NERC
NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

Security Perimeters that Span Geographic Locations (SuperESP)

Project 2016-02 CIP Standards - Virtualization

Project 2016-02 CIP Standards Drafting Team
July, 2020

RELIABILITY | RESILIENCE | SECURITY




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 Public Disclaimer

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.

Questions

Please use the Q&A feature in WebEx to ask any relevant questions during the presentation. We will be holding questions until the end of the presentation.

Disclaimer

*These changes to CIP standards are to **ENABLE** new methods/models*

NOT

***REQUIRE** Them*

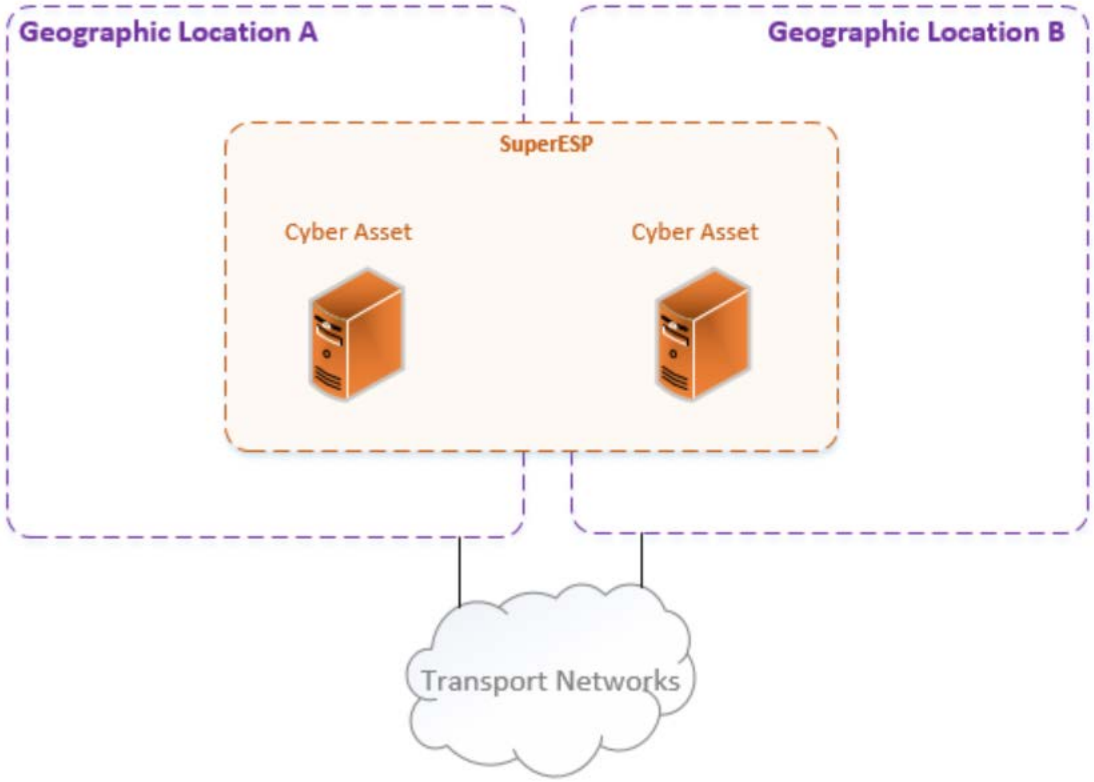
Agenda

- What is a SuperESP?
- What are some SuperESP use cases?
- What restricts the use of a SuperESP?
- Proposed changes to the Standard

SuperESP – What is it?

What is a SuperESP?

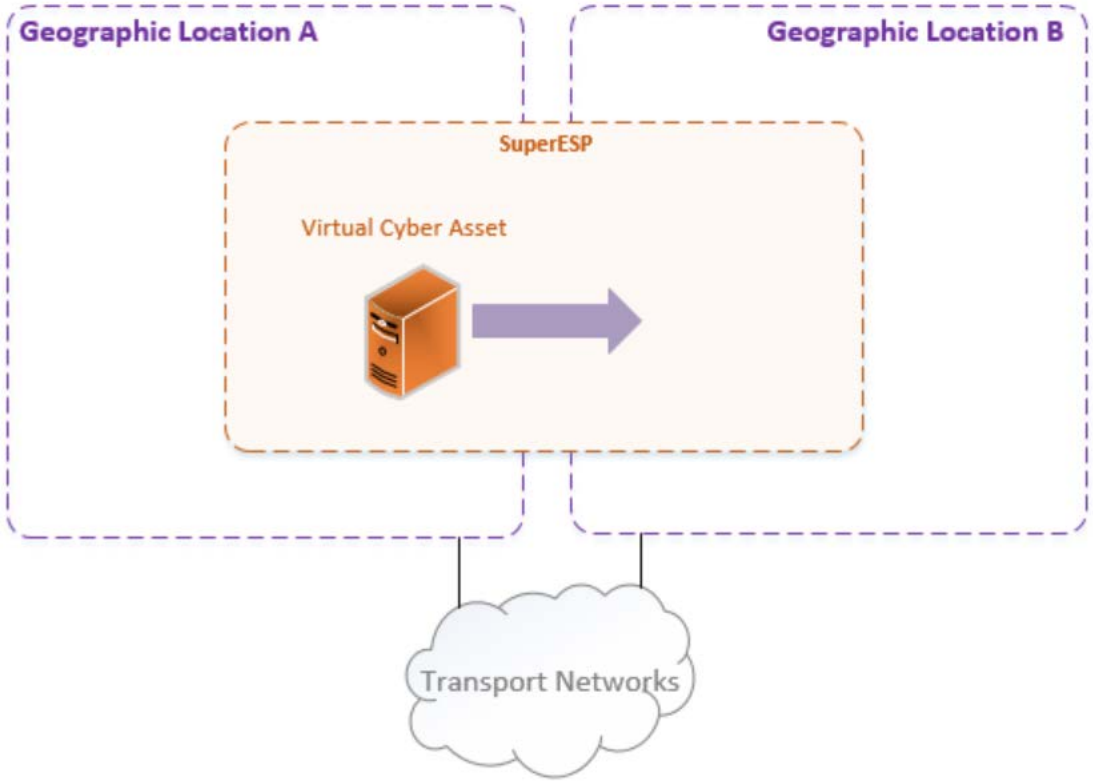
- An Electronic Security Perimeter that Spans Geographic Locations



SuperESP – Use Cases

Common SuperESP Use Cases

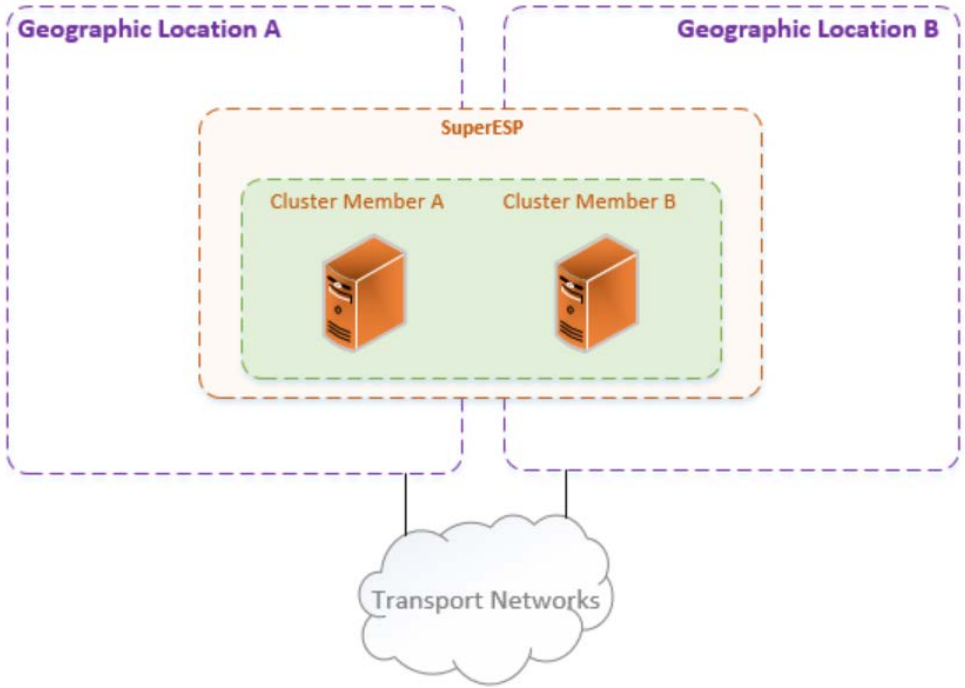
- Virtualization
  - Migrating Workloads Between Datacenters



SuperESP – Use Cases

Common SuperESP Use Cases

- Reliability and Redundancy
  - Enables Clusters that Span Geographic Locations
  - Simplifies Disaster Recovery Scenarios



SuperESP – Current Restrictions

Current Restrictions Preventing the Use of a SuperESP

- CIP-005-5 Exemption 4.2.3.2
  - Cyber Assets associated with communication networks and data communication links between discrete Electronic Security Perimeters.

SuperESP – Current Restrictions

Current Restrictions Preventing the Use of a SuperESP

- CIP-005-5 Requirement 1.2
  - All External Routable Connectivity must be through an identified Electronic Access Point (EAP).

SuperESP – Current Restrictions

Current Restrictions Preventing the Use of a SuperESP

- CIP-006 Part 1.10
  - Restrict physical access to cabling and other nonprogrammable communication components used for connection between applicable Cyber Assets within the same Electronic Security Perimeter in those instances when such cabling and components are located outside of a Physical Security Perimeter. (continued…)

SuperESP – Proposed Changes

Proposed Changes to clarify the use of a SuperESP

- CIP-005-7 Exemptions
  - 4.2.3.2. Cyber Assets or Virtual Cyber Assets associated with communication links logically isolated from, but not providing logical isolation for, BES Cyber Systems or SCI.
  - 4.2.3.3. Cyber Assets or Virtual Cyber Assets associated with communication links between Cyber Assets or Virtual Cyber Assets performing logical isolation that extends to one or more geographic locations.

SuperESP – Proposed Changes

Proposed Changes to clarify the use of a SuperESP

- CIP-005-7 Requirement 1.3
  - Protect the confidentiality and integrity of the data traversing communication links that span multiple geographical locations, where methods from Part 1.1 or Part 1.2.2 are not applied, excluding Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers subject to CIP-012 and excluding time-sensitive protection or control functions between intelligent electronic devices (e.g., communications using protocol IEC TR-61850-90-5 R-GOOSE).

Virtual Machines and Containers – Wrap up

- Key Take-aways
  - A SuperESP is a electronic security perimeter that spans geographic locations.
  - Virtualization combined with a SuperESP clarify for easily migrating workloads and services between geographic locations.
  - A SuperESP allows for highly available clusters that span geographic locations.
  - These capabilities may enable entities to simplify their disaster recovery scenarios.
  - The changes proposed by the Standard Drafting Team enable entities to create an Electronic Security Perimeter that spans geographic locations while maintaining a high level of security and observability for the Bulk Electric System.

Q&A Objectives

- Informal Discussion
  - Via the Q&A feature
  - Chat only goes to the host, not panelists
  - Respond to stakeholder questions
- Other
  - Some questions may require future team consideration
  - Please reference slide number, standard section, etc., if applicable
  - Team will address as many questions as possible
  - Webinar and chat comments are not a part of the official project record
  - Questions regarding compliance with existing Reliability Standards should be directed to ERO Enterprise compliance staff, not the Standard Drafting Team.

Questions and Answers

Jordan Mallory
Jordan.Mallory@nerc.net