CIP-012-1 Small Group Advisory Session

General Session

Daniel Bogle, Principal CIP Assurance Advisor
March 8, 2022

Strong Regions + Strong NERC = Brilliant ERO

Disclaimer

The CIP-012-1 Workshop & Small Group Advisory Sessions (SGAS) provide an educational opportunity for registered entities to meet with NERC and Regional Entity representatives to discuss the CIP-012-1 Reliability Standard and possible compliance approaches in an open and non-audit environment. During the course of those discussions, the NERC and Regional Entity representatives may provide guidance on specific approaches for implementing the CIP-012-1 Reliability Standard. NERC and the Regional Entity representatives, however, cannot guarantee compliance if those approaches are used, as compliance is necessarily dependent on the manner in which the guidance is implemented. Additionally, there may be other ways to comply with the obligations of the requirements of the CIP-012-1 Reliability Standard that are not expressed during the CIP-012-1 Workshop and SGAS. Compliance will continue to be determined based on language in the NERC Reliability Standard(s) as they may be amended from time to time. Lastly, to encourage an open exchange of information, NERC and Regional Entity representatives will not use the content from the discussions at the SGAS as a basis for a subsequent compliance or enforcement action upon the effective date of the CIP-012-1 Reliability Standard.

Agenda

- **Introduction of ERO Enterprise Panel**
- **Background**
- **Topics of Interest**
  - *Control Center and associated data center(s)*
  - *Real-time Assessment / Real-time monitoring (RTA/RTM) scope*
  - *CIP Exceptional Circumstances*
  - *Security Objectives and Controls*
  - *Encryption Key Management*
  - *Examples of Compliance Artifacts*
  - *Internal Controls*
- **Next Steps**

ERO Enterprise Panel

- Facilitator
  - Daniel Bogle – Principal CIP Assurance Advisor, Compliance Assurance, NERC
- Panelist
  - Jess Syring – Compliance Monitoring Manager, CIP, MRO
  - Kenath Carver – Director, Cybersecurity Outreach and CIP Compliance, TexasRE
  - Morgan King – Senior Technical Advisor, Entity Monitoring, WECC

#OneEROEnterprise

Background

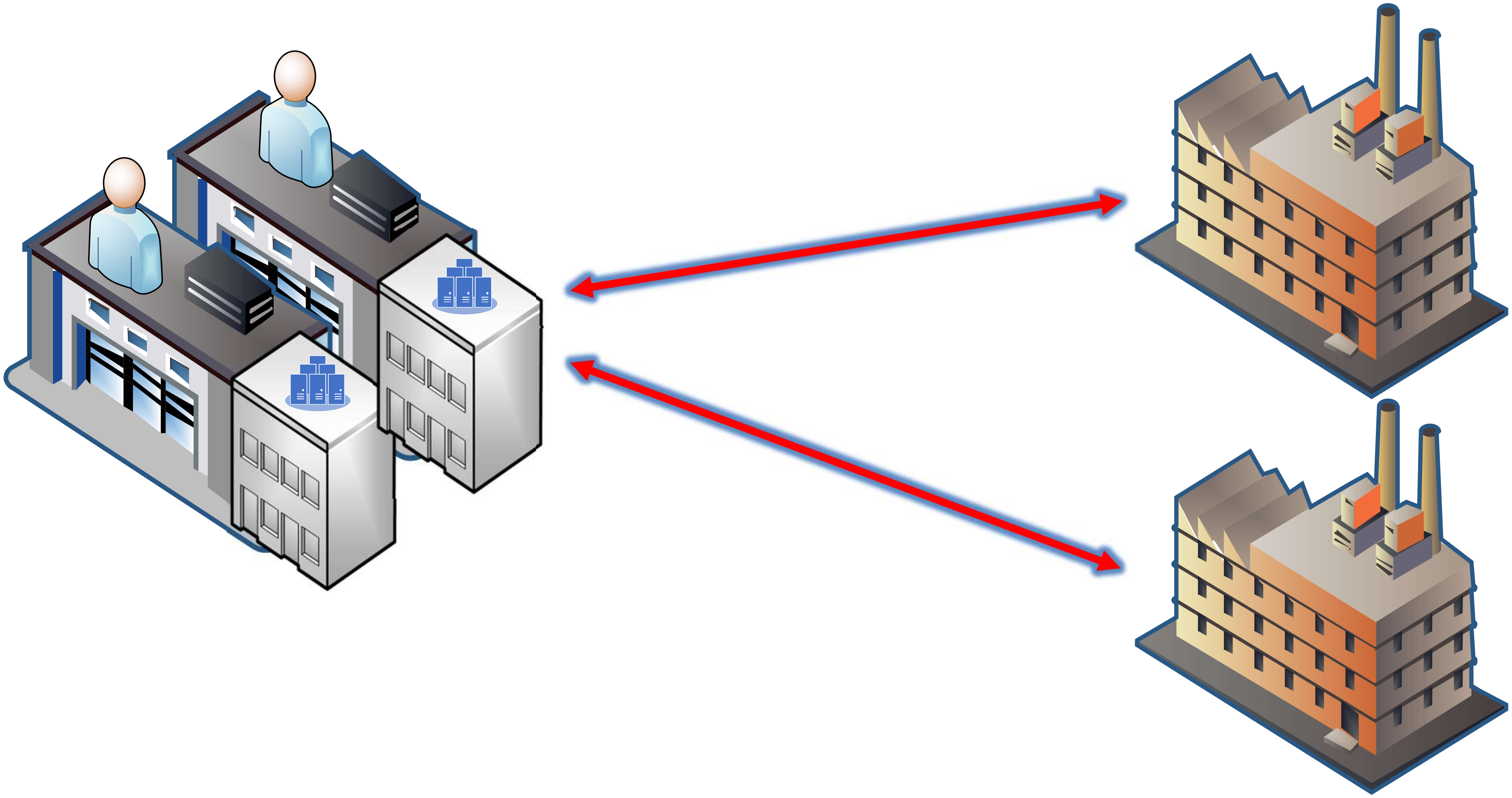
- CIP-012-1 – Communications between Control Centers
- FERC Approved – January 23, 2020
- Effective – July 1, 2022
- Future Modifications
  - CIP Standard Drafting Team Project 2020-04
    - Modifications to require protections regarding availability addressing FERC Order No. 866 directive
    - Proposed 24 month implementation for Version 2
  - The SDT is going to review the ballot comments and discuss an appropriate time line for next ballot posting.

Topics of Interest

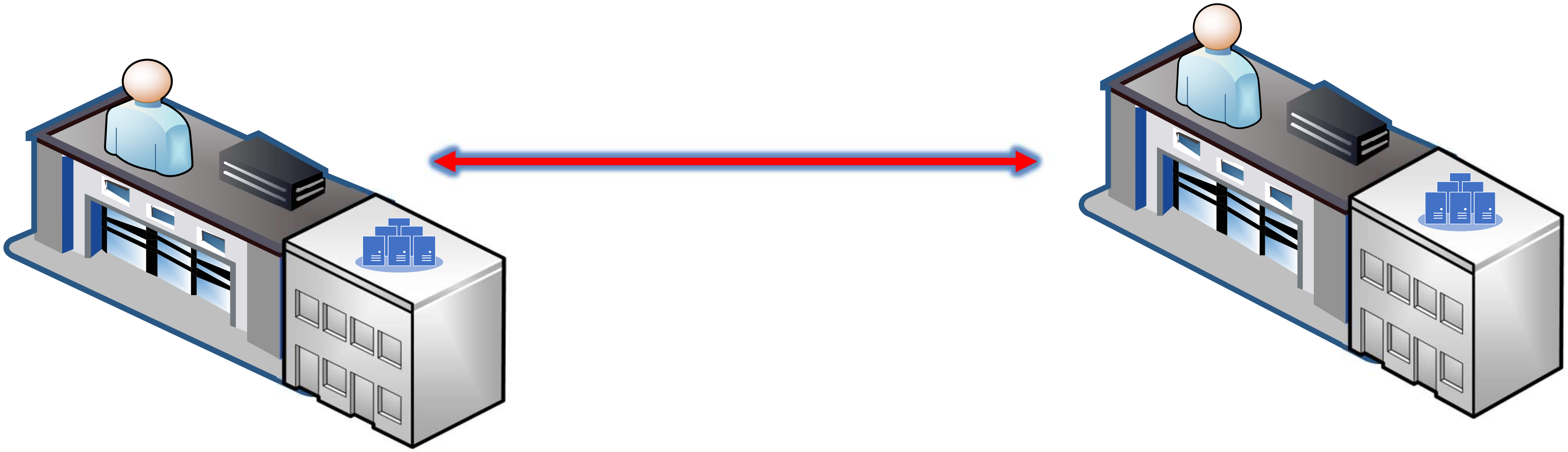
Control Center and associated data center

- Assessing applicability of CIP-012-1 to your entity
  - Is your entity a BA, RC, TOP, TO, GOP, or GO?
  - Does your entity have a Control Center?
- A data center is a Control Center
  - Facility Ownership
- Three scenarios of Control Center and its associated data center

Topics of Interest



Topic of Interest



Entity A

Primary Control Center

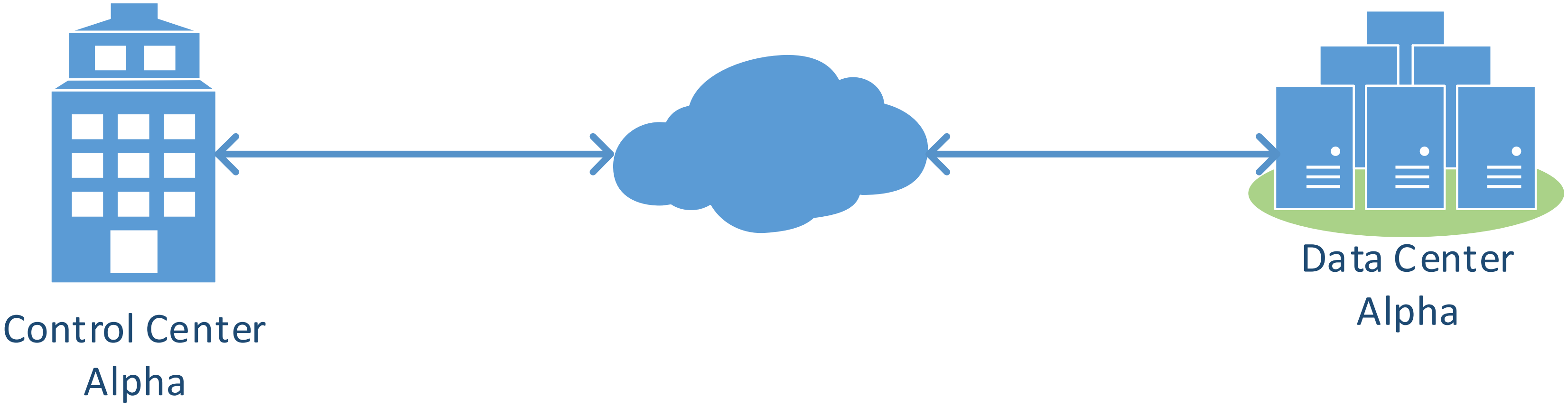
Data center

Entity A

Backup Control Center

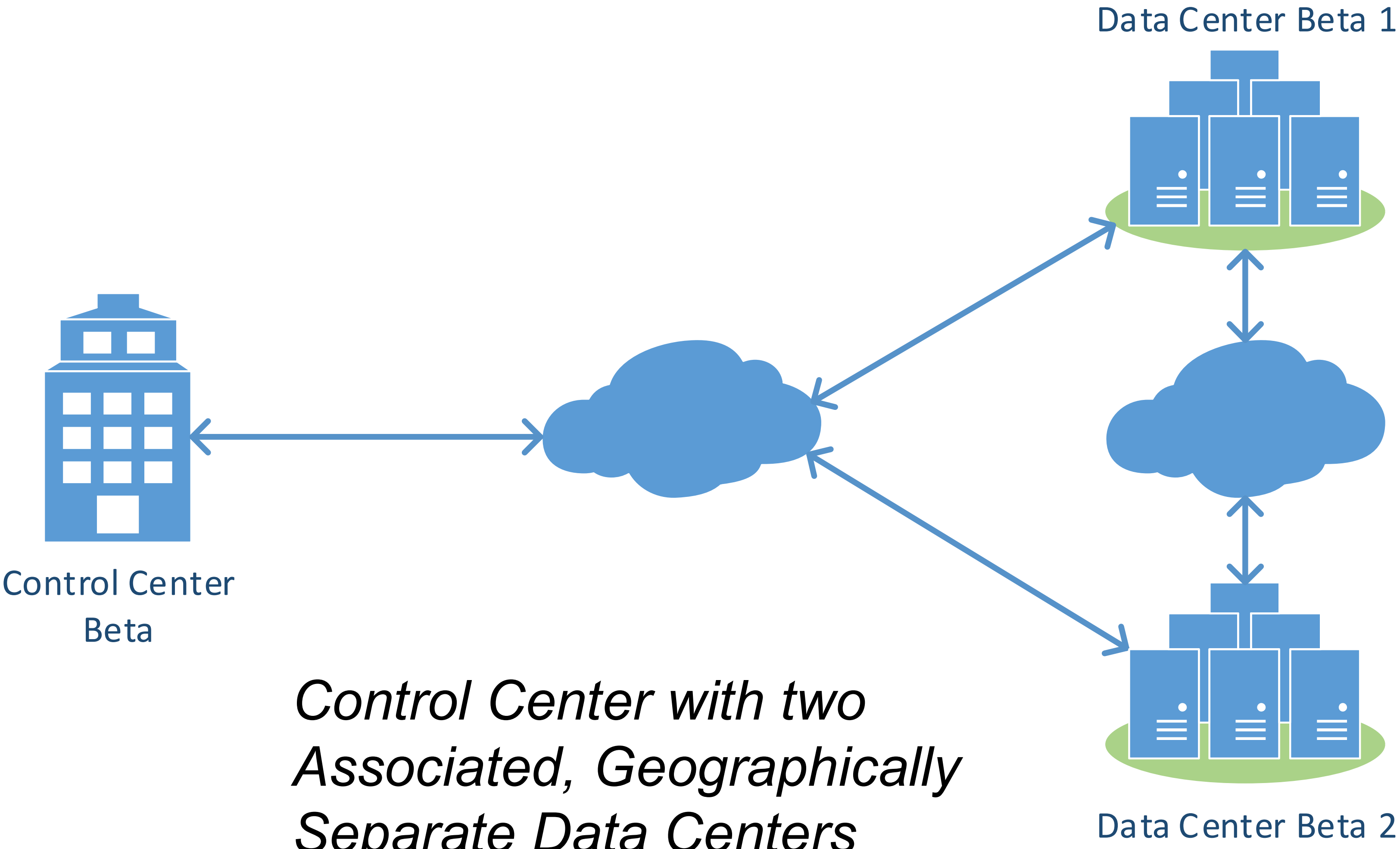
Data center

Topic of Interest



Control Center with an Associated, Geographically Separate Data Center

Topic of Interest



Data Center Beta 1

Control Center Beta

Data Center Beta 2

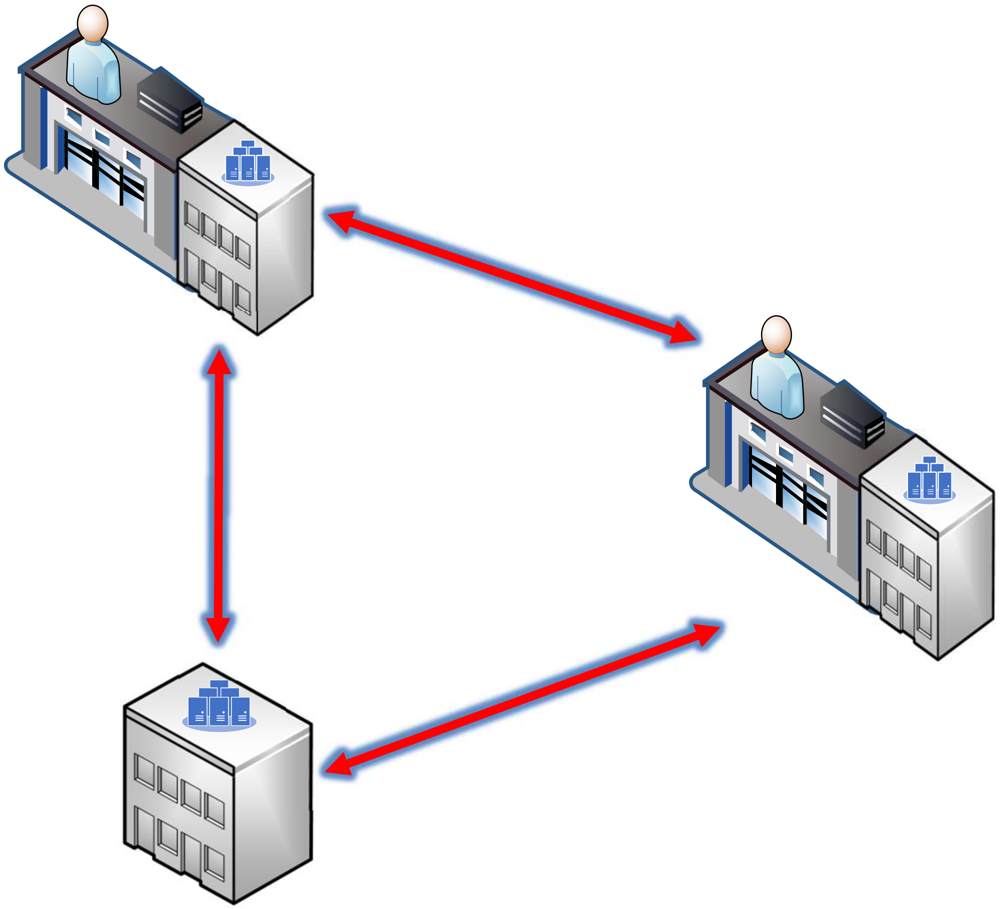
Control Center with two Associated, Geographically Separate Data Centers

Topic of Interest

Entity A

Control Center

Data center



Entity A or Entity B

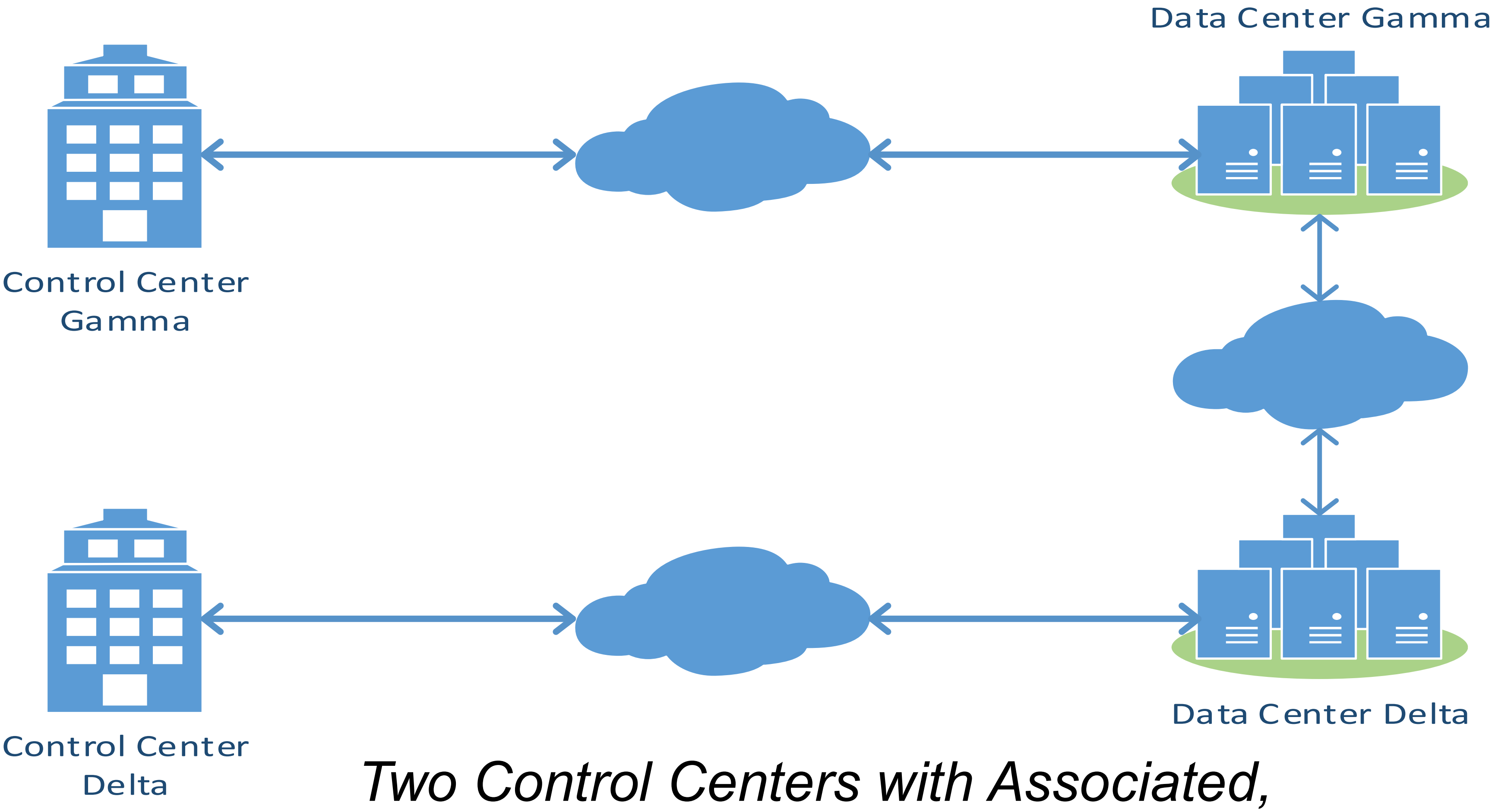
Control Center

Data center

Entity A

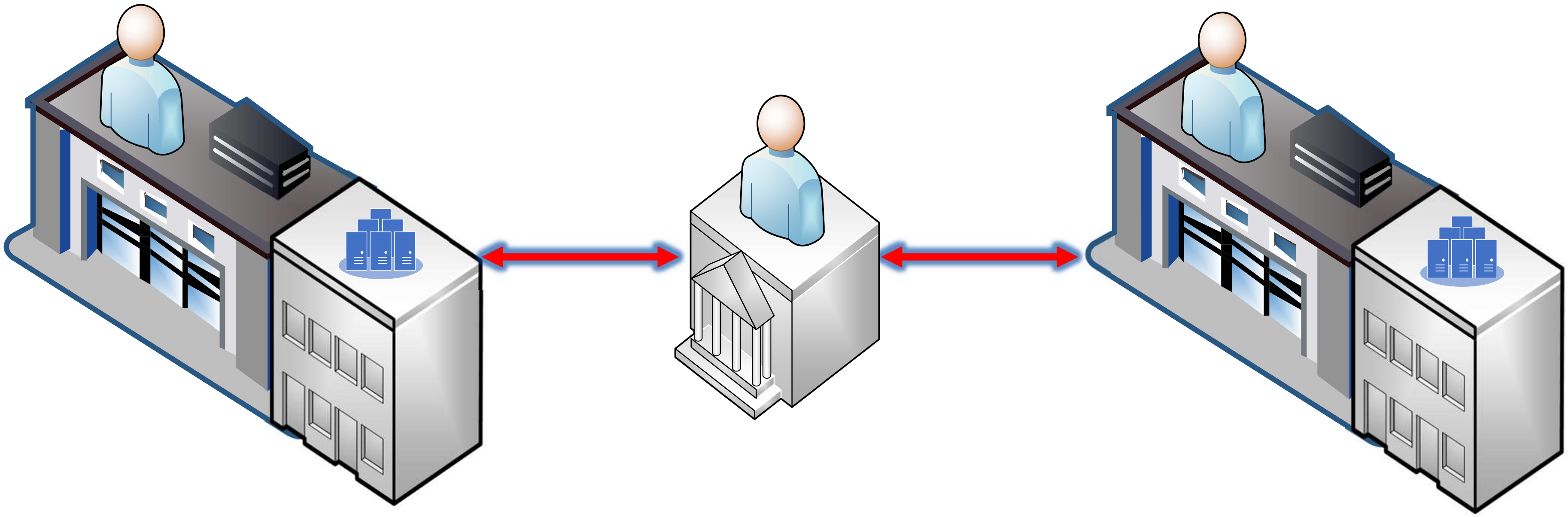
Data center

Topic of Interest



Two Control Centers with Associated, Geographically Separate Data Centers

Topic of Interest



Entity A

Control Center

Data center

Qualified Scheduling Entities (QSE)

Entity B

Control Center

Data center

RTA/RTM Scope

What defines RTA/RTM?

- General Guidance
  - Regardless of protocol and media
  - The Implementation Guidance and Technical Rationale
  - A good starting point is IRO-010-3/4 and TOP-003-4
  - Need to explain rationale, especially if your entity deviates from the IRO-010-3/4 and TOP-003-4 scope

Topic of Interest

CIP Exceptional Circumstances (CEC)

- CIP-012-1 Requirement R1 includes CEC clause
- NERC Glossary Definition - A situation that involves or threatens to involve one or more of the following, or similar, conditions that impact safety or BES reliability: a risk of injury or death; a natural disaster; civil unrest; an imminent or existing hardware, software, or equipment failure; a Cyber Security Incident requiring emergency assistance; a response by emergency services; the enactment of a mutual assistance agreement; or an impediment of large scale workforce availability.

Topic of Interest

Security Objectives and Controls

- Is encryption mandatory?
- Own, operate and manage comm link
- Possible method(s) that meet the security objectives:
    - Monitor,
    - Detect,
    - Alert,
    - Respond,
    - Physical Protections, and
    - Internal controls ensuring the confidentiality and integrity

Topic of Interest

Encryption Key Management

- Responsibilities – i.e., who is responsible?
- Symmetric or Asymmetric
- Consideration of the following may also be helpful in your determinations –
  - NIST Special Publication 800-53 Revision 5 (SC-12)
  - NIST Special Publication 800-57 Part 1 Revision 5
  - NERC | CIP-012-1 Implementation Guidance | March 2020, page 7

Topic of Interest

Examples of Compliance Artifacts

- Diagram(s)
- Network configuration(s)
  - Rulesets / Access Control Lists
  - Encryption
    - Key Management
- Network Monitoring
- Physical Protection(s)
- Agreements/contracts/etc.

Topic of Interest

Internal Controls

- Documentation
- Identification
- Implementation

Next Steps

- Small Group Advisory Sessions
- Frequently Asked Questions
  - Created / Posted to NERC website
- Possible future webinars

Questions and Answers