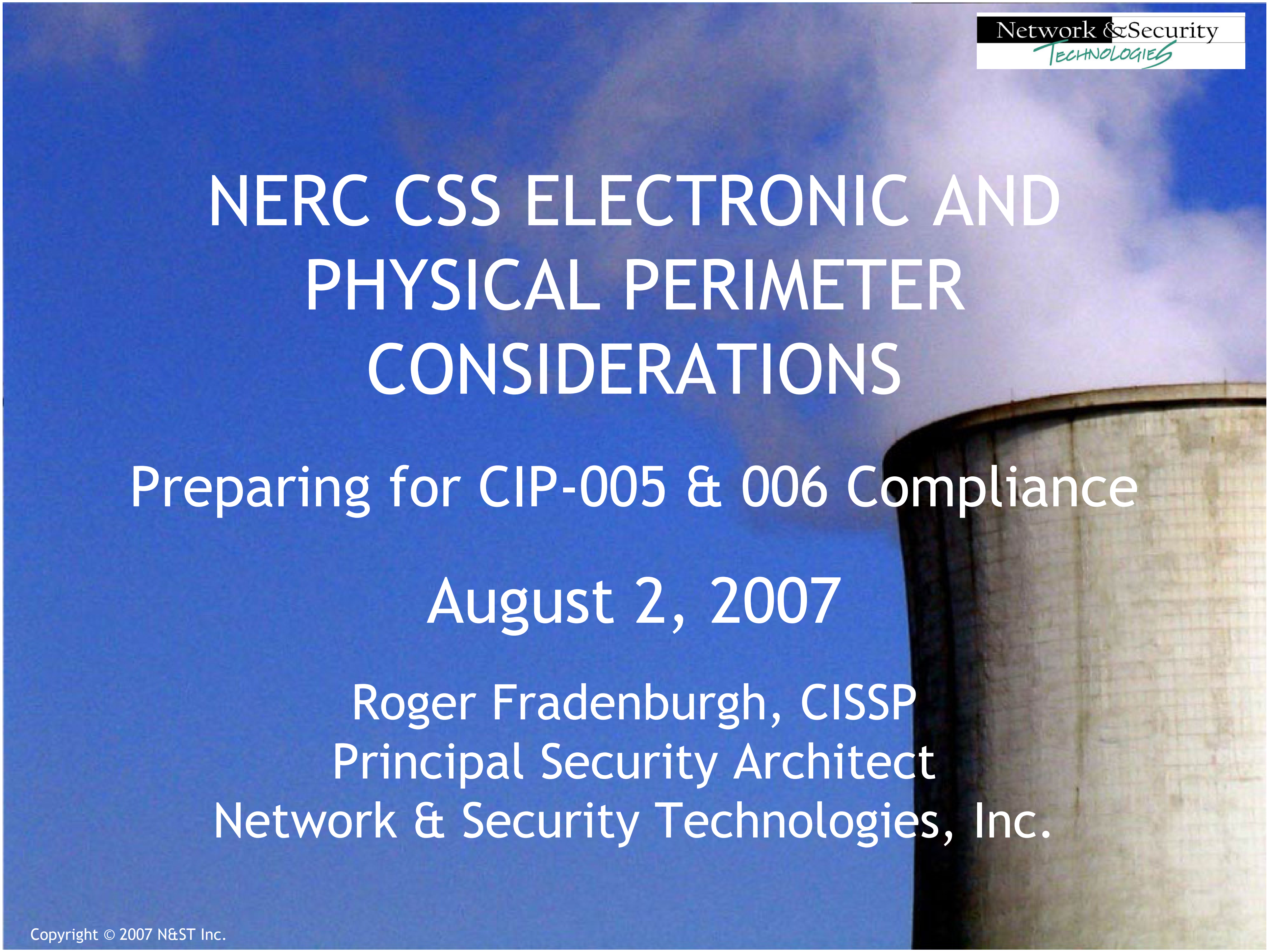
Network & Security Technologies



NERC CSS ELECTRONIC AND PHYSICAL PERIMETER CONSIDERATIONS

Preparing for CIP-005 & 006 Compliance

August 2, 2007

Roger Fradenburgh, CISSP
Principal Security Architect
Network & Security Technologies, Inc.

Agenda

- Introduction
- CIP-005 and 006 requirements
- General perimeter design considerations
- A perimeter design methodology
- Perimeter design examples
- CIP 005 and 006 required documents & records, ongoing compliance activities
- Wrap-up

Introduction Part I: About Us

- Network & Security Technologies, Inc. (N&ST)
  - A leader in Cyber Security for Bulk Electric System participants
    - Experience with numerous industry clients
  - Headquartered in New York
    - Employees in five states
  - A team of seasoned, vendor-neutral security professionals
    - Focused on building relationships with clients and helping them solve complex problems

Introduction Part II: About This Presentation

- Content largely derived from an N&ST report on perimeter designs prepared for and funded by EPRI EIS
- Purpose = Provide Bulk Electric System participants with:
  - Information about developing compliance strategies for CIP-005 and 006
  - A structured perimeter design methodology
  - Real-world examples
  - Information about ESP access controls
- Draft submitted June 12, 2007
  - Final version in progress

A (Very) Quick Aside: About the FERC NOPR

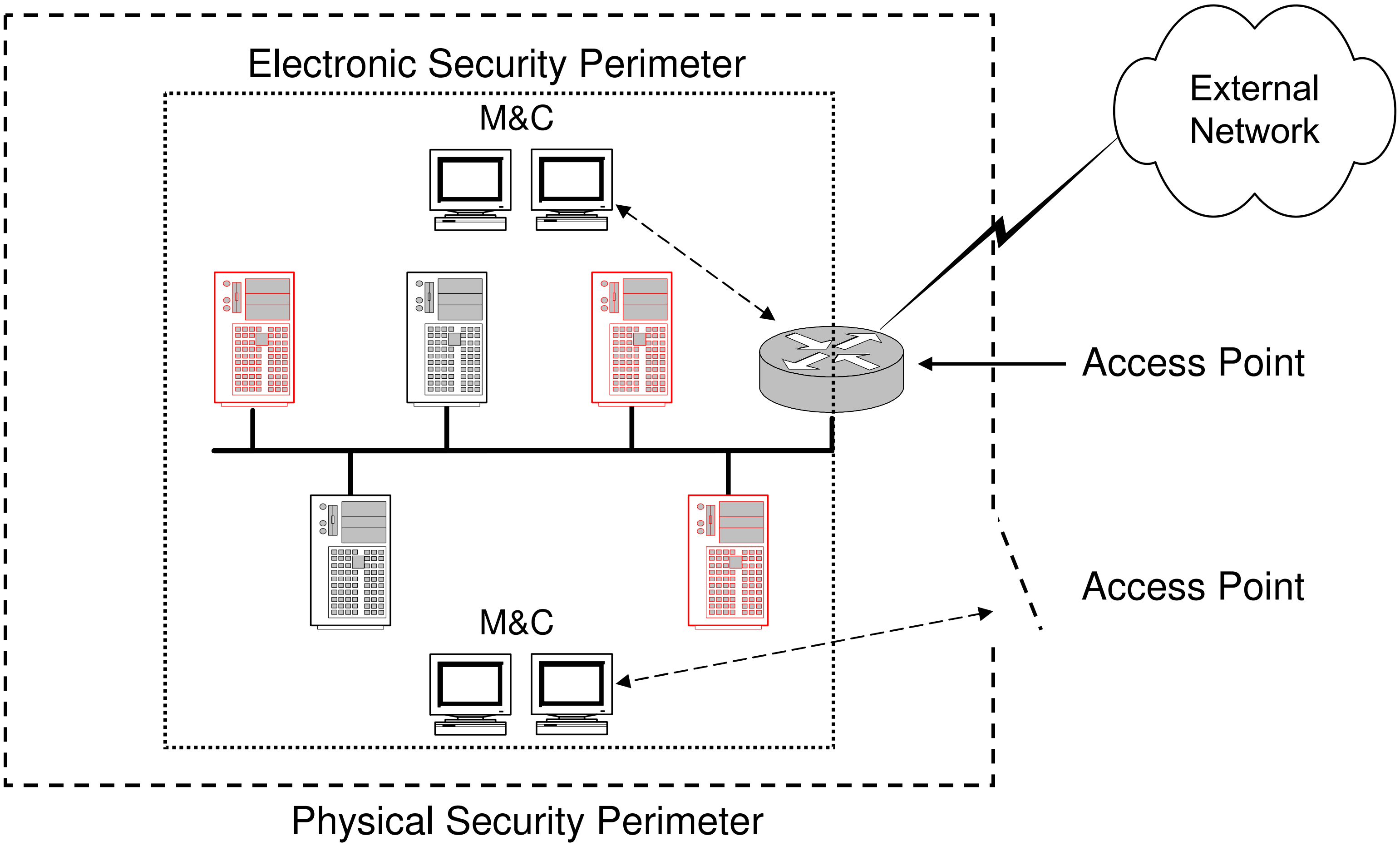
- Yes, I've read it
- No, I don't plan to talk about it
  - Well, maybe over lunch…

Agenda

- Introduction
- CIP-005 and 006 requirements
- General perimeter design considerations
- A perimeter design methodology
- Perimeter design examples
- CIP 005 and 006 required documents & records, ongoing compliance activities
- Wrap-up

Network & Security Technologies

Review of CIP-005 and 006 Principal Requirements



Review of CIP-005 and 006 Principal Requirements (2)

- CIP-005 and 006 also mandate:
  - Access control
    - Cyber and unescorted physical access by permission only (CIP-004 R4.)
  - Access monitoring and logging (7x24)
    - Including unauthorized access detection
  - Periodic testing
    - Cyber vulnerability assessment (CIP-005, annually)
    - Physical security systems test (CIP-006, every 3 years)
  - Extensive documentation and records

Things to Remember about CIP-005 and 006

- They do not mandate a one-to-one correlation between Electronic and Physical Security Perimeters
- Communication links between discrete ESPs are not subject to the CIP standards
  - However, network devices *inside* ESPs *are*
- Any network device that:
  - Interconnects an ESP and an external network, and
  - Permits the flow of data between the ESP and external systems,
  - Is an ESP access point and subject to the standards

Agenda

- Introduction
- CIP-005 and 006 requirements
- General perimeter design considerations
- A perimeter design methodology
- Perimeter design examples
- CIP 005 and 006 required documents & records, ongoing compliance activities
- Wrap-up

General Perimeter Design Considerations

- It will generally be the case that the fewer ESPs, the better
  - Fewer ESP access points to define, manage and monitor
- It will generally be beneficial to minimize the number of non-critical Cyber Assets within ESPs
  - Why = Requirements of CIP-007, “Systems Security Management,” must be applied to all Cyber Assets within ESPs
- These two goals may be difficult to reconcile

General Perimeter Design Considerations (2)

- How Electronic Security Perimeters are defined can impact Physical Security Perimeters
  - And vice-versa
- How perimeters are defined can impact costs to achieve compliance and maintain compliance
  - There may be trade-offs
- Responsible Entities should anticipate that in most cases, at least one ESP will be required within any building they own or lease that houses Critical Cyber Assets

General Perimeter Design Considerations (3)

- Designers should begin by determining if default perimeters around Critical Cyber Assets can be defined using existing network and physical infrastructures
  - Perimeter definition process should include discovery
- Remember CIP-002 qualifiers for Critical Cyber Assets:
  - Use of a routable protocol to communicate outside ESP(s)
  - Use of a routable protocol within a control center
  - Dial-up accessible

Agenda

- Introduction
- CIP-005 and 006 requirements
- General perimeter design considerations
- A perimeter design methodology
- Perimeter design examples
- CIP 005 and 006 required documents & records
- CIP 005 and 006 ongoing compliance activities
- Wrap-up

Perimeter Design Methodology

- A decision guide, not a cookbook
- Developed with the goals of:
  - Being applicable to both Electronic and Physical Security Perimeters, and
  - Helping all types and sizes of Responsible Entities make design decisions in an organized and structured manner

Perimeter Design Methodology: Preparation

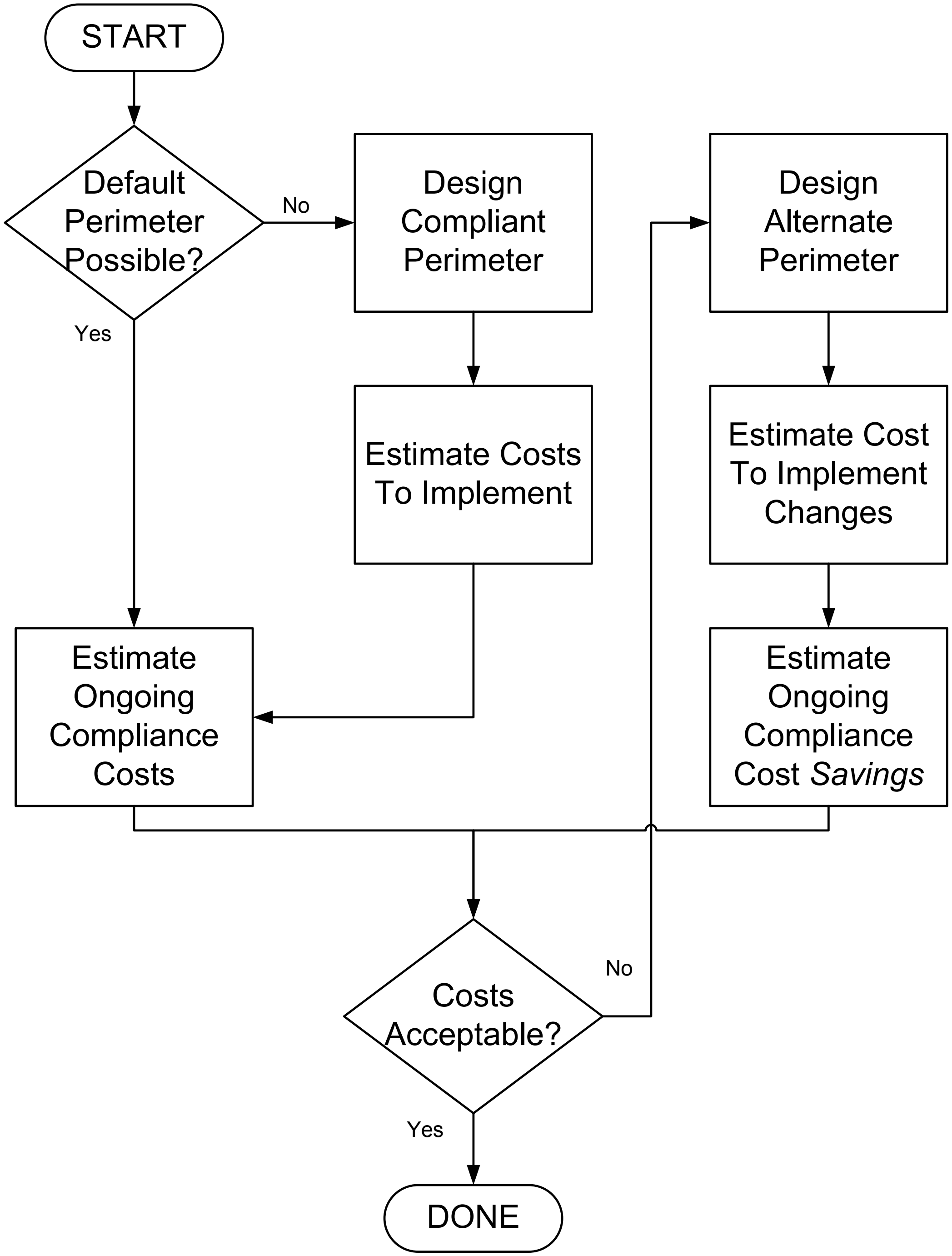
- Before starting, a design team should have:
  - The complete (and completed!) CIP-002 Critical Cyber Asset list
  - Complete and accurate information about the network and computing infrastructure
    - Must know both logical and physical locations of Critical Cyber Assets
  - Comparable information about existing physical security controls (buildings, computer rooms, etc.)

Perimeter Design Methodology: Preparation (2)

- The design team should also have information about:
  - Existing security monitoring capabilities
  - How logical and physical access permissions are managed
  - Cyber assets used to control and/or monitor logical or physical access
  - Non-critical Cyber Assets on the same network segments or in close physical proximity to Critical Cyber Assets

Perimeter Design Methodology: Preparation (3)

- The design team should also have information about:
  - Number of employees or 3rd-party personnel at sites housing Critical Cyber Assets
  - Current HR policies and procedures, esp. regarding background checks and security training
  - Current IT policies and procedures for protection of production cyber assets
- And then…


START
Default Perimeter Possible?
No
Yes
Design Compliant Perimeter
Estimate Costs To Implement
Design Alternate Perimeter
Estimate Cost To Implement Changes
Estimate Ongoing Compliance Costs
Estimate Ongoing Compliance Cost *Savings*
Costs Acceptable?
No
Yes
DONE

Identifying Default Perimeters Around Critical Cyber Assets

- ESP:
  - At the site in question, is there at least one network or subnet that is unique, in terms of its IP address, to that location?
    - Look for Layer 3 (IP) addressable network devices that might serve as ESP access points
  - If not, it will *probably* be necessary to deploy additional networking equipment

Identifying Default Perimeters Around Critical Cyber Assets (2)

- PSP:
  - At the site in question, are all Critical Cyber Assets within an access-controlled six-wall enclosure?
  - If not, it will *probably* be necessary to:
    - Build one, *or*
    - Move Critical Cyber Assets to an existing six-wall enclosure, *or*
    - Implement alternative measures to control physical access to Critical Cyber Assets as per CIP-006 R1.1

Possible Impacts of Design Choices on Compliance Costs

- Costs that *may* be affected by the # of non-critical Cyber Assets enclosed within an Electronic or a Physical Security Perimeter:
  - Configuration and Change Management (CIP-003)
  - Security Awareness Program (CIP-004)
  - Cyber Security Training (CIP-004)
  - Personnel Risk Assessments (CIP-004)
  - Online and Unescorted Physical Access and Access Rights Management (CIP-004)
  - Interactive Access Authentication Controls (CIP-005)
  - ESP and PSP access monitoring and logging
  - All CIP-007 requirements

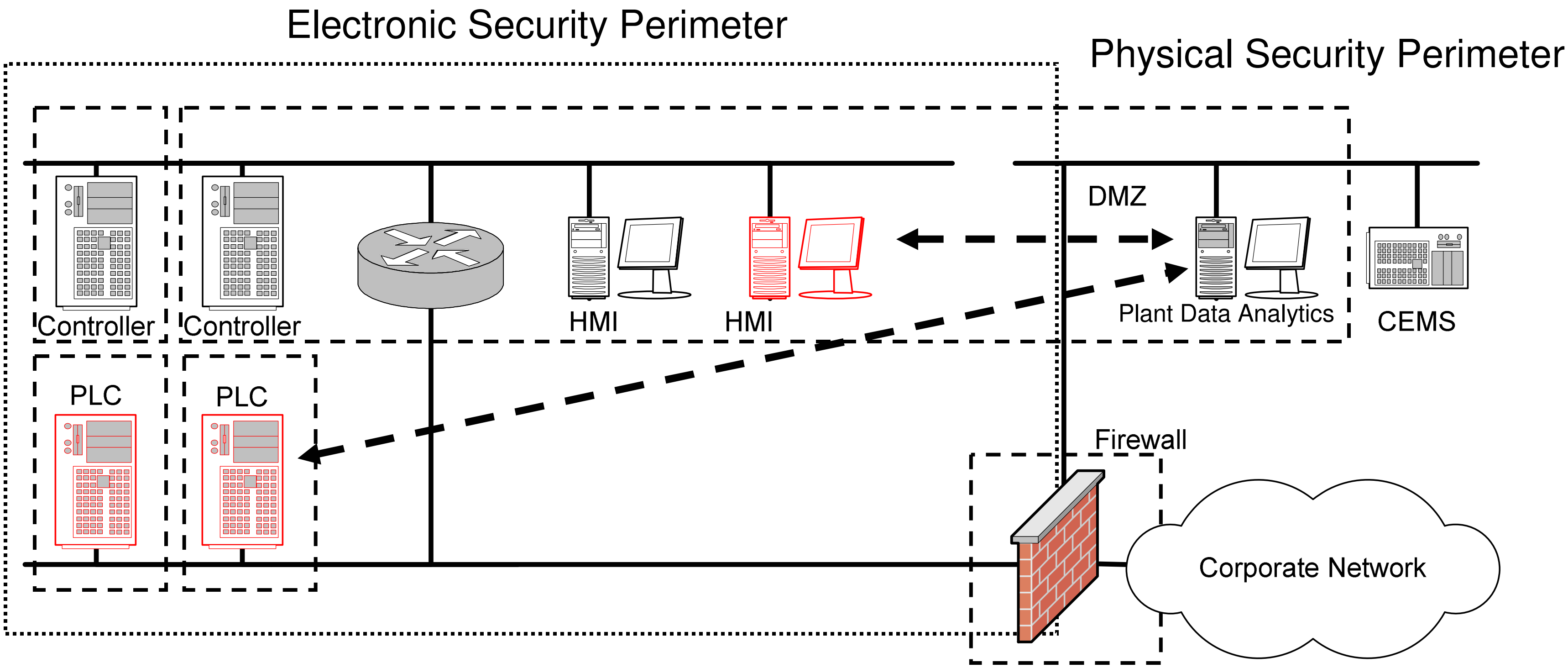
Agenda

- Introduction
- CIP-005 and 006 requirements
- General perimeter design considerations
- A perimeter design methodology
- Perimeter design examples
- CIP 005 and 006 required documents & records, ongoing compliance activities
- Wrap-up

Generating Plant – Example #1

- Cyber Assets essential to plant reliability are remotely accessible
  - Communicate with data collection & analysis system (e.g., PI System) using TCP/IP
- They are therefore Critical Cyber Assets
  - Must be within an Electronic Security Perimeter
  - All Cyber Assets within the ESP(s) must be within a Physical Security Perimeter

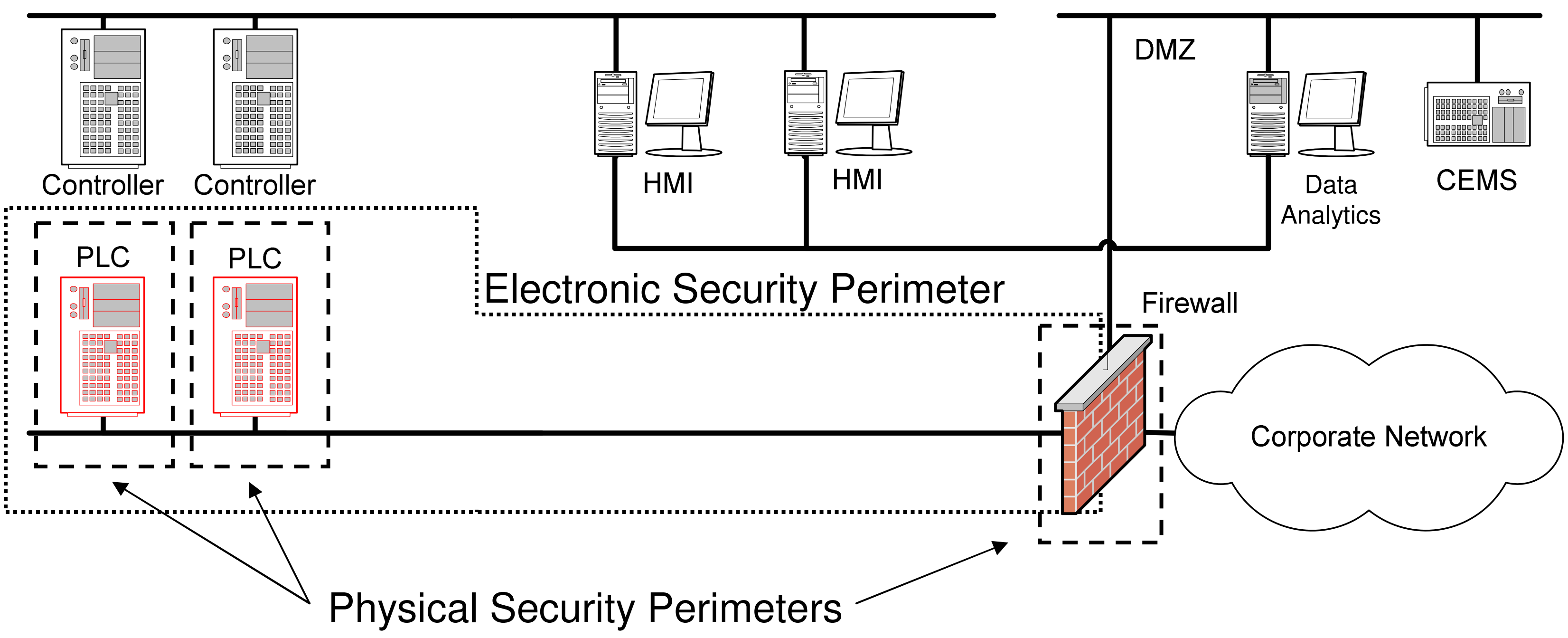
Generating Plant – Example #1



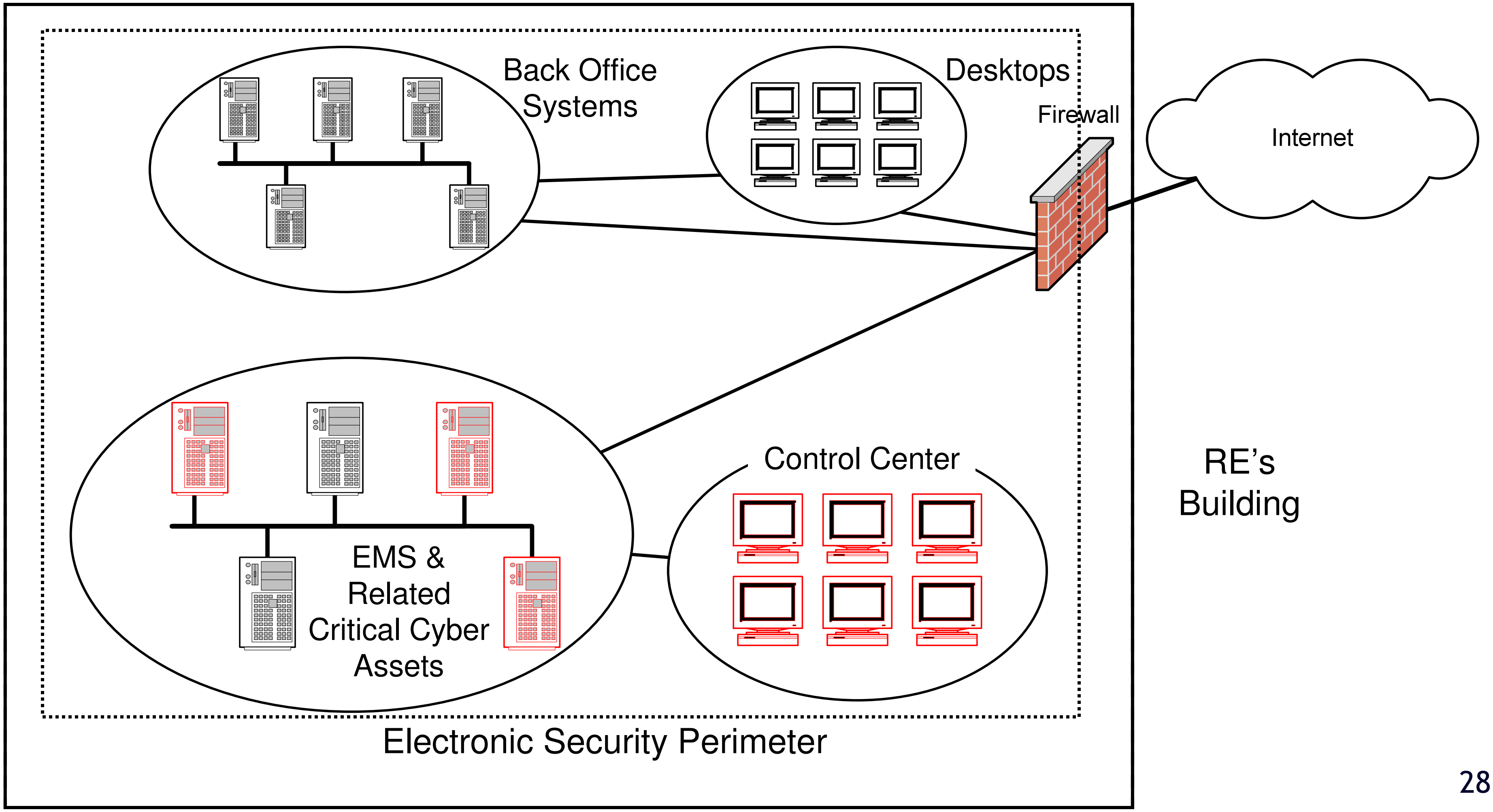
Generating Plant – Example #2

- PLCs essential to plant reliability are remotely accessible
  - Communicate with analysis system using TCP/IP
- They are, again, Critical Cyber Assets
  - Must be within Electronic and Physical Security Perimeters
- Controllers and HMIs are not remotely accessible and do not communicate with analysis system using a routable protocol
- They are not Critical Cyber Assets as defined by CIP Standards
  - No ESP required

Generating Plant – Example #2

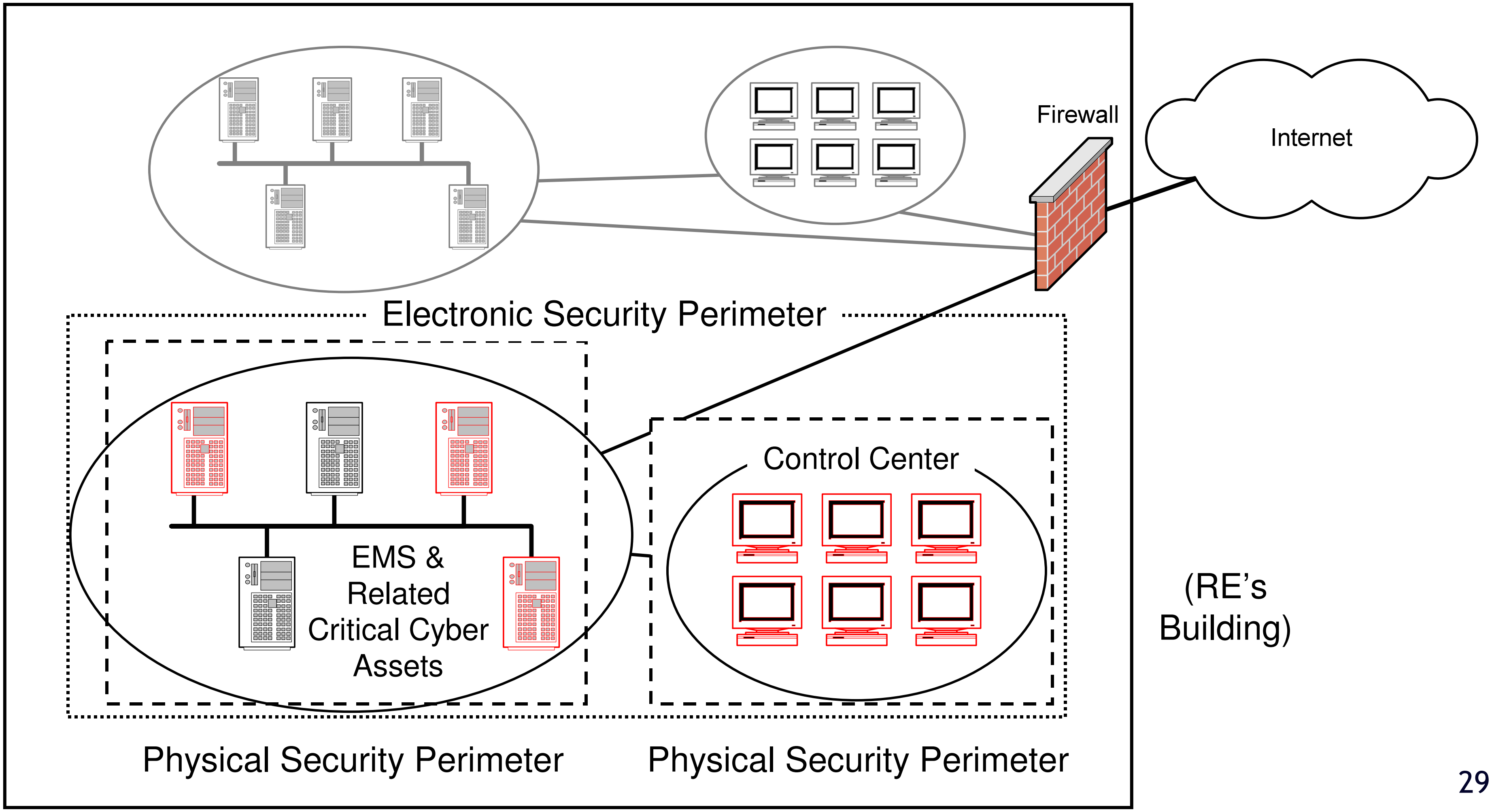


Control Center Example #1: Down-sizing an ESP and a PSP

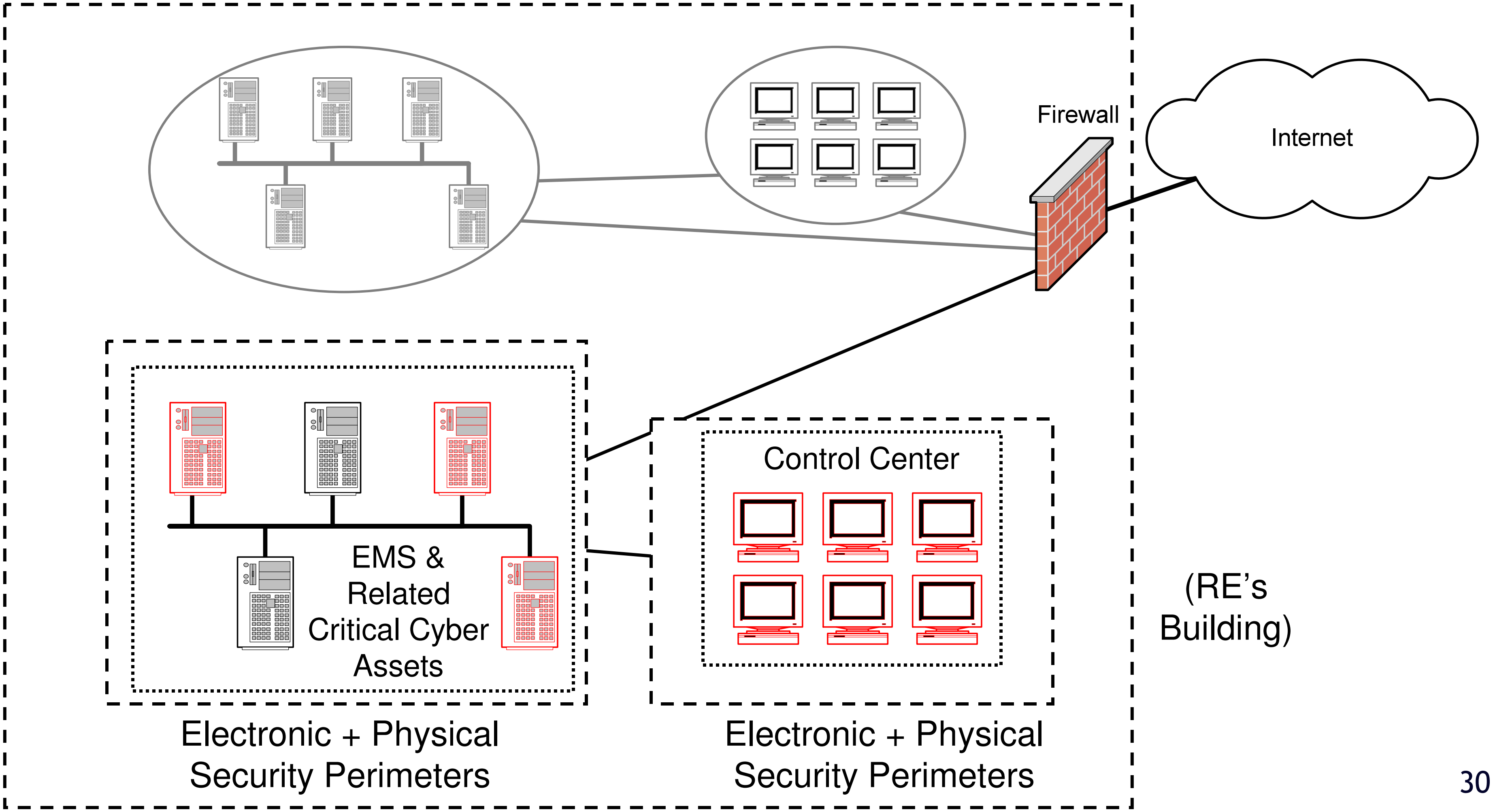


Network & Security Technologies

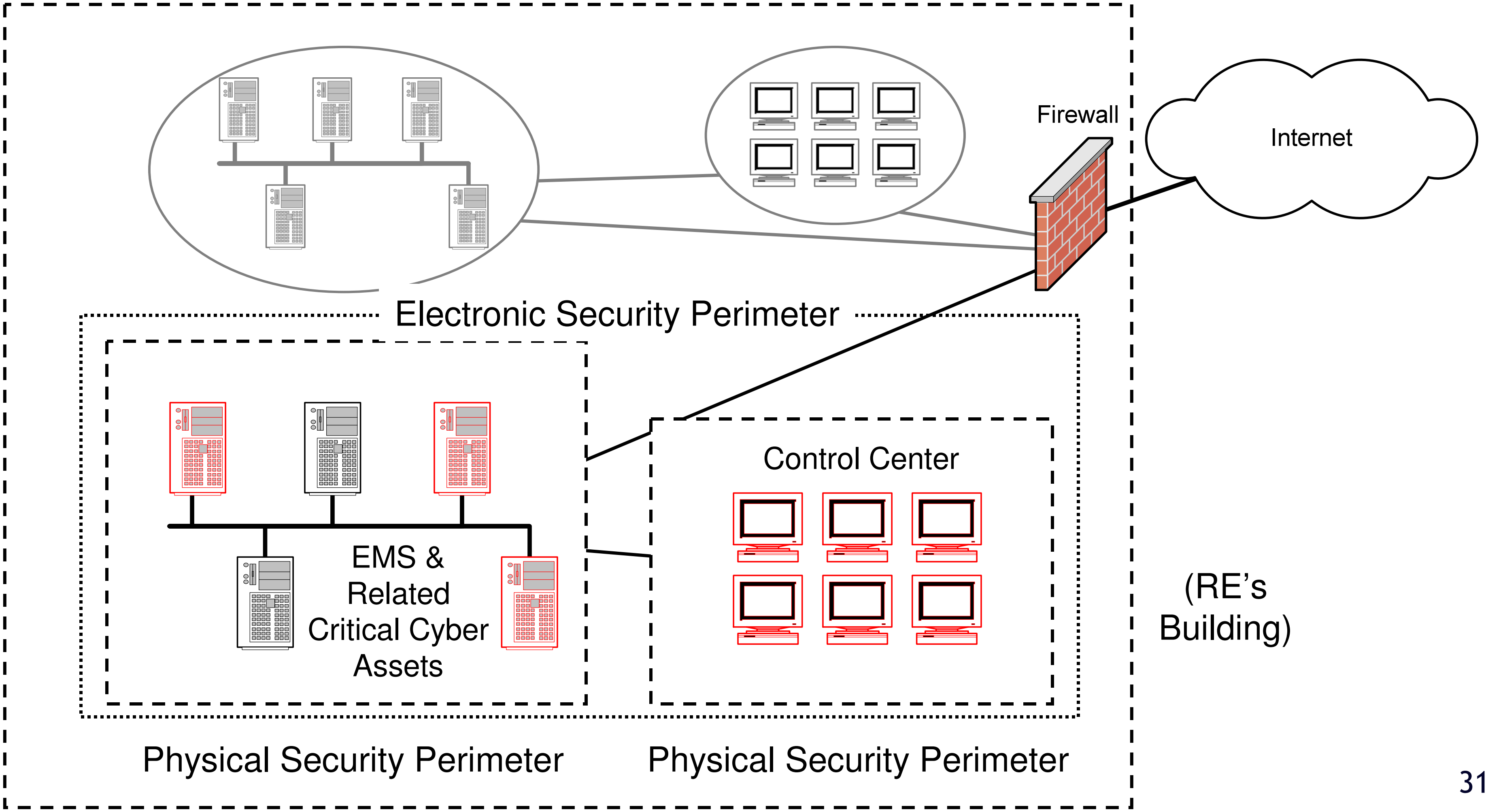
Control Center Example #1: Down-sizing an ESP and a PSP (2)


Firewall
Internet
Electronic Security Perimeter
EMS & Related Critical Cyber Assets
Control Center
(RE's Building)
Physical Security Perimeter
Physical Security Perimeter

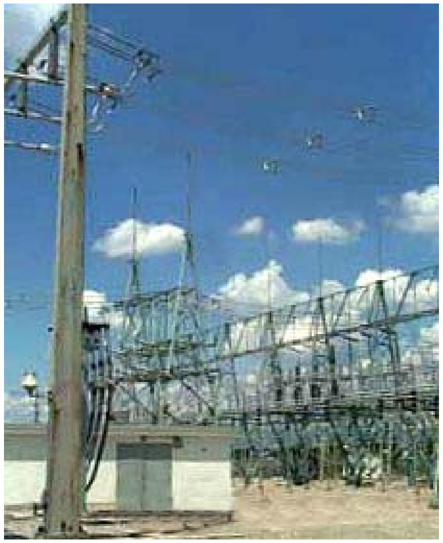
Control Center Example #2: Consolidating ESPs



Control Center Example #2: Consolidating ESPs (2)


Firewall
Internet
Electronic Security Perimeter
Control Center
EMS & Related Critical Cyber Assets
(RE's Building)
Physical Security Perimeter
Physical Security Perimeter

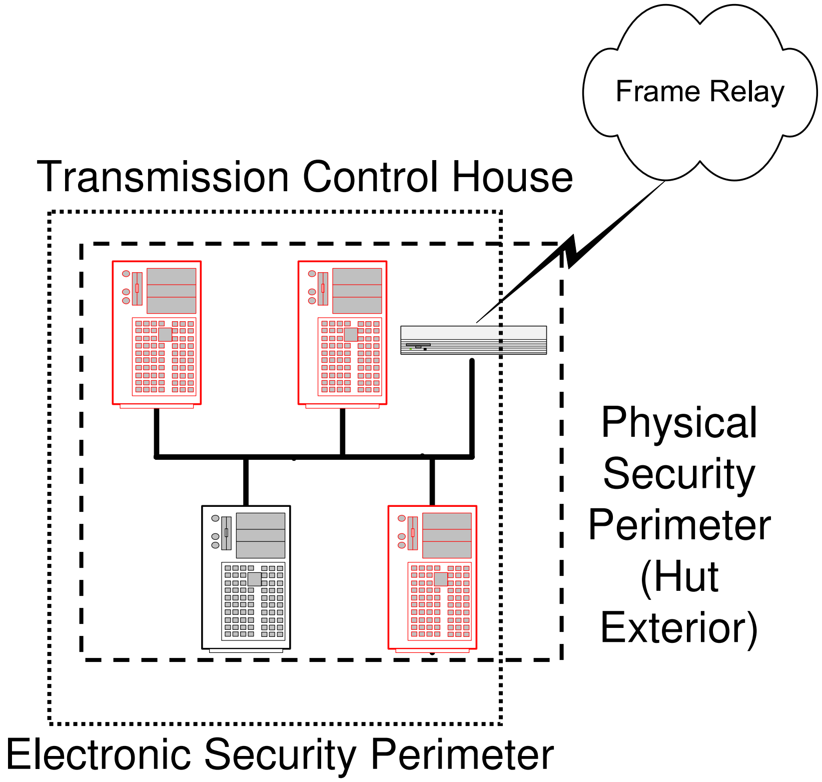
Substation (1/5)



- 345 kV Transmission Station Control House identified by the Responsible Entity as a Critical Asset
  - Associated Cyber Assets essential to its operation are Critical Cyber Assets
- Critical Cyber Assets were LAN connected to wide-area network via 2-port FRAD
  - Electronic and Physical Security Perimeters required

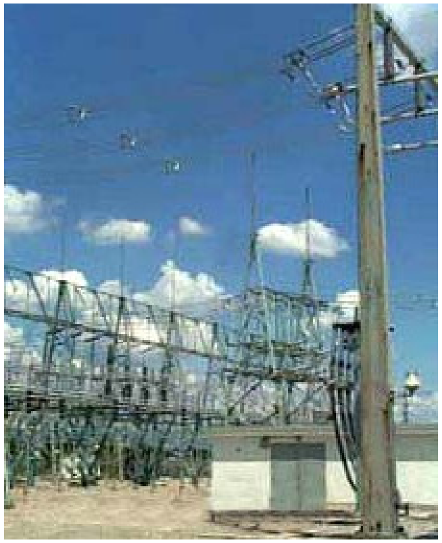
Substation (2/5)

- Presumptive Perimeter configuration:


Frame Relay
Transmission Control House
Physical Security Perimeter (Hut Exterior)
Electronic Security Perimeter

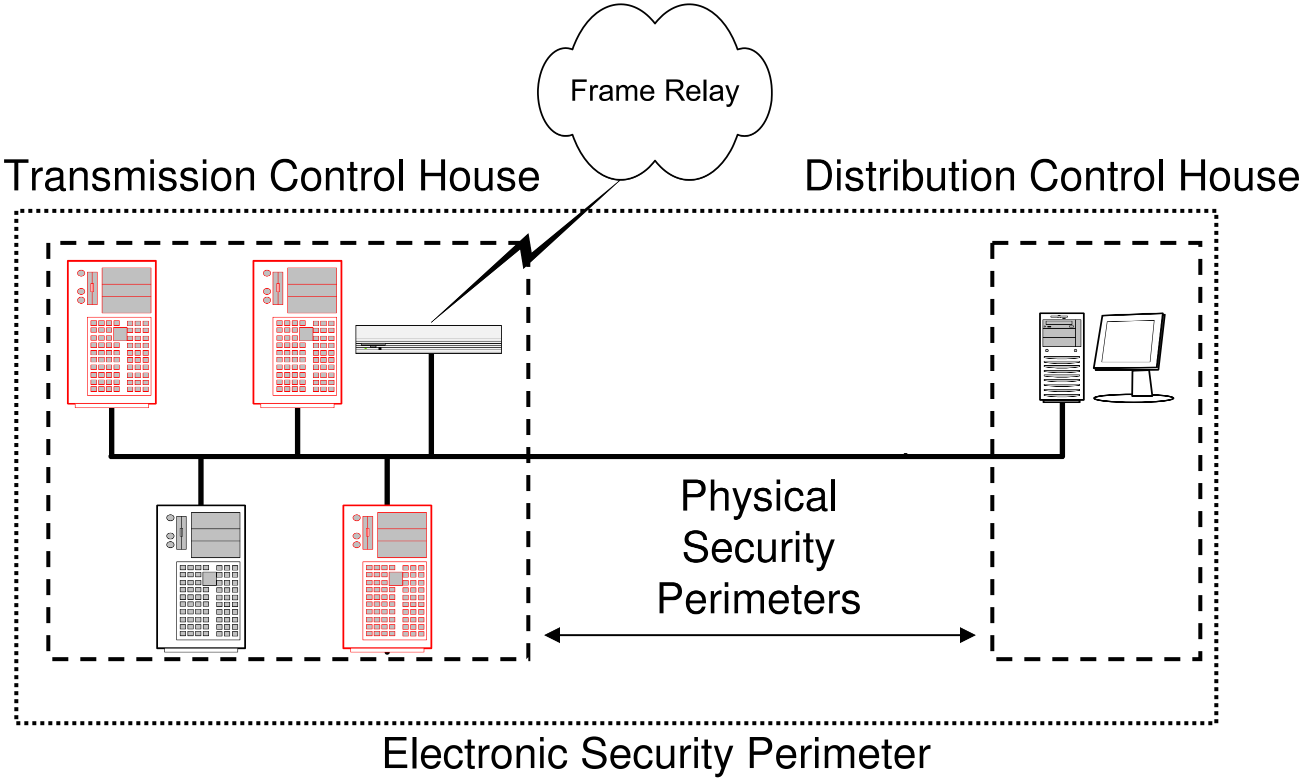
Substation (3/5)

- There was also a 34.5 kV Distribution Control House at this station
  - Transmission personnel escorting N&ST Consultants had never even been inside it
- It was discovered this hut contained a workstation *connected to the same LAN as the Transmission Control House*



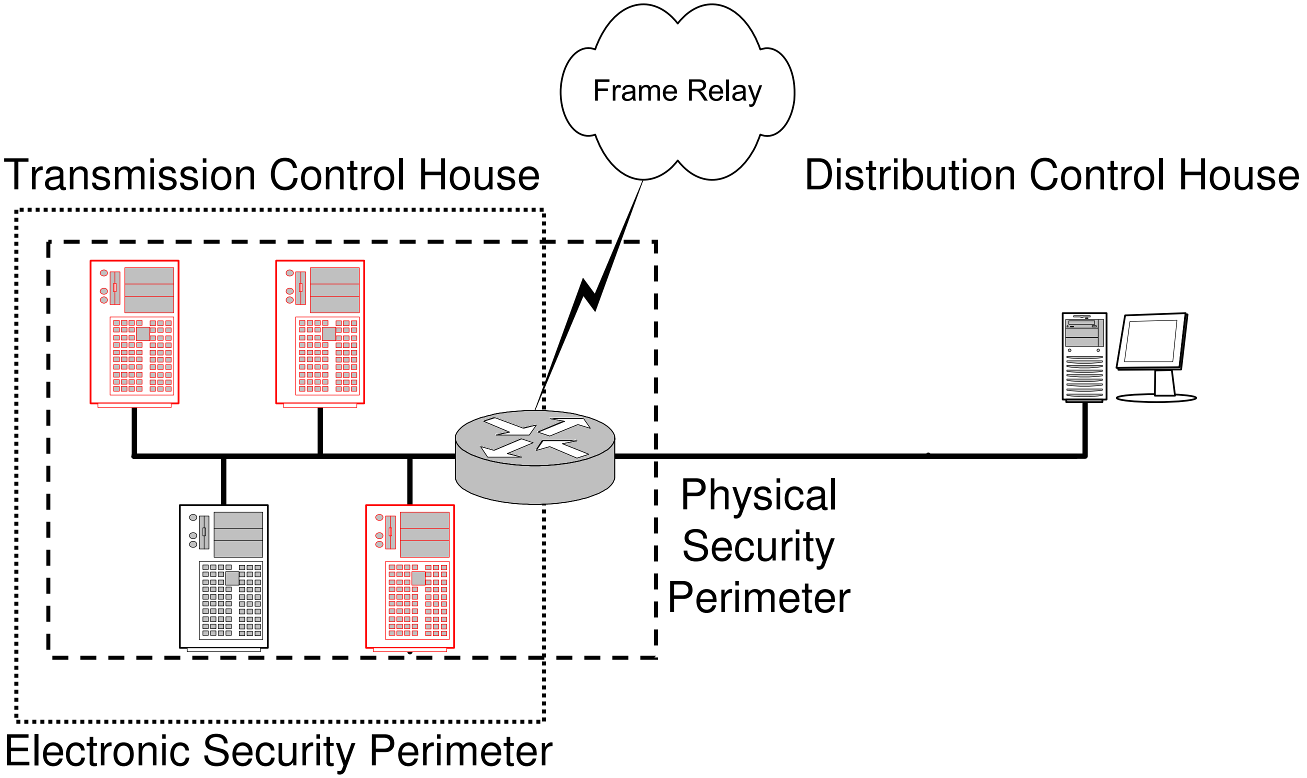
Substation (4/5)

- Absent any changes, would have to consider this type of Perimeter configuration:


Frame Relay
Transmission Control House
Distribution Control House
Physical Security Perimeters
Electronic Security Perimeter

Substation (5/5)

- Recommended alternative: Replace FRAD with filtering router for Layer 3 isolation between Transmission and Distribution Control systems


Frame Relay
Transmission Control House
Distribution Control House
Physical Security Perimeter
Electronic Security Perimeter

Agenda

- Introduction
- CIP-005 and 006 requirements
- General perimeter design considerations
- A perimeter design methodology
- Perimeter design examples
- CIP 005 and 006 required documents & records, ongoing compliance activities
- Wrap-up

CIP-005 Required Documents and Records (partial list)

- Electronic Security Perimeter Description, including:
  - All interconnected Cyber Assets within the ESP(s)
  - All ESP electronic access points
  - Cyber Assets deployed for access control and monitoring of access points
- Electronic Access Controls
  - Organizational processes, technical and procedural mechanisms
- Electronic Access Monitoring Processes
  - Unauthorized access detection & alerting or log review
  - Dial-up device monitoring (if required and technically feasible)

CIP-005 Required Documents and Records (2)

- Cyber Vulnerability Assessment Process
  - Verification of required ports & services
  - ESP access point discovery
  - Review of controls for default accounts, passwords, etc.
- Cyber Vulnerability Assessment Remediation Plan

- ESP Access Points Ports & Services Configurations
- Acceptable Use Banner Content (if required and technically feasible)
- Electronic Access Logs
- Cyber Vulnerability Assessment Results
- Vulnerability Remediation Status Reports (if req’d)

CIP-006 Required Documents and Records (partial list)

- Physical Security Plan
  - All Cyber Assets within an ESP must also reside within a Physical Security Perimeter
    - Or, develop and document alternative physical protection measures
  - Identify and protect Cyber Assets deployed for access control and monitoring of access points
- Physical Access Controls
  - *Must* employ one or more of methods specified in CIP-006 R2. (card key, special locks, etc.)
- Physical Access Monitoring Controls
  - *Must* employ one or more of methods specified in CIP-006 R3. (door & window alarms, human observers, etc.)

CIP-006 Required Documents and Records (2)

- Physical Access Logging Mechanisms
  - Must employ one or more of methods specified in CIP-006 R4. or an equivalent (card access system logs, CCTV tapes, etc.)

- Physical Access Logs
- Physical Security System Testing And Maintenance Records
- Access control, logging, & monitoring Outage Records

CIP-005 and 006 Ongoing Compliance Activities

Event	Required Action
Change to network or controls affecting ESP(s)	Update documentation within 90 days
Physical security system redesign or reconfiguration	Update physical security plan within 90 days

CIP-005 and 006 Ongoing Compliance Activities (2)

Schedule	Required Action
Every 90 days	Review/assess ESP access logs for attempted or actual unauthorized accesses (if required)
Annually	Perform Cyber Vulnerability Assessment
Annually	Review/update CIP-005 documents and procedures Review/update physical security plan
Every 3 Years	Perform testing and maintenance of all physical security mechanisms

Additional Information on Ongoing Compliance and Record Retention

- “NERC CIP CSS Compliance Reference”
  - Summary review of top-level CIP Standards, plus:
    - Information on typical organizational responsibilities for compliance
    - Document retention requirements
    - Timetable for ongoing compliance activities
  - Available at www.netsectech.com

Agenda

- Introduction
- CIP-005 and 006 requirements
- General perimeter design considerations
- A perimeter design methodology
- Perimeter design examples
- CIP 005 and 006 required documents & records, ongoing compliance activities
- Wrap-up

Contact Information

- Roger Fradenburgh, N&ST
  - Email: rfradenburgh@netsectech.com
  - Office: 978-505-1921

- Tom Kropp, EPRI EIS (Manager, CIP Programs)
  - Email: tkropp@epri.com
  - Office: 650-855-2751