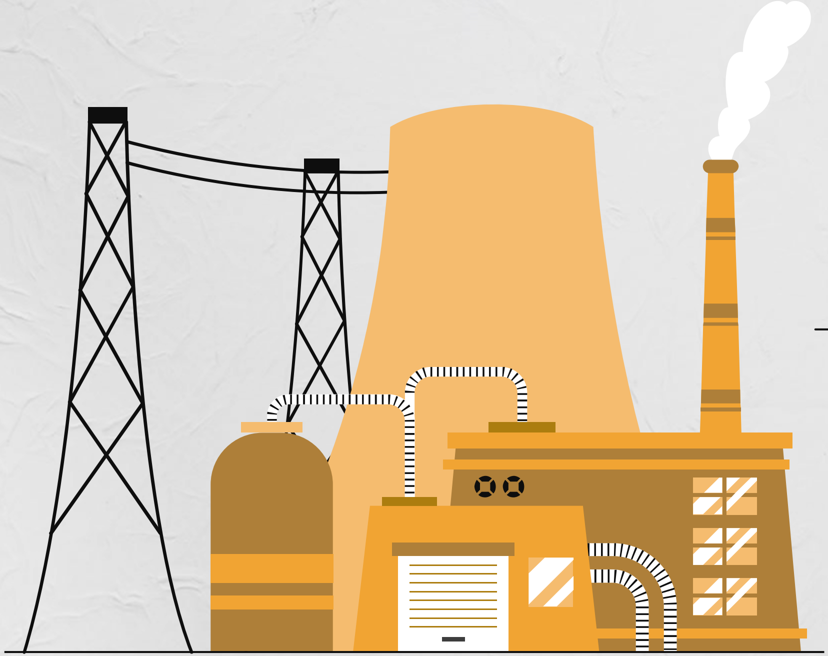


NERC-CIP

North American Electric Reliability Corporation
Critical Infrastructure Protection

CMPT 980 - FALL 2024 - GROUP 6

Table of contents

01 Introduction to NERC

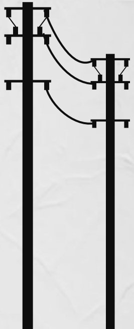
- What is NERC?
- Importance of NERC

02 Understanding NERC-CIP and Its Role

- What are CIP Standards?
- Scope of CIP

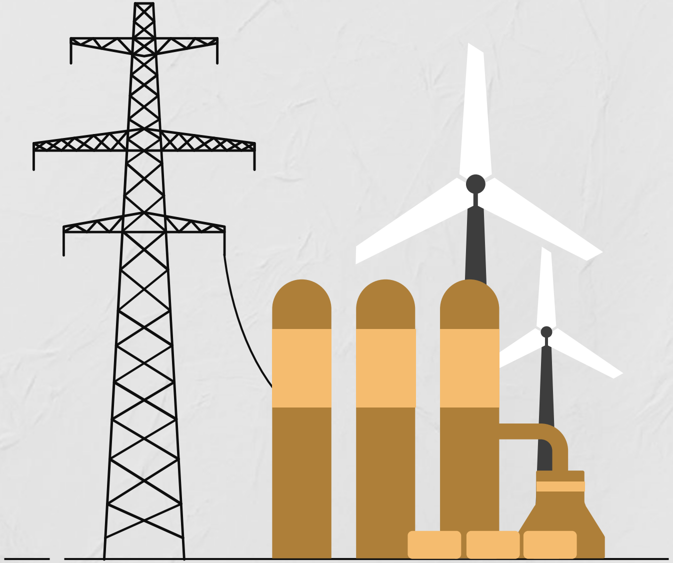
03 Q&A and Key Takeaways

- Questions

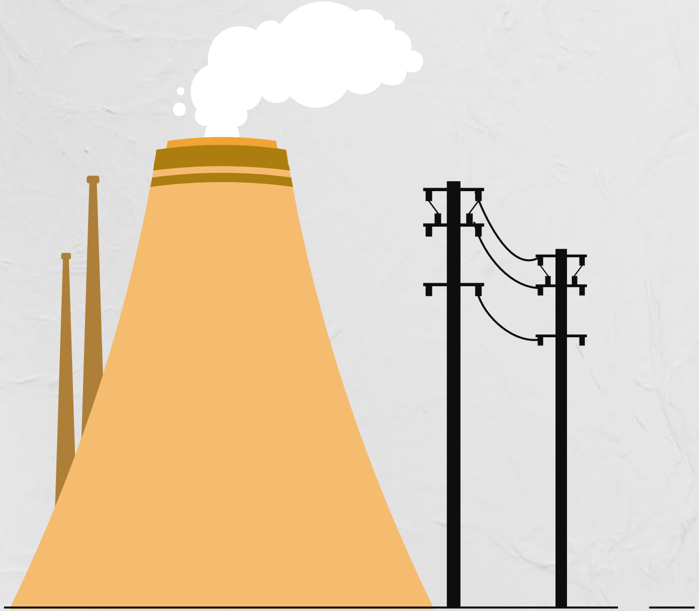


01

Introduction to NERC



North American Electric Reliability Corporation – Critical Infrastructure Protection

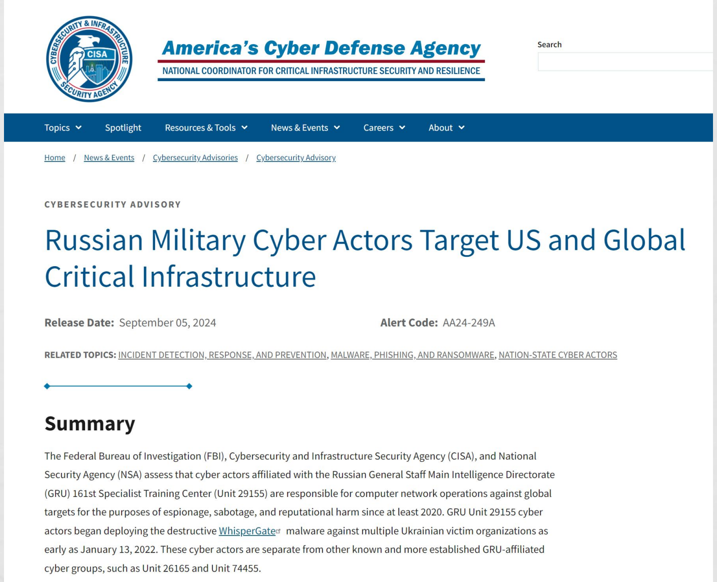


Role of NERC:

- NERC's primary mission is to ensure the security of the North American bulk power system
- NERC develops and enforces reliability standards, including the CIP standards, which are designed to protect critical cyber assets.
- NERC ensures that people and companies involved in generating and delivering electricity follow these standards through strict monitoring and enforcement.

Cyber Attack on Critical Infrastructure

- In 2022, Russian group hacked into the control rooms of power plants in Ukraine
- Similar attacks in 2015 and 2016 caused major power outages and disrupted communication.
- Key infrastructures have been targeted.
- Direct attacks for vulnerabilities are used to damage critical services.



America's Cyber Defense Agency

NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

Home / News & Events / Cybersecurity Advisories / Cybersecurity Advisory

CYBERSECURITY ADVISORY

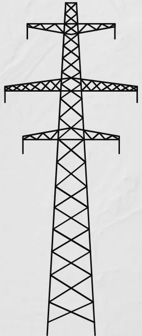
Russian Military Cyber Actors Target US and Global Critical Infrastructure

Release Date: September 05, 2024 **Alert Code:** AA24-249A

RELATED TOPICS: INCIDENT DETECTION, RESPONSE, AND PREVENTION, MALWARE, PHISHING, AND RANSOMWARE, NATION-STATE CYBER ACTORS

Summary

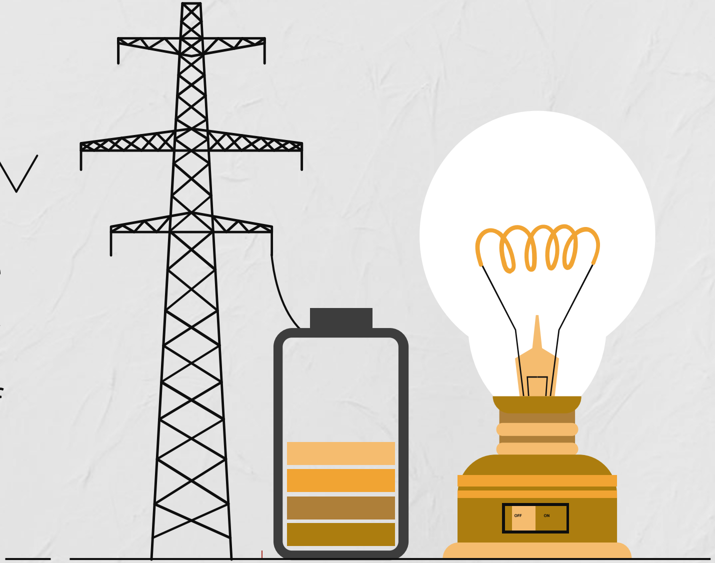
The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and National Security Agency (NSA) assess that cyber actors affiliated with the Russian General Staff Main Intelligence Directorate (GRU) 161st Specialist Training Center (Unit 29155) are responsible for computer network operations against global targets for the purposes of espionage, sabotage, and reputational harm since at least 2020. GRU Unit 29155 cyber actors began deploying the destructive WhisperGate malware against multiple Ukrainian victim organizations as early as January 13, 2022. These cyber actors are separate from other known and more established GRU-affiliated cyber groups, such as Unit 26165 and Unit 74455.



Why does this matter?

Over $1 Trillion predicted loss if Cyber Attacks were to happen *

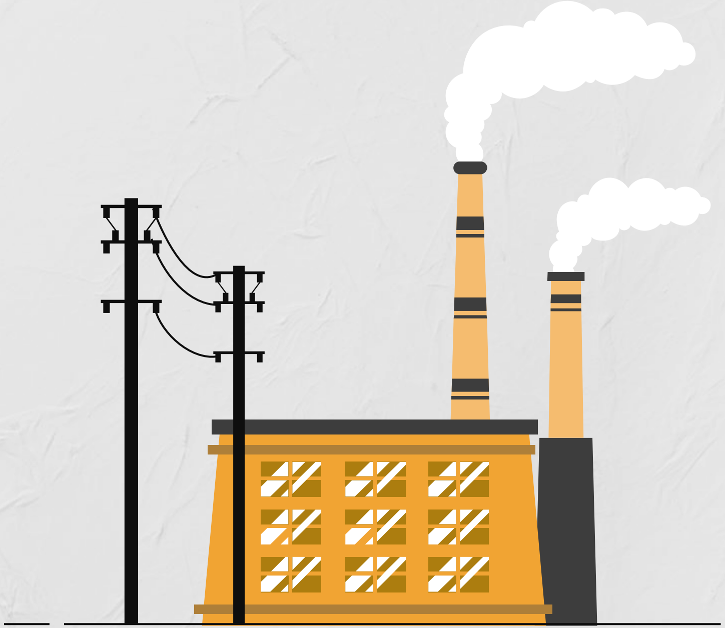
Cyber attacks on critical infrastructure have been on the rise. State-sponsored actors attempting to exploit vulnerabilities in the electric grid may cause a predicted loss of $1 trillion USD according to The Council of Insurance Agents & Brokers of America.



* Lloyd's Report: Cyberattack on US Power Grid Could Cost Over $1 Trillion Dollars

02

Understanding NERC-CIP and Its Role



Purpose of CIP Standards

As will be discussed, **14** key components make up the CIP standards.

Key Areas of NERC CIP Standards

1. System Identification and Configuration Management

- **CIP-002**: BES Cyber System Categorization
- **CIP-003**: Security Management Controls
- **CIP-010**: Configuration Change Management and Vulnerability Assessments
- **CIP-013**: Supply Chain Risk Management

2. Network, Physical and Data Security

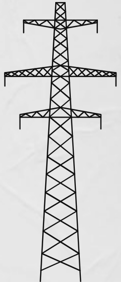
- **CIP-005**: Electronic Security Perimeters (ESP)
- **CIP-006**: Physical Security of BES Cyber Systems
- **CIP-007**: System Security Management
- **CIP-011**: Information Protection
- **CIP-015**: Internal Network Security Monitoring

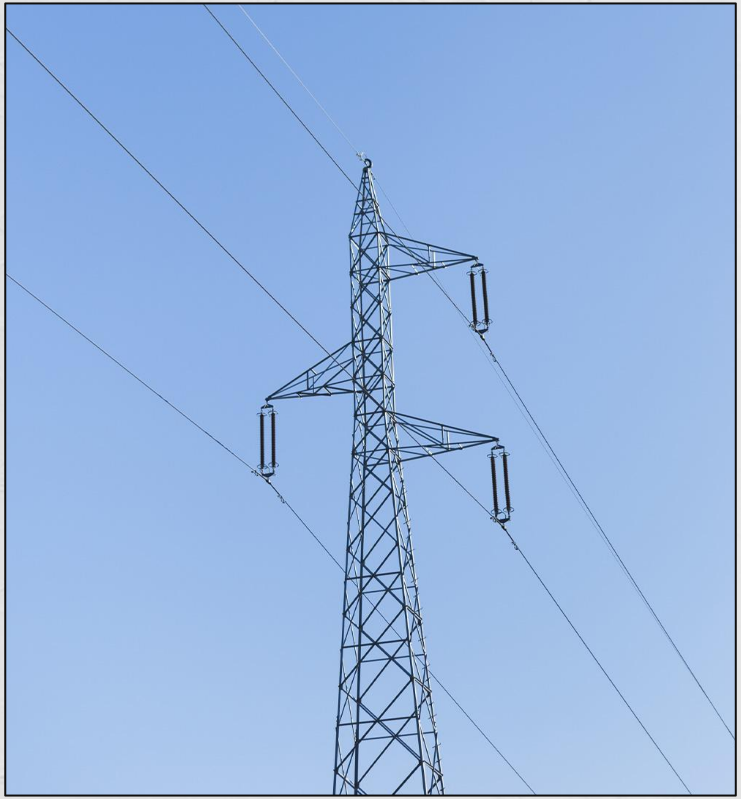
3. Incident Response and Recovery

- **CIP-008**: Incident Reporting and Response Planning
- **CIP-009**: Disaster Recovery Plans for BES Cyber Systems

4. Personnel and Access Management

- **CIP-004**: Personnel & Training





CIP-002: Bulk Electric System Cyber System Categorization

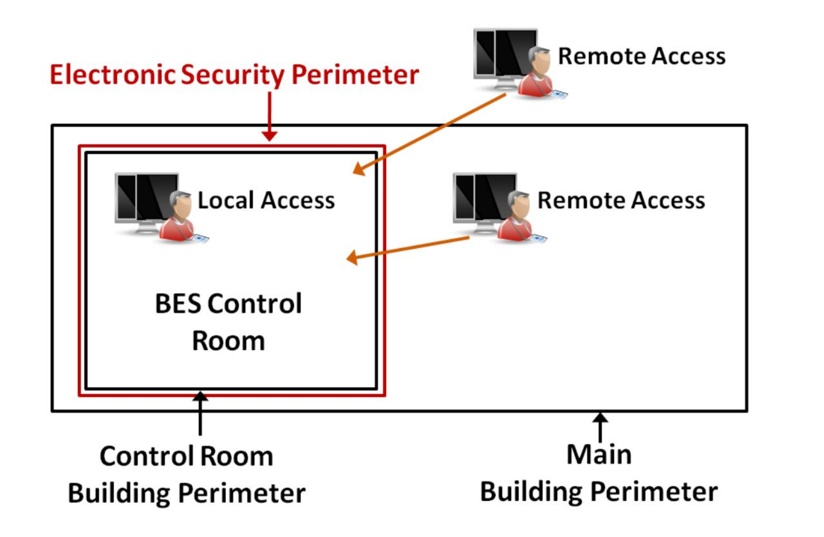
- Identify and categorize BES Cyber Systems based on their impact on the grid's reliability.
- Determine which BES and bulk electrical assets are critical.
- Assign High, Medium,or Low impact ratings to electrical assets and system.

CIP-003: Security Management Controls

- Establish governance for securing BES Cyber Systems.
- Develop and enforce cybersecurity policies and procedures to ensure consistent protection across all BES Cyber Systems.
- Ensure personnel training and awareness to address security threats and ensure compliance with established policies.

CIP-004: Personnel & Training

- Ensure personnel with access to critical systems are trustworthy and trained.
- Perform personnel risk assessments.
- Provide regular security awareness training.
- Control rights and access to critical infrastructure.



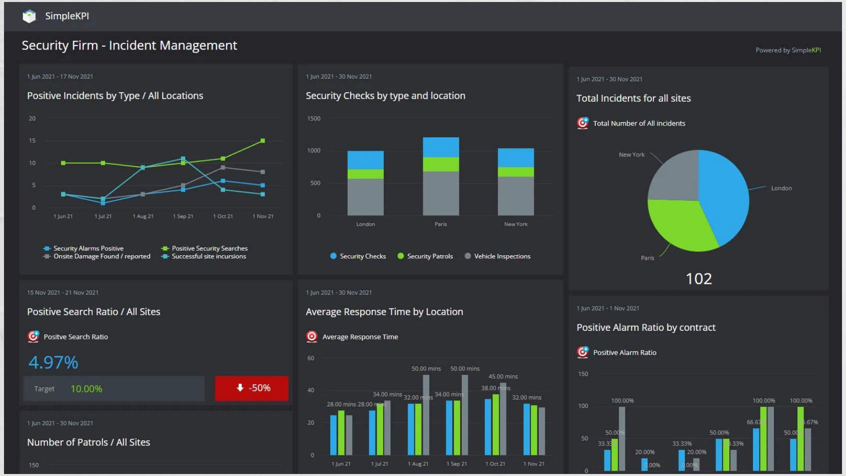
CIP-005: Electronic Security Perimeters (ESP)

- Protect BES Cyber Systems from unauthorized electronic access.
- Establish electronic boundaries around critical assets.
- Implement firewalls and authentication measures.

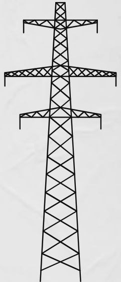
CIP-006: Physical Security of BES Cyber Systems

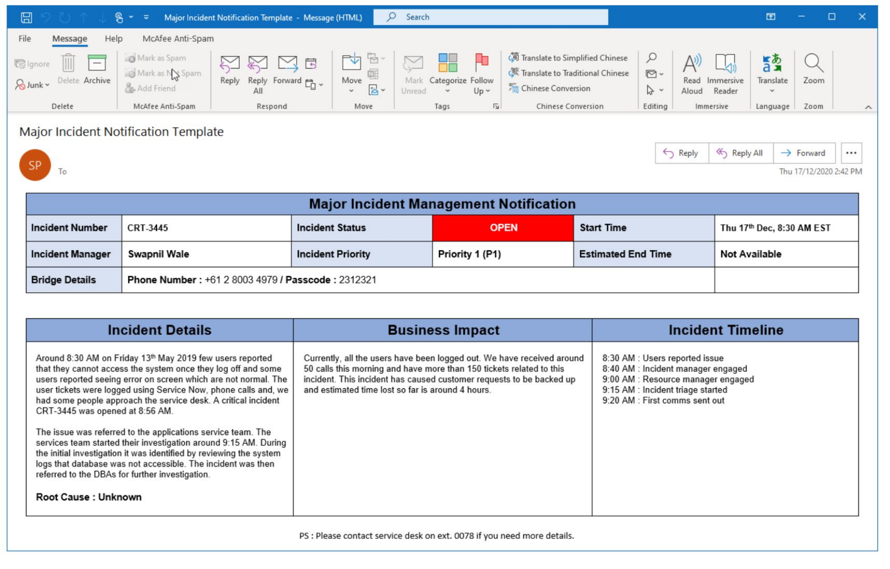
- Prevent unauthorized physical access to
- critical assets.
- Use locks, security doors, and fencing.
- Implement card readers or biometric systems.

CIP-007: System Security Management



- Manage BES cyber system security settings to protect against malicious threats.
- Apply updates and patches promptly to BES cyber assets.
- Use antivirus and anti-malware tools.





Major Incident Notification Template

Thu 17/12/2020 2:42 PM

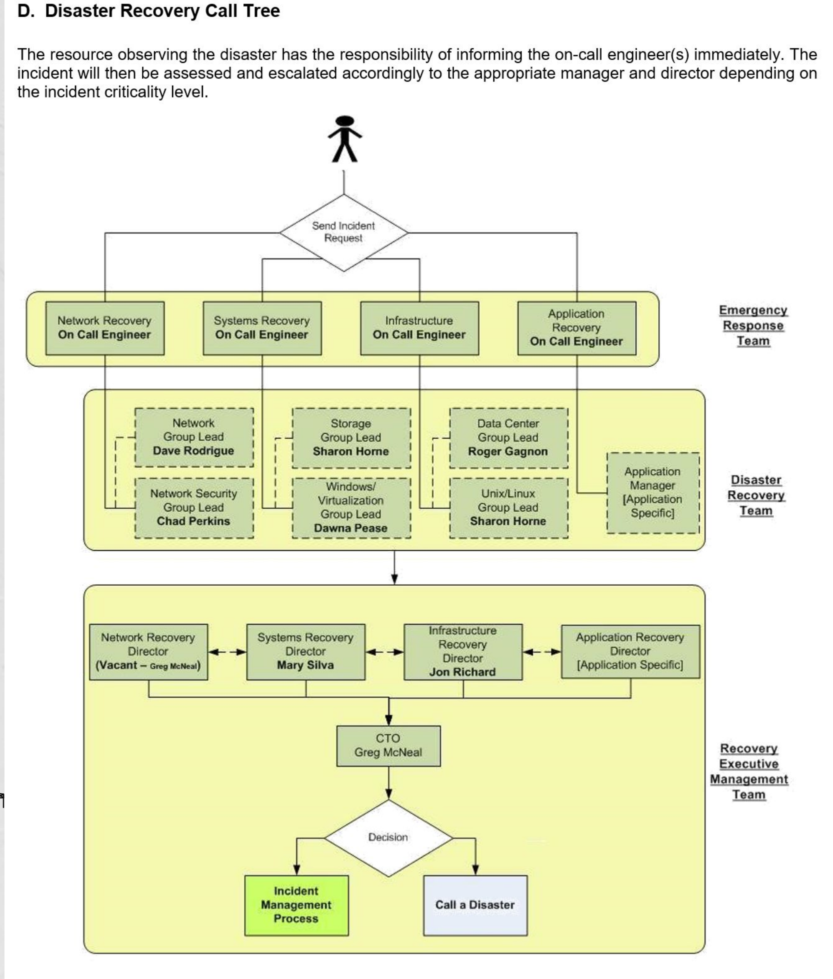
Major Incident Management Notification					
Incident Number	CRT-3445	**Incident Status**	**OPEN**	**Start Time**	**Thu 17th Dec, 8:30 AM EST**
Incident Manager	**Swapnil Wale**	**Incident Priority**	**Priority 1 (P1)**	**Estimated End Time**	**Not Available**
Bridge Details	**Phone Number :** +61 2 8003 4979 **/ Passcode :** 2312321				

Incident Details	Business Impact	Incident Timeline
Around 8:30 AM on Friday 13th May 2019 few users reported that they cannot access the system once they log off and some users reported seeing error on screen which are not normal. The user tickets were logged using Service Now, phone calls and, we had some people approach the service desk. A critical incident CRT-3445 was opened at 8:56 AM. The issue was referred to the applications service team. The services team started their investigation around 9:15 AM. During the initial investigation it was identified by reviewing the system logs that database was not accessible. The incident was then referred to the DBAs for further investigation. **Root Cause : Unknown**	Currently, all the users have been logged out. We have received around 50 calls this morning and have more than 150 tickets related to this incident. This incident has caused customer requests to be backed up and estimated time lost so far is around 4 hours.	8:30 AM : Users reported issue 8:40 AM : Incident manager engaged 9:00 AM : Resource manager engaged 9:15 AM : Incident triage started 9:20 AM : First comms sent out

PS : Please contact service desk on ext. 0078 if you need more details.

CIP-008: Incident Reporting and Response Planning

- Develop a response plan and maintain a response strategy.
- Notify authorities and key stakeholder of incidents within a reasonable timeframe.
- Create a lesson learned document and analyze incidents to improve defenses.



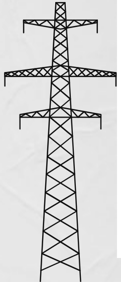
D. Disaster Recovery Call Tree

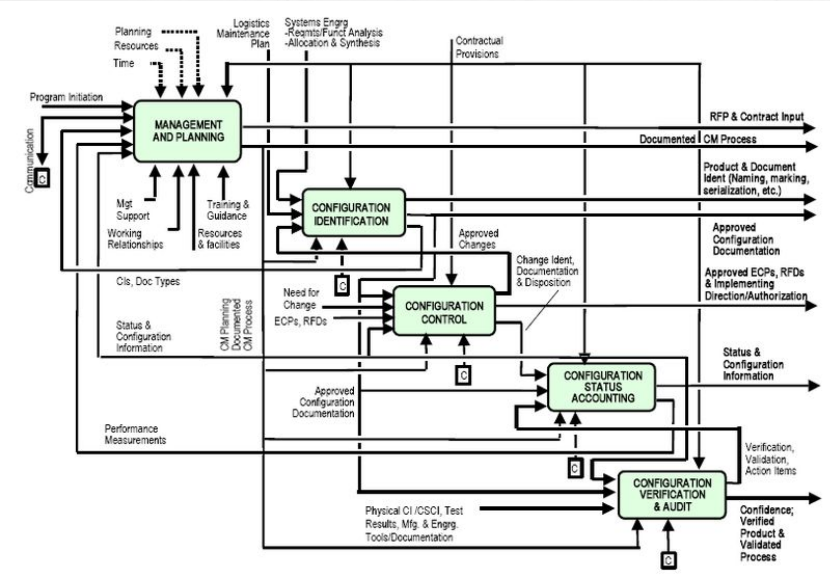
The resource observing the disaster has the responsibility of informing the on-call engineer(s) immediately. The incident will then be assessed and escalated accordingly to the appropriate manager and director depending on the incident criticality level.

Send Incident Request
Network Recovery On Call Engineer
Systems Recovery On Call Engineer
Infrastructure On Call Engineer
Application Recovery On Call Engineer
Emergency Response Team
Network Group Lead Dave Rodrigue
Network Security Group Lead Chad Perkins
Storage Group Lead Sharon Horne
Windows/ Virtualization Group Lead Dawna Pease
Data Center Group Lead Roger Gagnon
Unix/Linux Group Lead Sharon Horne
Application Manager [Application Specific]
Disaster Recovery Team
Network Recovery Director (Vacant – Greg McNeal)
Systems Recovery Director Mary Silva
Infrastructure Recovery Director Jon Richard
Application Recovery Director [Application Specific]
CTO Greg McNeal
Decision
Incident Management Process
Call a Disaster
Recovery Executive Management Team

CIP-009: Disaster Recovery Plans for BES Cyber Systems

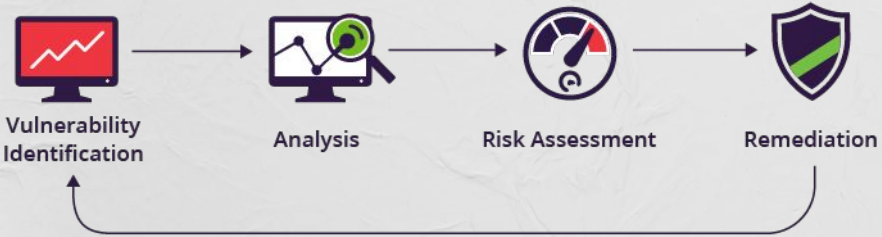
- Ensure the ability to recover critical systems quickly and efficiently after an incident.
- Document steps to restore systems.
- Regularly test and revise plans based on test results and changes.





CIP-010: Configuration Change Management and Vulnerability Assessments

- Track and approve all configuration changes to critical systems.
- Regularly assess critical assets for potential security weaknesses.
- Maintain and monitor system baselines to detect unauthorized changes.

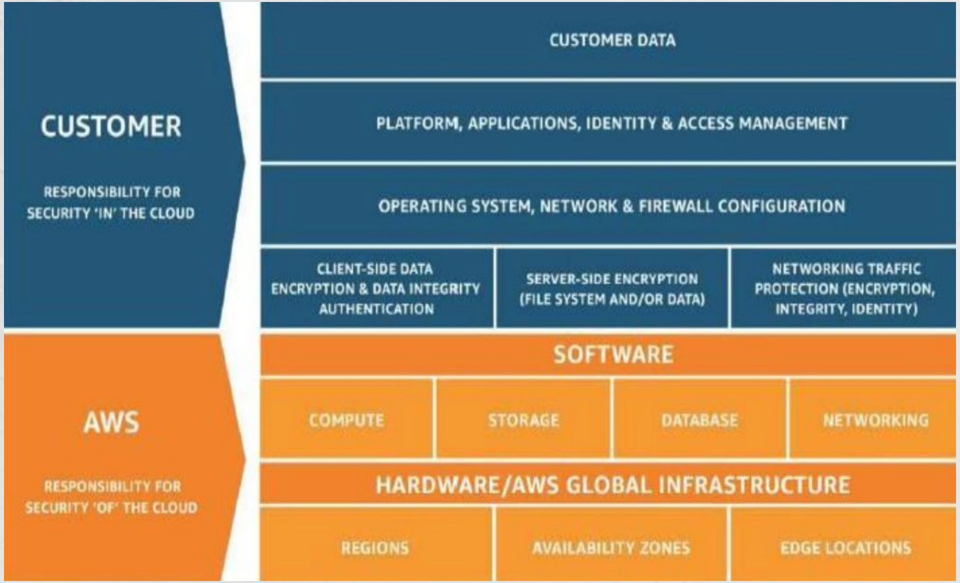


Vulnerability Identification

Analysis

Risk Assessment

Remediation



CUSTOMER

RESPONSIBILITY FOR SECURITY 'IN' THE CLOUD

CUSTOMER DATA

PLATFORM, APPLICATIONS, IDENTITY & ACCESS MANAGEMENT

OPERATING SYSTEM, NETWORK & FIREWALL CONFIGURATION

CLIENT-SIDE DATA ENCRYPTION & DATA INTEGRITY AUTHENTICATION

SERVER-SIDE ENCRYPTION (FILE SYSTEM AND/OR DATA)

NETWORKING TRAFFIC PROTECTION (ENCRYPTION, INTEGRITY, IDENTITY)

AWS

RESPONSIBILITY FOR SECURITY 'OF' THE CLOUD

SOFTWARE

COMPUTE

STORAGE

DATABASE

NETWORKING

HARDWARE/AWS GLOBAL INFRASTRUCTURE

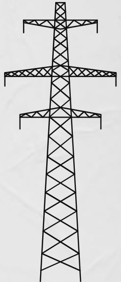
REGIONS

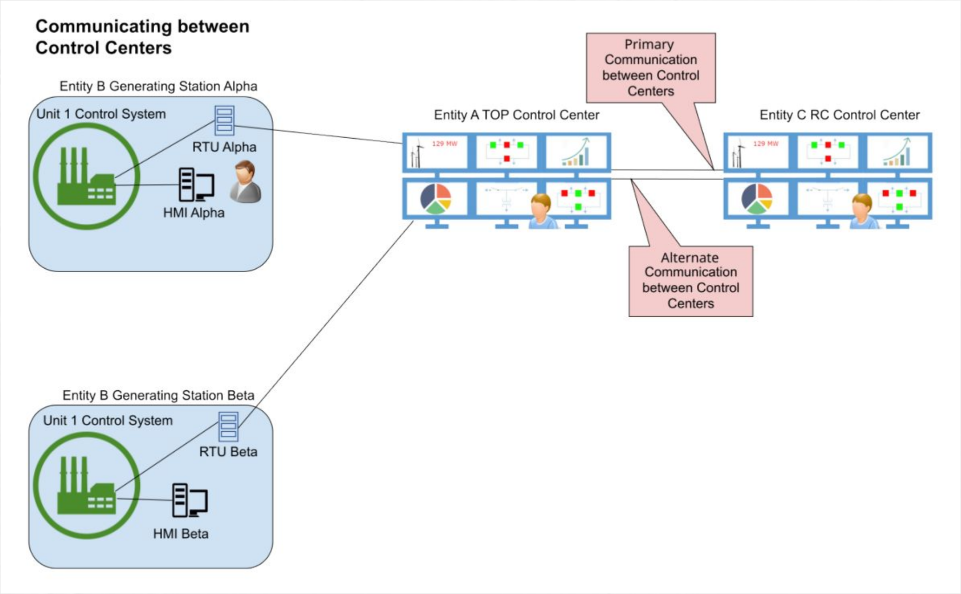
AVAILABILITY ZONES

EDGE LOCATIONS

CIP-011: Information Protection

- Prevent unauthorized access to BES Cyber System Information.
- Support the protection of BES Cyber Systems against compromise.
- Mitigate risks that could lead to misoperation or instability of the Bulk Electric System.



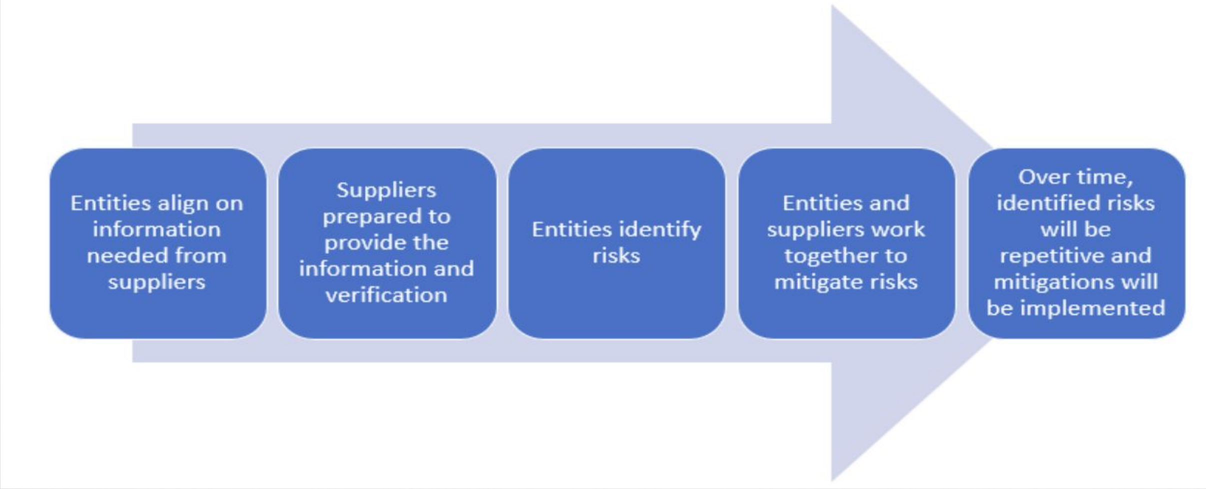

Communicating between Control Centers
Entity B Generating Station Alpha
Unit 1 Control System
RTU Alpha
HMI Alpha
Entity A TOP Control Center
Primary Communication between Control Centers
Entity C RC Control Center
129 MW
129 MW
Alternate Communication between Control Centers
Entity B Generating Station Beta
Unit 1 Control System
RTU Beta
HMI Beta

CIP-012: Communications between Control Centers

- Protect the confidentiality of Real-time Assessment and Real-time monitoring data.
- Ensure the integrity of data transmitted between Control Centers.
- Safeguard critical communication channels to maintain reliable operations.

CIP-013: Supply Chain Risk Management

- Mitigate cyber security risks to the reliable operation of the Bulk Electric System (BES).
- Implement security controls for supply chain risk management.
- Protect BES Cyber Systems (BCS) from supply chain-related vulnerabilities.



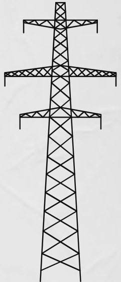
Entities align on information needed from suppliers

Suppliers prepared to provide the information and verification

Entities identify risks

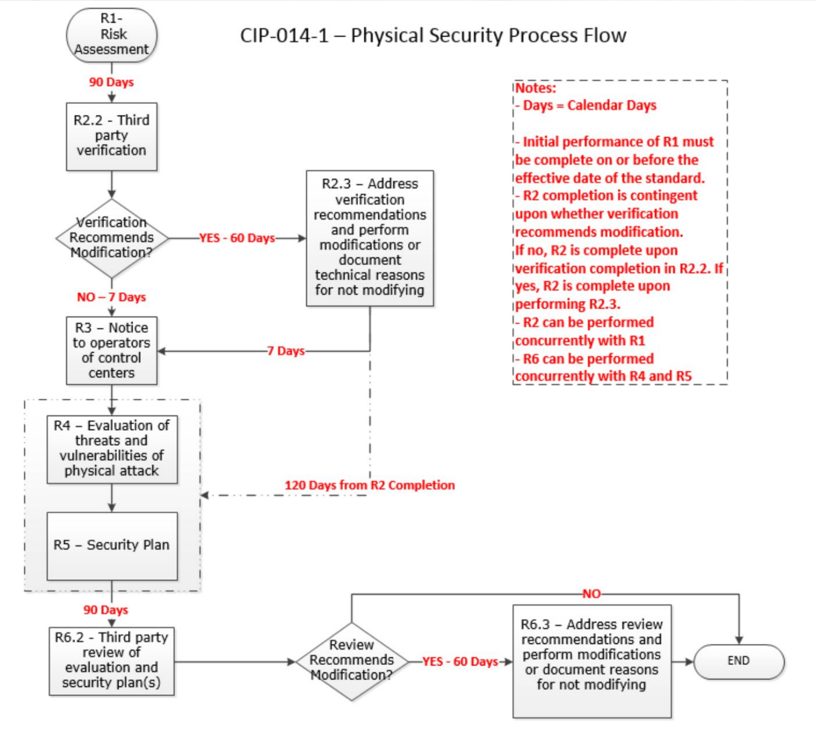
Entities and suppliers work together to mitigate risks

Over time, identified risks will be repetitive and mitigations will be implemented



CIP-014: Physical Security

- Identify and protect critical Transmission stations and substations.
- Safeguard associated primary control centers from physical attacks.
- Prevent widespread instability, uncontrolled separation, or Cascading within an Interconnection.

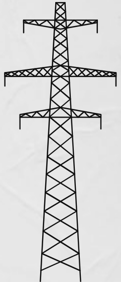


CIP-014-1 – Physical Security Process Flow

R1- Risk Assessment
90 Days
R2.2 - Third party verification
Verification Recommends Modification?
YES - 60 Days
R2.3 – Address verification recommendations and perform modifications or document technical reasons for not modifying
NO – 7 Days
R3 – Notice to operators of control centers
7 Days
R4 – Evaluation of threats and vulnerabilities of physical attack
120 Days from R2 Completion
R5 – Security Plan
90 Days
R6.2 - Third party review of evaluation and security plan(s)
Review Recommends Modification?
YES - 60 Days
R6.3 – Address review recommendations and perform modifications or document reasons for not modifying
NO
END

Notes:
- Days = Calendar Days

- Initial performance of R1 must be complete on or before the effective date of the standard.
- R2 completion is contingent upon whether verification recommends modification.
If no, R2 is complete upon verification completion in R2.2. If yes, R2 is complete upon performing R2.3.
- R2 can be performed concurrently with R1
- R6 can be performed concurrently with R4 and R5



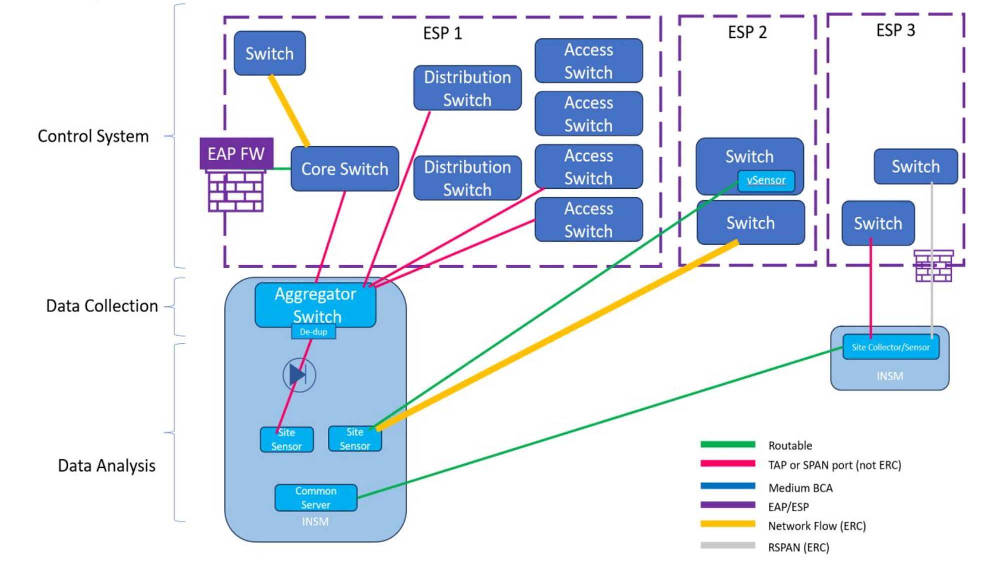


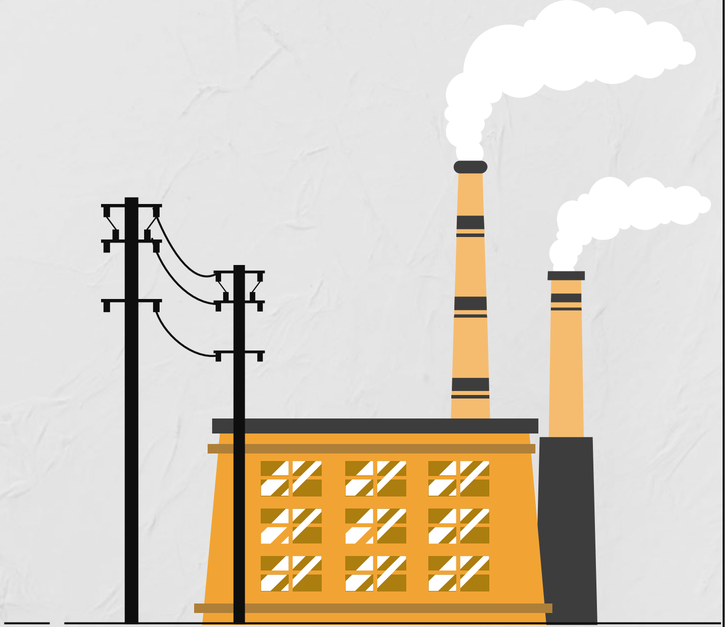
Figure 1

CIP-015 (NEW): Internal Network Security Monitoring

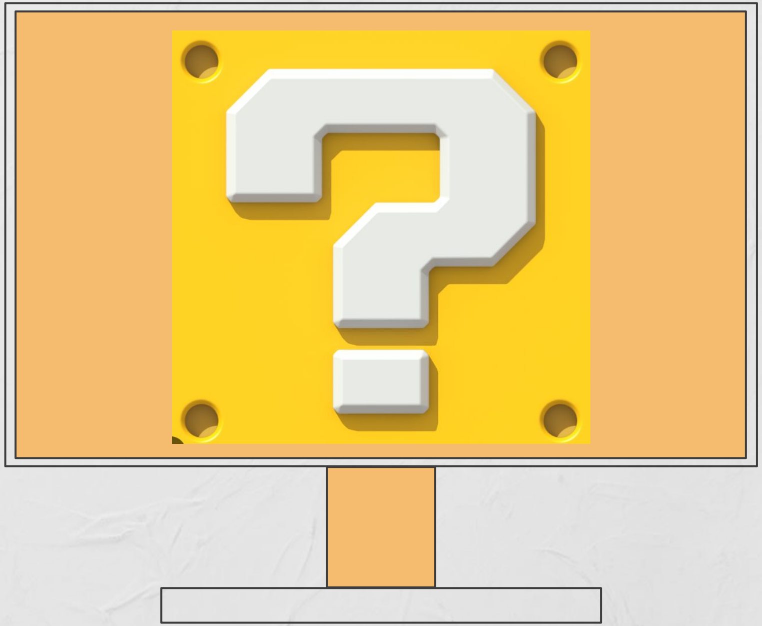
- Enhance detection of anomalous or unauthorized network activity.
- Facilitate improved response to potential cyber attacks.
- Support faster recovery from network security incidents.

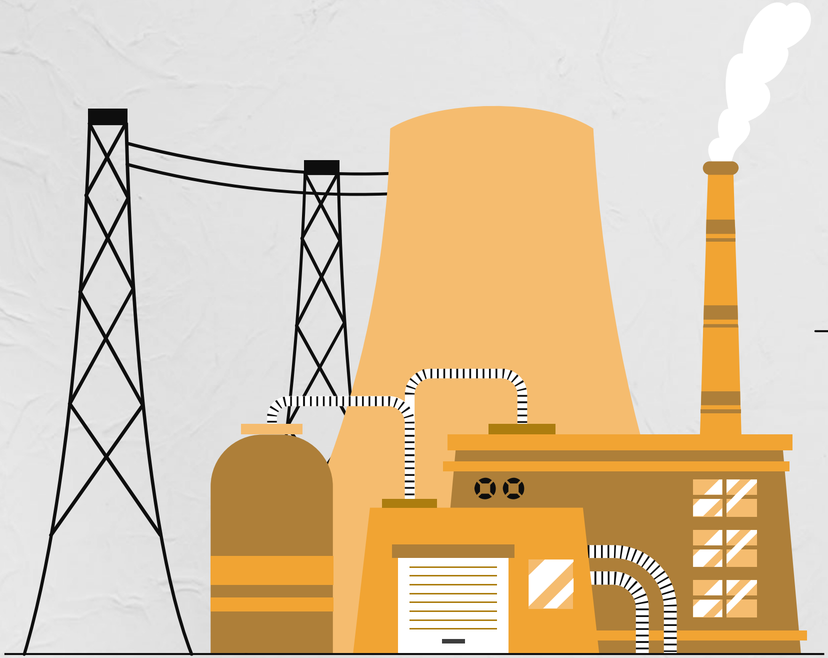
03

Q&A



Any Questions?





Thank you