USAID
FROM THE AMERICAN PEOPLE

USEA
United States Energy Association

NERC CIP

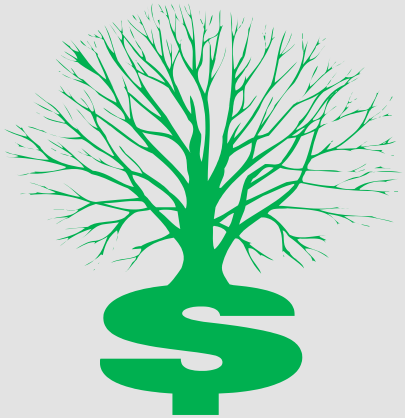
Cybersecurity Standards and Best Practices:
Part 1 - US Standards (NERC CIP)

Speakers

Tim Conway
– SANS Institute
– Instructor

Dean Parsons
– Herjavec Group
– SANS Certified Instructor

Critical Infrastructure Protection



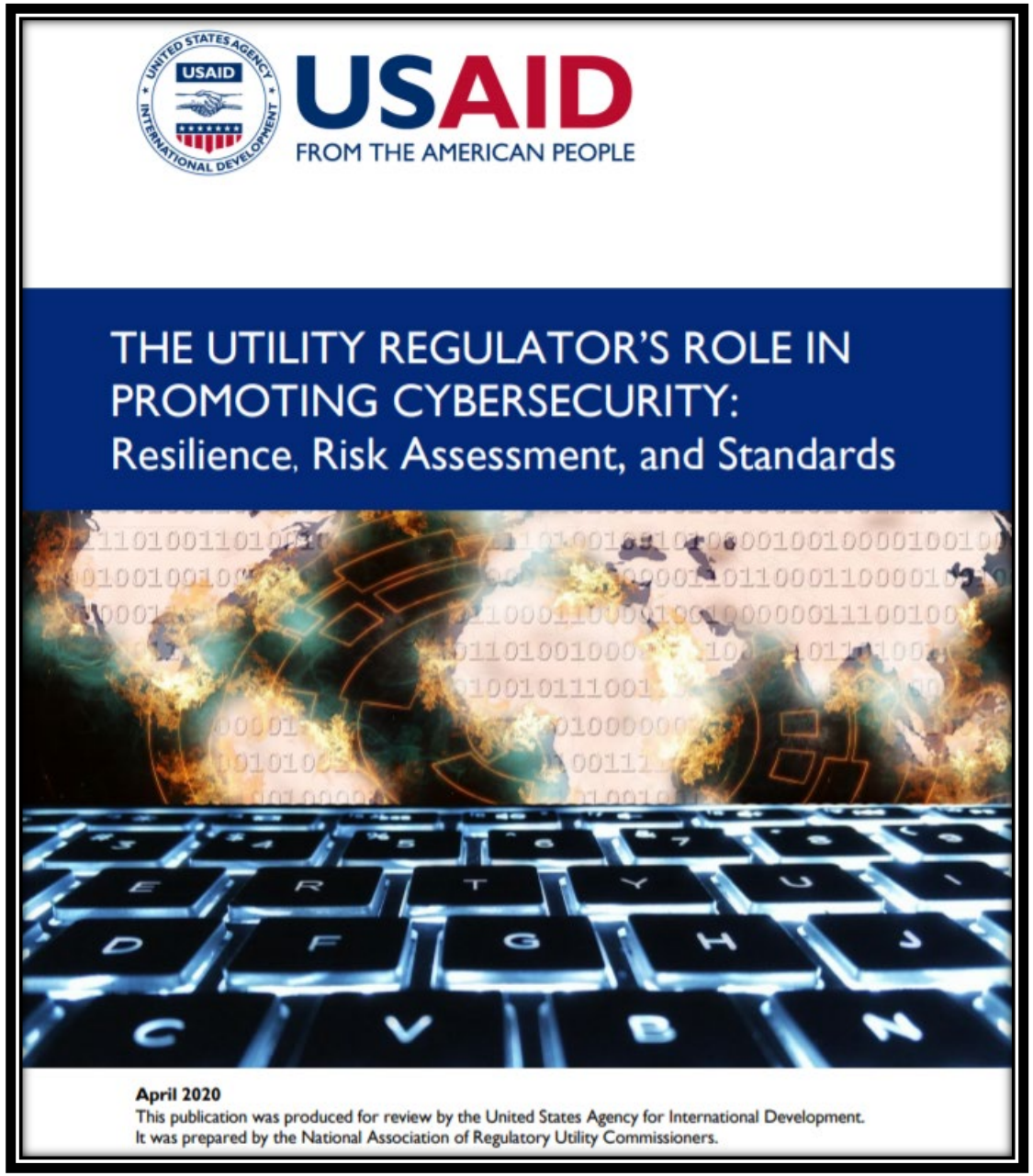
NERC CIP Basics

CIP Best Of

CIP Lessons Learned and Fails

NERC CIP

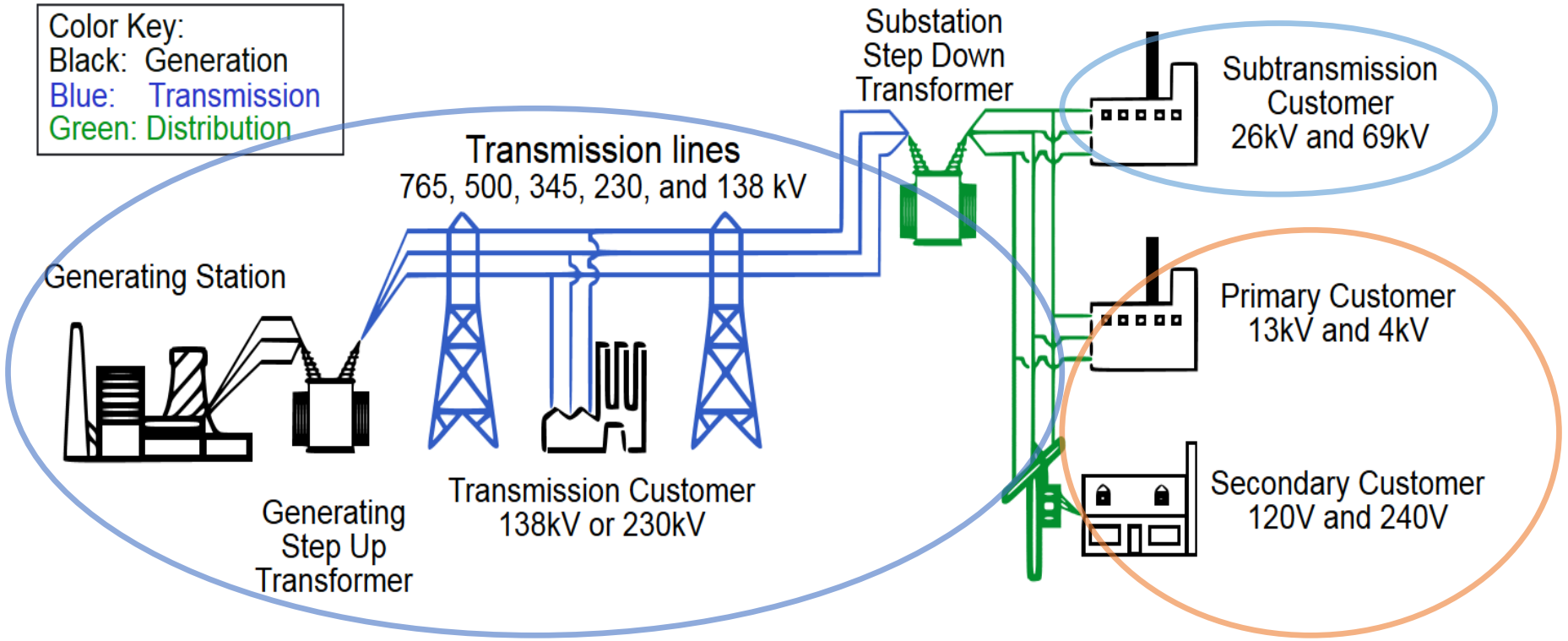
NERC CIP Basics



- Capture a dialog across individuals who have designed, implemented, managed and maintained various Standards programs
- Educate on challenges
- Capture lessons learned
- Provide guidance on how to move forward
- Attempt to stop Standards explosion for each implementation

What Is NERC CIP?

Requirements designed to ensure physical and electronic security of Cyber Assets required for operating North America's BES



Current CIP Standards in Effect *

Standard - Version	Standard Name
CIP-002-5.1	BES Cyber System Categorization
CIP-003-8	Security Management Controls
CIP-004-6	Personnel & Training
CIP-005-6	Electronic Security Perimeter(s)
CIP-006-6	Physical Security of BES Cyber Systems
CIP-007-6	System Security Management
CIP-008-5	Incident Reporting and Response Planning
CIP-009-6	Recovery Plans for BES Cyber Systems
CIP-010-3	Configuration Change Management and Vulnerability Assessments
CIP-011-2	Information Protection
CIP-012-1	Communications Between Control Centers
CIP-013-1	Supply Chain Risk Management
CIP-014-2	Physical Security

CIP-002 Scoping Standard

- Identify in scope sites:
  - Control Centers and Backup Control Centers
  - Transmission substations
  - Generation resources
  - Systems and facilities critical for grid restoration, including blackstart generation and cranking paths
  - Remedial Action Schemes

- Determine in scope BES Cyber Assets

CIP-003 Policy and Governance + Low Requirements ☺ or ☹

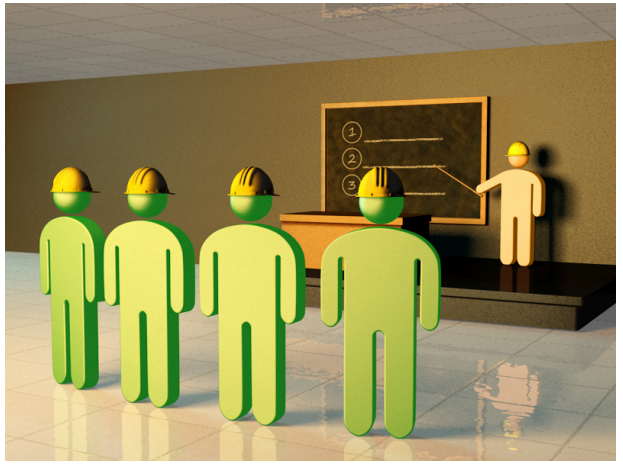
- Establishes CIP Senior Manager requirements and identifies required policies for High and Medium
  - ✓ 1.1 Personnel & training (CIP-004)
  - ✓ 1.2 Electronic Security Perimeters (CIP-005) including Interactive Remote Access
  - ✓ 1.3 Physical security of BES Cyber Systems (CIP-006)
  - ✓ 1.4 System security management (CIP-007)
  - ✓ 1.5 Incident reporting and response planning (CIP-008)
  - ✓ 1.6 Recovery plans for BES Cyber Systems (CIP-009)
  - ✓ 1.7 Configuration change management and vulnerability assessments (CIP-010)
  - ✓ 1.8 Information protection (CIP-011)
  - ✓ 1.9 Declaring and responding to CIP Exceptional Circumstances

- Also identifies four / six required policies and plans for Lows
  - ✓ Cyber security awareness;
  - ✓ **Physical security controls;**
  - ✓ **Electronic access controls**;
  - ✓ Cyber Security Incident response

✓Malicious code risk mitigation for Transient Cyber Assets & Removable Media;
✓Declaring & responding to CIP Exceptional Circumstances

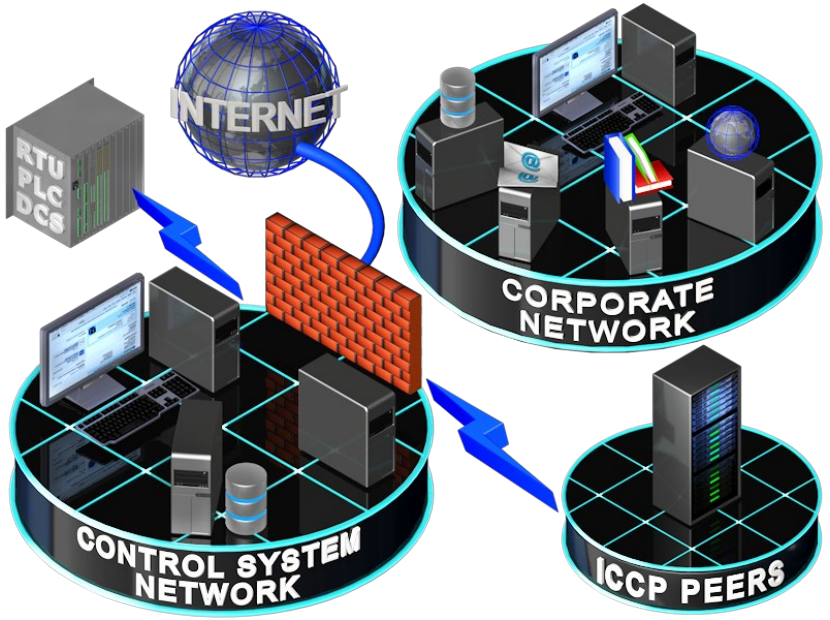
CIP-004 Personnel Management

- Establishes required personnel quarterly security awareness training and annual training requirements for those with access
- Requirements for entities to perform Personnel Risk Assessments and background checks
- Electronic and Physical access control reviews and authorization verification as well as timely revocation when necessary



CIP-005 Electronic Security Perimeter

- Establishes electronic perimeters around BES Cyber Systems
- Defines requirements around External Routable Connectivity and allowed communications
- Also addresses requirements around remote access to BES Cyber Systems



CIP-006 Physical Security Perimeter

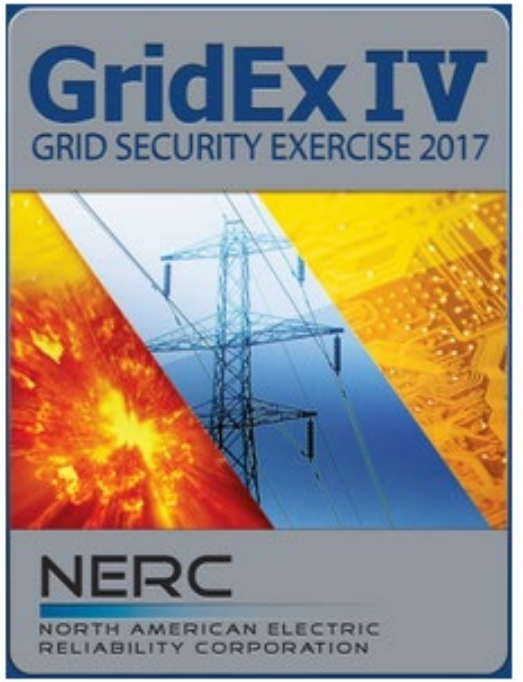
- Establishes physical perimeter around BES Cyber Systems
- Provide monitoring and alerting of unauthorized access
- Establish visitor escort and control program

CIP-007 System Security Management

- Harden and manage in scope BES Cyber Assets:
  - Ports and Services – logical and physical
  - Security Patch Management – identify, apply, or mitigate
  - Malicious Code Prevention – mitigate threat of malicious code
  - Security Event Monitoring – log, alert, and review
  - System Access Control – account and password management

CIP-008 Incident Response

- Requires an incident response plan
  - Identify, classify, and respond to Cyber Security incidents
  - Reporting requirements for RCSI
- Test and update the incident response plan



Change is Coming

164 FERC ¶ 61,033
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM18-2-000; Order No. 848]

Cyber Security Incident Reporting Reliability Standards

(Issued July 19, 2018)

AGENCY: Federal Energy Regulatory Commission.

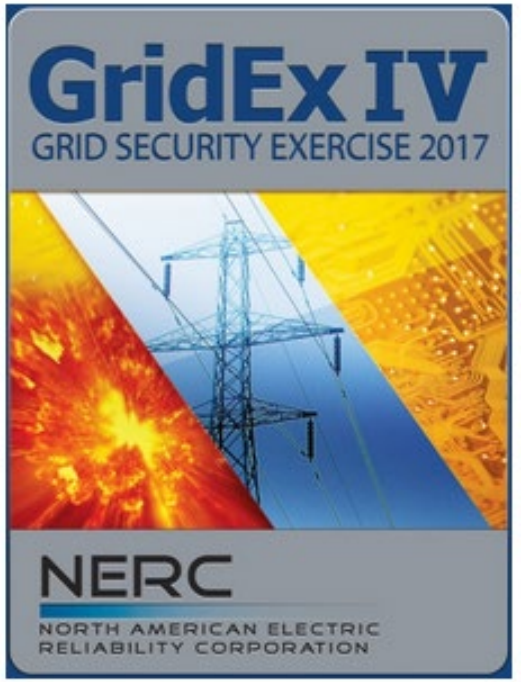
ACTION: Final rule.

SUMMARY: The Federal Energy Regulatory Commission (Commission) directs the North American Electric Reliability Corporation (NERC) to develop and submit modifications to the NERC Reliability Standards to augment the mandatory reporting of Cyber Security Incidents, including incidents that might facilitate subsequent efforts to harm the reliable operation of the bulk electric system (BES).

- Report–compromise, or attempt to compromise, the ESP or associated EACMS
- Require minimum reporting detail
- Reporting timeline
- Reporting to DHS as well as E-ISAC
- NERC to develop summary reports to FERC

CIP-009 Recovery Plans for BES Cyber Systems

- Requires BES Cyber System recovery plans
  - Backup capability of information necessary to restore BES Cyber Assets
  - Verification that backups performed are valid
- Test and update the recovery plans



Standard EOP-008-1 — Loss of Control Center Functionality

A. **Introduction**

1. **Title:** **Loss of Control Center Functionality**
2. **Number:** **EOP-008-1**
3. **Purpose:** Ensure continued reliable operations of the Bulk Electric System (BES) in the event that a control center becomes inoperable.

CIP-010 Change Management

- Develop baselines for BES Cyber Systems
  - Operating system or firmware
  - Commercial and open source software intentionally installed
  - Logical network accessible ports
  - Security patch level
- Test and verify changes do not effect security controls
- Monitor for unauthorized changes to baseline
- Perform vulnerability assessments
- Transient Cyber Asset and Removable Media requirements

CIP-011 Information Protection

- Process to identify BES Cyber System Information and protect it from unauthorized access
  - During data storage
  - Data transit
  - Data use
- Process for disposal or sanitization

Color	When should it be used?	How may it be shared?
RED	Sources may use TLP: RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused.	Recipients may not share TLP: RED information with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.
AMBER	Sources may use TLP: AMBER when information requires support to be effectively acted upon, but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.	Recipients may only share TLP: AMBER information with members of their own organization who need to know, and only as widely as necessary to act on that information.
GREEN	Sources may use TLP: GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector.	Recipients may share TLP: GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels.
WHITE	Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.	TLP: WHITE information may be distributed without restriction, subject to copyright controls.

CIP-012 Communications between Control Centers

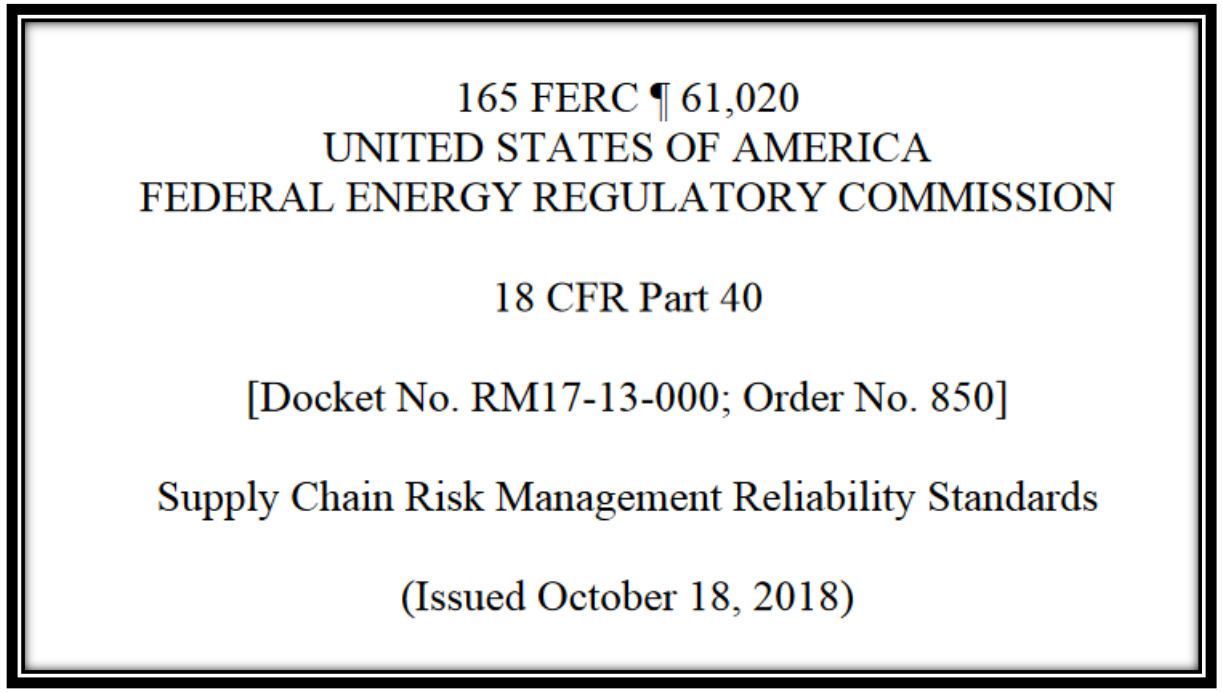
1.1. Identification of security protection used to mitigate the risks posed by unauthorized disclosure and unauthorized modification of Real-time Assessment and Real-time monitoring data while being transmitted between Control Centers;

1.2. Identification of where the Responsible Entity applied security protection for transmitting Real-time Assessment and Real-time monitoring data between Control Centers; and

1.3. If the Control Centers are owned or operated by different Responsible Entities, identification of the responsibilities of each Responsible Entity for applying security protection to the transmission of Real-time Assessment and Real-time monitoring data between those Control Centers.

- Response to FERC directive in Order 822 to protect sensitive BES data and communications links between Control Centers
- Currently NERC BOT approved pending FERC approval
- Intended focus could be confusing with the use of capital "C" Control Centers

CIP-013 Supply Chain



165 FERC ¶ 61,020
UNITED STATES OF AMERICA
FEDERAL ENERGY REGULATORY COMMISSION

18 CFR Part 40

[Docket No. RM17-13-000; Order No. 850]

Supply Chain Risk Management Reliability Standards

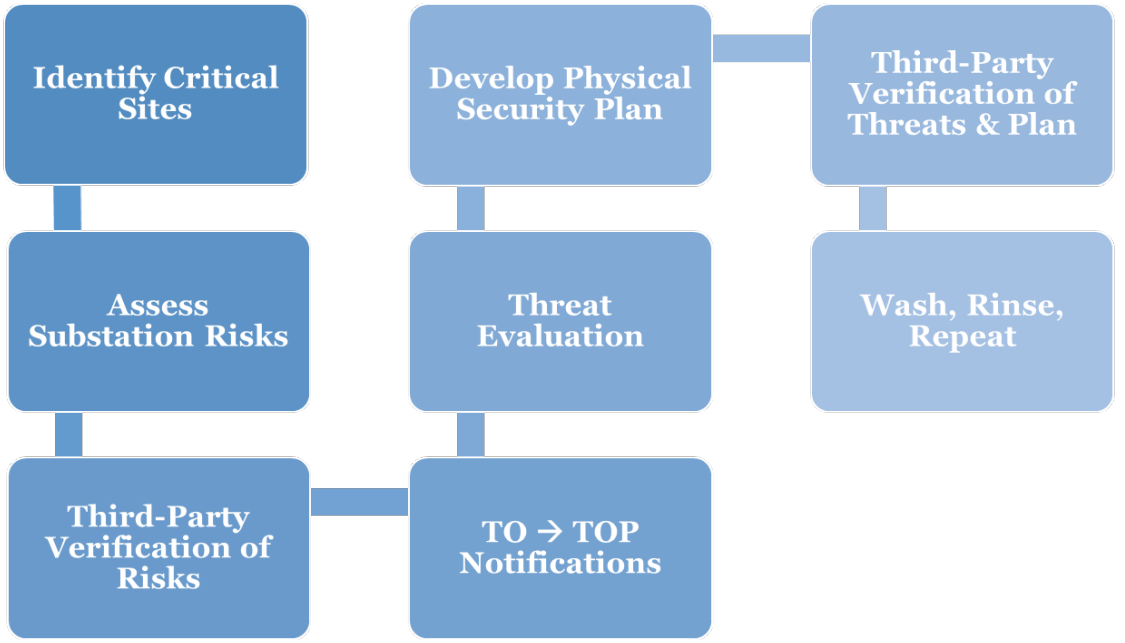
(Issued October 18, 2018)

* 7/1/2020

- Develop supply chain risk management plans
- Addressing identifying and assessing risk when procuring / transitioning
- Vendor incident / breach / vulnerability notification
- Software integrity and authenticity requirements
- Vendor remote access

CIP-014 Physical Security

- Perform Substation Risk Assessments
- Required Third-Party Verification of BES Reliability assessments
- Perform a physical security threat evaluation
- Required Third-Party Verification of physical security assessments

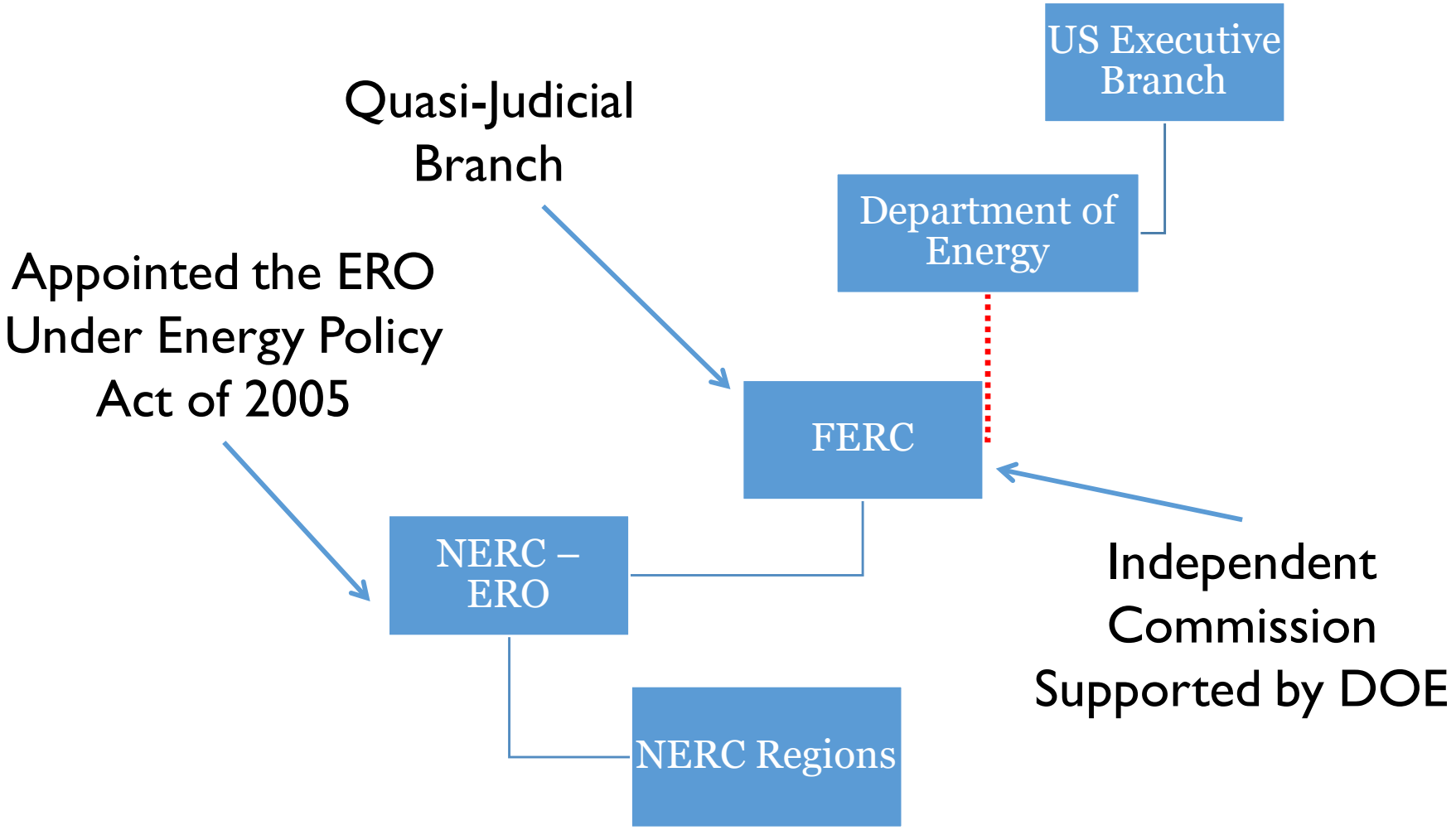


Asset Owner Perspective

NERC CIP

CIP Best Of

Defined Authority



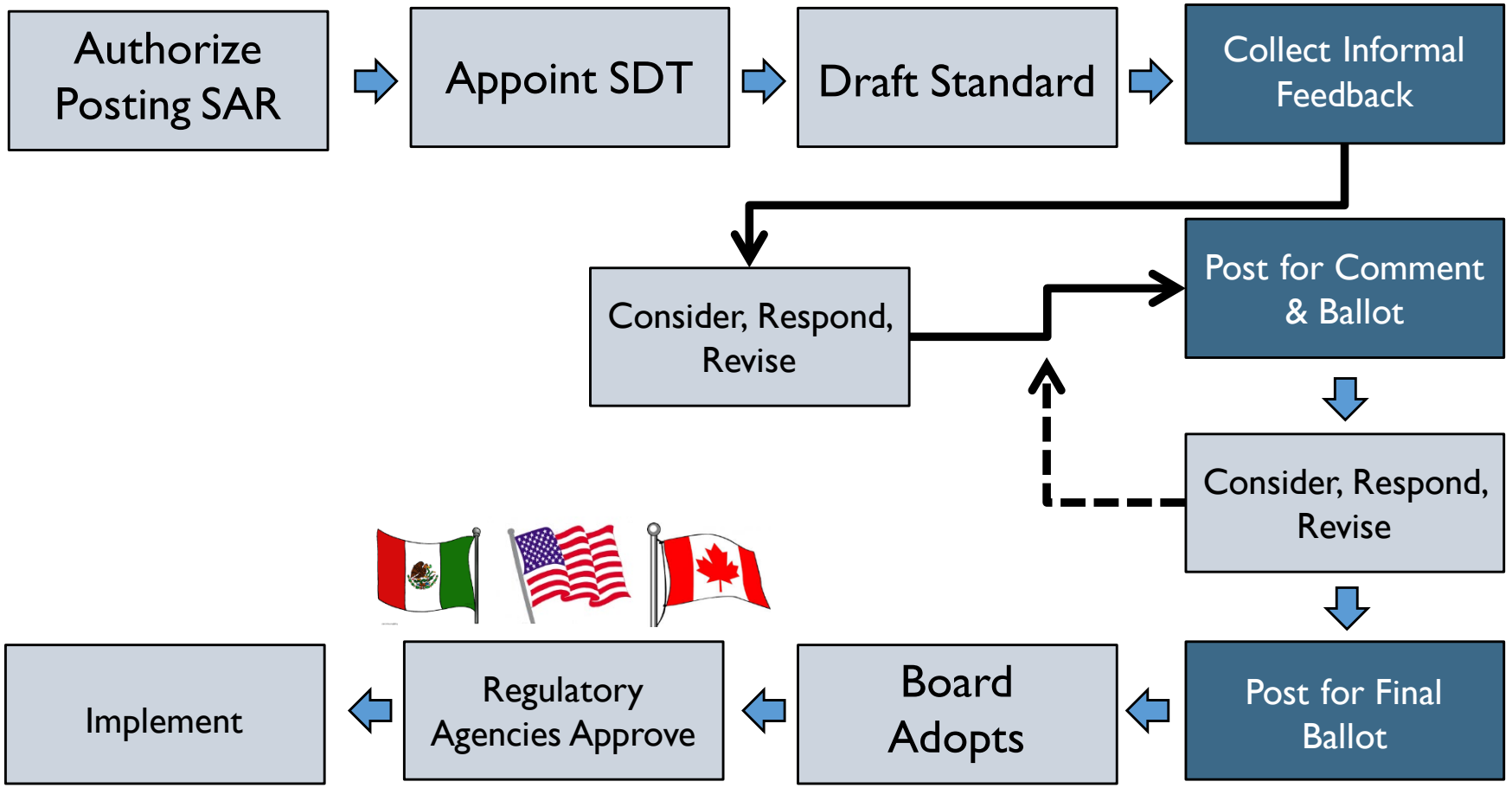
Enforcement

Penalty Matrix

Violation Risk Factor	Violation Severity Level							
	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 *

Limits are per day, per violation

Standards Development Process



Standards Balloting

- Open participation
- Balance of interest: by segment
- Notification of standards development
- Transparency
- Consideration of views and objections
- Consensus vote: registered entities only
  - quorum = 75% of participating ballot pool

$$\frac{\text{Yes + No + Abstain}}{\text{\# in Ballot Pool}}$$

  - 2/3 majority to affirm

$$\frac{\text{Yes}}{\text{Yes + No}}$$

- Timeliness

Focus on BES Reliability Operating Services (BROS)

BES Reliability Operating Services: Those services contributing to the real-time reliable operation of the Bulk Electric System (BES)

- Dynamic Response
- Balancing Load & Generation
- Controlling Frequency (Real Power)
- Controlling Voltage (Reactive Power)
- Managing Constraints
- Monitoring & Controlling
- Restoration of BES
- Situational Awareness
- Inter-Entity Real-Time Coordination and Communication

Standards Coverage

Assets

- Physical Protection
- Electronic Protection
- Lists of individual access

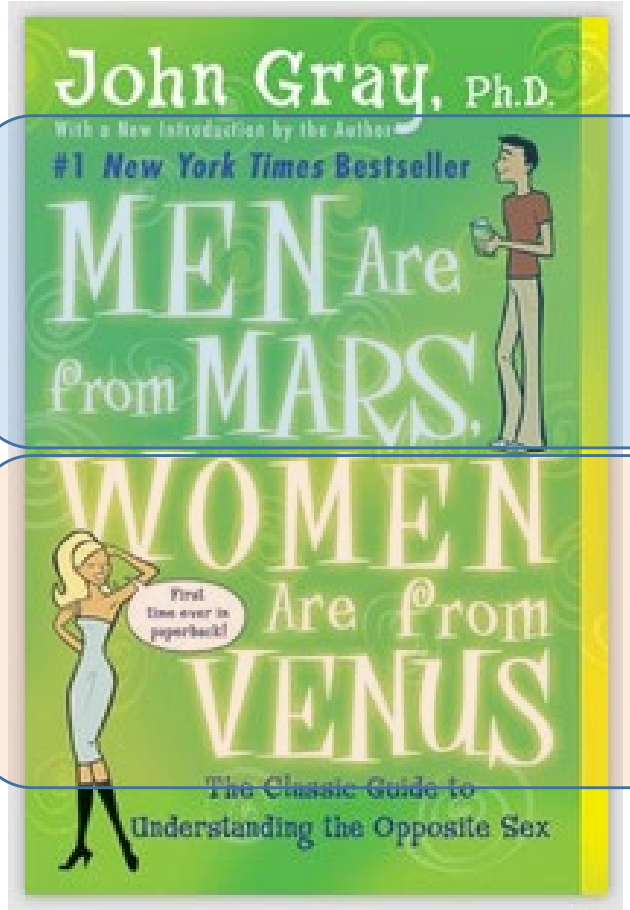
Information

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

People

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

IT & OT Inclusion



= OT

= IT

OT Learnings

- Admit you need IT
- Do not say air gap
- Consider misuse
- Provide a seat at the table
- Explain hardware restrictions, and device limitations with patience

IT Learnings

- Improve communications
- Deliver actionable info
- Do you need it
- Most everything has a reason
- Measure the right thing
- Balance compliance, security, and reliability

Team Learnings

- Focus on the mission
- Manage a complex system, safely and reliably
- Work together on projects from specification to implementation and define ongoing roles and responsibilities.

Security and Compliance Math

Truths

1. Security ≠ Compliance
2. Compliance ≠ Security

New Math

3. $$\frac{\text{Security} + \text{Magic}}{\text{Compliance}}$$

Managed Operational Assets

- Examples of routine CIP maintenance tasks assigned to CIP performers
- Pulled from CIP-002 through CIP-011 and TFE-related tasks as well as compliance process tasks

Recurring Activities (1)

15 Calendar Days	• CIP-007: Sample Log Review
35 Calendar Days	• CIP-007: Patch Evaluation • CIP-010: Baseline Review
Calendar Quarter	• Security Awareness Reinforcement • Verify Individuals with Active Electronic Access or Unescorted Physical Access

Recurring Activities (2)

15 Calendar Months

- CIP-002: BES Cyber System Identification
- CIP-003: CIP Senior Manager Approval of Policies
- CIP-004: Verify Access to BES Cyber System Information
- CIP-004: Verify Access Privileges
- CIP-004: Cyber Security Training
- CIP-004: Cyber Security Awareness Reinforcement
- CIP-007: Password Change
- CIP-008: Incident Response Plan Test
- CIP-009: Test Sample of Recovery Information
- CIP-009: Recovery Plan Test for High & Medium
- CIP-010: Paper or Active VA

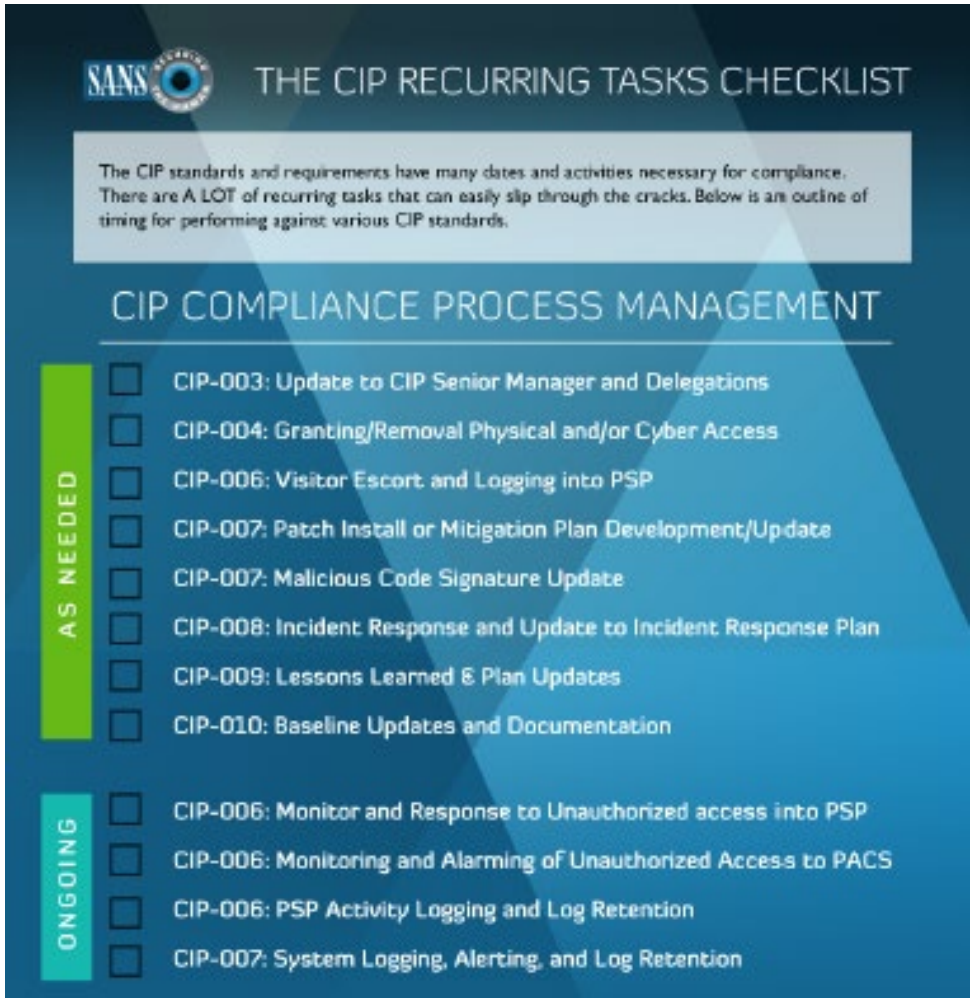
Recurring Activities (3)

24 Calendar Months	• CIP-006: Maintenance and Testing of PACS
36 Calendar Months	• CIP-003: Incident Response Plan Test for Low Impact • CIP-009: Recovery Plan Test for High Impact • CIP-010: Active VA for High Impact
7 Years	• CIP-004: Personnel Risk Assessment

Recurring Activities (4)

As needed	• CIP-003: Update to CIP Senior Manager and Delegations • CIP-004: Granting/Removal Physical and/or Cyber Access • CIP-006: Visitor Escort and Logging into PSP • CIP-007: Patch Install or Mitigation Plan Development/Update • CIP-007: Malicious Code Signature Update • CIP-008: Incident Response and Update to Incident Response Plan • CIP-009: Lessons Learned & Plan Updates • CIP-010: Baseline updates and documentation
On going	• CIP-006: Monitor and Response to Unauthorized access into PSP • CIP-006: Monitoring and Alarming of Unauthorized Access to PACS • CIP-006: PSP Activity Logging and Log Retention • CIP-007: System Logging, Alerting, and Log Retention

Infographic



https://securingthehuman.sans.org/

NERC CIP Best Of

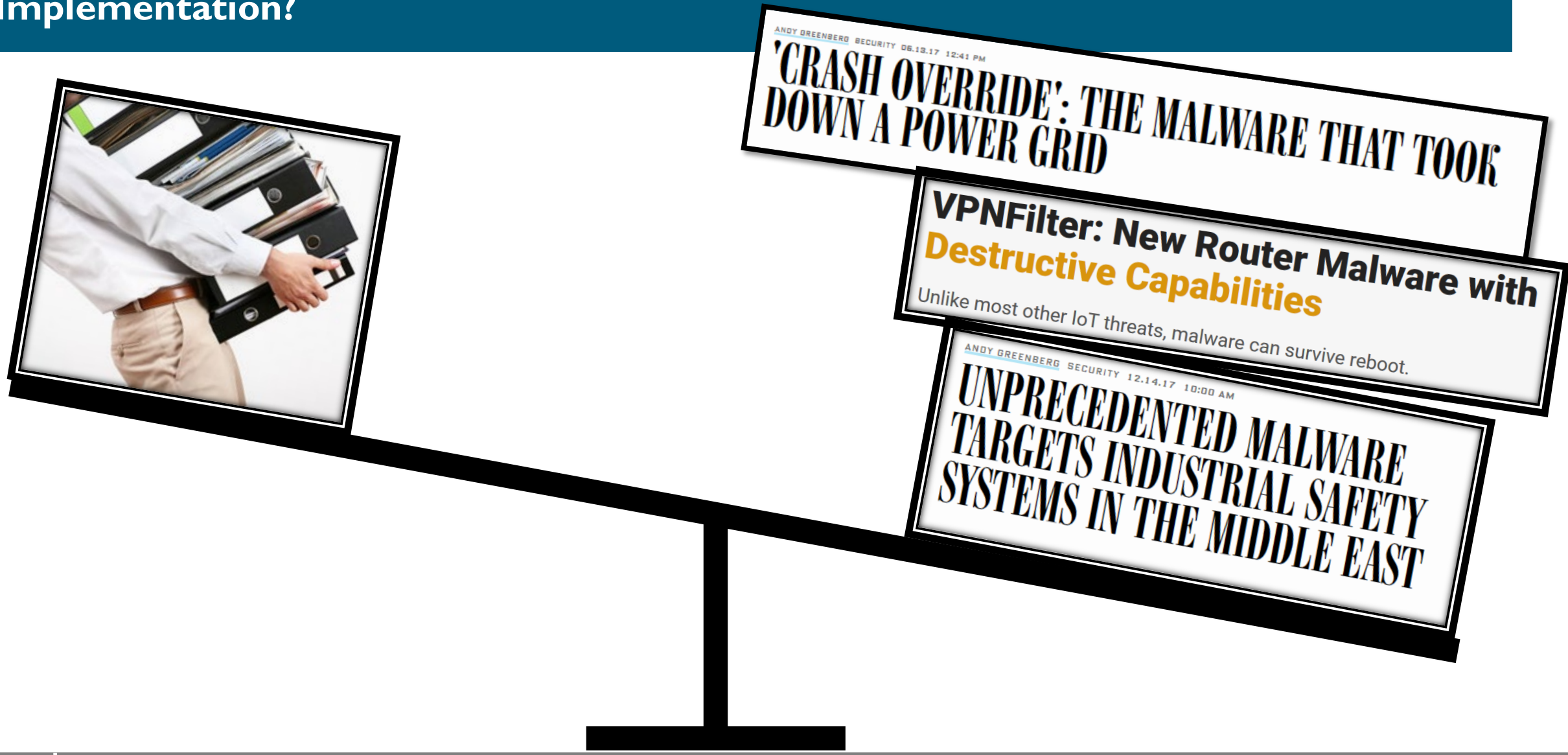
- Staggered Implementation with focus on wide area impact
- Asset owner standards development
- Peer evaluations during safe harbor period
- Financial enforcement capability
- Criteria based facility determination
- Systematic approach
- Non prescriptive
- Focus on Real Time operational impacts
- Inclusive of IT/OT assets
- Scope includes Cyber, Physical, Operations, and Personnel

Asset Owner Perspective

NERC CIP

CIP Lessons Learned and Fails

Implementation?



The CIP Versions

Culture of Compliance

- Commitment to Compliance:
  - Management culture that encourages compliance
  - Organizational chain allowing access to CEO/board
  - Established, formal program for internal compliance
  - Sufficient resources dedicated to the program
  - Tools and training sufficient to enable employees to comply
  - Systems and protocols for monitoring, identifying, and correcting possible violations
  - Compliance tied to performance objectives
  - Consequences for infractions

NERC CIP Lessons Learned

- Interpretation inconsistencies
- The stronger the internal controls program, the more violations
- Regulatory lag
- Potential innovation impacts
- TFE Process
- Fear of auditor greater than fear of attacker
- Programs can lean toward document driven compliance
- Predictive targets for adversaries
- Compliance / Audit economies demand funding and resources
- Need for funding and incentives

Asset Owner Perspective

Questions