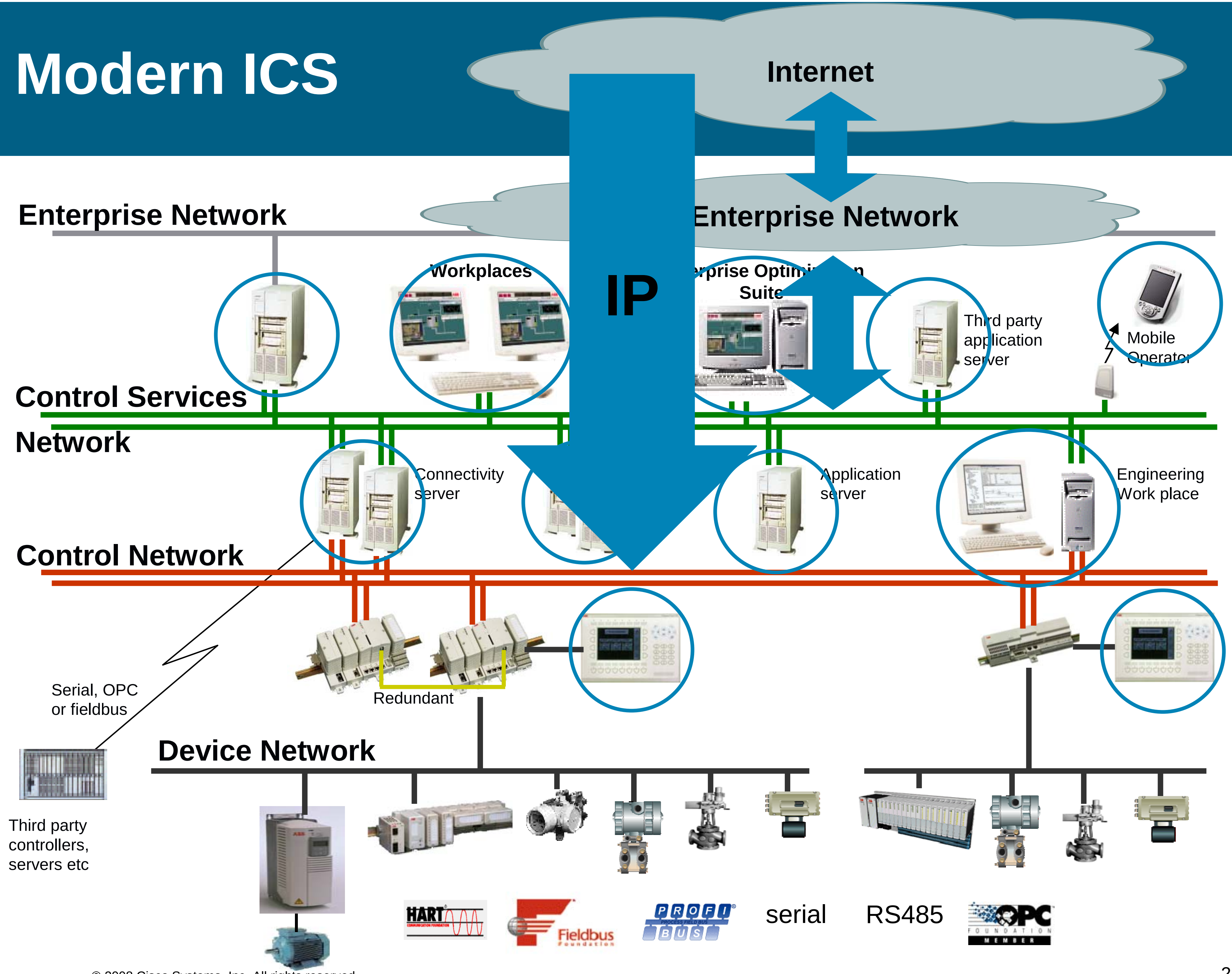
Secure Architecture for Critical Infrastructures

Michal Remper
systems engineer
mremper@cisco.com

Modern ICS


Internet
Enterprise Network
Enterprise Network
IP
Workplaces
Enterprise Optimization Suite
Third party application server
Mobile Operator
Control Services Network
Connectivity server
Application server
Engineering Work place
Control Network
Redundant
Serial, OPC or fieldbus
Third party controllers, servers etc
Device Network
HART
Fieldbus Foundation
PROFI BUS
serial
RS485
OPC FOUNDATION MEMBER

NERC-CIP

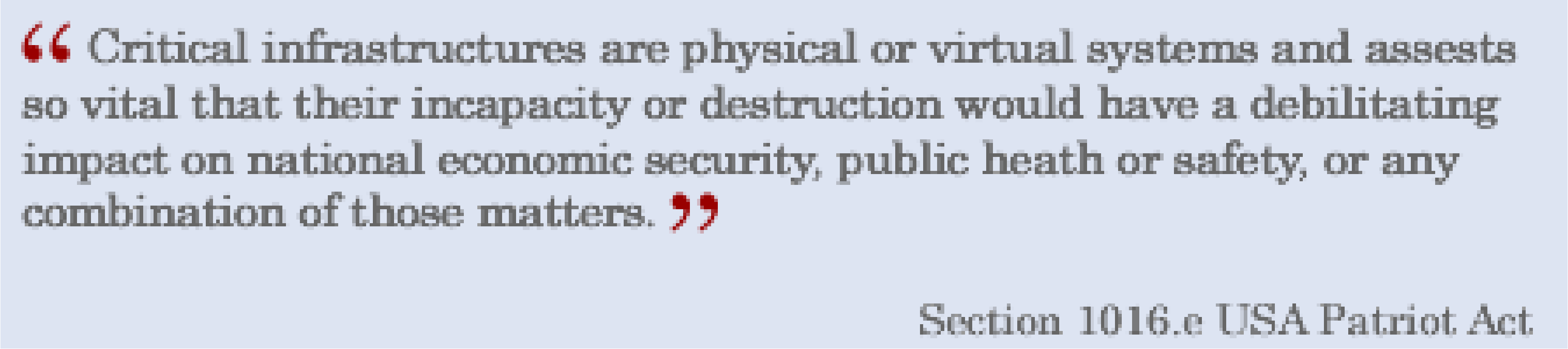
Critical Infrastructure Security

North American Regulations

NERC and other terms

- North American Electric Reliability Corporation (NERC)
- Federal Energy Regulatory Commission (FERC)
- National Institute of Standards and Technology (NIST)
- Critical Infrastructure Protection (CIP)

Critical Infrastructures Definition – USA Patriot Act



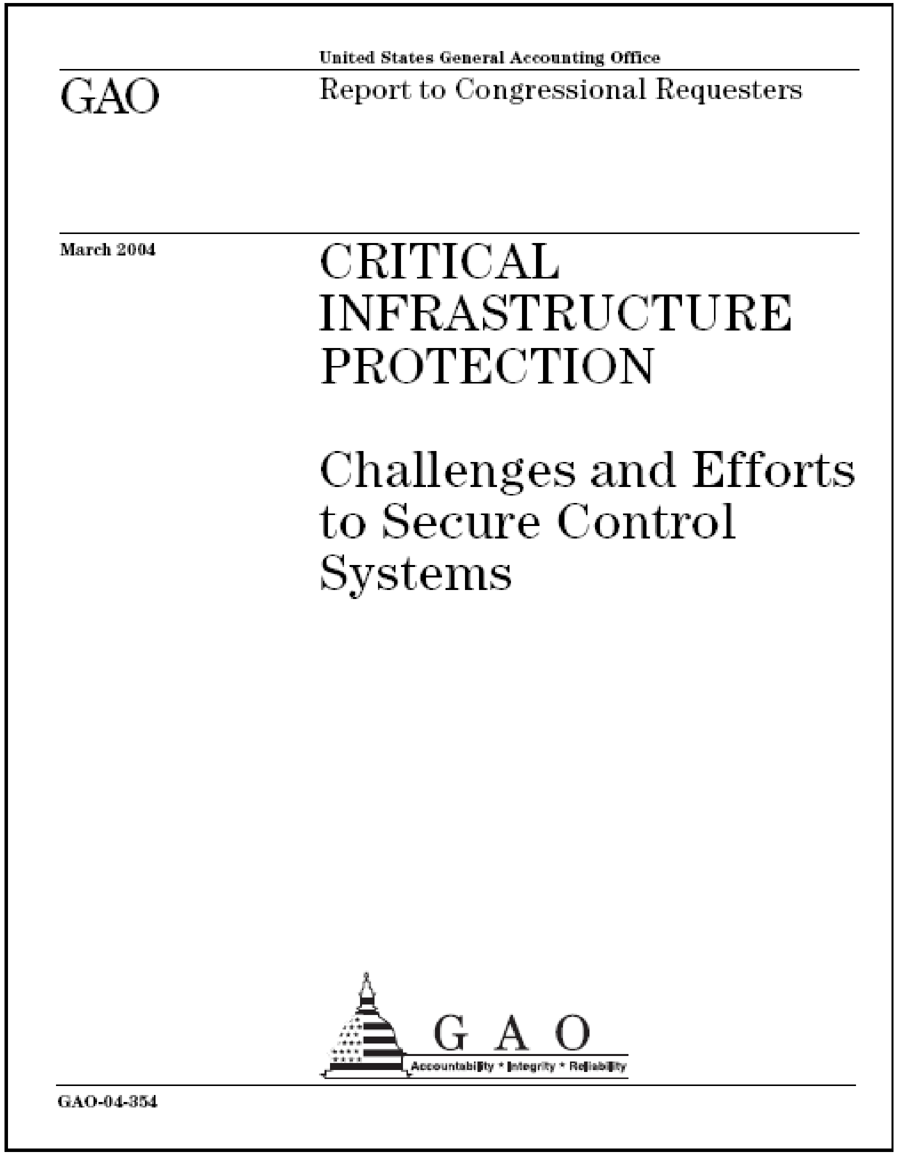
“Critical infrastructures are physical or virtual systems and assests so vital that their incapacity or destruction would have a debilitating impact on national economic security, public heath or safety, or any combination of those matters.”

Section 1016.e USA Patriot Act

Critical Infrastructure Protection

- Critical Infrastructure Protection or CIP is a national program to assure the security of vulnerable and interconnected infrastructures of the United States.
- In May 1998, President Bill Clinton issued Presidential directive PDD-63 on the subject of Critical Infrastructure Protection. This recognized certain parts of the national infrastructure as critical to the national and economic security of the United States and the well-being of its citizenry, and required steps to be taken to protect it.
- Updated on December 17, 2003 by President Bush through Homeland Security Presidential Directive HSPD-7 for Critical Infrastructure Identification, Prioritization, and Protection. The directive broadened the definition of infrastructure in accordance with the Patriot Act
- Outside the USA the term 'Critical Infrastructure Protection' refers to the doctrine or specific programs that secure and protect national critical infrastructure. The European Union directive EU COM(2006) 786 designates European critical infrastructure that, in case of fault, incident or attack, could impact both the country where it is hosted and at least one other European Member State.

Critical Infrastructure Protection-CIP



United States General Accounting Office

GAO

Report to Congressional Requesters

March 2004

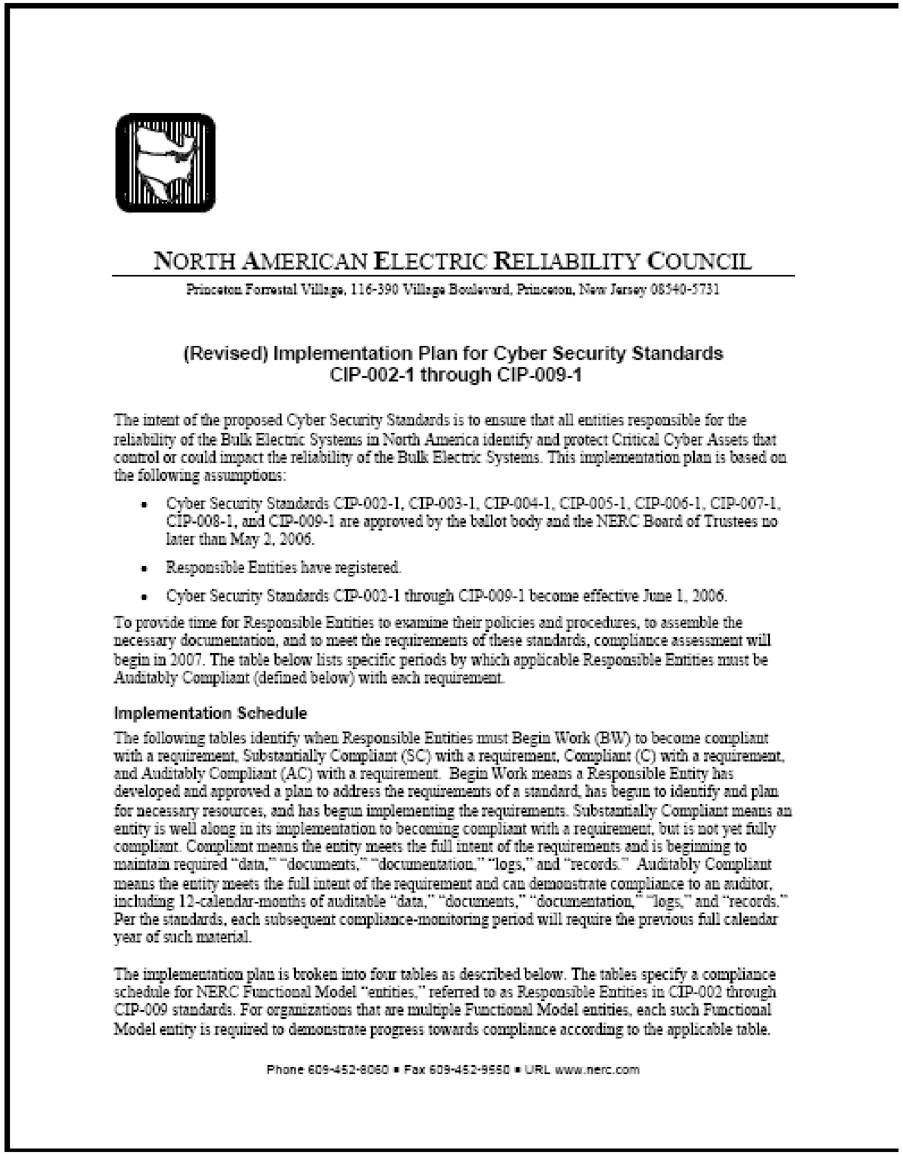
CRITICAL INFRASTRUCTURE PROTECTION

Challenges and Efforts to Secure Control Systems

GAO

Accountability * Integrity * Reliability

GAO-04-354



NORTH AMERICAN ELECTRIC RELIABILITY COUNCIL

Princeton Forrestal Village, 116-390 Village Boulevard, Princeton, New Jersey 08540-5731

(Revised) Implementation Plan for Cyber Security Standards
CIP-002-1 through CIP-009-1

The intent of the proposed Cyber Security Standards is to ensure that all entities responsible for the reliability of the Bulk Electric Systems in North America identify and protect Critical Cyber Assets that control or could impact the reliability of the Bulk Electric Systems. This implementation plan is based on the following assumptions:

- Cyber Security Standards CIP-002-1, CIP-003-1, CIP-004-1, CIP-005-1, CIP-006-1, CIP-007-1, CIP-008-1, and CIP-009-1 are approved by the ballot body and the NERC Board of Trustees no later than May 2, 2006.
- Responsible Entities have registered.
- Cyber Security Standards CIP-002-1 through CIP-009-1 become effective June 1, 2006.

To provide time for Responsible Entities to examine their policies and procedures, to assemble the necessary documentation, and to meet the requirements of these standards, compliance assessment will begin in 2007. The table below lists specific periods by which applicable Responsible Entities must be Auditably Compliant (defined below) with each requirement.

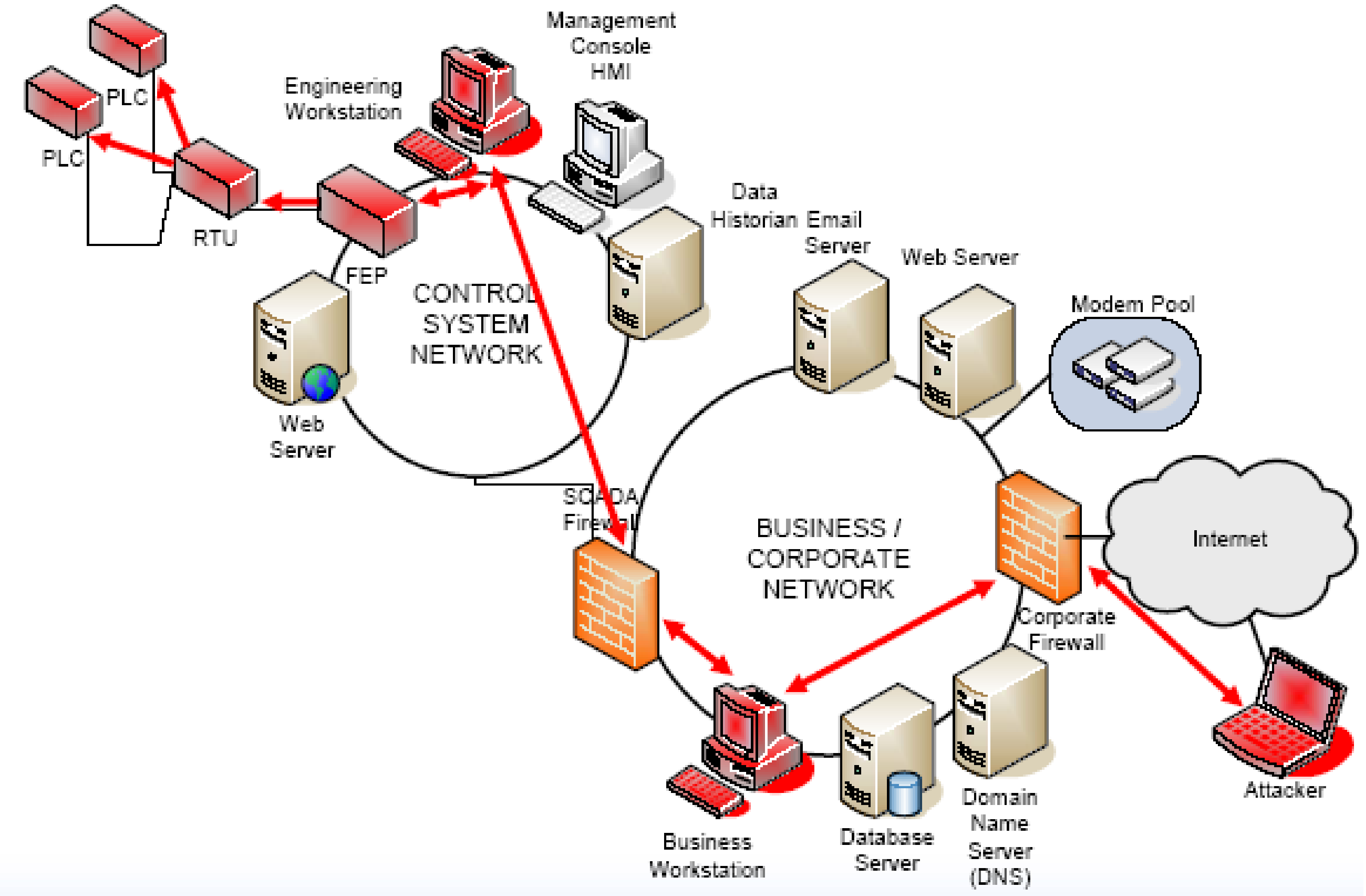
Implementation Schedule

The following tables identify when Responsible Entities must Begin Work (BW) to become compliant with a requirement, Substantially Compliant (SC) with a requirement, Compliant (C) with a requirement, and Auditably Compliant (AC) with a requirement. Begin Work means a Responsible Entity has developed and approved a plan to address the requirements of a standard, has begun to identify and plan for necessary resources, and has begun implementing the requirements. Substantially Compliant means an entity is well along in its implementation to becoming compliant with a requirement, but is not yet fully compliant. Compliant means the entity meets the full intent of the requirements and is beginning to maintain required "data," "documents," "documentation," "logs," and "records." Auditably Compliant means the entity meets the full intent of the requirement and can demonstrate compliance to an auditor, including 12-calendar-months of auditable "data," "documents," "documentation," "logs," and "records." Per the standards, each subsequent compliance-monitoring period will require the previous full calendar year of such material.

The implementation plan is broken into four tables as described below. The tables specify a compliance schedule for NERC Functional Model "entities," referred to as Responsible Entities in CIP-002 through CIP-009 standards. For organizations that are multiple Functional Model entities, each such Functional Model entity is required to demonstrate progress towards compliance according to the applicable table.

Phone 609-452-8060 ■ Fax 609-452-9550 ■ URL www.nerc.com

Why to Protect Critical Infrastructures ?



Nation’s Bulk Power Systems and NERC

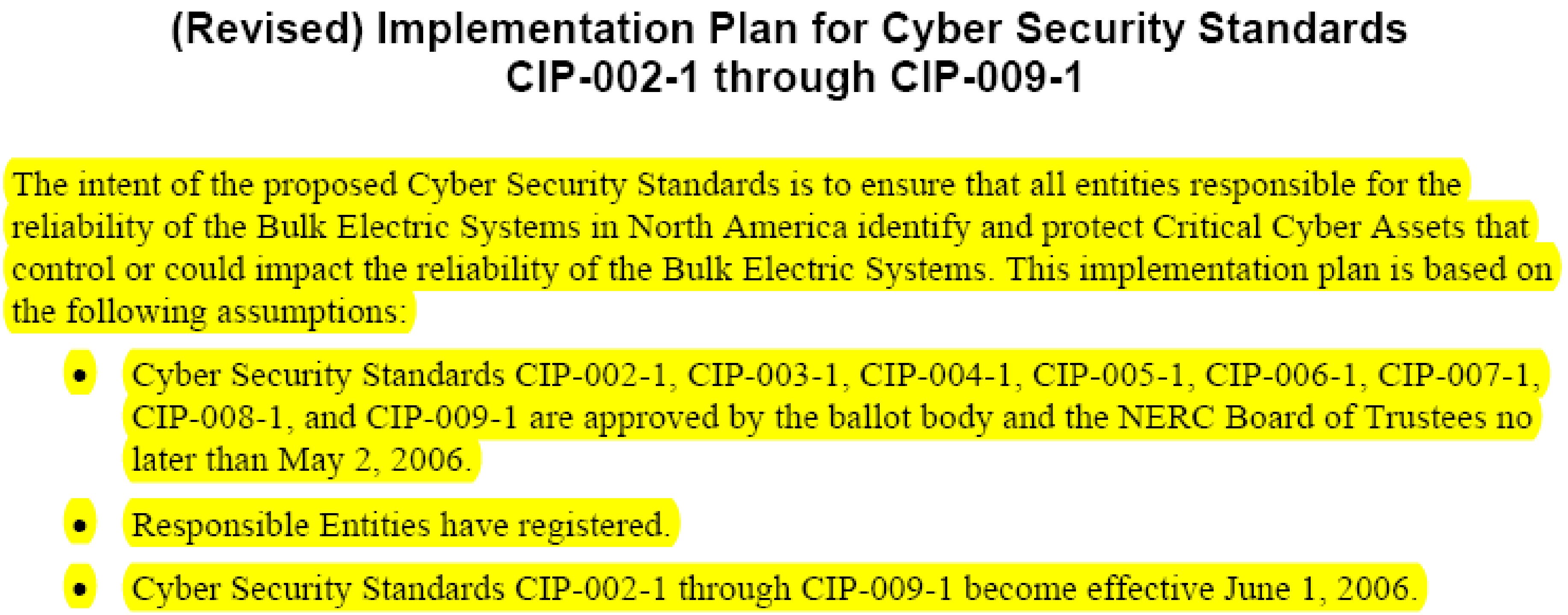
- NERC’s mission is to improve the reliability and security of the bulk power system in North America. To achieve that, NERC:

  1. Develops and enforces reliability standards
  2. Monitors the bulk power system
  3. Assesses future adequacy
  4. Audits owners, operators, and users for preparedness
  5. Educates and trains industry personnel.

- NERC is a self-regulatory organization that relies on the diverse and collective expertise of industry participants. As the Electric Reliability Organization, NERC is subject to audit by the U.S. Federal Energy Regulatory Commission (FERC) and governmental authorities in Canada (PSEPC).

CIP cont.

- The Federal Energy Regulatory Commission (FERC) on January 17th 2008 approved eight new mandatory critical infrastructure protection (CIP) reliability standards to protect the nation's bulk power system against potential disruptions from cyber security breaches. These reliability standards were developed by the North American Electric Reliability Corporation (NERC), which FERC has designated as the electric reliability organization (ERO).



(Revised) Implementation Plan for Cyber Security Standards CIP-002-1 through CIP-009-1

The intent of the proposed Cyber Security Standards is to ensure that all entities responsible for the reliability of the Bulk Electric Systems in North America identify and protect Critical Cyber Assets that control or could impact the reliability of the Bulk Electric Systems. This implementation plan is based on the following assumptions:

- Cyber Security Standards CIP-002-1, CIP-003-1, CIP-004-1, CIP-005-1, CIP-006-1, CIP-007-1, CIP-008-1, and CIP-009-1 are approved by the ballot body and the NERC Board of Trustees no later than May 2, 2006.
- Responsible Entities have registered.
- Cyber Security Standards CIP-002-1 through CIP-009-1 become effective June 1, 2006.

Compliance – as defined by NERC

- Meeting the requirements using the measures in each of the standards
- Compliance uses clear decision points
  - Yes or no
  - Done or not done
  - Seeks to know “what”, not “how”
- Not qualitative
- Formal audits, investigations, self-reporting, and spot checks
- Violations usually result in sanctions

Penalty Matrix*

	Violation Severity Level							
Violation Risk Factor	Lower		Moderate		High		Severe	
	Range Limits		Range Limits		Range Limits		Range Limits	
	Low	High	Low	High	Low	High	Low	High
Lower	$1,000	$3,000	$2,000	$7,500	$3,000	$15,000	$5,000	$25,000
Medium	$2,000	$30,000	$4,000	$100,000	$6,000	$200,000	$10,000	$335,000
High	$4,000	$125,000	$8,000	$300,000	$12,000	$625,000	$20,000	$1,000,000

FERC statutory limit: $1 million per day

Other limits may apply in Canada

***This matrix is still undergoing revision**

Brief History of CIP Standards

- CIP (Critical Infrastructure Protection)1200 approved in 2003 as Urgent Action item
- Applied to:
  - Balancing Authorities
  - Reliability Coordinators
  - Transmission Operators
- Permanent cyber security standards under development since then
- CIP 002-009 approved in May 2006
- Submitted to FERC on August 30, 2006

TOP 10 VULNERABILITIES OF CONTROL SYSTEMS AND THEIR ASSOCIATED MITIGATIONS – March 2007

Released by: NERC Control Systems Security Working Group

1. Inadequate policies, procedures and culture that govern control system security
2. Inadequately designed control system networks that lack sufficient defense-in-depth mechanisms
3. Remote access to the control system without appropriate access control
4. System administration mechanisms and software used in control systems are not adequately scrutinized or maintained
5. Use of inadequately secured WiFi wireless communication for control.
6. Use of a non-dedicated communications channel for command and control and/or inappropriate use of control system network bandwidth for non-control purposes.
7. Insufficient application of tools to detect and report on anomalous or inappropriate activity.
8. Unauthorized or inappropriate applications or devices on control system networks
9. Control systems command and control data not authenticated
10. Inadequately managed, designed, or implemented critical support infrastructure

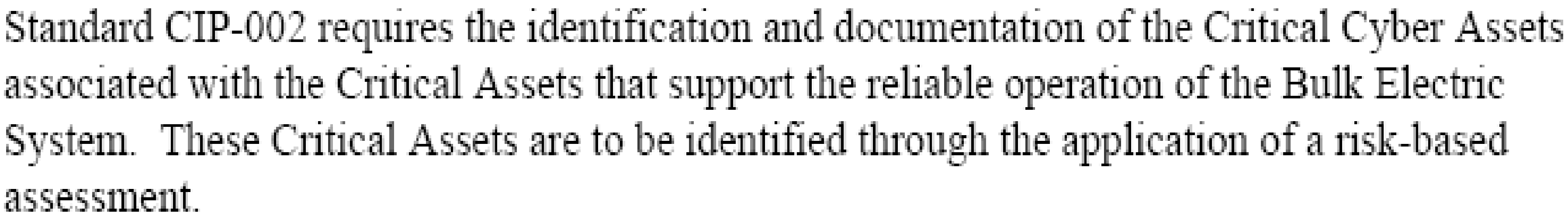
NERC Cyber Security Standards and Requirements

NERC CIP CYBER SECURITY STANDARDS
Eight Standards / 41 Requirements

CIP-002	*CIP-003*	*CIP-004*	*CIP-005*	*CIP-006*	*CIP-007*	*CIP-008*	*CIP-009*
CRITICAL CYBER ASSETS	**SECURITY MANAGEMENT CONTROLS**	**PERSONNEL AND TRAINING**	**ELECTRONIC SECURITY**	**PHYSICAL SECURITY**	**SYSTEMS SECURITY MANAGEMENT**	**INCIDENT REPORTING & RESPONSE PLANNING**	**RECOVERY PLANS FOR CCA**
1. CRITICAL ASSETS	1. CYBER SECURITY POLICY	1. AWARENESS	1. ELECTRONIC SECURITY PERIMETER	1. PLAN	1. TEST PROCEDURES	1. CYBER SECURITY INCIDENT RESPONSE PLAN	1. RECOVERY PLANS
2. CRITICAL CYBER ASSETS	2. LEADERSHIP	2. TRAINING	2. ELECTRONIC ACCESS CONTROLS	2. PHYSICAL ACCESS CONTROLS	2. PORTS & SERVICES	2. DOCUMENTATION	2. EXERCISES
3. ANNUAL REVIEW	3. EXCEPTIONS	3. PERSONNEL RISK ASSESSMENT	3. MONITORING ELECTRONIC ACCESS	3. MONITORING PHYSICAL ACCESS	3. SECURITY PATCH MANAGEMENT		3. CHANGE CONTROL
4. ANNUAL APPROVAL	4. INFORMATION PROTECTION	4. ACCESS	4. CYBER VULNERABILITY ASSESSMENT	4. LOGGING PHYSICAL ACCESS	4. MALICIOUS SOFTWARE PREVENTION		4. BACKUP & RESTORE
	5. ACCESS CONTROL		5. DOCUMENTATION	5. ACCESS LOG RETENTION	5. ACCOUNT MANAGEMENT		5. TESTING BACKUP MEDIA
	6. CHANGE CONTROL			6. MAINTENANCE & TESTING	6. SECURITY STATUS MONITORING		
					7. DISPOSAL OR REDEPLOYMENT		
					8. CYBER VULNERABILITY ASSESSMENT		
					9. DOCUMENTATION		

CIP-002 Critical Cyber Asset Identification

- Critical Asset identification
- Critical Cyber Asset identification
- Annual Review and Approval



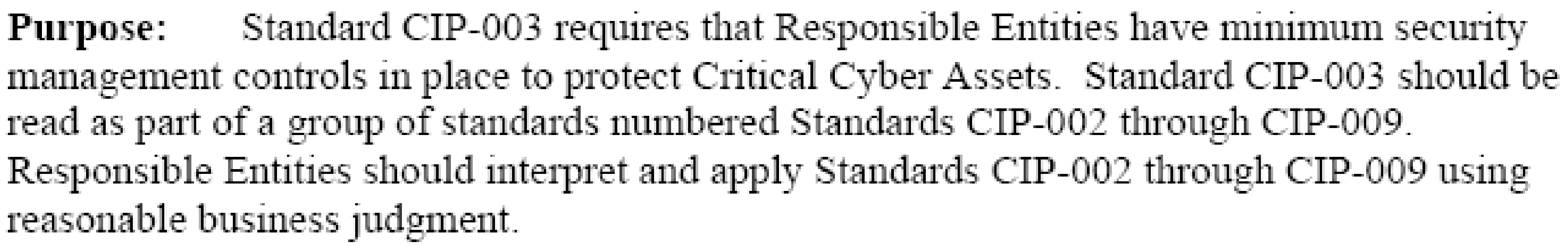
Standard CIP-002 requires the identification and documentation of the Critical Cyber Assets associated with the Critical Assets that support the reliable operation of the Bulk Electric System. These Critical Assets are to be identified through the application of a risk-based assessment.

Related Cisco Products/Services

- Cisco Campus Manager with Cisco LAN Management Solution (Cisco LMS), Cisco View
- Cisco Monitoring, Analysis and Reporting System (Cisco MARS)
- Cisco Network Compliance Manager
- Cisco NAC Profiler

CIP-003 Security Management Controls

- Cyber Security Policy (documentation and implementation)
- Leadership
- Exceptions
- Information Protection
- Access Control
- Change Control

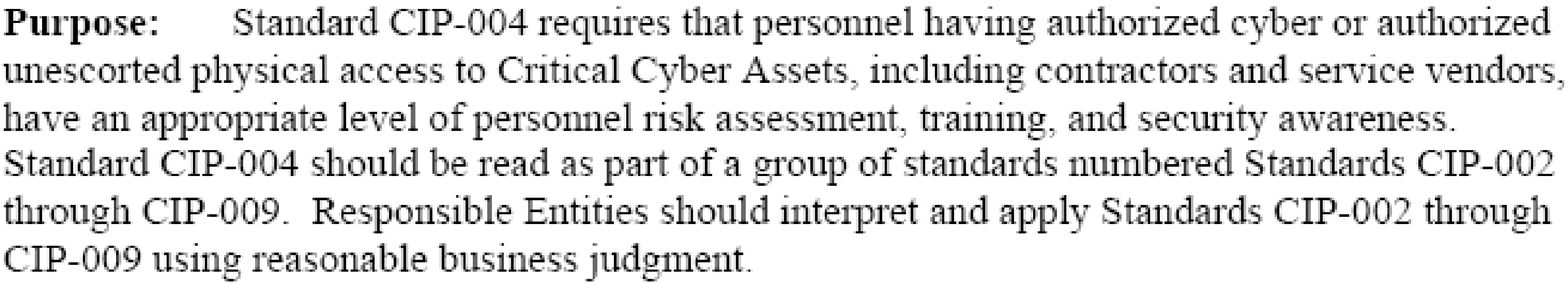


Purpose: Standard CIP-003 requires that Responsible Entities have minimum security management controls in place to protect Critical Cyber Assets. Standard CIP-003 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

- Related Cisco Products/Services
- Cisco Network Admission Control (Cisco NAC)
- User authentication through Cisco ACS (TACACS, RADIUS, LDAP, Dynamic Access Control)
- Cisco MARS

CIP-004 Personnel and Training

- **Awareness**
- **Training**
- **Personnel Assessment**
- **Access**

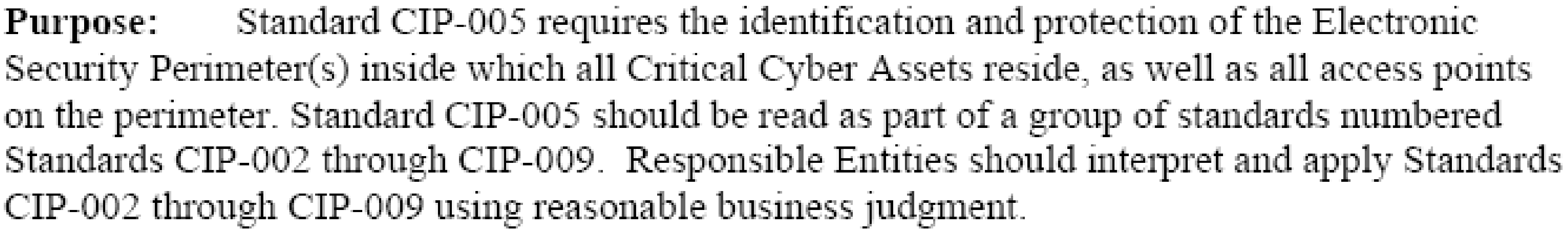


Purpose: Standard CIP-004 requires that personnel having authorized cyber or authorized unescorted physical access to Critical Cyber Assets, including contractors and service vendors, have an appropriate level of personnel risk assessment, training, and security awareness. Standard CIP-004 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

- **Related Cisco Products/Services**
- **Cisco Focused Technical Support (FTS)**
- **Network Optimization Support (NOS)**

CIP-005 Electronic Security Perimeter*

- **Electronic Security Perimeter**
- **Electronic Access Controls**
- **Monitoring Electronic Access**
- **Cyber Vulnerability Assessment**
- **Documentation**



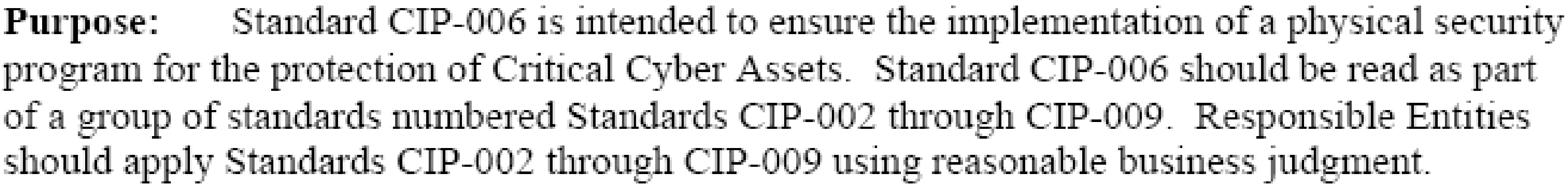
Purpose: Standard CIP-005 requires the identification and protection of the Electronic Security Perimeter(s) inside which all Critical Cyber Assets reside, as well as all access points on the perimeter. Standard CIP-005 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

Related Cisco Products/Services

- **Cisco Adaptive Security Appliances (Cisco ASA: Firewall, IPS, VPN modules)**
- **Integrated Security: IOS FW/IPS/VPN, Private VLANs**
- **Cisco NAC for wireless**
- **Cisco Wireless LAN Controller**

CIP-006 Physical Security

- **Physical Security Plan**
- **Physical Access Controls**
- **Monitoring Physical Access**
- **Logging Physical Work**
- **Access Log Retention**
- **Maintenance and Testing**



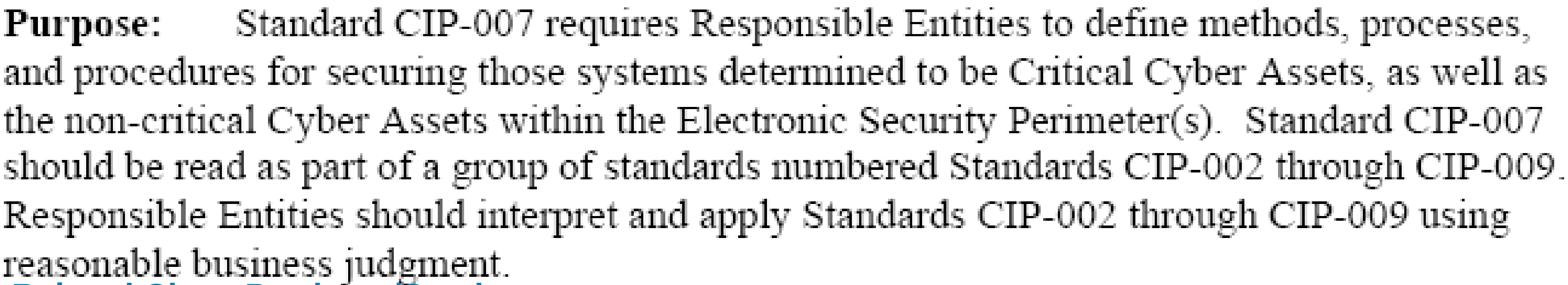
Purpose: Standard CIP-006 is intended to ensure the implementation of a physical security program for the protection of Critical Cyber Assets. Standard CIP-006 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.

Related Cisco Products/Services

- **Cisco IP Cameras**
- **Cisco IP Gateway Encoders**
- **Cisco Stream manager**
- **Hardened enclosure**
- **Physical Cable locks**
- **Cisco MARS**

CIP-007 System Security Management

- Test Procedures
- Maintenance and Testing
- Ports and Services
- Security Patch Management
- Malicious Software Prevention
- Account Management
- Security Status Monitoring
- Disposal or Re-deployment
- Cyber Vulnerability Assessment
- Documentation



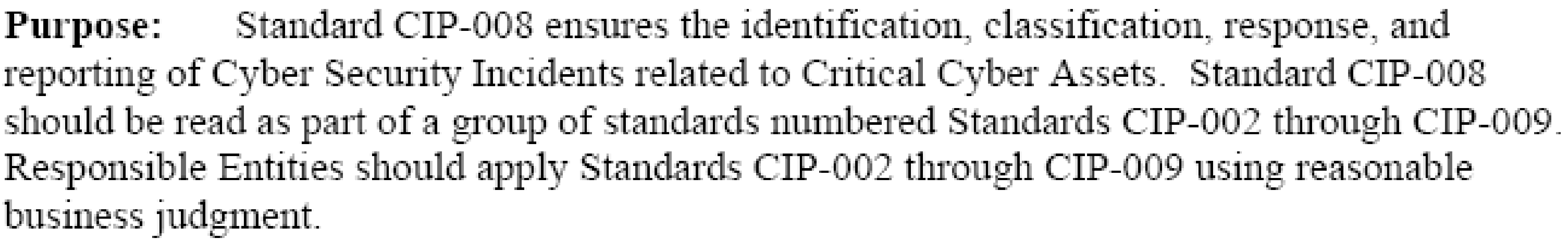
Purpose: Standard CIP-007 requires Responsible Entities to define methods, processes, and procedures for securing those systems determined to be Critical Cyber Assets, as well as the non-critical Cyber Assets within the Electronic Security Perimeter(s). Standard CIP-007 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should interpret and apply Standards CIP-002 through CIP-009 using reasonable business judgment.

Related Cisco Products/Services

- Cisco Security Agent (CSA)
- Cisco ACS (secure system administration, AAA)
- Cisco IPS
- Cisco Configuration Assurance System (CAS
- Cisco MARS, Cisco NCM, Syslog
- Cisco NAC and Port Security

CIP-008 Incident Reporting and Response

- **Cyber Security**
- **Incident Response Plan**
- **Documentation**



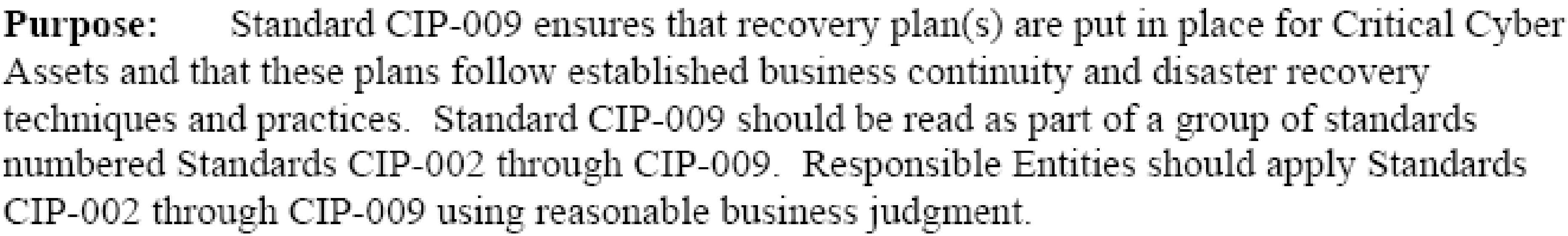
Purpose: Standard CIP-008 ensures the identification, classification, response, and reporting of Cyber Security Incidents related to Critical Cyber Assets. Standard CIP-008 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.

Related Cisco Products/Services

- **Cisco Security IntelliShield**
- **Cisco MARS**
- **Cisco NCM, Cisco AS, MARS**

CIP-009 Recovery Plans for Critical Assets

- **Recovery Plans**
- **Exercises**
- **Change Control**
- **Backup and Restore**
- **Testing Backup media**



Purpose: Standard CIP-009 ensures that recovery plan(s) are put in place for Critical Cyber Assets and that these plans follow established business continuity and disaster recovery techniques and practices. Standard CIP-009 should be read as part of a group of standards numbered Standards CIP-002 through CIP-009. Responsible Entities should apply Standards CIP-002 through CIP-009 using reasonable business judgment.

Related Cisco Products/Services

- **Cisco disaster recovery manager**
- **CiscoWorks Resource Manager**
- **Cisco disaster recovery best practices**
- **Cisco SAN products for disaster recovery and business continuity**

Power Grid Evolution

Power utility trends

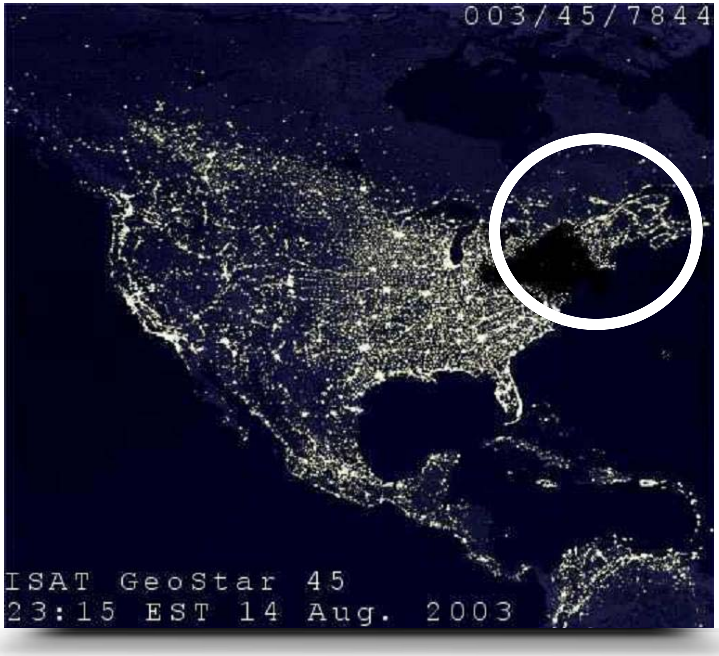
Power Utilities: Key Trends

- **Ethernet is expanding into the grid**
  - Billions are being allocated to update power grids across the globe
  - Ethernet is becoming the standard for substation and grid communications
  - Demand for ruggedized Ethernet switches and routers is surging
  - "Smart grid" technologies that are Ethernet enabled are being deployed
  - The power grid is being brought into the 21st century
- **Smart grid technologies are surging**
  - Substation automation and integration, smart meters, home area networks, smart homes, smart home controllers, renewable energy resources
  - Every upgrade brings demand for Ethernet communications
  - Nearly every utility in the world is considering one or all of these initiatives
- **Regulations are coming**
  - NERC-CIP – critical infrastructure mandate in North America that is driving networking in the grid ($1m/day fines if not compliant by June '09)
  - Similar regulations are on the drawing board for Europe and China

Smart Grid / Substation Automation Drivers

- Mass infrastructure build out / upgrade
  - Demand is outpacing supply
  - Infrastructure is outdated
  - Large scale and costly blackouts are becoming frequent
  - Reactive vs. proactive systems
  - Government regulations (NERC-CIP)
    - North American regulations
    - $1m / day minimum penalty for non-compliance
    - Audits start June 2009
    - Similar regulations coming world wide

- Influx of technology
  - Electric Power Research Institute (EPRI) estimates $100b to upgrade power grid infrastructure from 2003-2013
  - Distributech estimates were at $900b from $2008-$2018



Smart Energy Alliance

CISCO
ORACLE
Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING
hp
invent
intel
IBM

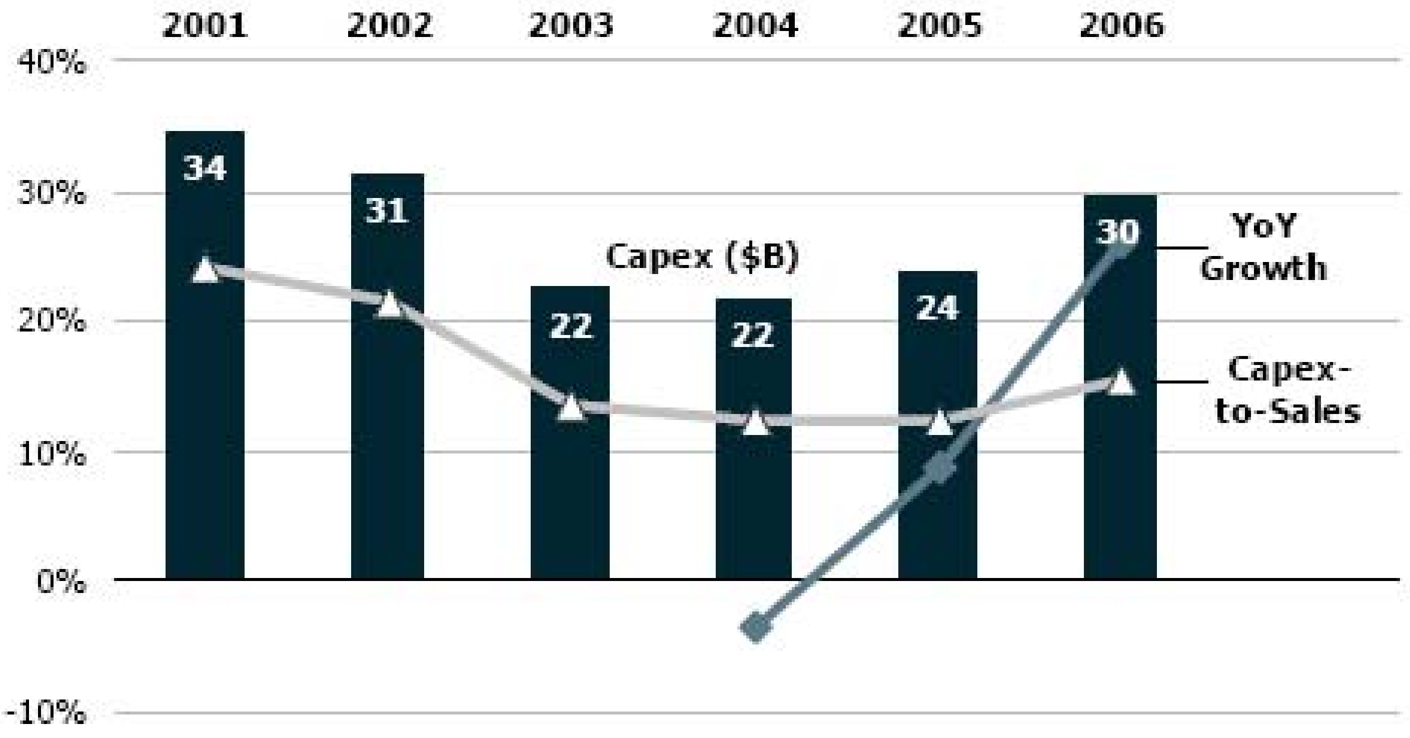
Electric Utility Vertical (SmartGrid)

- **"$800 - $900 billion will be invested in next 15yrs"**
  - – Former Secretary of Energy
  - – CEO of PNM Resources (Large US utility)
- Ave. Home – increase 33% size & 32% demand
- US usage – twice as fast as committed resources
- Peak demand – 18% increase over 10 yrs
- Many states – trajectory to fall below target capacity
- Regulation for renewable energy is increasing
- India & China – each projected to grow as big as US & Europe combined

CapEx Trend in US Utilities

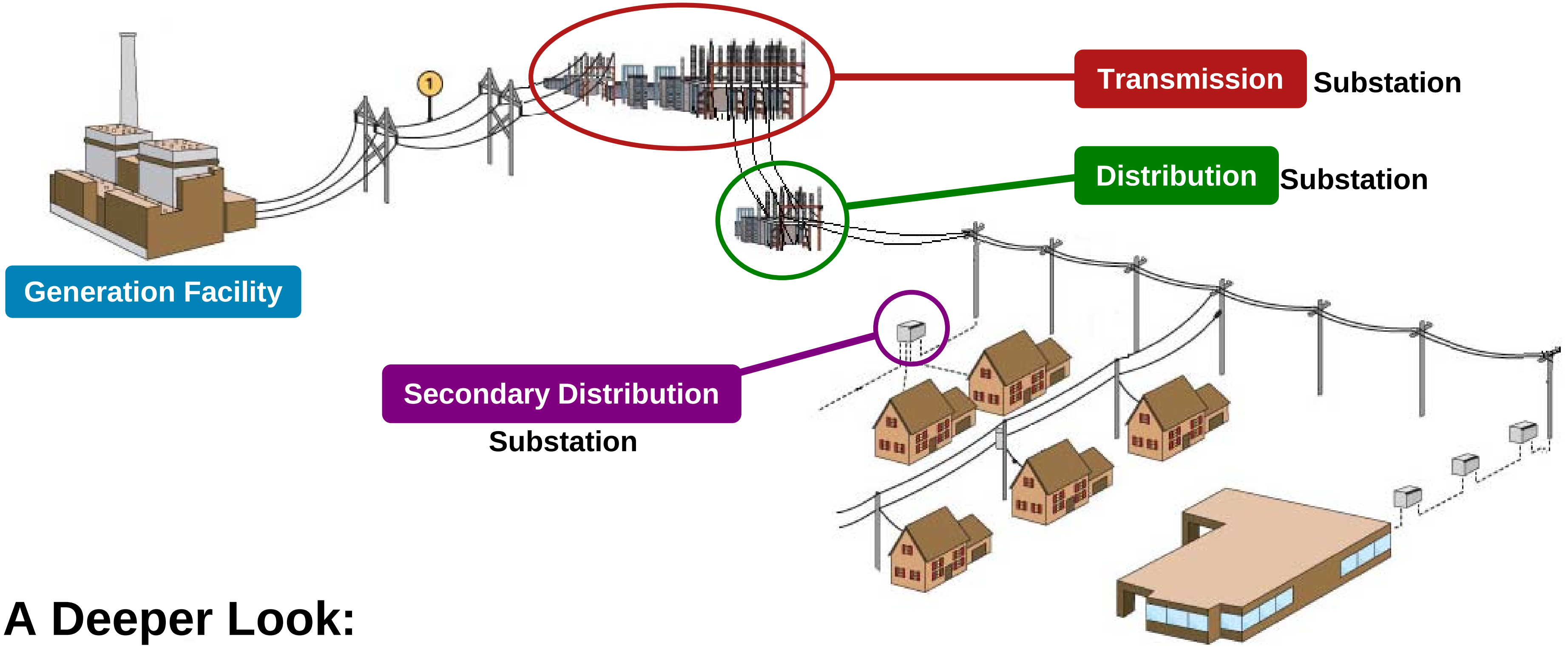
Genuity

Exhibit 3: U.S. power utility industry capex trends, 2001-2005



Source: Genuity Capital Markets, Capital IQ

Traditional Electric Utility Landscape



A Deeper Look:

- Transmission & Distribution Subs
(High to medium voltage or core substations)
  - 275,000 core substations
  - 5-7 IE switches per sub, 1 industrial router per sub
- Secondary Distribution Subs
(Low voltage or secondary subs)
  - Estimated at 100x T&D subs (27.5 million world wide)
  - 1 IE switch per sub / 1 industrial router per sub

In the US

- Primary Substation > 69kV
- Secondary Substations < 69kV

Core Substation Dynamics (High & Medium Voltage)

Core

Transmission Distribution Subs

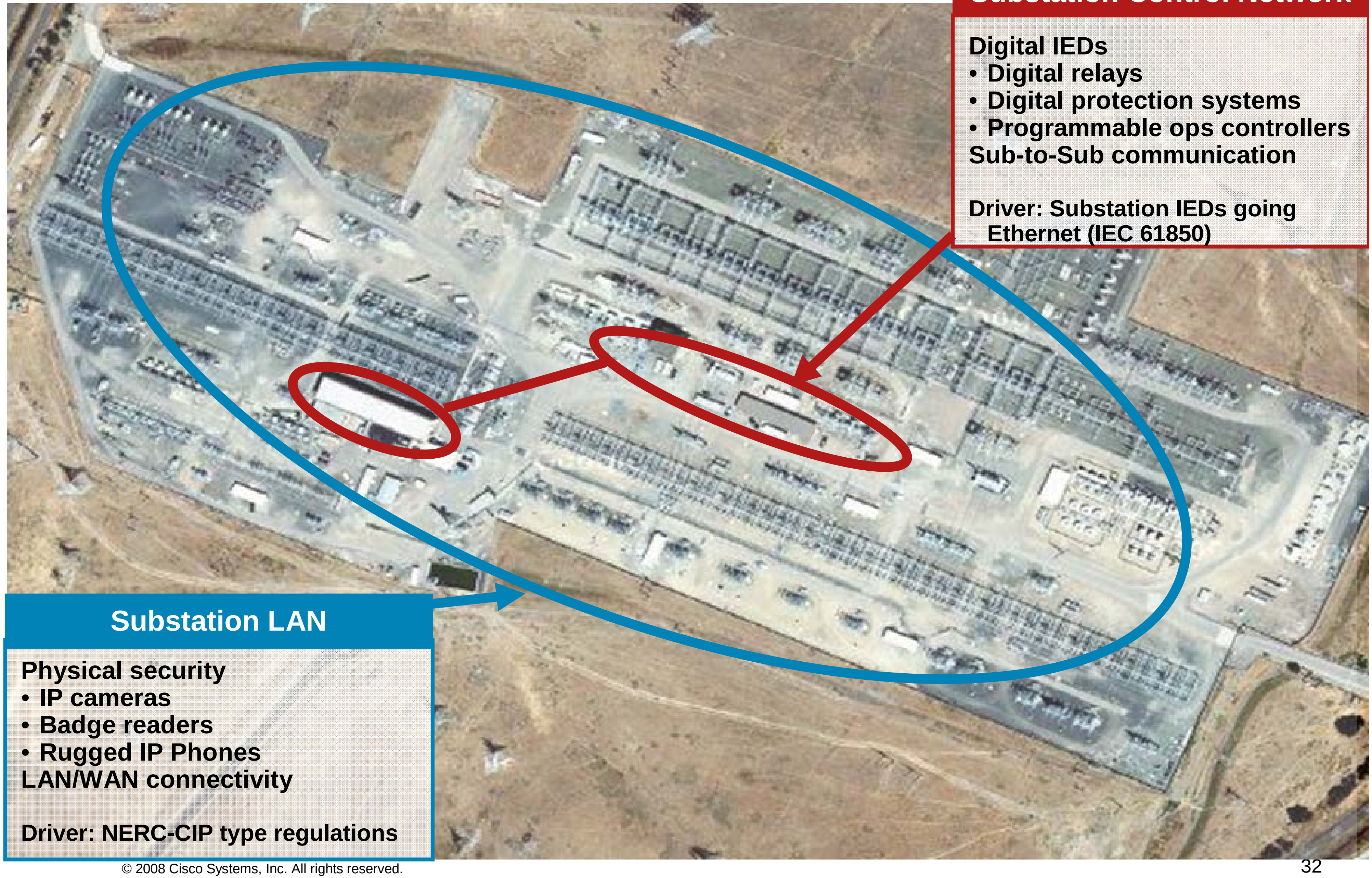
- High to medium voltage substations
- Above ground substation control houses
- 19 inch rack mounted components
- Extended power requirements
- Some environmentally controlled most are not
- All require “substation compliance” equipment (IEEE 1613 & IEC 61850)

Secondary Substation Dynamics (Low Voltage)

Secondary Distribution Subs

- Low voltage substations
- Small cabinets
- Typically underground in Europe
- Typically above ground in North America
- Space is limited
- Din rack mount or wall mount
- Extended power options
- Legacy connections
- Long distance connections
- All require “substation compliance” equipment (IEEE 1613 & IEC 61850)

Ethernet in the Core Substation (High & Medium Voltage subs)



Substation Control Network

Digital IEDs

- Digital relays
- Digital protection systems
- Programmable ops controllers

Sub-to-Sub communication

Driver: Substation IEDs going Ethernet (IEC 61850)

Substation LAN

Physical security

- IP cameras
- Badge readers
- Rugged IP Phones

LAN/WAN connectivity

Driver: NERC-CIP type regulations

Substation LAN (Cisco's physical security solutions)

Substation LAN

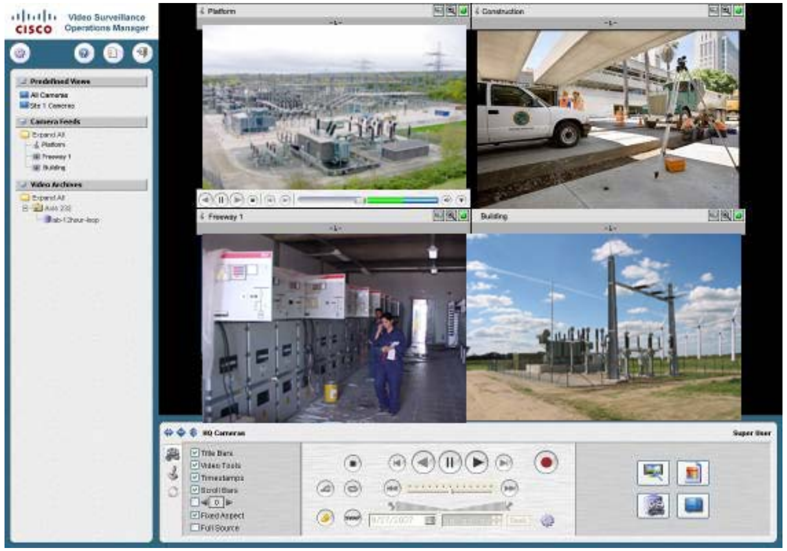
Physical security
• IP cameras
• Badge readers
• Rugged IP Phones
LAN/WAN connectivity

Driver: NERC-CIP type regulations

- **Network-based video**
  - Surveillance software, cameras, appliances, and routers
  - Single and multi site surveillance
  - Live and recorded video from any place at any time
  - For wired, wireless and mobile deployments

- **Network-based physical access control**
  - Connects existing door hardware (badge readers, locks) to the network
  - Enables centralized monitoring, control and response

- **Network-based incident communications**
  - Connects radios, cell phones and IP phones
  - Enables immediate response to events



Substation Control Network (IED communication)

- **Intelligent Electronic Devices (IED)**
  - Devices in the substation that have made the transition from electromechanical to digital
  - Ethernet enabled and driving industrial networking

Substation Control Network

Digital IEDs
- Digital relays
- Digital protection systems
- Programmable ops controllers

Sub-to-Sub communication

Driver: Substation IEDs going Ethernet (IEC 61850)

IEDs from Schweitzer Engineering Laboratories, Inc

Digital Protection System

SEL

Feeder Protection Relay

Digital Relay

Programmable Operations Controller

Rugged Computer

Other IED Vendors

GE

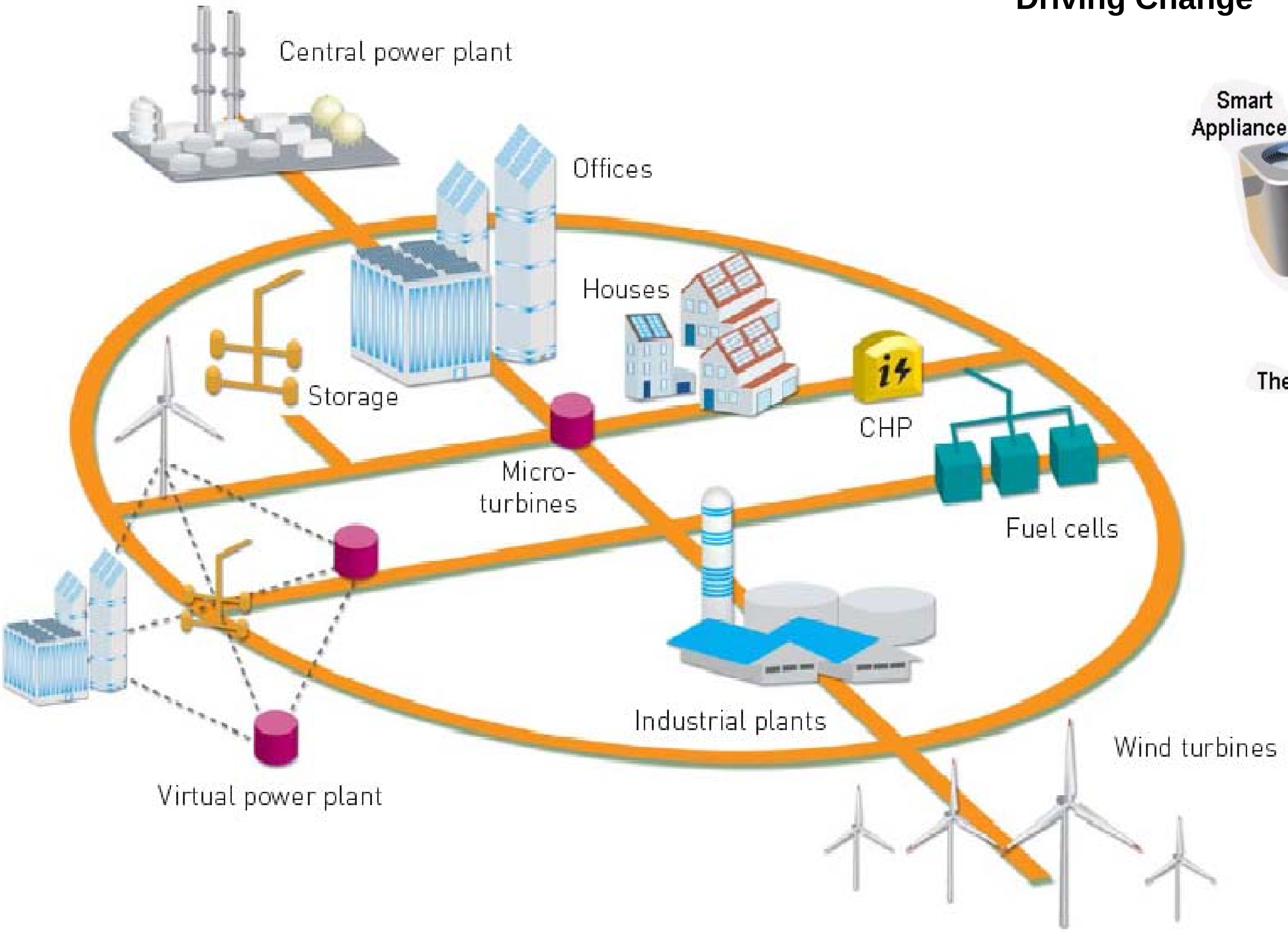
ABB

SIEMENS

AREVA

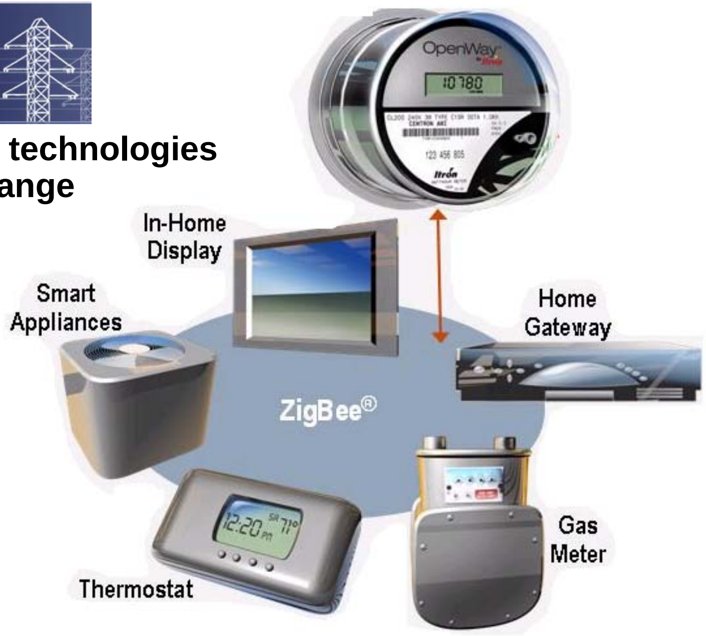
The Move to Smart Grid

Power grids of the future will be more dynamic, more efficient, and more flexible



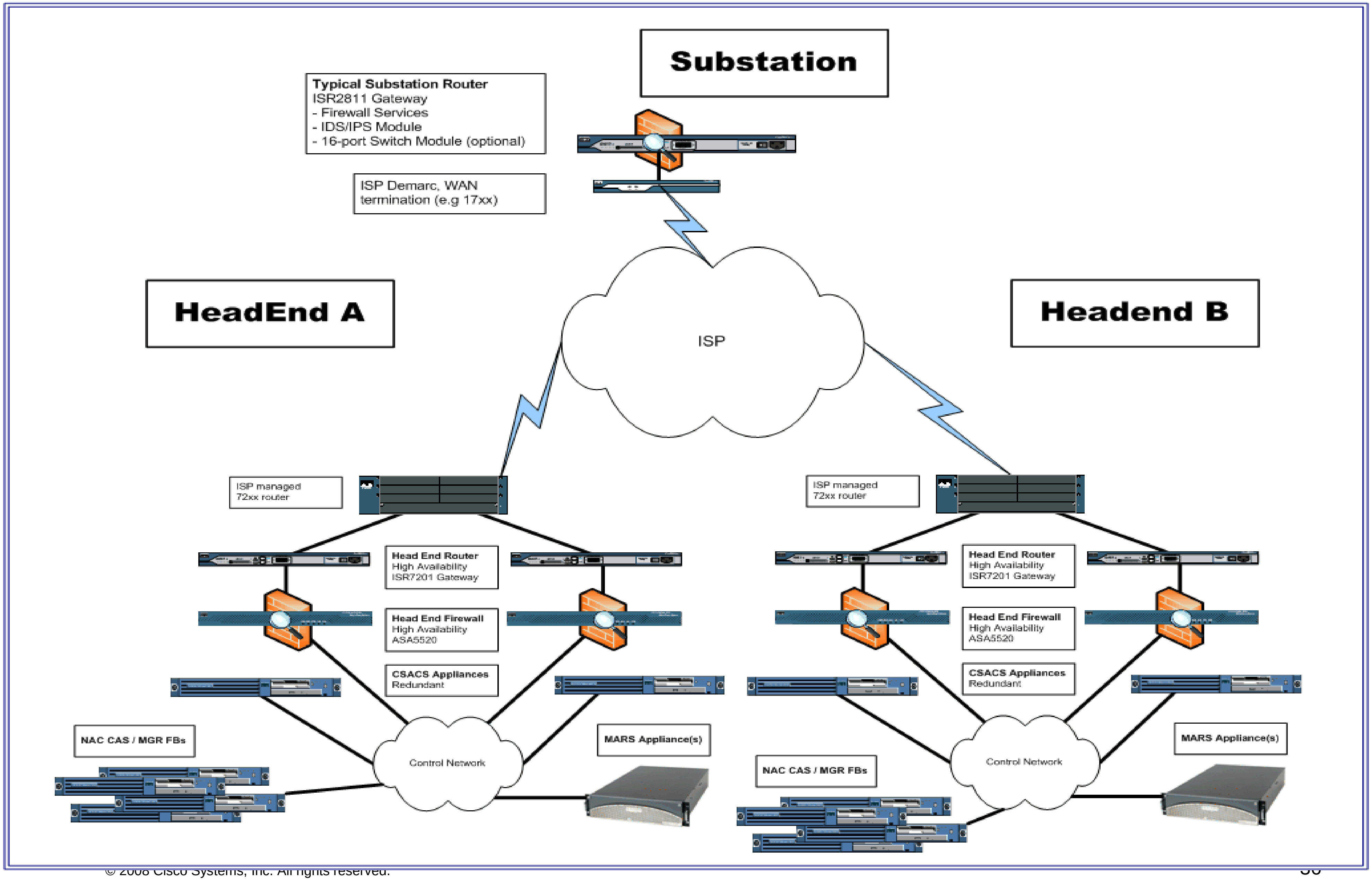
SMART GRID NEWSLETTER

Smart Grid technologies Driving Change



- **Every utility in the world is currently evaluating smart grid technologies**

Secure Substation


Substation
Typical Substation Router
ISR2811 Gateway
- Firewall Services
- IDS/IPS Module
- 16-port Switch Module (optional)
ISP Demarc, WAN termination (e.g 17xx)
HeadEnd A
ISP
Headend B
ISP managed 72xx router
ISP managed 72xx router
Head End Router
High Availability
ISR7201 Gateway
Head End Router
High Availability
ISR7201 Gateway
Head End Firewall
High Availability
ASA5520
Head End Firewall
High Availability
ASA5520
CSACS Appliances
Redundant
CSACS Appliances
Redundant
NAC CAS / MGR FBs
Control Network
MARS Appliance(s)
NAC CAS / MGR FBs
Control Network
MARS Appliance(s)