

- Describe the NIST Risk Management Framework and related NIST standards and guidelines (hereafter referred to as the “RMF model”)
- Present our understanding of the NERC CIP model
- Compare the RMF model with the NERC CIP model
- Explore harmonizing the NERC CIPs with NIST SP 800-53, Rev 2 Moderate Baseline
- Suggest modifications to the NERC CIPs
- Assist NERC in adopting the modifications, if requested

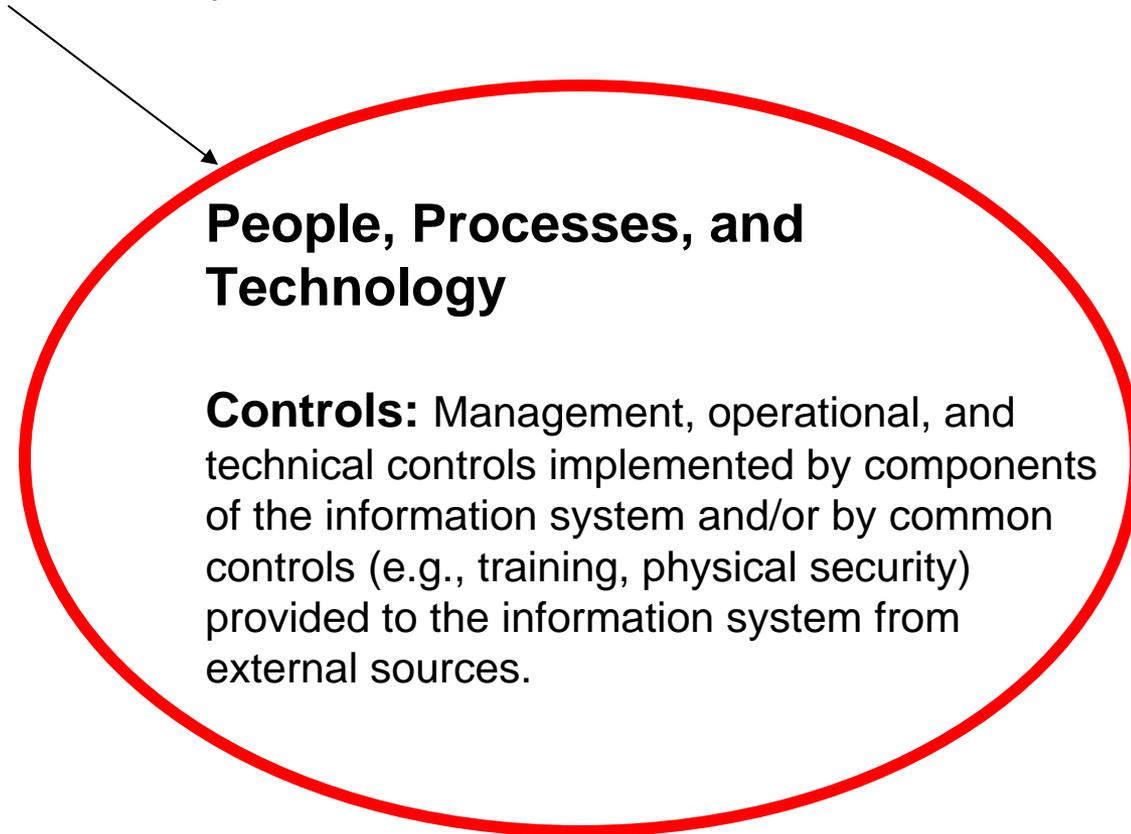
- Attempting to do a fair analysis and comparison of the two approaches
- Acknowledge we may not have full understanding of the NERC approach/model — encourage discussion on this topic as we move forward
- Want to provide NERC drafting committee with a better understanding of the NIST approach/model
- Share insights learned performing analysis/comparison of the two approaches
- Committee decides on direction of the modified CIPs
- NIST is ready to help if the committee wishes to incorporate any of the NIST approach into the CIPs

NIST Risk Management Framework

Terms from the NIST Glossary:

- **Information System:** [44 U.S.C., Sec. 3502][OMB Circular A-130, Appendix III] A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. [Note: Information systems consist of people, processes, and technology.]
- **Accreditation (authorization to operate):** [FIPS 200, NIST SP 800-37] The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls.
- **Certification (assessment of security controls):** [FIPS 200, NIST SP 800-37] A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.
- **Accreditation Boundary:** [NIST SP 800-37] All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected. Synonymous with the term security perimeter defined in CNSS Instruction 4009 and DCID 6/3.

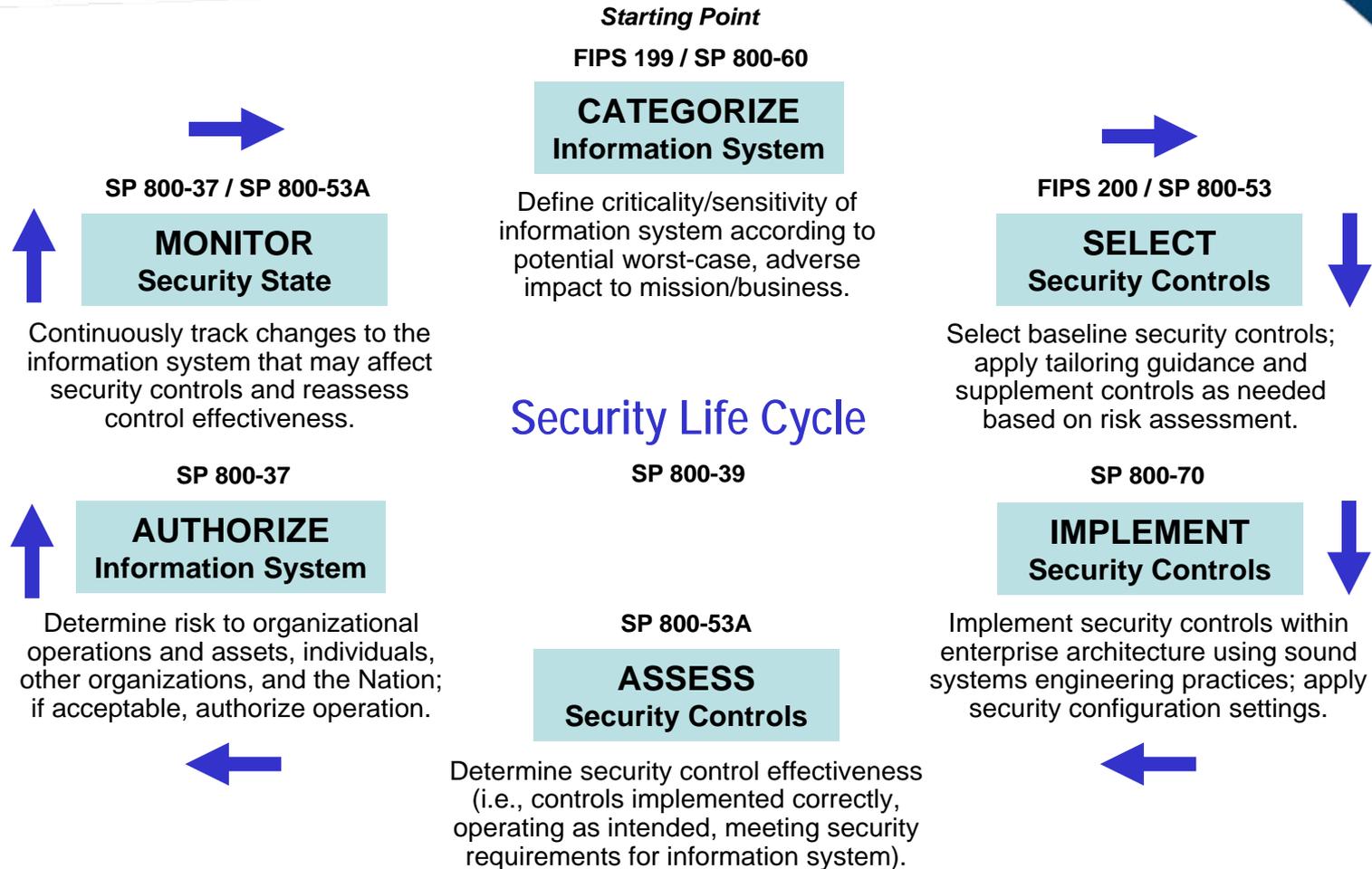
Accreditation Boundary



NIST Risk Management Framework

- The information/control system under consideration is defined by the accreditation boundary.
- All information system components are within the logical boundary (i.e., there are no information system components on the boundary, **unlike the ESP boundary defined in the CIPs**).
- Selected security controls from SP 800-53 (i.e., requirements) are satisfied by the information system components and/or by common controls.
- Common controls (e.g., training, physical security) are provided to the information system from external sources.
- Security controls are implemented within the components of the information system as determined (i.e., allocated) by the system design and engineering
- Security controls are not expected to be implemented in every component of the information system, **unlike the CIPs**.

Risk Management Framework



Important Concepts within the RMF

- Information system focus, including accreditation boundary concept (all components of the information system are within the accreditation boundary)
- Risk management framework defines overall risk management process to be followed for an information system
- Categorization of potential impact required (Low, Moderate, High)
- Level of rigor is based on categorization
- Information system control selection includes baseline, tailoring, and supplementation based on risk assessment
- Security Plan required for each information system
- Security controls are implemented:
 - Within the components of the information system as determined (i.e., allocated) by the system design and engineering
 - By common controls (e.g., training, physical security) provided to the information system from external sources.

Important Concepts within the RMF

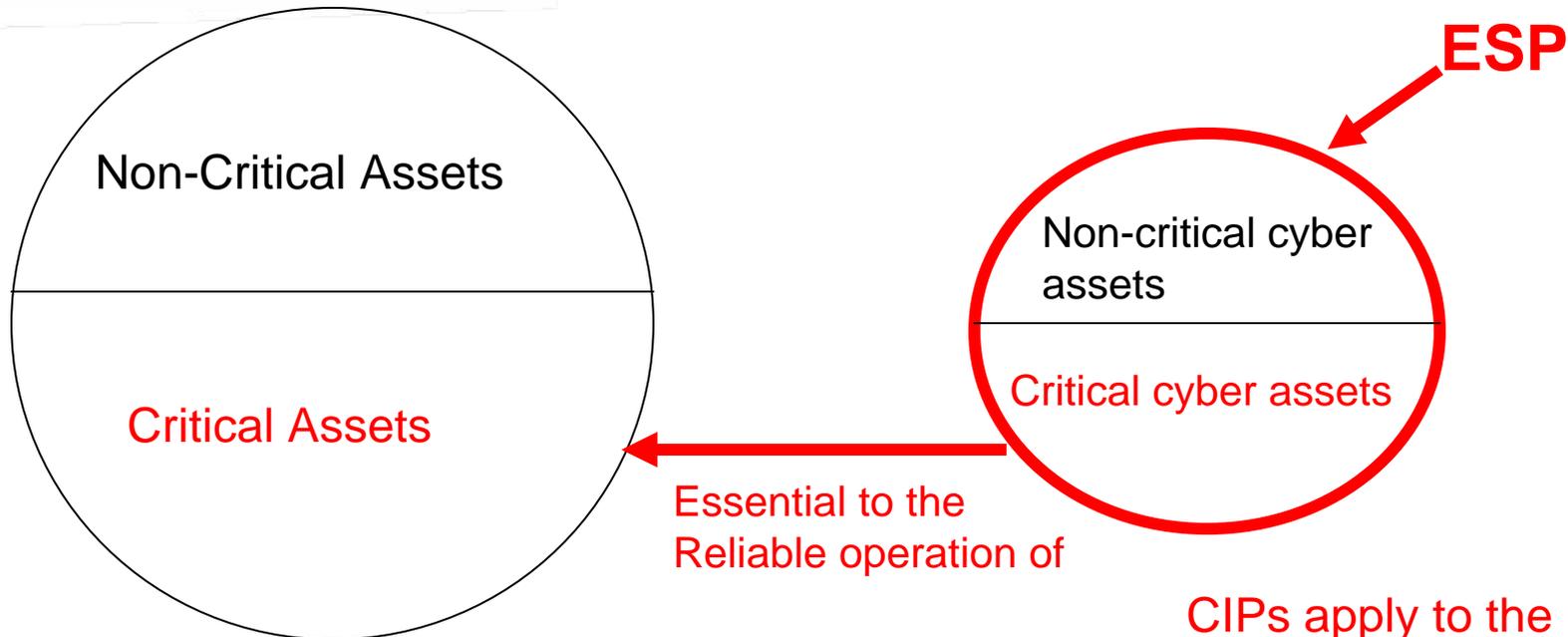
- Security assessment plan is required
 - Control-specific assessment procedures are defined
 - Assessment of controls by independent assessor
- Organization official authorizes system operation based on acceptance of residual risk
- Continuous monitoring of the status of security controls and system configuration changes
- Addresses trust model and trust relationships with business partners and external service providers

NERC and CIP Model

Terms from the NERC Glossary:

- **Assets:** Facilities, systems, and equipment
- **Critical Assets:** Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.
- **Cyber Assets:** Programmable electronic devices and communication networks including hardware, software, and data.
- **Critical Cyber Assets:** Cyber Assets essential to the reliable operation of Critical Assets.

CIP Model



Assets: Facilities, systems, and equipment

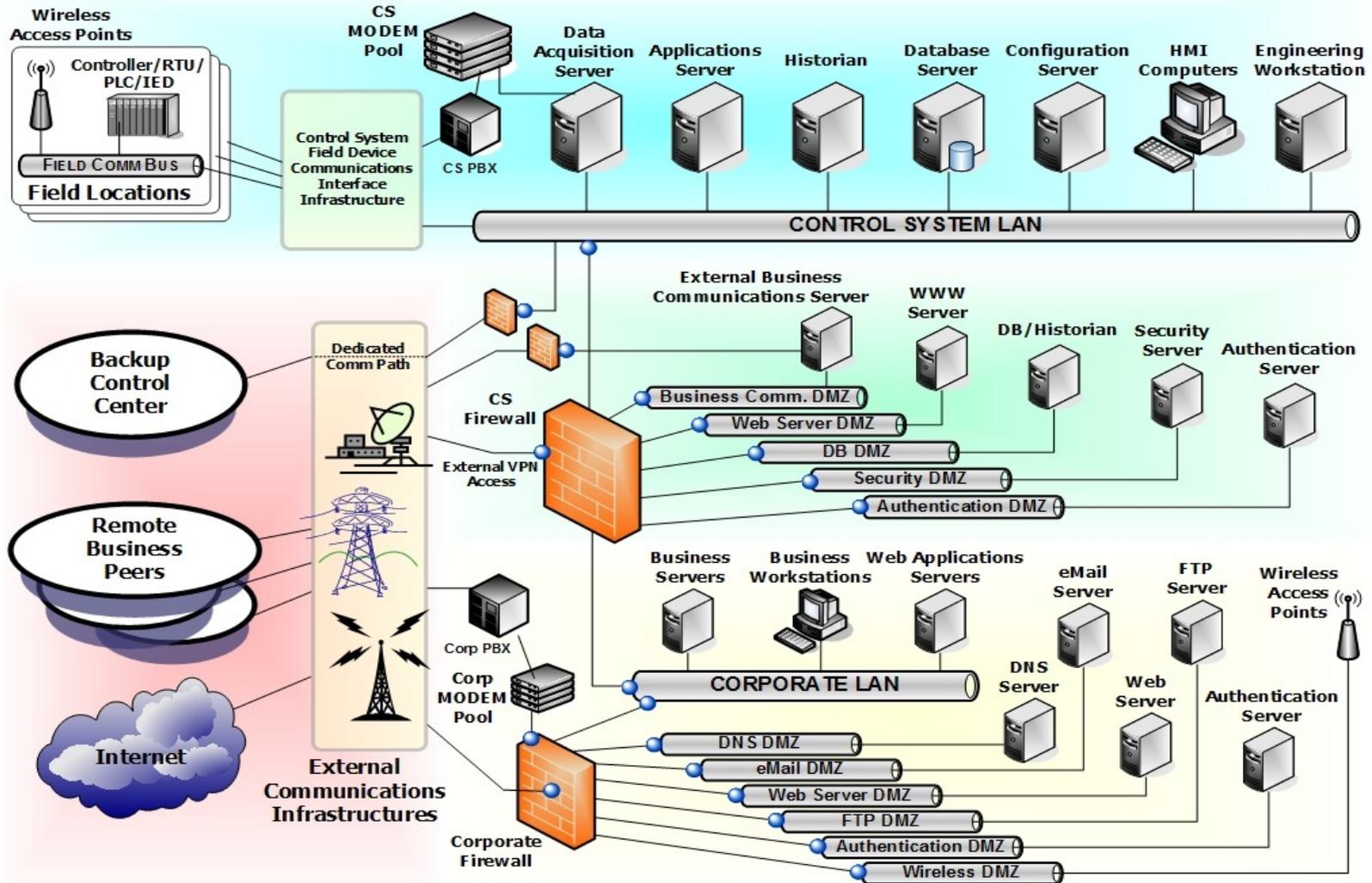
Critical Assets: Facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of the Bulk Electric System.

CIPs apply to the ESP and cyber assets within the ESP

The ESP contains critical cyber assets and, possibly non-critical cyber assets.

- ESP (CIP 005)
- Cyber assets within the ESP (CIP 007)
- Support of cyber assets
 - Security management (CIP 003)
 - Personal & training (CIP 004)
 - Physical security (CIP 006)
 - Incident reporting & response planning (CIP 008)
 - Recover plans for critical cyber assets (CIP 009)

Generic Control System Model



Electronic Security Perimeter

- The logical border surrounding a network to which Critical Cyber Assets are connected and for which access is controlled.
 - CIP-005 R.1 & R1.4 imply that an ESP contains both critical and non-critical cyber assets
 - Critical and non-critical cyber assets within an ESP are under the control of the Responsible Entity (RE).

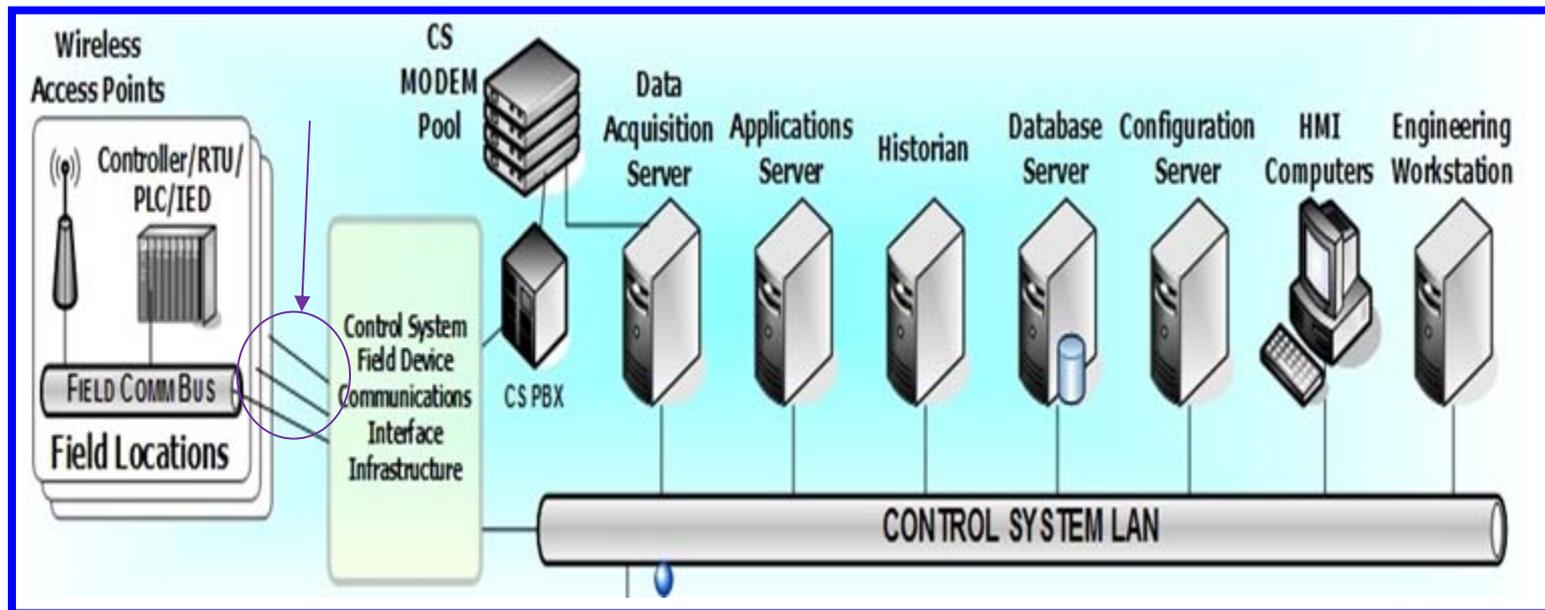
R1. Electronic Security Perimeter — The Responsible Entity shall ensure that every Critical Cyber Asset resides within an Electronic Security Perimeter. The Responsible Entity shall identify and document the Electronic Security Perimeter(s) and all access points to the perimeter(s).

R1.4. Any non-critical Cyber Asset within a defined Electronic Security Perimeter shall be identified and protected pursuant to the requirements of Standard CIP-005.

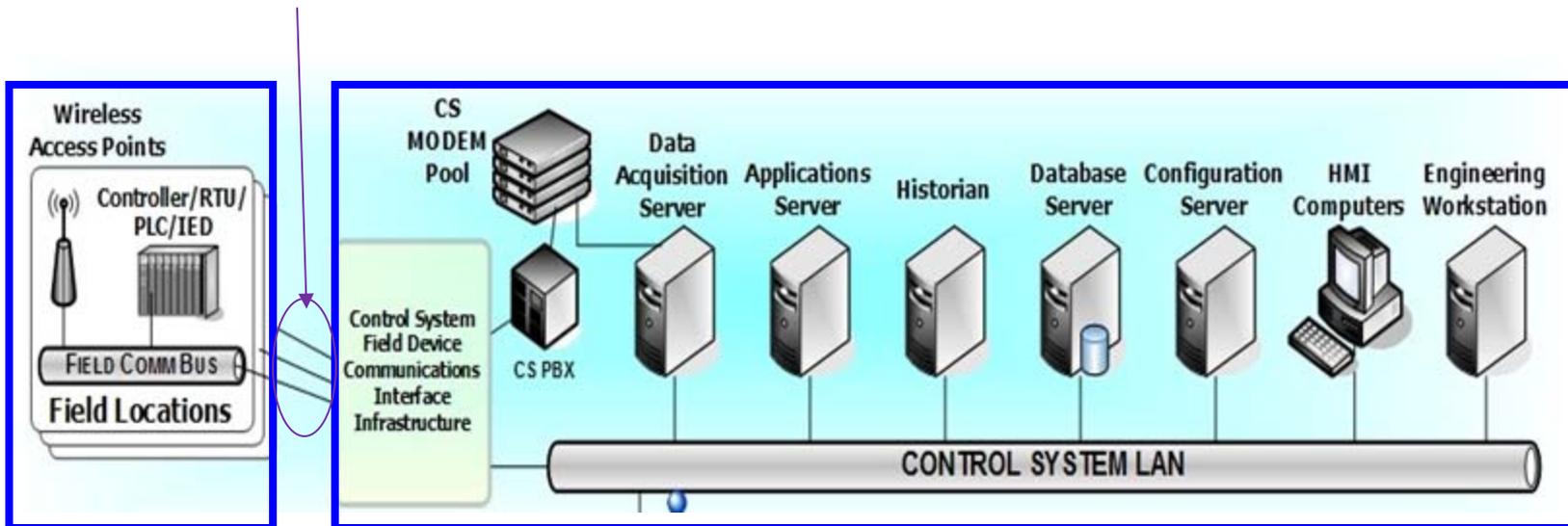
Determining the ESP (or ESPs) in the Generic Control System Model.

Are all of the following reasonable ESP configurations?

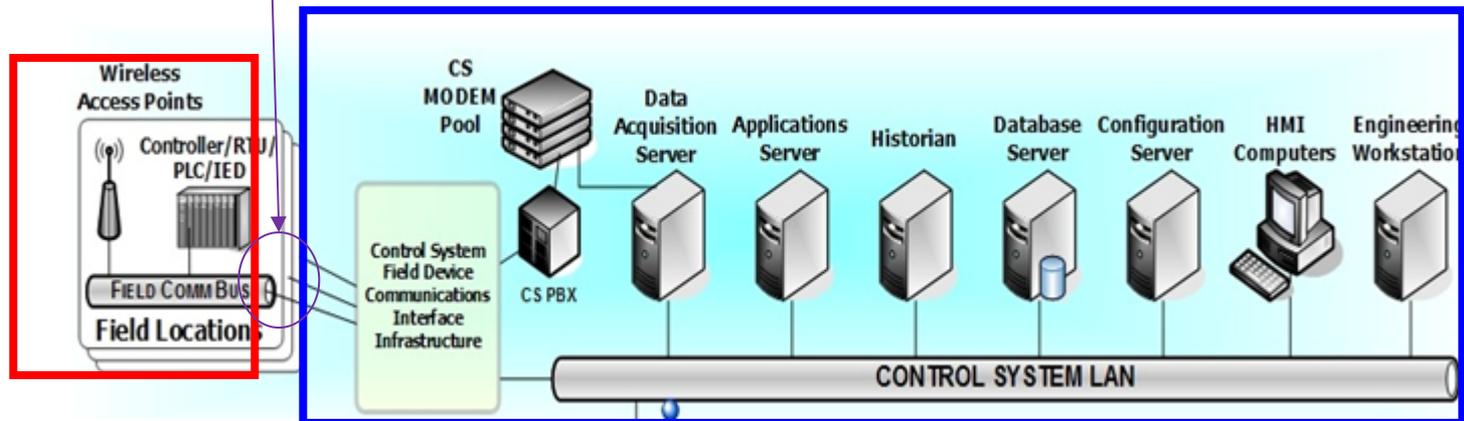
One ESP: All cyber assets, including the communication paths, are under the control of the Responsible Entity (RE)



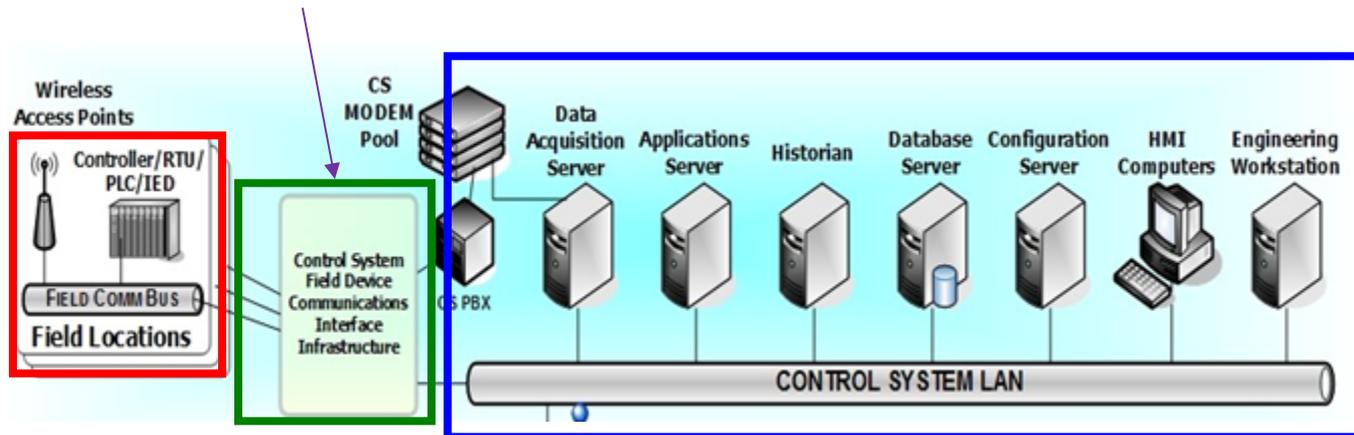
One ESP: All cyber assets, except the communication paths, are under the control of the Responsible Entity (RE)



Two ESPs: The ESPs are under the control of different REs. The communications paths are not under the control of either RE.



Three ESPs: The communications are in an ESP. Each ESP is under the control of a different RE.



Compare NIST & the NERC/CIP approach

Similarities

- Holistic approaches: both address technology, management & operational aspects of security
- Concepts of external/internal to boundary (ESP & accreditation boundary)

Conceptual Model Differences

- NIST
 - Information system view
 - All information system components are within accreditation boundary, including people, processes, and technology
 - Security requirements are allocated to components
 - Allows holistic defense-in-depth approach through system design & engineering

- NERC
 - Critical asset, cyber asset, & critical cyber asset view
 - Concept of protecting perimeter (i.e., ESP) & contents within ESP; contents only include cyber assets. People & processes addressed by additional CIPs.
 - Security requirements are applied to all components (i.e., all cyber assets)
 - Treating boundary and contents separately (e.g., in CIPs 5 & 7) can lead to inefficiency, inconsistency, and vulnerabilities

Additional Differences

- RMF concepts
 - Management of risk vs. compliance with requirements (CIPs)
 - Categorization of potential impact (Low, Moderate, High)
 - Security plan
 - Security testing and evaluation procedures and methods
 - Authorization to operate
 - Continuous Monitoring
 - Common controls
 - Trust model as basis for trust between business partners & external service providers
- Wireless not addressed in CIPs

Explore Harmonizing the NERC CIPs with NIST's Moderate Baseline

- Add material to make the NERC CIPs comparable to NIST's Moderate baseline
 - Policy requirement to each CIP
 - Guidance
 - Augment CIP requirements
 - Security Test and Evaluation
- Replace the concept of technical feasibility with an exception process
- Merge CIPs 005 & 007

Example of CIP Augmentation

- Process followed
 - Examined mapping exercise results
 - Reviewed CIP 005 & 800-53 Moderate baseline to identify gaps
 - Added material to existing requirements or added new requirements to close gaps
- Provide CIP 005 augmentation example to NERC development team
- Assist NERC in augmenting remaining CIPs, if requested

B. Requirements

R0. Cyber Security Perimeter Policy and Procedures — The Responsible Entity shall: develop, disseminate, and periodically review update: (i) a formal, documented, policy on the protection of all Cyber Security Perimeter(s), the cyber assets contained within, and identification and authentication. This policy shall address purpose, scope, roles, responsibilities, management commitment, coordination among Responsible Entity's sub-entities, and compliance; and (ii) formal, documented procedures to facilitate the implementation of this policy and associated controls.

GUIDANCE: this requirement does not prescribe an organization structure for the Responsible Entity 's cyber security policy. The Cyber Security Perimeter Policy and Procedures may be included as part of the general information security policy for the Responsible Entity, or the ICS cyber security policy.

CIP-005

B. Requirements

R0. Policy and Procedures

R1. Electronic Security
Perimeter

R2. Electronic Access
Controls

R3. Monitoring Electronic
Access

R4. Cyber Vulnerability
Assessment

R5. Documentation Review
and Maintenance

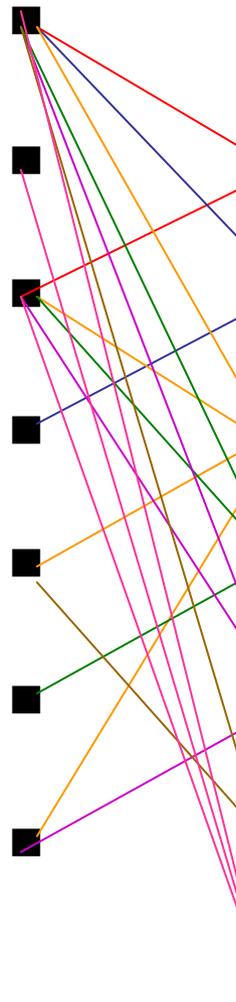
R6. Identification and
Authentication

—— Indicates controls (or part of controls) added to CIP requirement

NIST SP 800-53

Relevant Control Families

- AC: Access Control
- AU: Auditing and Accountability
- CA: Certification, Accreditation & Security Assessments
- CM: Configuration Management
- IA: Identification & Authentication
- RA: Risk Assessment
- SC: System and Communication Protection



CIP-005

B. Requirements

NIST SP 800-53

Access Control

R0. Policy and Procedures



AC-1 Access Control Policy and Procedures

R1. Electronic Security
Perimeter



AC-2 Account Management

AC-3 Access Enforcement

R2. Electronic Access
Controls



AC-4 Information Flow Enforcement

AC-5 Separation of Duties

AC-6 Least Privilege

R3. Monitoring Electronic
Access



AC-7 Unsuccessful Login Attempts

AC-8 System Use Notification

AC-9 Previous Logon Notification

R4. Cyber Vulnerability
Assessment



AC-10 Concurrent Session Control

AC-11 Session Lock

AC-12 Session Termination

R5. Documentation Review
and Maintenance



AC-13 Supervision and Review—Access Control

AC-14 Permitted Actions without Identification or Authentication

R6. Identification and
Authentication



AC-15 Automated Marking

AC-16 Automated Labeling

AC-17 Remote Access

AC-18 Wireless Access Restrictions

AC-19 Access Control for Portable and Mobile Devices

AC-20 Use of External Information Systems

— Indicates controls (or part of controls) added to CIP requirement

CIP-005

B. Requirements

R0. Policy and Procedures



R1. Electronic Security
Perimeter



R2. Electronic Access
Controls



R3. Monitoring Electronic
Access



R4. Cyber Vulnerability
Assessment



R5. Documentation Review
and Maintenance



R6. Identification and
Authentication



NIST SP 800-53

Identification & Authentication

IA-1 Identification and Authentication
Policy and Procedures

IA-2 User Identification and
Authentication

IA-3 Device Identification and
Authentication

IA-4 Identifier Management

IA-5 Authenticator Management

IA-6 Authenticator Feedback

IA-7 Cryptographic Module Authentication

— Indicates controls (or part of controls) added to CIP requirement

CIP-005

B. Requirements

R0. Policy and Procedures

R1. Electronic Security
Perimeter

R2. Electronic Access
Controls

R3. Monitoring Electronic
Access

R4. Cyber Vulnerability
Assessment

R5. Documentation Review
and Maintenance

R6. Identification and
Authentication

NIST SP 800-53

Configuration Management

CM-1 Configuration Management Policy and Procedures

CM-2 Baseline Configuration

CM-3 Configuration Change Control

CM-4 Monitoring Configuration Changes

CM-5 Access Restrictions for Change

CM-6 Configuration Settings

CM-7 Least Functionality

CM-8 Information System Component Inventory

— Indicates controls (or part of controls) added to CIP requirement

CIP-005

B. Requirements

R0. Policy and Procedures

R1. Electronic Security
Perimeter

R2. Electronic Access
Controls

R3. Monitoring Electronic
Access

R4. Cyber Vulnerability
Assessment

R5. Documentation Review
and Maintenance

R6. Identification and
Authentication

NIST SP 800-53

Auditing and Accountability

- **AU-1** Audit and Accountability Policy and Procedures
- **AU-2** Auditable Events
- **AU-3** Content of Audit Record
- **AU-4** Audit Storage Capacity
- **AU-5** Response to Audit Processing Failures
- **AU-6** Audit Monitoring, Analysis, and Reporting
- **AU-7** Audit Reduction and Report Generation
- **AU-8** Time Stamps
- **AU-9** Protection of Audit Information
- **AU-10** Non-repudiation
- **AU-11** Audit Record Retention

— Indicates controls (or part of controls) added to CIP requirement

CIP-005

B. Requirements

- R0. Policy and Procedures ■
- R1. Electronic Security Perimeter ■
- R2. Electronic Access Controls ■
- R3. Monitoring Electronic Access ■
- R4. Cyber Vulnerability Assessment ■
- R5. Documentation Review and Maintenance ■
- R6. Identification and Authentication ■

NIST SP 800-53 Risk Assessment

- RA-1 Risk Assessment Policy and Procedures
- RA-2 Security Categorization
- RA-3 Risk Assessment
- RA-4 Risk Assessment Update
- RA-5 Vulnerability Scanning

— Indicates controls (or part of controls) added to CIP requirement

CIP-005

B. Requirements

NIST SP 800-53

SC: System and Communication Protection

R0. Policy and Procedures



R1. Electronic Security Perimeter



R2. Electronic Access Controls



R3. Monitoring Electronic Access



R4. Cyber Vulnerability Assessment



R5. Documentation Review and Maintenance



R6. Identification and Authentication



■ SC-1 System and Communication Protection Policy and Procedures

■ SC-7 Boundary Protection

■ SC-9 Transmission Confidentiality

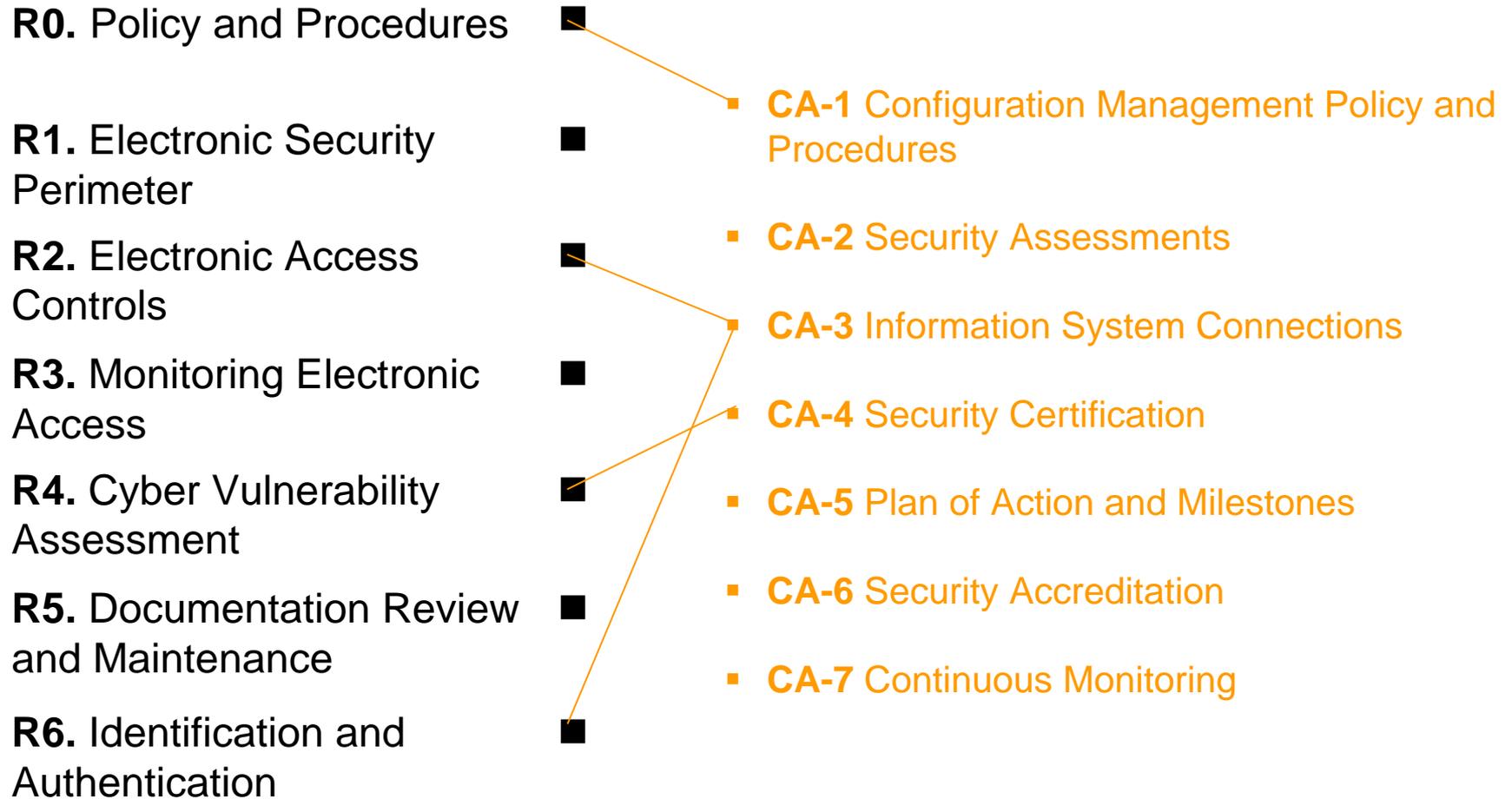
— Indicates controls (or part of controls) added to CIP requirement

CIP-005

B. Requirements

NIST SP 800-53

Certification, Accreditation, and Security Assessments



— Indicates controls (or part of controls) added to CIP requirement

- Add a new security assessment requirement based on:
 - SP 800-53 CA-2 Security Assessments
 - SP 800-53A Section 3.2 contains security assessment requirements

- **Example requirement:** Responsible Entity must develop detailed information security testing standards, processes, and procedures that provide direction and guidance on security testing.
 - See example augmented CIP-005 R4 for additional details

- SP 800-53A *Guide for Assessing the Security Controls in Federal Information Systems* can serve as the basis for selection and tailoring of processes and procedures.

Suggestion for Replacing “Technical Feasibility” with an “Exception Process”

- The Responsible Entity may take exception to any Requirement based on specified conditions. See example augmented CIP-005 Section A.6 for details
- The Responsible Entity shall document all exceptions in an Exception Plan provided to the ERO and Regional Reliability Organization.
- The Exception Plan must be approved annually by a Responsibility Entity senior manager.
- The Exception Plan must be approved annually by the Regional Reliability Organization, or the ERO if there is no applicable RRO.
- The ERO must annually audit compliance with the Exception Plan and provide FERC with an annual high-level, wide-area analysis regarding the effects of all exceptions on the reliability of the Bulk-Power System.

Merge CIP-005 & CIP-007

- CIP-005 R4 and CIP-007 R8 are quite similar.
 - CIP-005 addresses the perimeter
 - CIP-007 addresses the contents of the perimeter.
- Treating perimeter and contents separately can lead to inefficiency, inconsistency, and vulnerabilities