COMPLIANCE NOTES:

Understanding NERC CIP 012-1 & ensuring your organization is compliant

Standards set out in the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) govern critical infrastructure, requiring utility companies in North America to adhere to a set of cybersecurity measures. Within this, Reliability Standard CIP 012-1 (Cyber Security – Communication Between Control Centers) came into enforcement on July 1st, 2022. This regulation aims to mitigate risks posed by unauthorized disclosure, unauthorized modification of Real-time Assessment and modification of data being transmitted between Control Centers.

Although CIP-012-1 could be considered high-level, it lacks examples of how compliance should be achieved. However, supporting documentation such as 'Implementation Guidance for CIP-012-2' (CIP 12 Guidance) and 'NERC Reliability Standard 12' (NPCC White Paper) provide further clarity and suggestions on how responsible entities can comply.

Introducing security controls between Control Centers can be a concern for telecommunication engineers with the responsibility for managing such infrastructure, due to the risk of potential disruption in this critical operating environment.

This Compliance Brief identifies and considers:

1. A summary of the requirements arising from CIP 012-1 that entities in scope have to comply with
2. Examples and suggestions set out in NERC's Implementation Guidance and NPCC's White Paper regarding methods for compliance with CIP 012-1
3. Challenges and concerns associated with such methods
4. How challenges and concerns can be avoided by introducing security controls that do not interfere with the underlying network infrastructure.

THE REQUIREMENT

R1. - "The Responsible Entity shall 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."

(R1 is supplemented with sub-requirements R1.1-R1.4 which are discussed individually below)

"The plan shall include Identification of security protection 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."

The CIP Guidance notes that physical or logical protection (or a combination of both) may be used as appropriate. It suggests that physical protection may be appropriate if the two Control Centers in which data is being transmitted between are sufficiently close in proximity that the cabling and connections can physically protect the data.

However, the NPCC White Paper notes that the majority of the data that falls within the scope of CIP 0-12-1 will need to be logically protected by means of encrypting the data in transit between the Control Centers.

The CIP Guidance gives examples of how usage of logical protection can be identified:

- Export of the configuration of a firewall showing the configuration of a VPN tunnel and the routing that directs applicable data through the VPN
- 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

CIP Guidance also states that there are different methodologies that can be utilized for logical protection. For example, an entity could implement a Virtual Private Network (VPN) connection that secures data with IPsec encryption. Alternatively, rather than applying protection to communication links, it could be applied to the data itself using application-layer encryption (SSL/TLS).

CIP 0-12-1 CHALLENGE 1 – COMPLEXITY CAUSED BY STANDARD ENCRYPTION SOLUTIONS

Standard network-based encryption solutions like MACsec (Layer 2) and IPsec (Layer 3) are problematic to an operating environment for many reasons, including:

- Implementation is complex and time-consuming as configuration changes are often needed
- Performance issues may arise due to the unknown impact of latency associated with encryption
- Network visibility may be reduced. When packet headers are encrypted, QoS markings are lost and troubleshooting and monitoring tools cannot function.
- Ongoing management of network appliances becomes more complex.

Additionally, implementing TLS (Transport Layer Security) will only provide application-level encryption, rather than encrypting the entire payload. This may leave an entity vulnerable. Also, TLS introduces additional latency to the network that may be unacceptable.

R1.2 "The plan shall include identification of where the Responsible Entity applied security and availability protections as required in Part 1.1."

Having identified the type of security measures that have been applied to protect Real-time Assessment and monitoring data, entities are required to identify exactly where such protection has been applied. This can be demonstrated through the use of a network diagram. In some scenarios, this may be straightforward, especially if the same entity owns both of the Control Centers in which Real-time Assessment and monitoring data is being transmitted between, and a single encrypted tunnel is used as the method of data protection.

Complexity in this scenario can arise when Real-time Assessment and monitoring data is being transmitted between Control Centers owned and operated by different entities.

R1.3 - "If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers."

CIP 12 Guidance notes that it is important for entities to document ownership responsibilities It describes a scenario where Real-time Assessment and monitoring data is transmitted between Control Center A (owned by entity A) and Control Center B (owned by entity B). In such an example, the entities have agreed that they are each responsible for one end of the VPN configuration on their respective WAN routers and have agreed to a 30-character pre-shared key for IPSec authentication.

Alternatively, the entities may agree to use digital certificates for IPSec for authentication, with one party taking responsibility for ownership of the certificate of authority.

CIP 0-12-1 CHALLENGE 2 – COMPLEXITY CAUSED BY AN ENCRYPTION SOLUTION BETWEEN CONTROL CENTERS OWNED BY DIFFERENT ENTITIES

CIP 12 Guidance suggests using either IPSec for authentication with pre-shared keys, or with digital certificates.

In order to generate a pre-shared key, both entities must decide upon a key (which is most likely saved within an email, text, or document.) This opens up the possibility of the keys being compromised in the event of a network breach or phishing attack. Additionally, the keys are not automatically rotated, and each organization would need to agree on the new key and implement this within the router. This makes management of the process very complex in larger environments, this also does not scale well.

The use of digital certificates can provide authentication in this scenario, they can take a long time to obtain, and one of the entities must take ownership of managing the certificate of authority. This leaves the second entity vulnerable to the first entity's timeframes and operational procedures in the event of an issue with the certificate.

If using either IPSec with pre-shared keys or with digital certificates, anyone with access to the router has access to the keys and certificates because there is no separation of duties. In turn, a misconfiguration by an entity on either side of the tunnel can cause an outage.

OVERCOMING CHALLENGES

CHALLENGE 1: COMPLEXITY CAUSED WITH STANDARD ENCRYPTION

Certes Networks patented Layer 4 Encryption Solution secures data in transit independently from the underlying network. Removing the burden of security from the underlying network infrastructure means that an operating environment can ensure the security requirements of CIP 12 can be met – without changing the underlying infrastructure, or compromising performance and visibility. By encrypting Real-time Assessment and monitoring data using Layer 4, entities will experience the following benefits:

- **Ease of Implementation**. Certes Networks' solutions can be implemented with zero changes to firewalls, switches or routers needed.
- **Maintaining Network Visibility**. Our solution encrypts only the data 'payload', leaving the packet headers visible. This ensures that an entity's network visibility will be maintained and troubleshooting and monitoring tools will not be impacted.
- **Encryption 'off-loading'**. Certes Networks' devices remain transparent to the underlying network infrastructure, meaning that latency can remain within the microsecond range.
- **Policy Definition**. Policies can be created to encrypt data or alternatively allow it to be sent 'in the clear.'. It should be noted that CIP 12 only requires Real-time Assessment and monitoring data to be encrypted. Therefore, a policy can be created to encrypt this with a separate policy to ensure all other traffic transmitted between Control Centers is sent 'in the clear.'

- **Micro-Segmentation.** Unique encryption keys can be applied to each data flow. Therefore, Real-time Assessment and monitoring data can be logically isolated and segmented from all other traffic, further mitigating the risk of it being compromised or disclosed.
- **Observability**. Certes Networks' observability engine provides contextual metadata that enables rapid detection of any out-of-policy traffic flow, allowing an entity a fast and rapid response. A policy change can be administered easily to ensure continuous compliance with CIP 12 requirements.
- **Audits**. Automated reports can be produced to (1) identify where Real-time Assessment and monitoring data is being transmitted, and (2) how and where, in real-time, protection is being applied to satisfy the requirements of CIP 12.

CHALLENGE 2: COMPLEXITIES ARE CAUSED WHEN CONTROL CENTERS ARE OWNED BY DIFFERENT ENTITIES

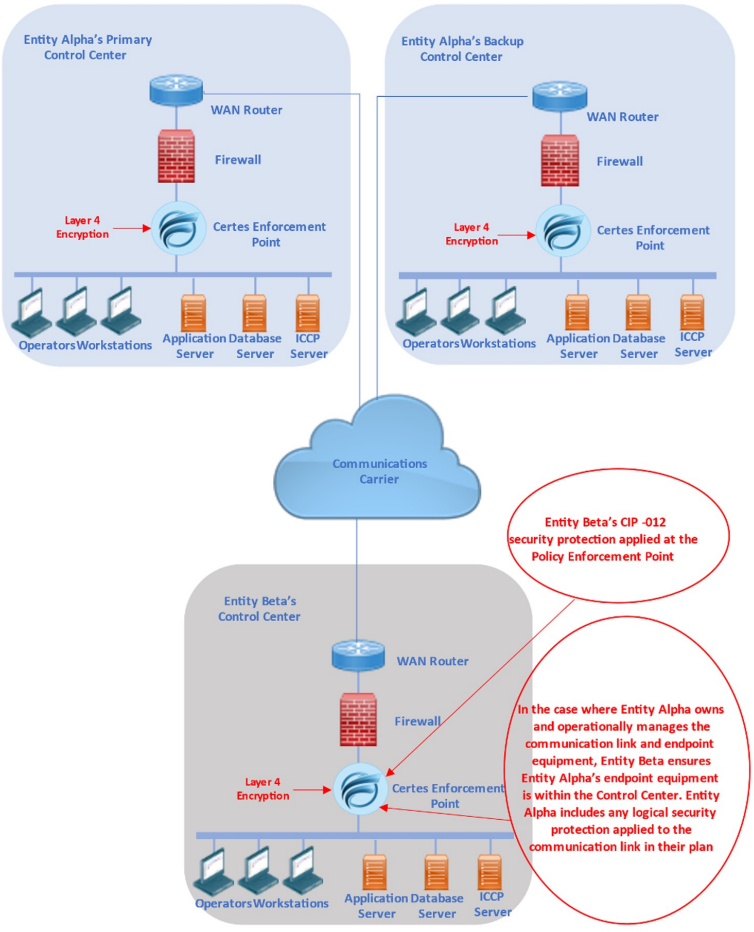
As a transparent overlay to the network, Certes Networks' Layer-4 solution reduces the complexity of deploying data security and key management when Control Centers are owned by different entities.

The management platform (CFNC) is a multi-user solution, and provides role-based (for example; owners of policies and encryption keys, operators and users) access controls that allow each entity to designate users to perform certain actions on both the Certes Enforcement Points and the CFNC.

In addition, robust auditing and logging capabilities track when a user performs an action in the system, such as configuring a CEP or deploying or changing policies. The audit logs indicate the name of the user that initiated the action. These logs can be viewed for further remediation or recordkeeping purposes by the CFNC or externaly.

The diagram below illustrates how and where Certes Networks' devices can be placed within a Control Center environment to help meet the requirements of CIP 0-12-1.

IDENTIFICATION OF WHERE SECURITY PROTECTION IS APPLIED



Like all other CIP standards, compliance with CIP 0-12-1 will be monitored as a part of NERC's Compliance Monitoring and Enforcement Program which monitors, assesses and enforces compliance with all Reliability Standards. Audits may be conducted by NERC's Regional Entities.

A copy of the Audit Worksheet for CIP-012-1 used during the audit process can be found at the following link: ://www.nerc.com/pa/comp/Pages/Reliability-Standard-Audit-Worksheets-(RSAWs).aspx

The Audit Worksheet requires entities to provide a brief explanation setting out how an entity complies with the requirements of CIP-012-1. The technical and compliance team at Certes Networks has provided an example response of how this could be answered if Certes Networks Layer-4 solution is used.

If you would like a copy of this, the document can be downloaded here:

https://certesnetworks.com/nerc-audit-worksheet/

CERTES NETWORKS

Contact Certes Networks

300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

Tel: 1 (888) 833-1142
Fax: 1(412) 262-2574

info@certesnetworks.com
sales@certesnetworks.com