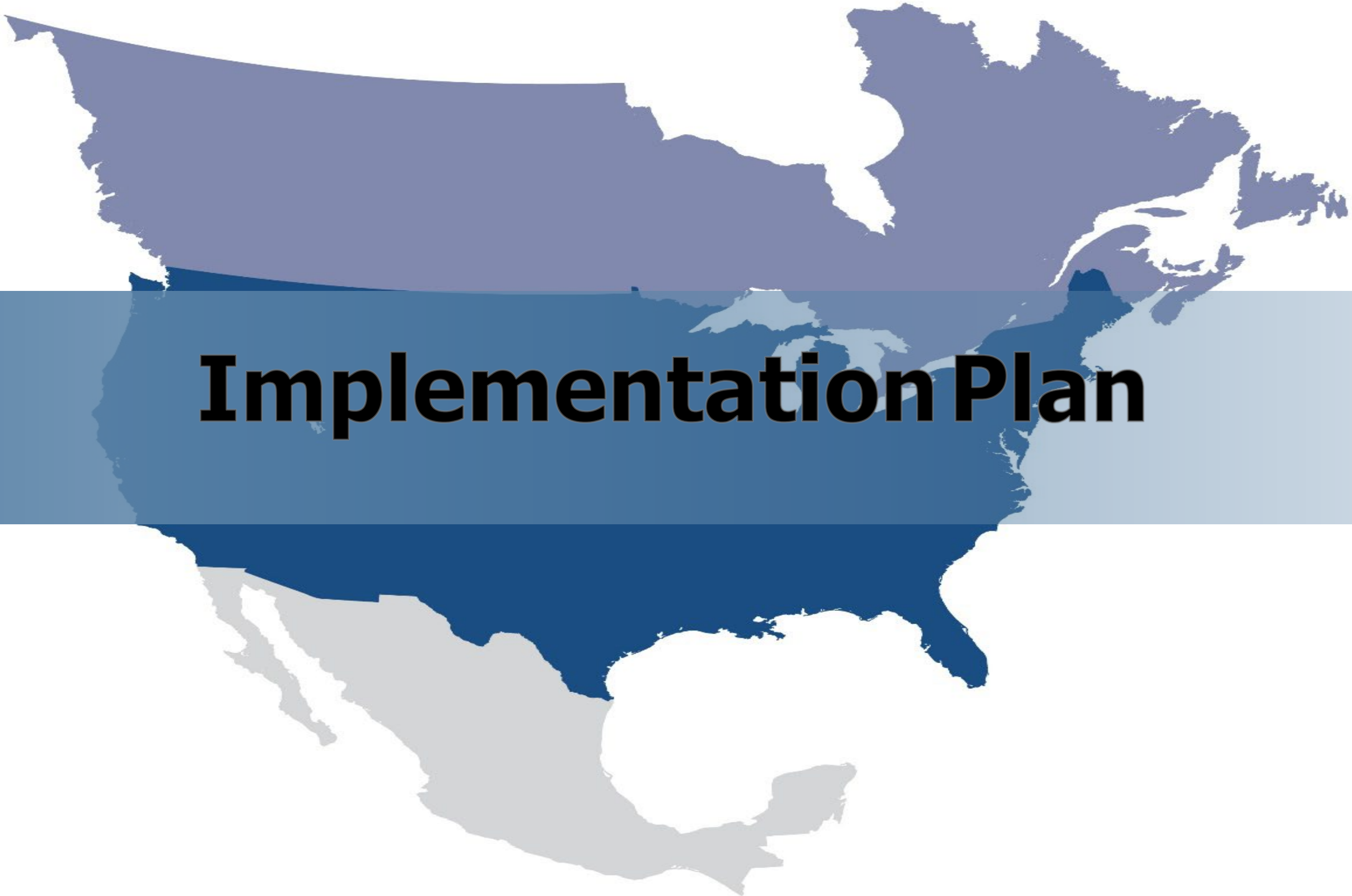
Entity Alpha's CIP-012 logical security protection applied

Entity Alpha's CIP-012 physical security protection applied as Physically secured area

Entity Beta's CIP-012 security protection applied

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 PSP. 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



Implementation Plan

Implementation Plan for CIP-012

- **The 24 Calendar Months**

Effective Date Reliability Standard CIP-012-2 – Cyber Security – Communications between Control Centers Where approval by an applicable governmental authority is required, Reliability Standard CIP-012-2 shall become effective on the first day of the first calendar quarter that is twenty-four (24) 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.

Next Steps

Next Steps

- Posting
  - Project Page 2020-04
  - 45-day comment period and formal ballot September 19 – November 2, 2023
- Point of contact
  - Ben Wu, Senior Standards Developer
  - Ben.Wu@nerc.net or call 470-542-6882
- Webinar posting
  - Three business days
  - Standards Bulletin

Questions and Answers