

NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Access Control and CIP

10/20/2011

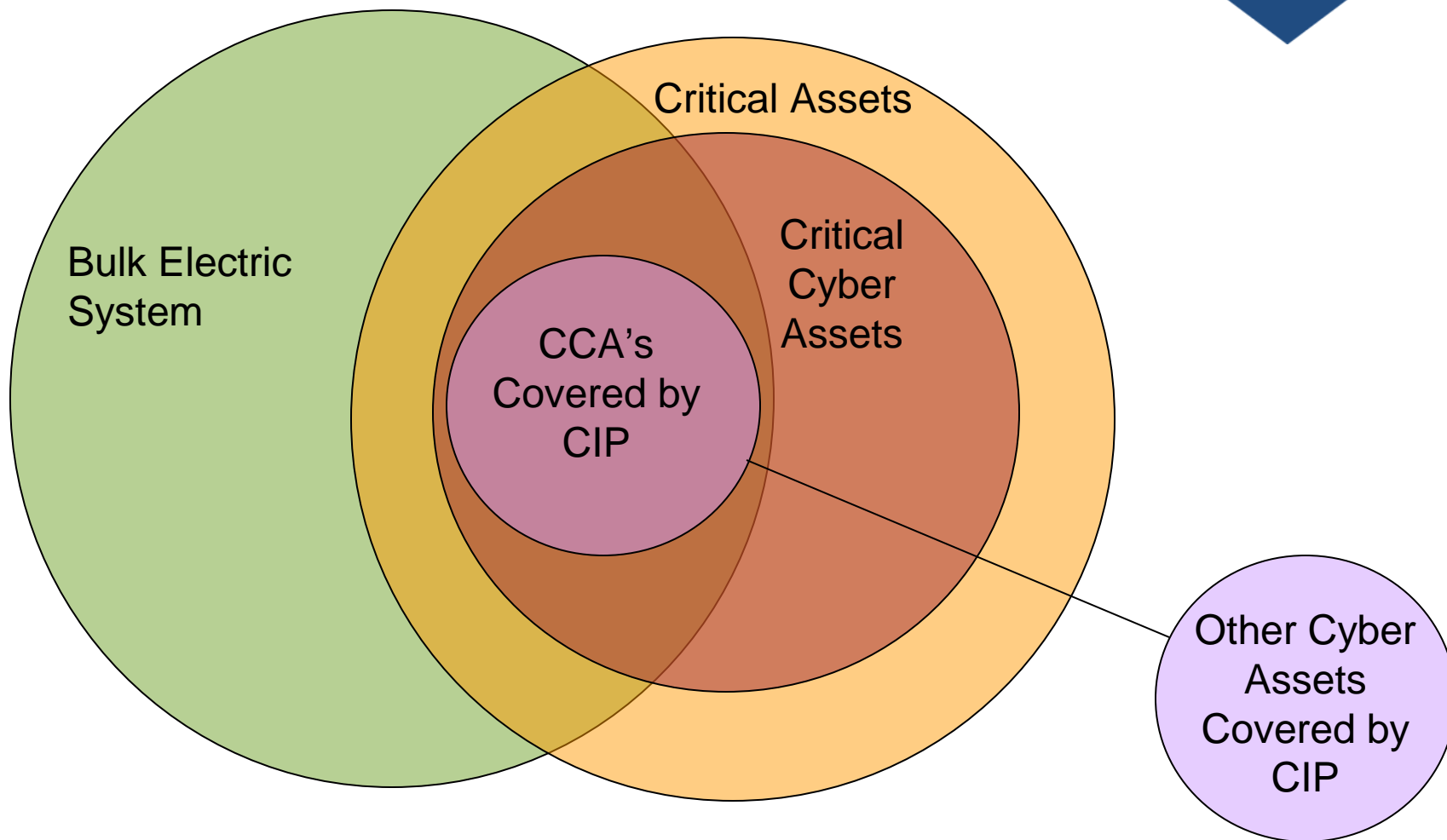
RELIABILITY | ACCOUNTABILITY



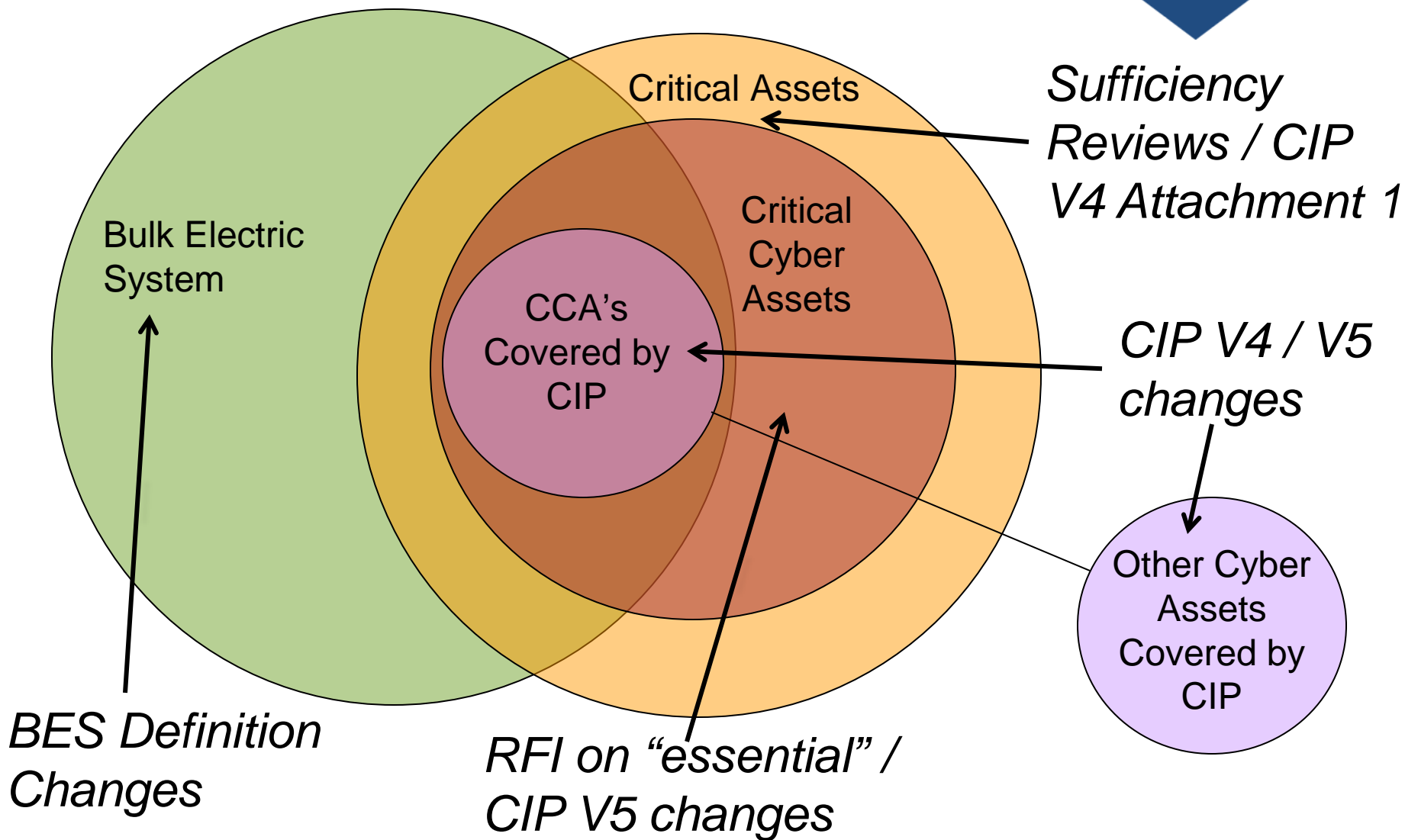
- Access Control Requirements
- Impact on Entities
- Risk Discussion
- Response Discussion
- Future pursuit

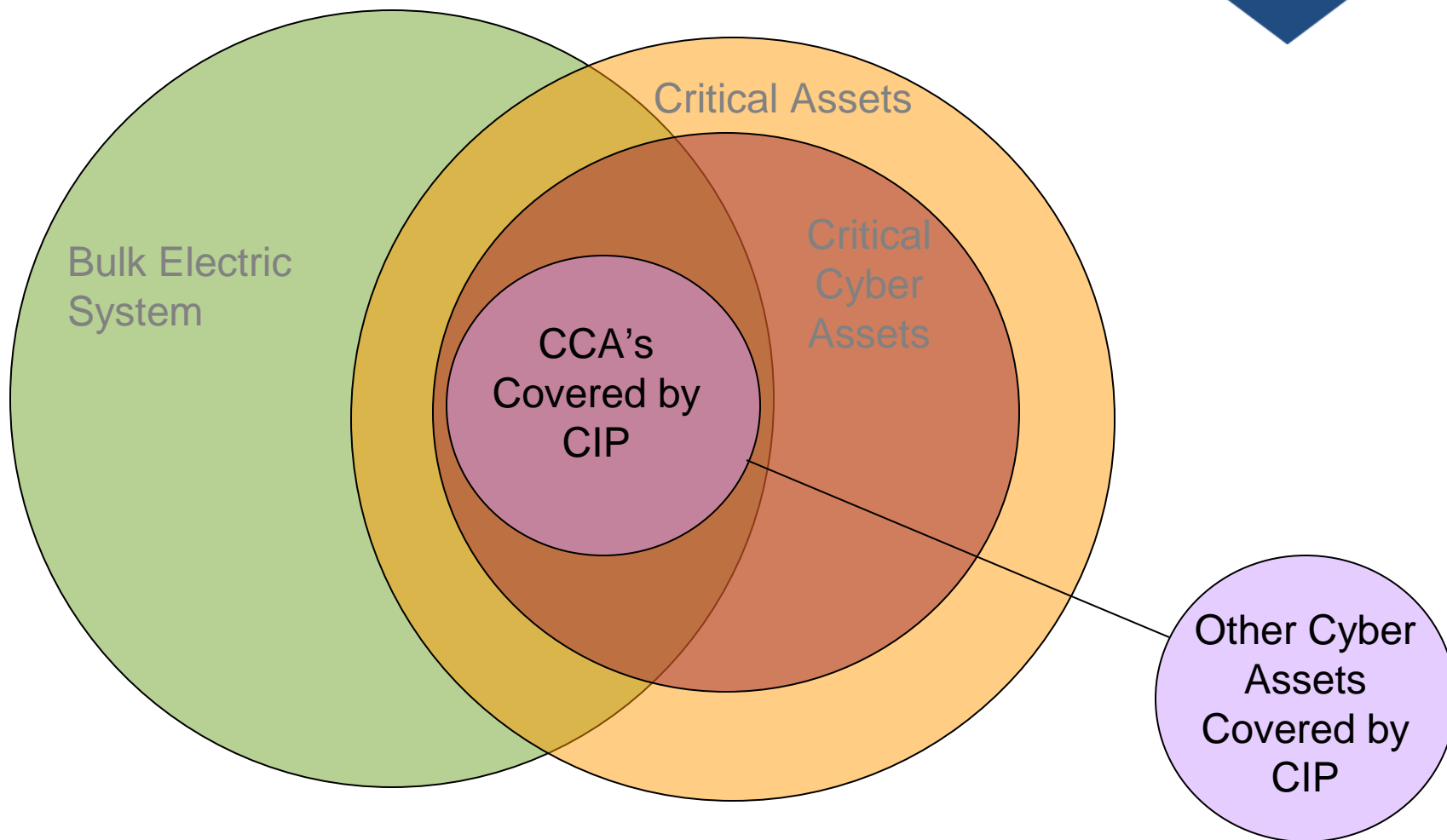
Let's Talk CIP





The CIP You Thought You Knew





Access Control Requirements

- CIP-003 R5



Requirement language:

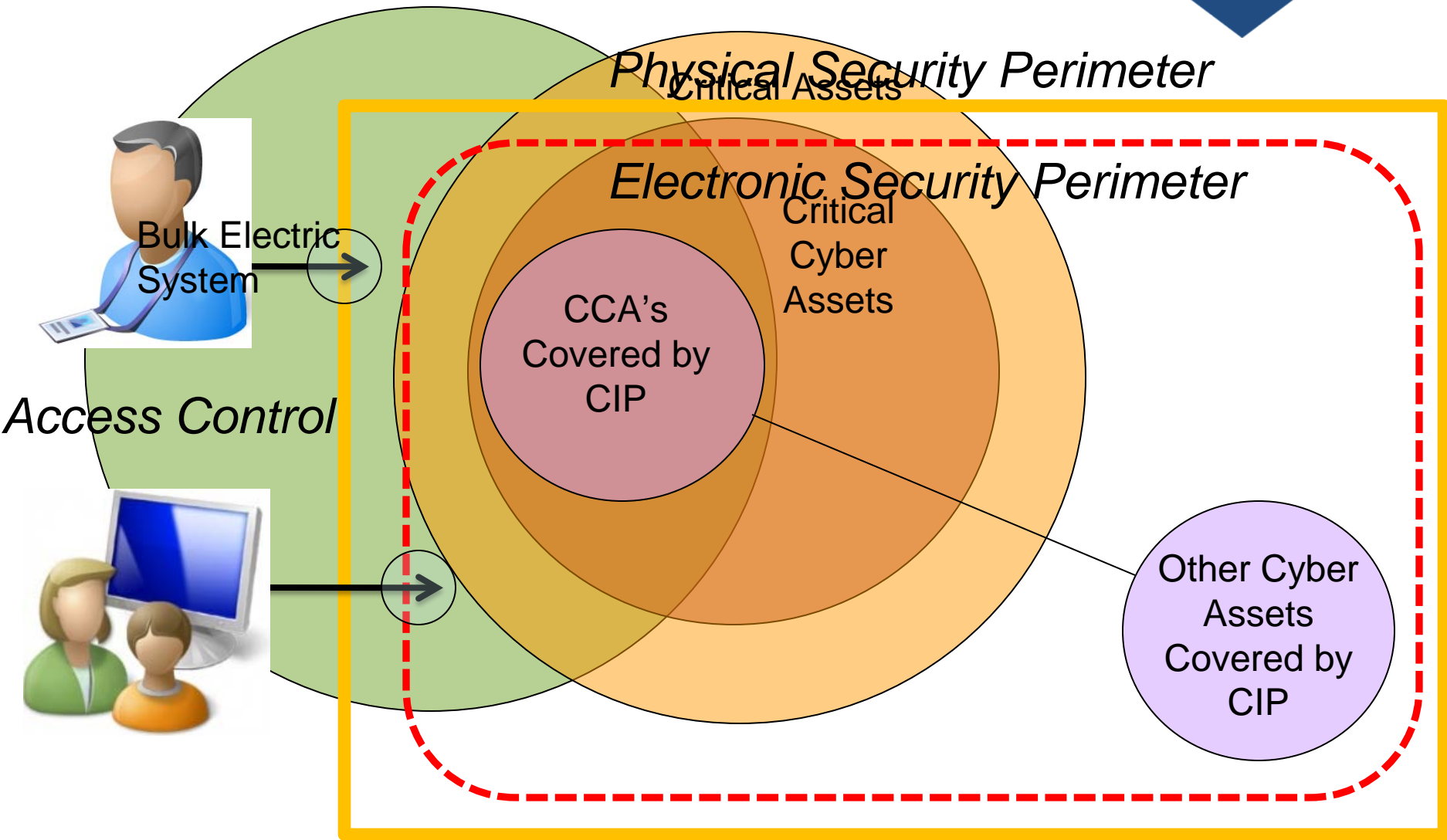
R5. Access Control — The Responsible Entity shall ***document and implement a program for managing access to protected Critical Cyber Asset information.***

R5.1. The Responsible Entity shall ***maintain a list of designated personnel who are responsible for authorizing logical or physical access to protected information.***

- CIP-003 R5
- **CIP-004 R4**

Requirement language:

R4 Access — The Responsible Entity shall maintain list(s) of personnel with ***authorized cyber or authorized unescorted physical access to Critical Cyber Assets***, including their specific electronic and physical access rights to Critical Cyber Assets.



- CIP-003 R5
- CIP-004 R4
- CIP-005 R1.5, R2



Requirement language:

R1.5. Cyber Assets used in the access control and/or monitoring of the Electronic Security Perimeter(s)



Novell.



tripwire



ArcSight



- CIP-003 R5
- CIP-004 R4
- CIP-005 R1.5, R2
- **CIP-006 R1 – R6 all**



Requirement language:

R2. Protection of Physical Access Control Systems — Cyber Assets that authorize and /or log access to the Physical Security Perimeter(s)



Impact on Entities



Assets

- Physical Protection
- Electronic Protection
- Lists of individual access



Information

- Physical Protection
- Electronic Protection
- Lists of individuals who control access



People

- Qualifications for access (PRA / Training)
- Approval for access
- Removal of access

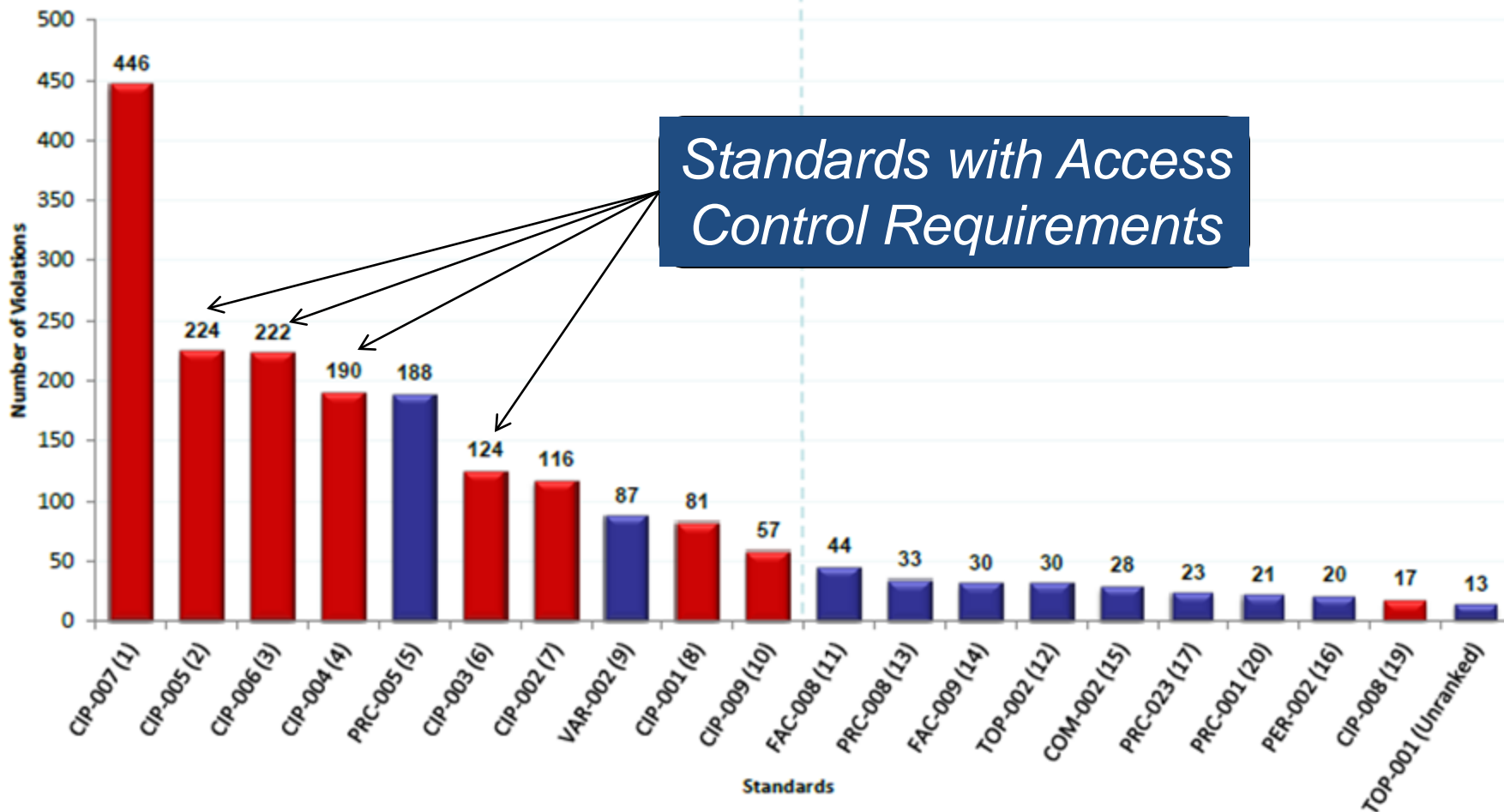
Risk Discussion

	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

1 Million Dollars a day per day - per violation



Previous 12 Months Violations Through August 31, 2011



Ne



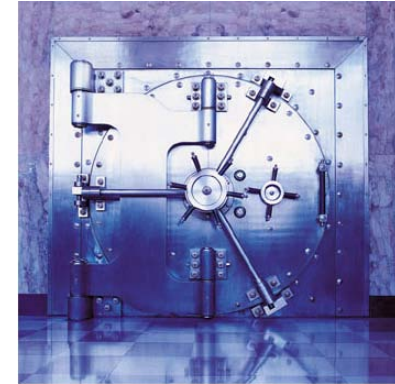
**NEW TERROR
EXTREMISTS**
U.S. UTILITIES AT RISK

W32.Duqu
The precursor to the next Stuxnet

Contents

Executive summary

Everything is an island



Response Discussion

- ACAT
 - Avoid
 - Control
 - Accept
 - Transfer



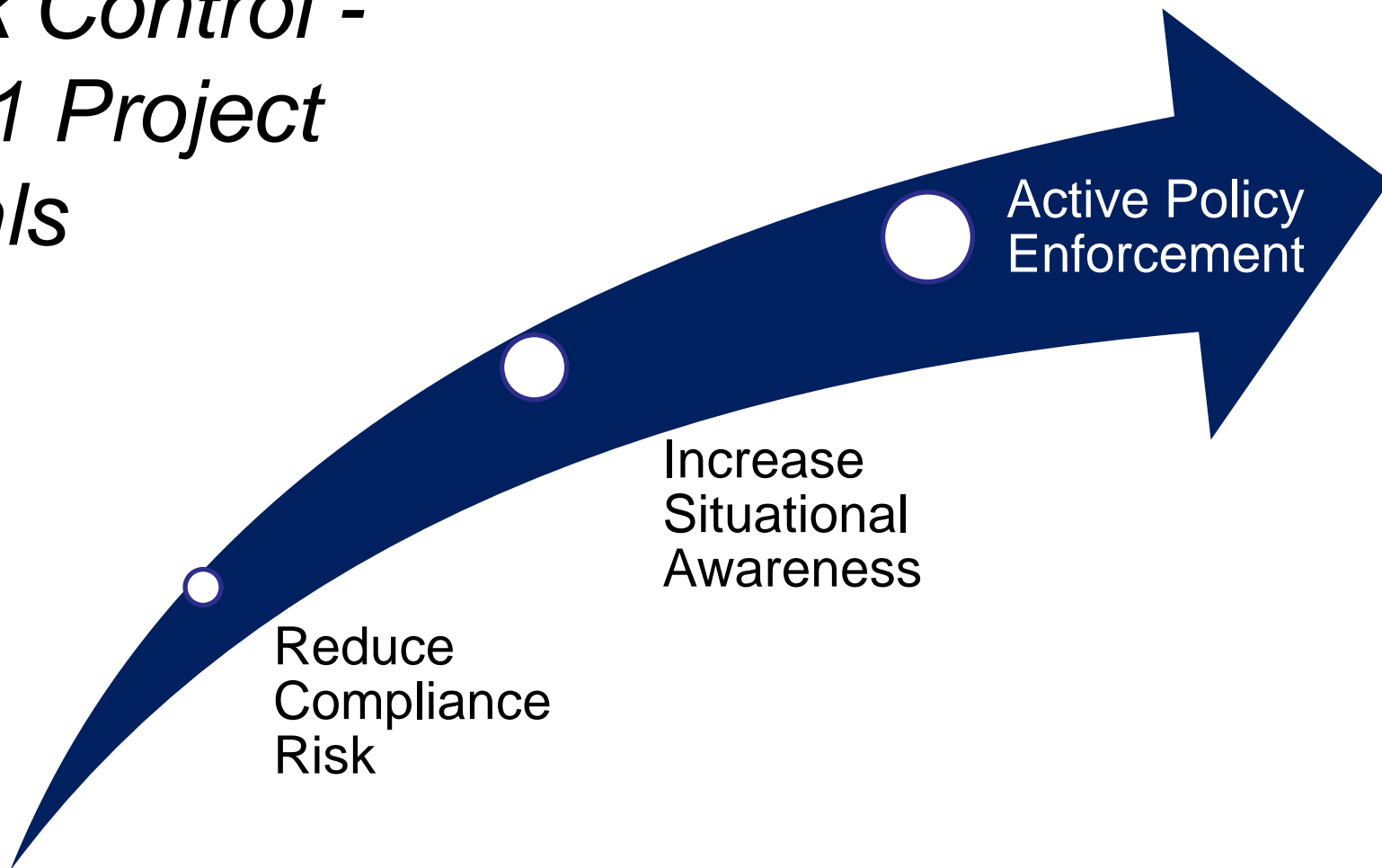
Everything is an island



Build Bridges



Risk Control - 2011 Project Goals



Reduce Compliance Risk

- Unique Id
- Simplify quarterly review
- Reduce human performance errors

Increase Situational Awareness

- Employee actions
- Training records
- PRA records
- Reporting

Active Policy Enforcement

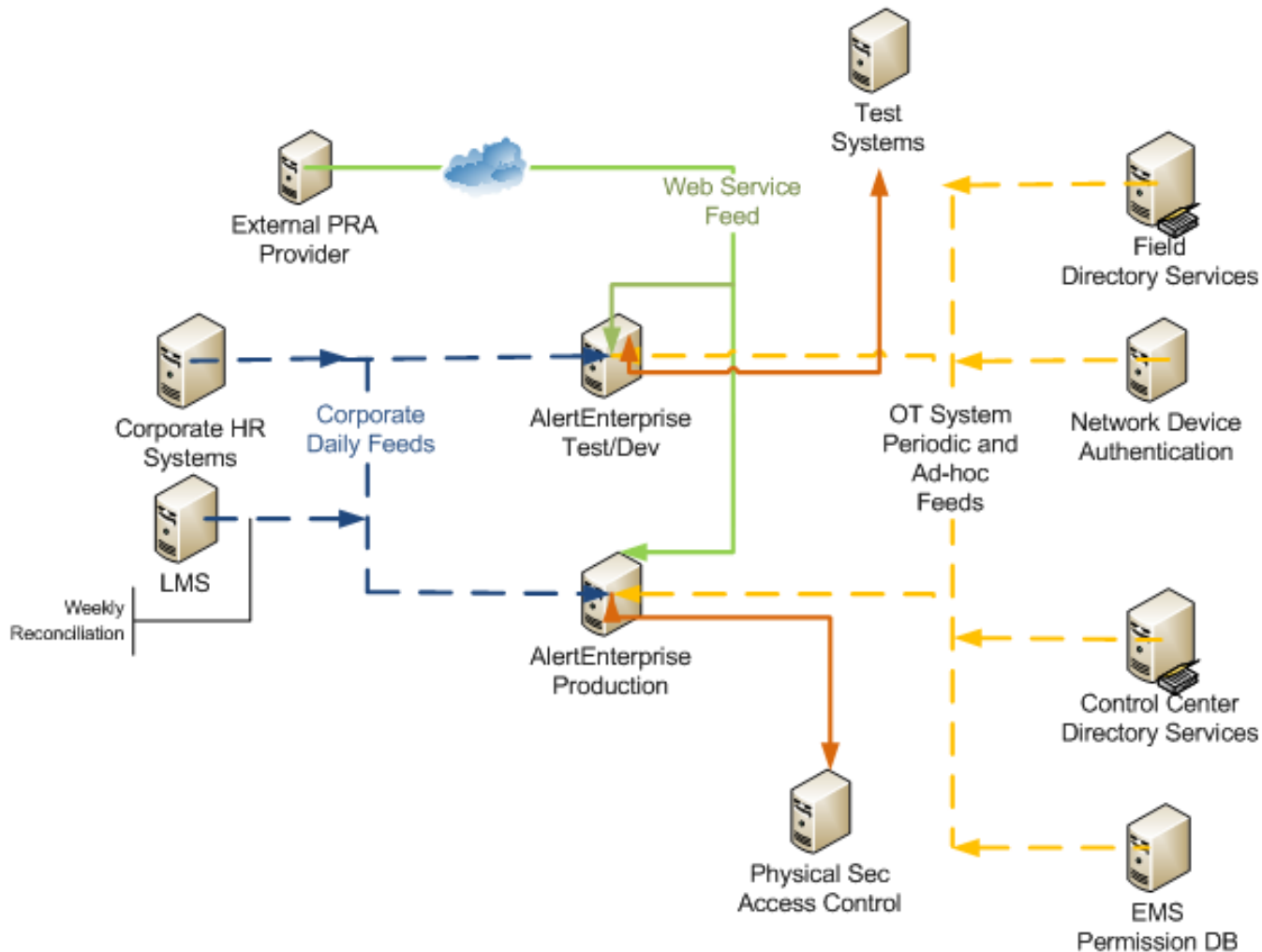
- Trigger Notification
- Disable physical access
- Disable cyber access

Connections:

Corporate HR
Corporate LMS
3rd party PRA

Operations Tech –
Directory Services
Network Auth
Physical Security
App Proprietary DB

Operations Tech
Test Systems



Future Pursuits

- Control Center Implementation
 - Increased awareness of events
 - Operator authentication
 - Operator multiple physical locations
 - Operator log on duration
 - Increased inputs to include system events and awareness data feeds

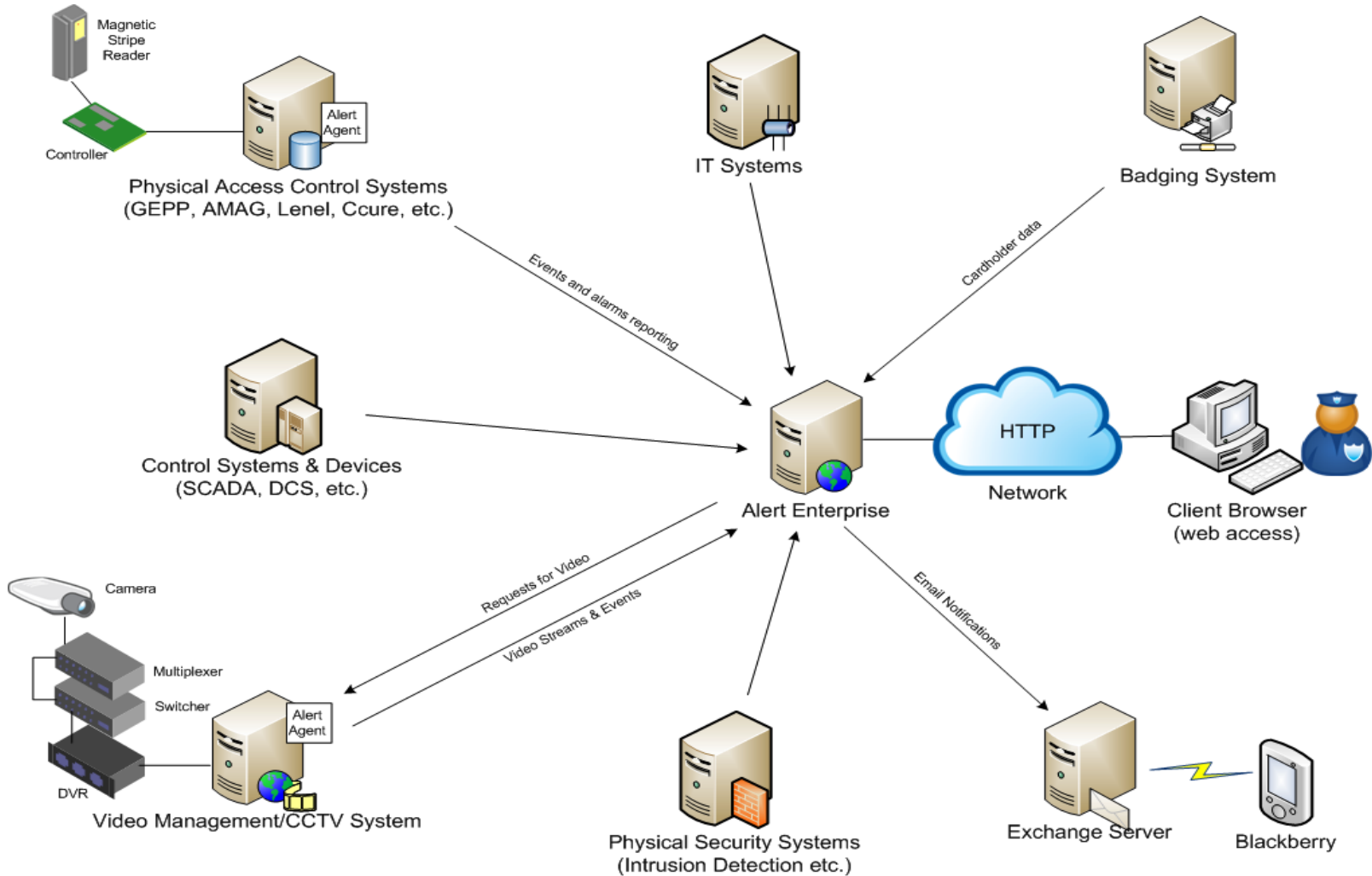


- Field Implementations
 - Substation environments
 - Gen station environments
- Non-CIP
 - FERC regulations
 - Natural Gas facilities



Everything is an island





The dashboard consists of six panels:

- Incident User Risk Analysis:** A tree diagram showing 'Sub-station 1 SCADA' connected to 'Network 1', 'Network 2', 'Network 3', 'Users', 'Risks', and 'Change Logs'. 'Users' is further connected to 'JonesMa', 'BrownEt', 'DavisAn', and 'MileDa'.
- Live Video Feed:** A 3D virtual environment of a control room with a smaller inset window showing a live video feed of a control room.
- Incident Confirmation:** A task card for 'Task ID #1 Manual' with status 'Task has been successfully closed'. Task: 'Situation Analysis and Incident Confirmation'. Assigned To: 'Tom Hopkins'. Priority: 'High'. Start: '25 Feb 09 10:45PM'. Status: 'Closed'. Precedence: '1'. Due By: '25 Feb 09 10:50PM'. Incident: 'Confirm'. Includes a 'Comments' text box.
- Incident Report:** A 'High Alert- PI Notification' with a red warning icon. Severity: 'High'. Details: 'High Alert - PI Notification Manager Protective Relay Set Point Change'. Last Physical Access: 'JonesMa' at 'TIME: 16:26'.
- Grid View - Affected Consumer Area:** A satellite map showing a grid of consumer areas including Lambton, Swansea, High Park, Brockton Village, Roncesvalles, Parkdale, and The Queensway-Humber Bay.
- Incident Location:** Two images: a 3D rendering of a power plant and a satellite view of a power plant site.

Executive and Management



