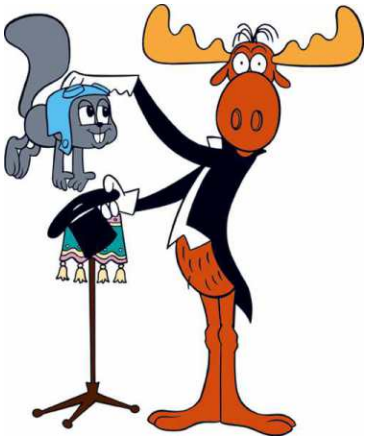
# Impact of NERC CIP Version 5 on Synchrophasor Systems

What the heck do we do NOW? or

What are the CIP implications for a substation if we install synchrophasor infrastructure?



NASPI North American SynchroPhasor Initiative

# Disclaimer

While I have worked with others in the development of this presentation, I take sole responsibility for the contents. In other words, don't blame them for what is stated here.

Also, I recommend you work with your company's NERC CIP experts to truly determine the impact of NERC CIP Version 5 on your Synchrophasor systems.

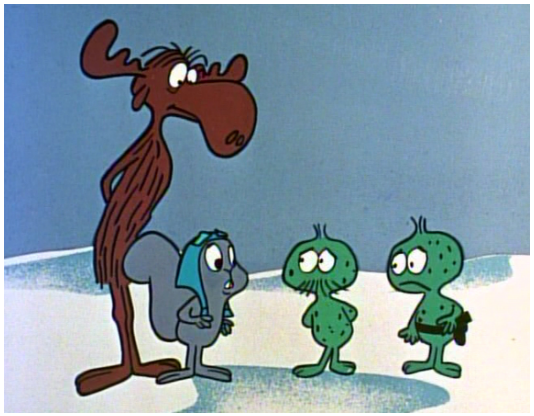
# Overview

- Assumptions about synchrophasor systems
- New CIP version 5 requirements – summary of changes from prior CIP
- Specific provisions of CIP v5 and how they apply to synchrophasor systems

# Major changes from CIP v3 to CIP v5

**CIP Version 3**

- Critical Assets and Critical Cyber Assets
- Interpretation possible by the asset owner as to which facilities were critical and how to protect them



**CIP Version 5**

- BES Cyber System
- Prescriptive with bright line definitions about functionality and what to protect.
- V5 more focused on possible impact of security problem
- NERC CIP v5 go into effect on 4/1/2016
- Different levels of physical security requirements as well

# Assumptions

- Existing Synchrophasor Systems used for Situational Awareness
- Existing Systems are already NERC CIP Version 3 compliant
- This is not a detailed analysis, but a high level review.

# High-level conclusions re CIPv5 and Synchrophasor systems

1. CIPv5 requirements will apply to all synchrophasor data networks that deliver PMU data used by operations within 15 minutes
2. CIPv5 will mean that PMUs using ERP covered by (1) installed in transmission substations fall inside physical security perimeters and most likely are part of the BES Cyber System.
3. CIPv5 will mean that synchrophasor data used for situational awareness should be given the same protected status as SCADA or EMS data.
4. All facets of Communications Networks, including those that are external to an entity, are being considered for inclusion in the new standard. Protections of non-programmable elements as well as the mandatory use of encryption to protect data in transit will be the subject of a forthcoming NERC technical conference.

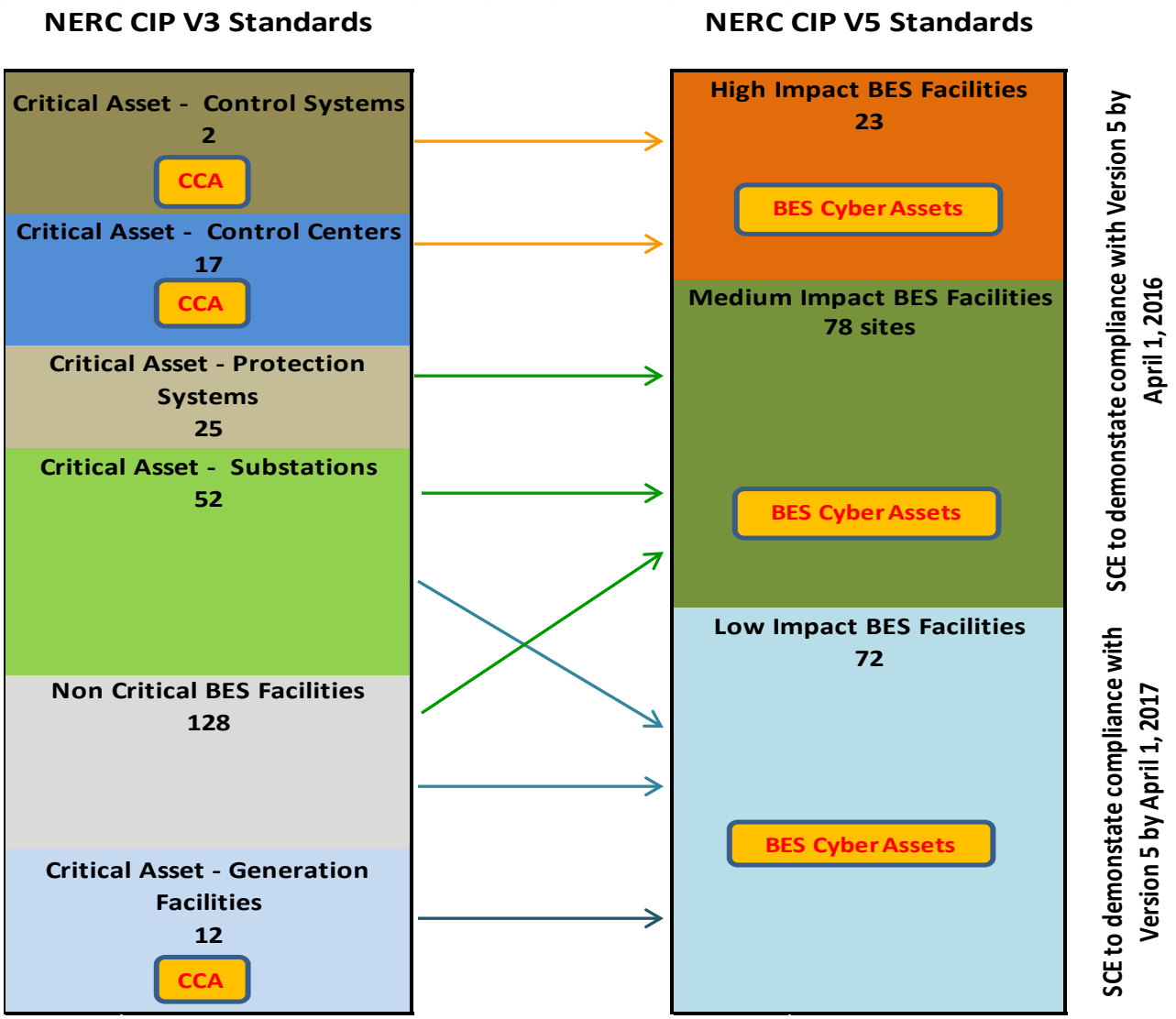
THIS IS ALL SUBJECT TO INTERPRETATION BY ENTITY CYBER SECURITY EXPERTS

# The NERC CIP Standards

## V3 & V5 standards apply to individual cyber assets

| Standard | Version 3 Description | Version 5 Description |
|---|---|---|
| 002 | Asset Identification based on risk | Asset identification methodology based on reliability impact |
| 003 | Security Management Controls | Security management controls (Change Management and Information protection removed) |
| 004 | Personnel and training | Personnel, training and access |
| 005 | Electronic Security Perimeters | Electronic Security perimeters |
| 006 | Physical Security | Physical Security |
| 007 | Systems security | Systems Security (Vulnerability assessment removed) |
| 008 | Incident reporting and response planning | Incident reporting and response planning |
| 009 | Disaster recovery | Disaster recovery |
| 010 | New in V5 | Change management and vulnerability assessments |
| 011 | New in V5 | Information Protection |

# SCE Analysis of NERC CIP Footprint V3 – V5



# CIP 002-5 – Asset Identification

Identify and categorize BES Cyber Systems and Cyber Assets for the application of cyber security requirements

- V3 to V5
  - V3 allows entities to develop a methodology to identify facilities and systems based on “guidelines”
  - V5’s “Bright Line Criteria” prescribe detailed guidelines such as:
    - Control centers used to perform functional obligations of a Transmission Operator (TO) or Generation Operator (GO)
    - Transmission facilities operated at 500kV or above
    - Transmission facilities that perform generator interconnector functions
- Functional – Program Approach
  - Develop a Entity NERC BES Asset Management Program to:
    - Develop and implement an asset tracking system
    - Standardize record keeping methods, processes and procedures
- To-dos and challenges develop governance model
  - Asset identification methodology has to be developed for V5
  - Increase in the number of assets to be identified and tracked
  - Maintenance of documentation of assets has to be coordinated, automated and standardized

# CIP 003-5 – Security Management Controls

Specify management controls to establish responsibility and accountability

- V3 to V5
  - V3 prescribed high level requirements for policy, governance and change management
  - V3 Information Protection and Change Management requirements moved to a stand-alone standard
  - V5 prescribes policies and programs such as Personnel and Training and System Security
- Functional – Program Approach
  - Evaluate sufficiency of Entity cybersecurity policies
  - Develop governance structure incorporating functional programs (e.g., Change Management, Access Management)
- To-dos and challenges
  - Current governance structure and practices may be insufficient and inefficient
    - Delegation agreements are not standardized in task, responsibility and ownership allocation
    - Reliance on ad-hoc agreements to achieve compliance goals
  - Policies to address low impact facilities have to be developed

# CIP 004-5 – Access Management

Protect BES cyber systems by limiting access as well as conducting training, awareness and personnel risk assessments

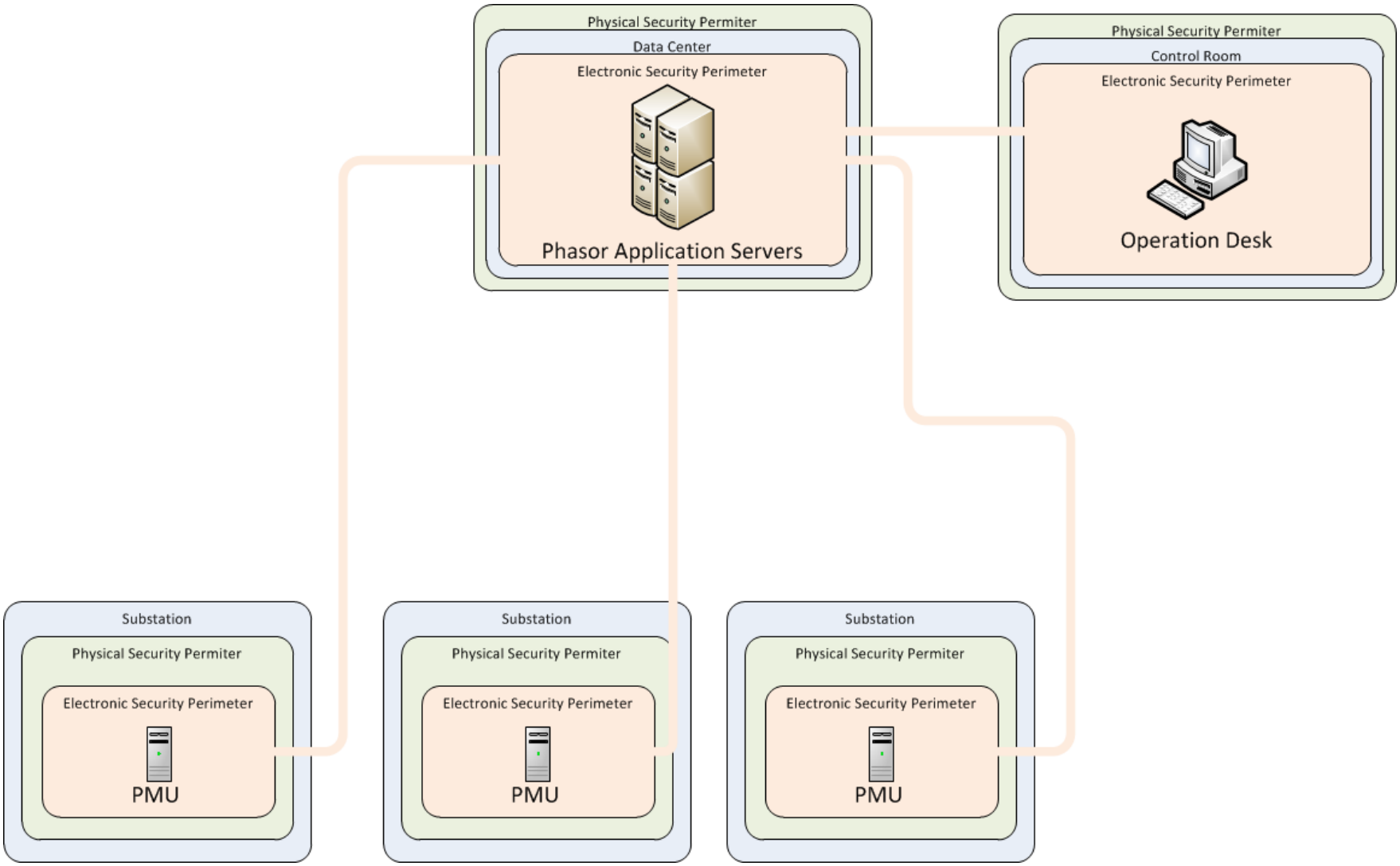
- V3 to V5
  - V3 training requirements allowed Entity to determine content
  - V3 Access management requirements required access revocation to be completed in 24 hours or 7 days
  - V5 requirements are based on impact level of asset
    - V5 training and personnel risk assessment requirements are prescriptive
    - V5 access revocation requirements changed and include protected information access
- Functional – Program Approach
  - Develop a cybersecurity Training & Awareness program to manage training lifecycle
  - Develop Access Management Program to manage access lifecycle
- To-dos and challenges
  - Substantial increase in number of personnel
  - Automated system (MAP) to record and track qualifications and access rights is under development
  - Access revocation to Protected Information is an untested capability

# CIP 005-5 – Electronic Security Perimeter

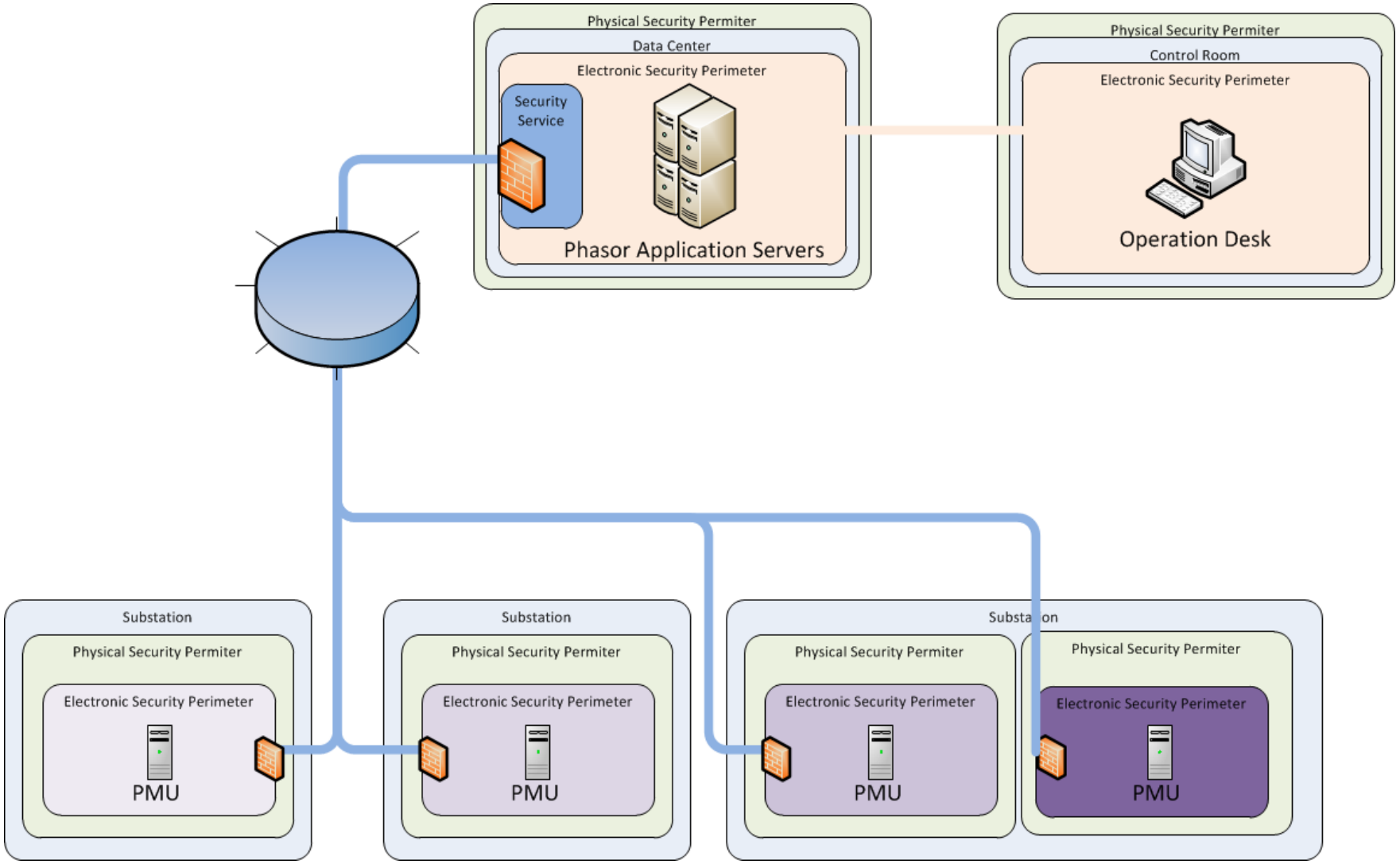
Manage electronic access by specifying electronic security perimeters

- V3 to V5
  - V3 required the creation of electronic security perimeters and controls such as restricted access, limiting services and functions of ports
  - V5 has reorganized requirements to match impact levels and focused attention on electronic controls at discrete devices
    - Vulnerability assessment requirement moved to CIP 010, access management moved to CIP 004, monitoring requirements consolidated in CIP 007
  - V5 prescribes controls for interactive remote access
- Functional – Program Approach
  - Develop a common or standardized cybersecurity program that will develop and implement solutions tailored for operational environments
  - Develop and enforce a security architecture for NERC sites by means of Systems Security and Monitoring Program
- To-dos and challenges
  - Technical means to create electronic security perimeters and methods to detect malicious communications for substation networks are untested
  - Implementation in a large number of sites
  - Ability to test for vulnerabilities using automated methods (i.e., scripts vs. a paper exercise) is untested.

# NERC CIP Version 3 Security Perimeters



# NERC CIP Version 5 Security Perimeters

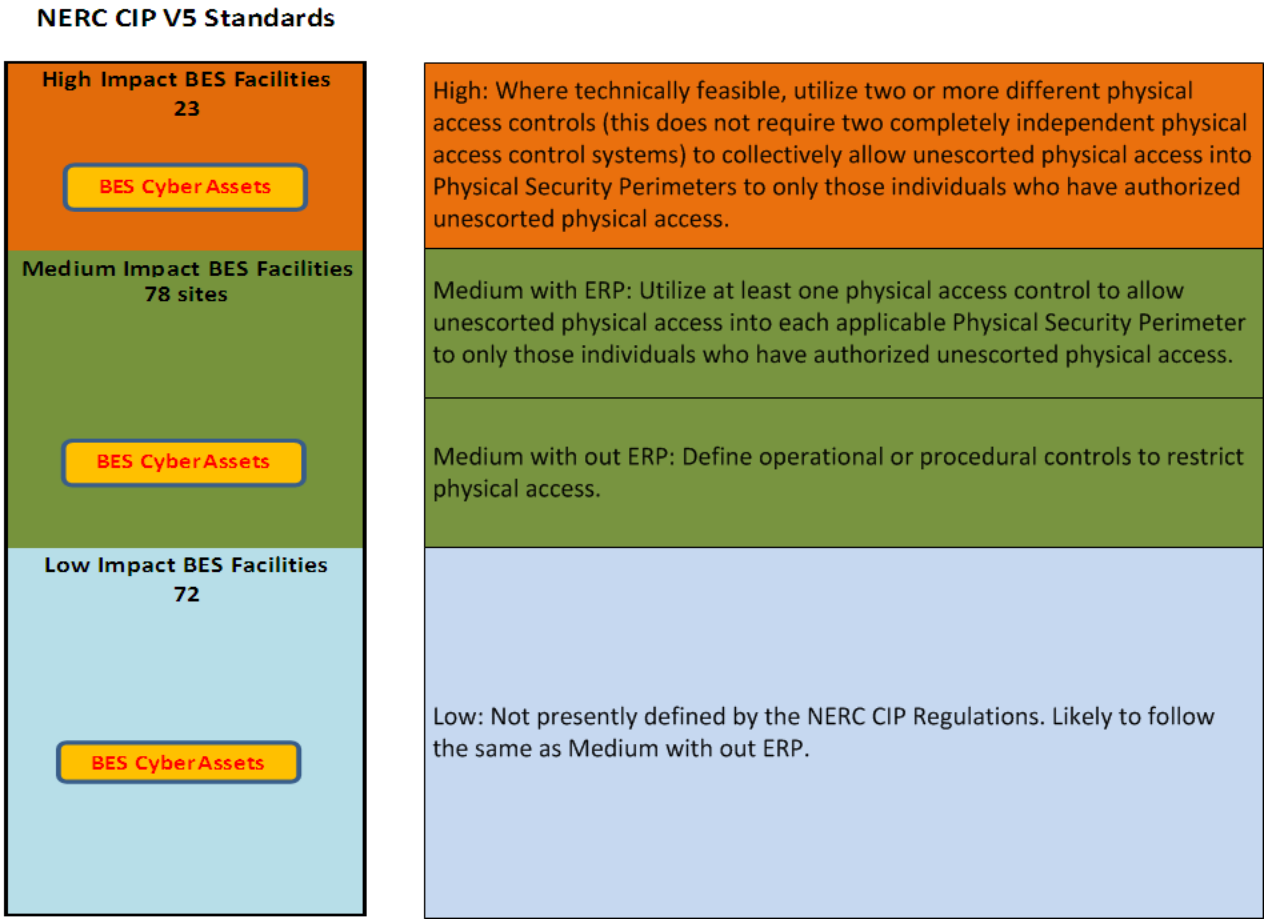


# CIP 006-5 – Physical Security

Manage physical security for BES Cyber Systems

- V3 to V5
  - V3 physical access controls are uniform for all assets
  - V3 requires monitoring, alerting, logging of perimeters
  - V3 visitor management could be designed by the Entity
  - V5 physical access controls are tailored to impact level
    - High impact facilities require two means of access control
    - Response to alarms within 15 minutes
    - Visitor management is prescriptive
- Functional – Program Approach
  - Develop a Physical Security and Visitor Management Program
  - Integrate Physical Security System maintenance with programs to manage technology for other NERC assets
- To-dos and challenges
  - Incomplete physical security control design for low impact facilities
  - Implementation at a large number of sites (100+)

# Example PSP Impact by Level



# CIP 007-5 – Systems Security Management

Manage system security by implementing technical, operational and procedural requirements

- V3 to V5
  - Testing and vulnerability assessment (VA) requirements moved out of CIP 007-5
  - V5 requirements are tailored by impact level
  - More fidelity in areas such as:
    - Patch Management - Clear timelines to evaluate and *implement* patches
    - Logging - Components of logs, e.g. successful and failed attempts, malicious code detection
- Functional – Program Approach
  - Develop a comprehensive change management program to coordinate and standardize management of systems
  - Develop standardized processes for functions such as patching and account management
- To-dos and challenges
  - Technical means to implement controls such as account management and malicious software prevention in a substation environment is untested
  - There are no programs or procedures in place to perform tasks such as patch management, management of ports and services in a substation environment
  - But technical challenges for existing systems may not be substantial

# CIP 008-5 – Incident Reporting

Manage cybersecurity incidents by developing and implementing response plans

- V3 to V5
  - V5 requires a review of a response plan after a test or after an actual incident
  - V5 mandates communication of changes to response plans to responsible personnel
- Functional Program Approach
  - Develop a coordinated incident response program to govern activities across all asset owners
  - Automate incident response workflows for all SMEs to streamline communications of incidents or changes to plans
- To-dos and challenges
  - Changes in V5 are minor but increase in scope will require a coordinated action plan to comply
  - Cybersecurity SMEs are not currently embedded in T&D operations
  - There are no incident response plans specific to cybersecurity for substation assets

# CIP 009-5 – Disaster Recovery

Recover reliability functions by specifying recovery plan requirements to support continued stability operability and reliability

- V3 to V5
  - V5 requires “preservation” of data that triggered the activation of a recovery plan
  - V5 requires backups for all substation equipment
- Functional - Program Approach
  - Develop a coordinated disaster recovery program to govern activities across all asset owners
  - Disaster recovery plans should focus the recovery of entire systems to an operational level
- To-dos and challenges
  - Full-scale testing and back-up capability for all substation devices is not currently available
  - An integrated program that can perform this function by owning, maintaining, validating and exercising disaster recovery plans has not been developed

# CIP 010-5 – Configuration Change Management and Vulnerability Assessments

To prevent and detect unauthorized changes to BES Cyber systems

- V3 to V5
  - V3 Change and Configuration Management was one requirement with elements of change controls in other requirements
  - V5 Change Management is a prescriptive stand-alone standard
    - Entities are required to develop and deploy rigorous and structured change management practices
    - Requirement to perform vulnerability assessments
- Functional - Program Approach
  - Develop NERC change management program supported by technology for automation of change records
  - Designate system custodians with responsibility to implement change controls prescribed by the program within org units
- To-dos and challenges
  - An integrated program has not been developed
  - An ill-designed or poorly executed program poses significant compliance risk across all CIP standards
  - Technical ability to perform vulnerability assessments for control systems potentially an untested capability
  - There is no standardized automation solution to track changes, approvals and enforce workflows

# CIP 011-5 – Information Protection

Prevent unauthorized access to BES Cyber System information

- V3 to V5
  - V3 Information protection program could be designed by the Entity
  - V5 Information protection is a prescriptive stand-alone standard
    - Entities are required to document methods and demonstrate actions to identify and protect documents
    - Explicit requirement to “prevent retrieval” of information prior to the reuse of an asset with such information
- Functional - Program Approach
  - Update and standardize existing Information Protection Program
- To-dos and challenges
  - An integrated program that can enable enforcement of controls in a consistent manner has not been developed
  - Technical solution to identify, protect and limit access to information artifacts is not available
  - The scope of information artifacts (e.g. relay settings) that have to be evaluated is very large
  - Management of access rights for contractors and off-site vendors with electronic access

# Serial Connected Devices

- All BES Cyber Systems are in scope of all the CIP V5 standards
- However, for certain requirements, the type of connectivity limits applicability
- Note that it is protocol-based, not transport-based
- Routable protocols can run  over serial transports
- PMUs will likely be Classified in the Medium (with or without externally routable protocol) at a minimum if used by the entity for Situational Awareness

# Presentation contributors

- Raghu Rayalu (SCE)
- Anthony Johnson (SCE)
- Dan Brancaccio (Bridge Energy Group)
- Alison Silverstein (NASPI)
- Jim McNierney (NYISO)
- Scott Mix (NERC)