

Critical Infrastructure Protection Standards Update

NPCC Fall Workshop
November 8, 2018

Agenda

- CIP Modifications SDT
- Incident Reporting and Response Planning
- Communications between Control Centers
- Low Impact
- Supply Chain Risk Management

CIP Modifications SDT

- IROL
 - CIP-002
 - CIP-003
 - CIP-014
- Virtualization
 - Posted last week for 45 day informal comment period
 - Redlines and comment form available

Incident Reporting and Response Planning

- CIP-008
- FERC Order 848
- “attempts to compromise”
- Definitions
 - Reportable Cyber Security Incident
 - Reportable Attempted Cyber Security Incident
- ICS-CERT & E-ISAC
- OE-417 leverage?

Incident Reporting and Response Planning

continued

- Reportable Time tables “determined”
 - 1 hour
 - 5 days
 - Information to report
- 25% industry approval
- Next posting
 - Nov 14
 - 15 day comment period

Communications between Control Centers

- CIP-012
- Pending FERC approval
- Control Center definition for this Standard
- Responsible Entities
 - BA, GOP, GO, RC, TOP, TO
- For “real-time data specification elements”
see TOP-003 and IRO-010

Communications between Control Centers

continued

Exemption - A Control Center that transmits to another Control Center Real-time Assessment or Real-time monitoring data pertaining only to the generation resource or Transmission station or substation co-located with the transmitting Control Center.

Communications between Control Centers

continued

R1

Shall implement, **except under CIP Exceptional Circumstances**, one or more documented plan(s) to mitigate the risks **posed by** unauthorized disclosure **and unauthorized** modification of Real-time Assessment and Real-time monitoring data while being transmitted between any applicable Control Centers.

Low Impact

- CIP-003
- Applicable January 1, 2020
- Transient Cyber Assets & Removable Media
- Identify / Inventory
 - Centralize / Decentralize

Low Impact

Security Considerations for TCA

- Processes and Evidence
- Important Bridges Airgaps
- Can leverage High / Medium
- Liability statement
 - Cannot transfer risk
 - Software / firmware patches vs service agreement
- If Entity doesn't approve of vendor methods or software?

Supply Chain Risk Management

- CIP-013, CIP-005 and CIP-010
- FERC Approved
- Next presentation

Questions



NERC

NORTH AMERICAN ELECTRIC
RELIABILITY CORPORATION

Supply Chain Update

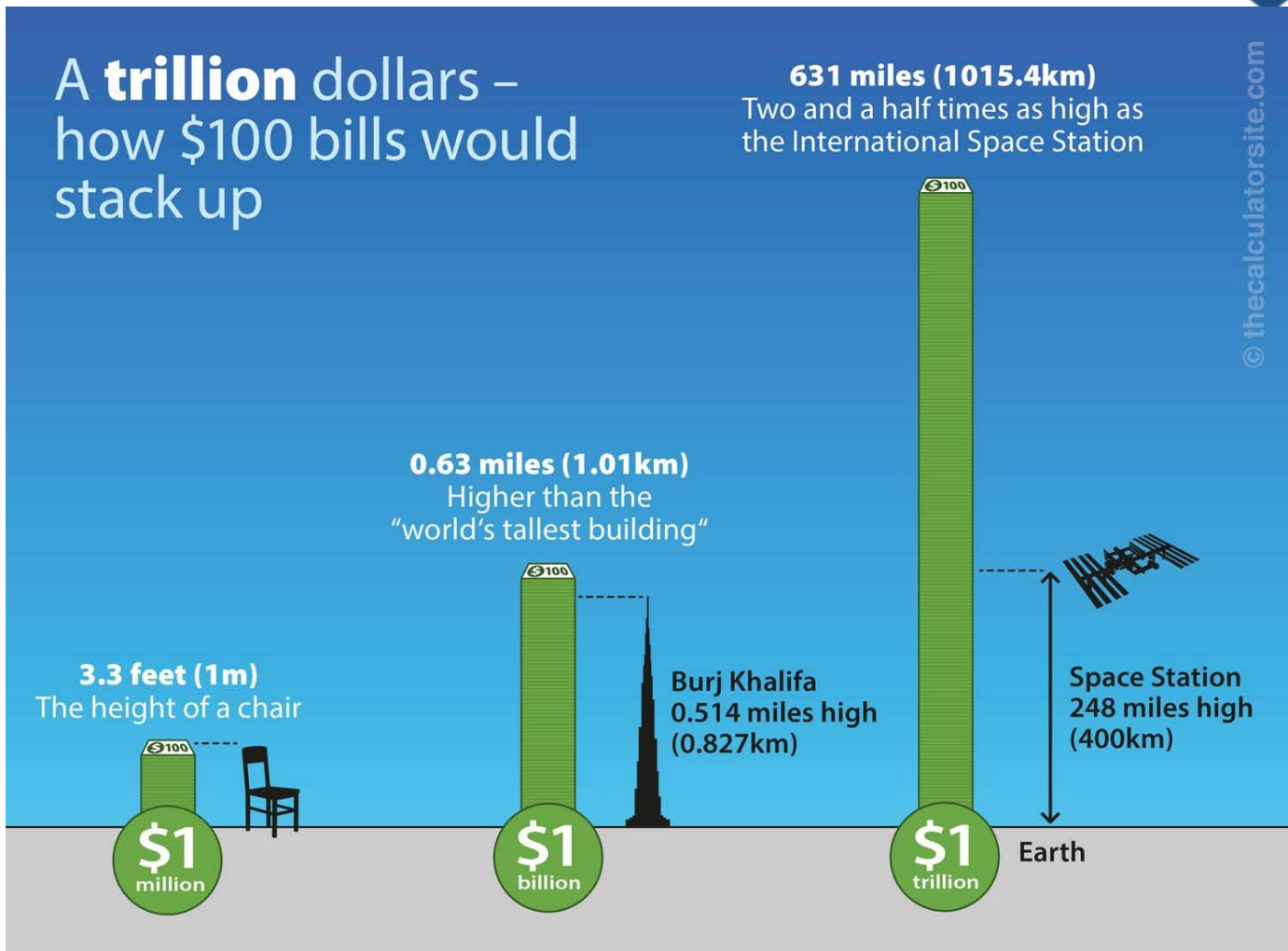
Daniel Bogle, Senior CIP Assurance Advisor, Compliance Assurance
NPCC Compliance Workshop
November 8, 2018

RELIABILITY | ACCOUNTABILITY



- Ransomware attacks every 40 seconds (2016) – Kapersky
- Business ransomware demands averaged between \$500 – \$2,000 dollars. – Datto
- In 2019, Ransomware attacks expected to be every 14 seconds.
- Ransomware is costing businesses more than \$75 billion per year. – Datto
- Predicted that cybercrime will cost the world \$6 trillion annually by 2021, up from \$3 trillion in 2015. - Cybersecurity Ventures

How much is \$3 trillion?



Source: The Calculator Site

- Background

- FERC issued Order No. 829 on July 21, 2016
- NERC Board Approved the Standard in August 2017
- Standard filed in September 2017
- FERC approved Final Rule October 18, 2018

- Status

- Final ballot
 - CIP-013-1 – 84.2%
 - CIP-005-6 – 88.8%
 - CIP-010-3 – 81.4%

- NERC created a supply chain standard webpage
- Critical Infrastructure Protection Committee (CIPC) to establish advisory task force
 - Advise on activities to support standard implementation
 - Develop schedule for webinars, workshops, and technical conferences in coordination with NERC and the Regional Entities
 - Document existing risks and develop security guidelines
- NERC and Regions to conduct small group advisory sessions
- NERC and Regions to offer outreach and readiness evaluations

- NERC used EPRI to conduct risk study
 - Assessment of product/manufacturer types used on the Bulk Electric System (BES)
 - Analysis & applicability to BES Cyber Assets
 - Analysis of best practices and standards in other industries to mitigate supply chain risks
 - Analysis of generalized vendor practices and approaches used to mitigate supply chain risks
- NERC to recruit industry experts and vendors to participate in supply chain risk study
- E-ISAC to engage Department of Energy and Department of Homeland Security to explore information sharing opportunities and future supply chain risk assessment activities

- Substation Networking Equipment
 - Two Vendors / 55%
- BES Cyber Systems Operating System
 - One Vendor / 87%
- EMS Vendors
 - Two Vendors / ~60%
- Remote Terminal Unit
 - No vendor more than 20% of market

- NERC and E-ISAC to continue utilizing NERC Alerts to communicate supply chain risks
- E-ISAC including supply chain risk topic in GridEx IV
- NERC to capture supply chain standard resources on webpage
- NERC and Regions to include supply chain topic at planned workshops and seminars in 2018
 - NERC to conduct additional webinars and technical conferences

- ERO Enterprise endorsed Implementation Guidance
 - CIP-013-1-R1-R2-R3 Implementation Guidance
 - Based on April 2017, Draft 2 of Standard
 - CIP-010-3 R1.6 Software Integrity and Authenticity
 - NATF Initiated

- Seven entities across all Regions except for SPP-RE
- Common questions / concerns
 - 12 month versus 18 month implementation
 - Addition of low impact BES Cyber Systems, EACMS, PACS
 - Large number of vendors to assess
 - One entity claimed over 20,000
 - Validation of software
 - Periodical auditing of vendors required by Standard?
 - Contract negotiations – Evidence required to demonstrate compliance?
 - Entity shall develop a plan, and provide evidence that the plan is implemented
 - “Vendor” is not defined term
 - CIP Standards impacted (CIP-013, CIP-005, and CIP-010)

- Additional Small Group Advisory Sessions?
- Analysis on effectiveness
- Department of Homeland Information and Communications Technology (ICT) Supply Chain Task Force
 - Part of newly established National Risk Management Center



Questions and Answers



2018 NPCC Fall Compliance & Standards Workshop

NAGF Overview and Update

Wayne Sipperly
NAGF Executive Coordinator
wsipperly@generatorforum.org

Agenda



- **NAGF Overview**
- **Collaboration: Groupsite**
- **NAGF Working Groups and Members**
- **Recent Activities**
- **How to join the NAGF**
- **Questions**

Who/What is the NAGF?



The NAGF is an independent, member-driven, non-profit organization of generator owners and operators, focused on NERC and other grid reliability issues.

The NAGF's mission is to promote the safe, reliable operation of the generator segment of the bulk power system through generator owner and operator collaboration with others who have a vested interest in the reliable operation of the bulk power system.

NAGF Value Proposition



Helping electric generator owners and operators to successfully navigate the changing energy sector, with a focus on reliability, resiliency and the regulatory environment.

*The NAGF is an independent, member driven organization whose collective knowledge and expertise conveys significant influence to regulators and the industry. The NAGF communicates the technical capabilities, constraints, and economics of generator equipment to inform and **help guide reliability policy**. The NAGF provides member companies with multiple information resources and open source peer collaboration to address the challenging issues facing the industry.*

Key NAGF features:

- *Generator technology and ownership model agnostic.*
- *Multiple information sharing resources for our members.*
- ***Regulatory policy influence for the generation sector.***

Collaboration: Groupsite

[SUMMARY](#)[COMMUNICATE ▾](#)[SHARE ▾](#)[NETWORK ▾](#)[WORKING GROUPS ▾](#)[MORE ▾](#)[MANAGER ▾](#)[MY SETTINGS ▾](#)[HELP ▾](#)Notifications **3** [Edit](#)

Everything ▾

SEARCH

Go

Welcome to the North American Generator Forum

The North American Generator Forum (NAGF) was founded in 2009 as a vehicle for utility and non-utility owned generator owners and/or operators to address issues related to registration, compliance, standards development and other NERC-related topics. In 2013, the North American Generator Forum, Inc. became a non-profit, dues-based corporation.

We provide entities who are generator owners and operators in North America a means to collaborate and communicate with FERC, NERC, the Regional Entities, the Canadian Provinces and other organizations with missions similar to ours, with the ultimate goal of improving the reliability of the bulk power system.

More information is available at: <http://generatorforum.org/>

REQUEST TO JOIN BY CLICKING HERE

THIS GROUP CONSISTS OF

[Edit](#) **504**

Group
Members
you can
connect with

**222**

Discussions
you can
join

**606**

Files
you can
download

UPCOMING EVENTS

[Edit](#) 

Low Impact Procedure Sharing ...
Monday, 12:30PM - 1:30PM EST
Telecon/Online Mtg



Standard Review Team
Wednesday, 10:00AM - 11:00AM CST
Conference Call

RECENT ACTIVITY**ALL**[DISCUSSIONS](#)[DISCUSSIONS](#)[NETWORK](#)[MORE ▾](#) [Edit](#)

Show: [All](#) | [Today](#) | [This Week](#) | [Since My Last Update](#) (Digest)



Aaron F. joined the group
by Aaron F. about 5 hours ago

[Welcome him](#)[Endorse him](#)

NAGF Working Groups



- Lessons Learned
- Peer Review
- Security Practices / CIP
- Standards Review Team
- Training
- Variable Resources

NAGF members



AMEA	DTE Energy	Indeck Energy	NRG	TVA
APGI	Duke Energy	Ingleside Cogen, LP	PG&E	Tri-State G&T
Ameren Missouri	E.ON	Invenergy	Pattern Gulf Wind	TEP
American Electric Power	EDP Renewables	KCP&L	Pattern Energy Group	US SBU
AECI	ENGIE	Lewis County PUD	Penobscot Energy	US BR
Austin Energy	Entergy	MMWEC	PSGC	Vistra Energy
Avista Corp	Essential Power	MEAG Power	Santee Cooper	WEC Energy Group
Basin Electric Power	EthosEnergy	MidAmerican Energy	SCE&G	Westar Energy
Black Hills Corporation	Exelon Generation	Minnesota Power	Southern Company	Xcel Energy
Braintree Electric Light	First Energy Corp.	NAES Corporation	Southwest Generation	
Capital Power	FMPA	NYP&A	SunPower	
CCI Rensselaer	FPL	NextEra Energy	Sunflower Electric	
Chelan County PUD	Great River Energy	North Carolina Electric	Talen Energy	
Dominion Energy	IL G&E/KY Utilities	NCPA	TECO	

NAGF's dual focus



- Compliance with existing Standards
 - ✓ “The here and the now”
 - ✓ Collaborative efforts
 - ✓ Best Practice sharing
 - ✓ Discussion boards, file cabinet, etc. on Groupsite

- Shaping policy
 - ✓ Helping paint the futurescape
 - ✓ Ensuring the unique perspective of the generation segment is understood and accounted for.
 - ✓ Improve “first time success” of new regulations

Recent Activities



➤ FERC Communications

➤ FERC Office of Electric Reliability (OER) Conference Calls:

- ✓ CIP Lessons Learned from FERC led audits
 - o Opportunity for FERC to share findings with NAGF
 - o <https://www.ferc.gov/legal/staff-reports/2017/10-06-17-CIP-audits-report.pdf>
- ✓ Inverters, Changing Resource Mix, and Variable Generation
 - o Opportunity for NAGF to transfer knowledge and share information with FERC staff.
 - o FERC is very interested in pairing energy storage with variable generation (solar/wind).
- ✓ Generator Siting Educational Discussion
 - o Opportunity for NAGF to transfer knowledge and share information with FERC staff.
 - o Generation build and location factors
 - o Grid Reliability Implications

Recent Activities

(continued)



➤ FERC Communications:

- ✓ Meeting with FERC Commissioners
 - NAGF representatives met with each of the FERC Commissioners and/or advisors at the FERC Office in Washington DC.
 - Items discussed:
 - ❖ Renewables and DG/DER integration with the BPS
 - ❖ Primary Frequency Response and non-synchronous resource impacts
 - ❖ Cyber Security
 - ❖ Resiliency
- ✓ FERC Technical Conference
 - 4 Discussion Panels:
 - ❖ The Changing ERO Enterprise, Standards, and Reliability
 - ❖ Advancing Reliability and Resilience of the Grid
 - ❖ Managing the New Grid
 - ❖ Addressing the Evolving Cybersecurity Threat

Recent Activities

(continued)



➤ NERC Communications:

- ✓ NAGF Survey Results shared with NERC:
 - o Gas Generation Supply
 - o NERC Reliability Guideline: Generating Unit Operations During Complete Loss of Communications.
 - o Generator Winter Weather Preparation.
- ✓ NAGF Standards Review Team (SRT) Working Group
 - o Submit comments as part of NERC Balloting and Commenting process
 - o Periodic Standard Reviews
 - o NERC Projects

Recent Activities

(continued)



➤ NERC Communications:

- ✓ NERC Gas Infrastructure Risk Workshop
 - o Discussed recommendations from *2017 NERC Special Reliability Assessment: Potential Bulk Power System Impacts Due to Severe Disruption on the Natural Gas System*
 - o Discussion centered on fuel assurance concerns for generators
 - o Next Steps:
 - ❖ NERC Planning Committee to form a task force to develop new Reliability Guide for including fuel assurance and fuel disruption risk into BPS planning studies
 - ❖ Possible SAR for enhancing NERC Reliability Standards to consider fuel assurance and fuel disruption risk in planning study requirements
 - ❖ Identify tools and resources to solve natural gas interoperability concerns
 - ❖ Enhance NERC GADS database to include fuel availability.

Recent Activities

(continued)



➤ **NERC Communications:**

- ✓ Inverter-based Resource Performance Task Force (IRPTF)
 - o NERC Reliability Guideline: BPS-Connected Inverter Based Resource Performance
- ✓ Continuing Work
 - o SAR for PRC-024 to resolve inconsistencies in Standard
 - o IRPTF to continue to develop guidance for inverter performance which can be written into Interconnection Agreements
 - o IEEE working on development of a new performance standard P2800 – Interconnection and Interoperability of Inverter-Based Resources Interconnecting with Associated Transmission Electric Power Systems
 - ❖ Will be the accompanying Standard to IEEE 1547 (Distribution-level inverters) but for BPS inverters

Recent Activities

(continued)



➤ NERC Communications:

- ✓ NAGF-ESIG Frequency **Response and Storage** Workshop
 - o Participants included DOE, FERC, NERC, NAGF, ISO/RTOs, ESIG and OEMs
 - o Focus on technical capabilities **and economics** of non-synchronous technologies and how to incorporate into energy/essential reliability services markets.
 - o Key take aways:
 - ❖ Continue to study capabilities of all technologies and how to make them work together
 - ❖ Identify market constraints that prevent some generation resources from utilizing their attributes
- ✓ NAGF/Resources Subcommittee Primary Frequency Response Webinars on November 13:
 - o 10:00 -11:30 – PFR from Steam Generation
 - o 2:00 – 3:30 – PFR from Simple-Cycle and Combined-Cycle

Recent Activities

(continued)



➤ **2018 NAGF Annual Meeting & Compliance Conference**

- ✓ NERC CEO Jim Robb Keynote Address
- ✓ Dual Track Presentations for O&P and CIP:
 - o Protection System Coordination – PRC-025, PRC-026, and PRC-027
 - o PFR Inner & Outer Loop Controls
 - o BAL-003 Update
 - o NAGF Supply Chain White Paper
 - o Project 2016-02 CIP Modifications
 - o CIP Low Impact Implementation Experience
 - o NPCC Physical and Cyber Security Outreach update

Recent Activities

(continued)



- **NAGF Cyber Security Supply Chain White Paper**
 - ✓ Process and Timeline
 - ✓ WP Highlights
 - Risk Based
 - Initial Risk Screen
 - Vendor Supply Chain Risk Assessment
 - Scorecard to document analysis
 - ✓ Coordination with NATF and others
 - ✓ Posted on the NERC Supply Chain Risk Mitigation Program website: <https://www.nerc.com/pa/comp/Pages/Supply-Chain-Risk-Mitigation-Program.aspx>

Recent Activities

(continued)



➤ NAGF Peer Review Program

- ✓ Modeled after the NATF program
- ✓ Initial Peer Review completed September 2018
- ✓ One 150MW Gas Peaking Facilities located in ERCOT
- ✓ Five (of 6 available) Focus Areas:
 - o Compliance
 - o Protection Systems and Maintenance
 - o Cyber and Physical Security
 - o Operations
 - o Modeling and Modeling Verification
- ✓ No Compliance Issues were identified
- ✓ A number of Recommendations were identified and are being considered by the host entity.

Joining the NAGF



Visit our website: <http://nagf.groupsite.com/>

Click on: **REQUEST TO JOIN BY CLICKING HERE**

-Or-

Send an email requesting membership to:
wsipperly@generatorforum.org

Q & A

Physical Security Outreach and Identified Trends

Pete Scalici, CHPP
Senior CIP Specialist

The NPCC PHYSICAL SECURITY OUTREACH ASSESSMENT PROGRAM



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

WHAT IS IT?

- A **FREE** program for NPCC registered entities
- **NO** connection with compliance or standards
- **NOT** judgmental
- **NO** down side for the entity
- Exchange of knowledge and information
- Cooperative effort to increase security and reliability

Physical Security

IS IT JUST GUNS, GATES AND GUARDS?
ONLY AMATEURS THINK SO!



Safety vs Security



THEY ARE NOT THE SAME!!



Risk



WHAT IS IT?

Is the Risk to the Grid or Your Business
Determine what YOUR risk is.
Acceptable levels of risk?



Vulnerability

- Assessments determine vulnerabilities
- Site specific enhancements
- Past incidents – learn from them
- Design Basis Threat
- VISA

Current Trends

COPPER THEFT IS STILL A BIG PROBLEM-

but is it really just copper theft?

- NEW ROUNDS OF VEHICULAR ATTACKS (Europe, NYC)
- SUICIDE BOMBERS
- ACTIVE SHOOTER/WORKPLACE VIOLENCE
- LACKADAISICAL ATTITUDE TOWARDS PHYSICAL SECURITY

UNTIL SOMETHING HAPPENS!!!

Security costs, it doesn't make money

- DRONE USAGE

Drones



- Right now laws as they exist support the drone operator.
- There is a lot of discussion on defense against drones but right now, there is little you can do.
- To change this, YOU, as industry, must let your elected representatives know your concerns and the need to have laws enacted so you can defend your sites.

Common Security Shortfalls

- Upkeep of fencing, gaps and holes
- Testing of security systems
- Integration with other departments (working in silos, lack of communication)
- Maintaining contact with Law Enforcement and other First Responders
- Vegetation Management around fence lines
- Poor placement of lighting that washes out cameras
- Lack of non-disclosure agreements
- Community Outreach Programs
- Old or outdated equipment (life cycles expired)

Information Sources

- NERC E-ISAC
- NYPD SHIELD- CTSHIELD@NYPD.ORG
- LOCAL JTTFs- FBI LOCAL OFFICES
- INFRAGUARD- FBI LOCAL OFFICES
- DHS HSINs

Contact Information

Due to extensive travel it is best to contact me
via e mail at this address:

pscalici@npcc.org



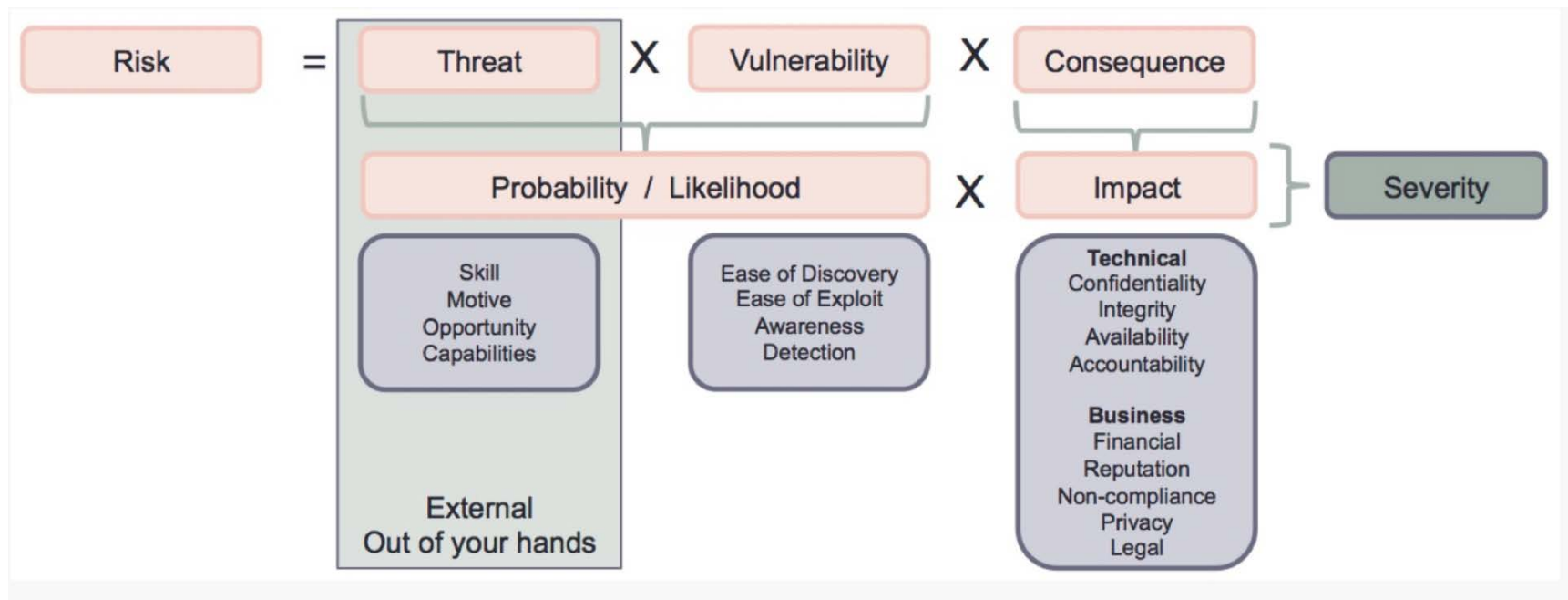


Cybersecurity Risks and Outreach

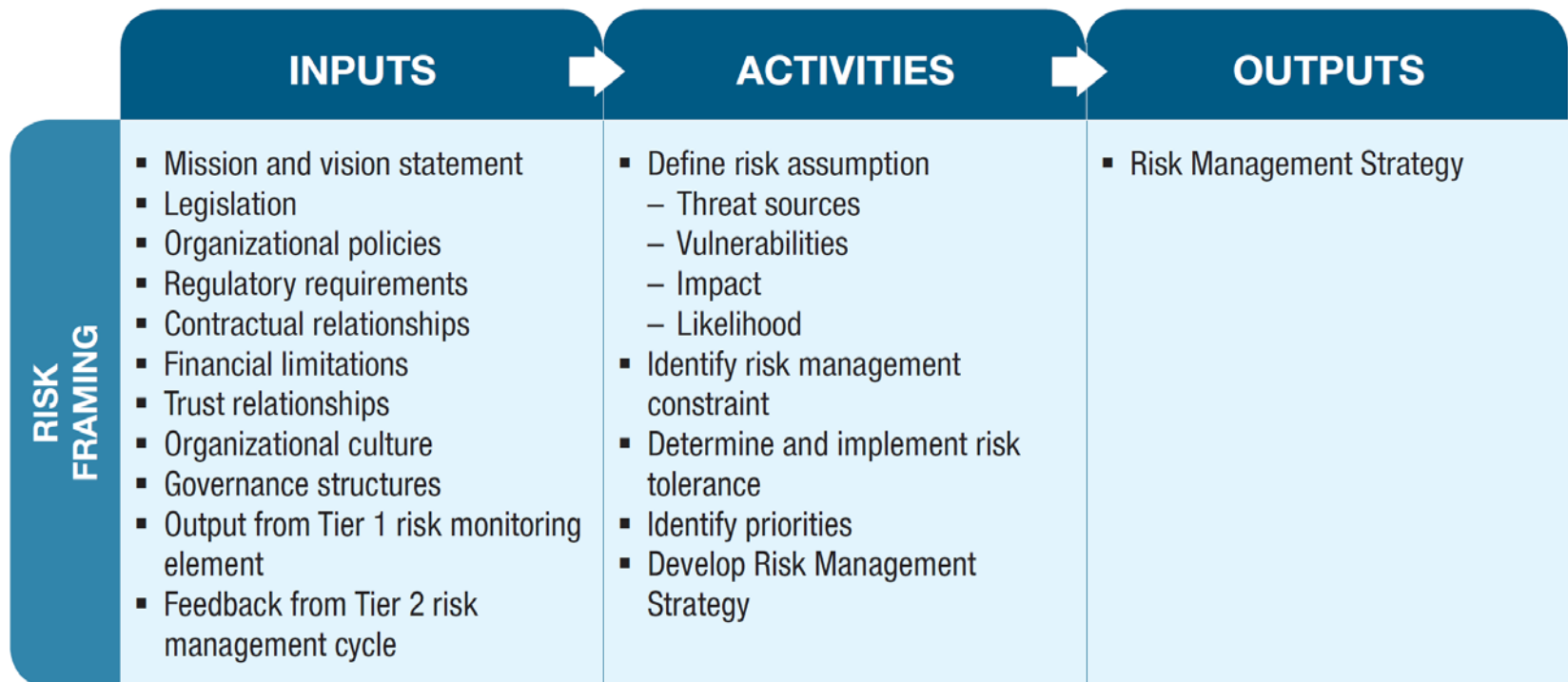
Jenifer Wallace Farrell, CISSP, CISA

Senior CIP Analyst

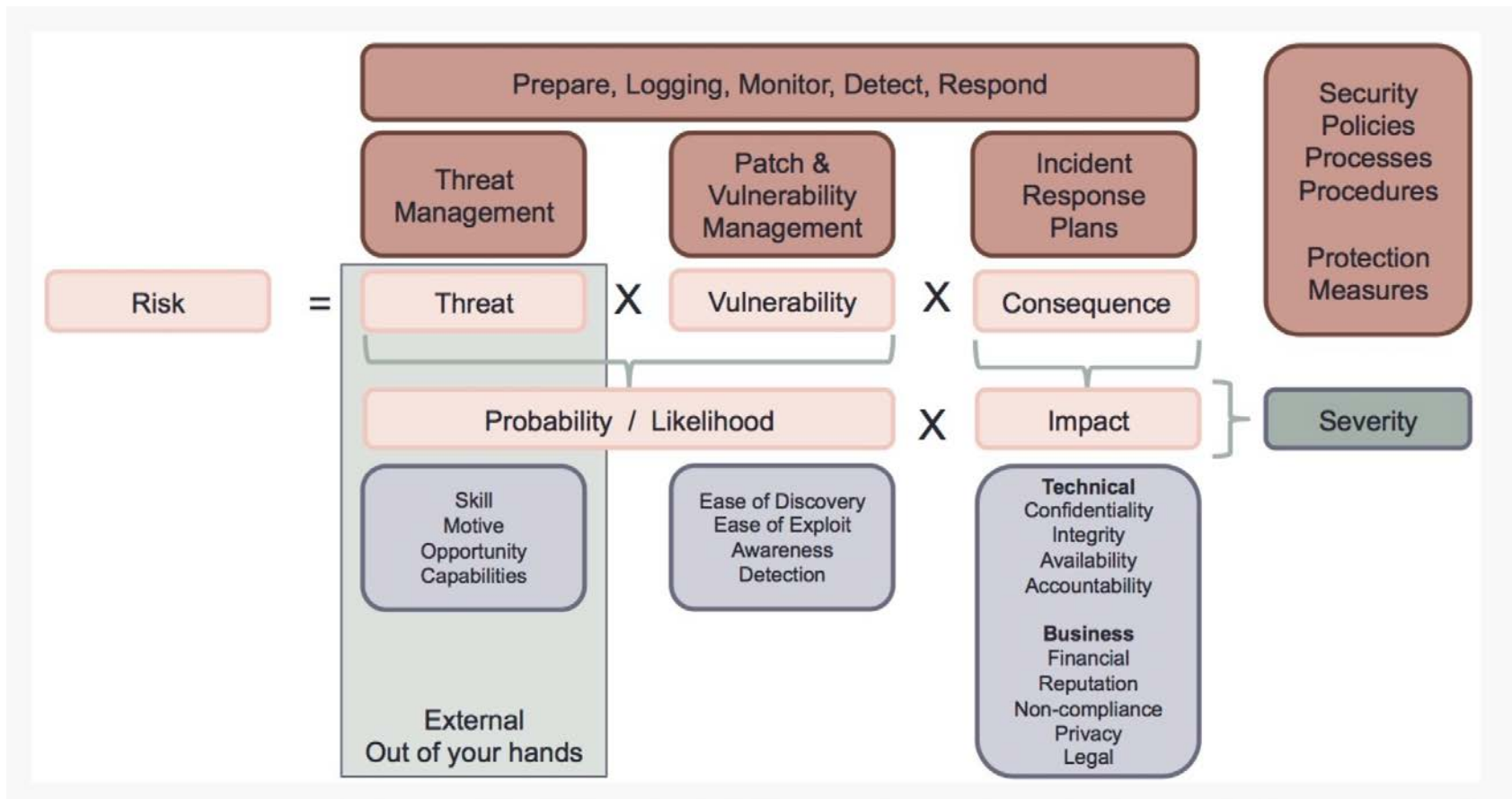
Risk



Risk Framing



Risk Management



Risk Management Process

- Resources:
 - <https://www.energy.gov/sites/prod/files/Cybersecurity%20Risk%20Management%20Process%20Guideline%20-%20Final%20-%20May%202012.pdf>
 - <https://ics-cert.us-cert.gov/content/overview-cyber-vulnerabilities>
 - <https://securityintelligence.com/simplifying-risk-management/>

Cybersecurity Controls

- Center for Internet Security
 - CIS Controls
 - CIS Benchmarks
 - MS-ISAC Advisories
 - Risk Assessment Method
 - Automated Assessment
- <https://www.cisecurity.org/cybersecurity-tools/>

CIS Controls

BASIC CIS Controls

1) Inventory and Control of Hardware Assets

2) Inventory and Control of Software Assets

3) Continuous Vulnerability Management

4) Controlled Use of Administrative Privileges

5) Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

6) Maintenance, Monitoring, and Analysis of Audit Logs

CIS Controls

Foundational CIS Controls

7) Email and Web Browser Protections

8) Malware Defenses

9) Limitation and Control of Network Ports, Protocols, and Services

10) Data Recovery Capabilities

11) Secure Configuration for Network Devices, such as Firewalls, Routers, and Switches

12) Boundary Defense

13) Data Protection

14) Controlled Access Based on the Need to Know

15) Wireless Access Control

16) Account Monitoring and Control

CIS Controls

Organizational CIS Controls

17) Implement a Security Awareness and Training Program

18) Application Software Security

19) Incident Response and Management

20) Penetration Tests and Red Team Exercises

CIS Control Resources

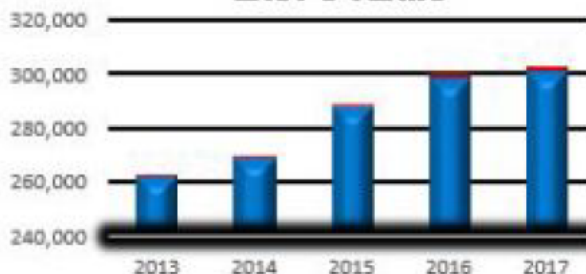
- Learn more about the CIS organization:
 - <https://www.cisecurity.org/about-us/>
- Download Critical Security Controls V7:
 - <https://learn.cisecurity.org/20-controls-download>
- Other resources:
 - <https://www.auditscripts.com/free-resources/critical-security-controls/>

FBI IC3 2017 Internet Crime Report



Important Stats

**IC3 COMPLAINTS
LAST 5 YEARS**



**# Of Complaints
Reported Since
Inception ('00)
4,063,933**

Approximately 284,000
Average Complaints
Received Each Year

\$1.42 Billion
Victim Losses in 2017

Over 800
Average Complaints
Received Per Day

Business Email Compromise

- Targets
 - Businesses that work with foreign suppliers
 - Businesses that perform wire transfers
- Compromise Techniques
 - Social Engineering
 - Computer Intrusion

Ransomware

- Targets
 - Businesses and specific employees
- Techniques
 - Spear phishing
 - Remote Desktop Protocol

Tech Support Fraud

- Targets
 - All individuals
- Techniques
 - Telephone calls
 - Pop-up and locked screens
 - Search engine advertising
 - URL hijacking/typosquatting
 - Phishing emails

IC3 Report

- FBI IC3 2017 Internet Crime Report
 - https://pdf.ic3.gov/2017_IC3Report.pdf

US-Cert Alert (TA18-074A)

Threat Actor tactics, techniques, and procedures:

- Spear-phishing emails (from compromised legitimate account)
- Watering-hole domains
- Credential gathering
- Open-source and network reconnaissance
- Host-based exploitation, and
- Targeting industrial controls system (ICS) infrastructure

US-Cert Alert (TA18-074A)

Detection and Prevention Measures

- Log collection
- Compare IP addresses, domain names, and file hashes to those in IOC package
- <https://www.us-cert.gov/ncas/alerts/TA18-074A>

Threat Feeds / Podcasts / Tools

- E-ISAC
 - <https://www.eisac.com/resources/bulletins>
- SANS – Internet Storm Center
 - <https://isc.sans.edu/threatfeed.html>
 - <https://isc.sans.edu/block.txt>
 - <https://isc.sans.edu/podcast.html>
- Free Online Tools for Looking up Potentially Malicious Websites
 - <https://zeltser.com/lookup-malicious-websites/>

Awareness

- Demo: The Ukraine Event In a Box – SANS ICS Security Summit 2017
 - <https://youtu.be/sHv3e8-dm5A>
- Demo: Social Engineering – Vishing
 - <https://youtu.be/lc7scxvKQOo>

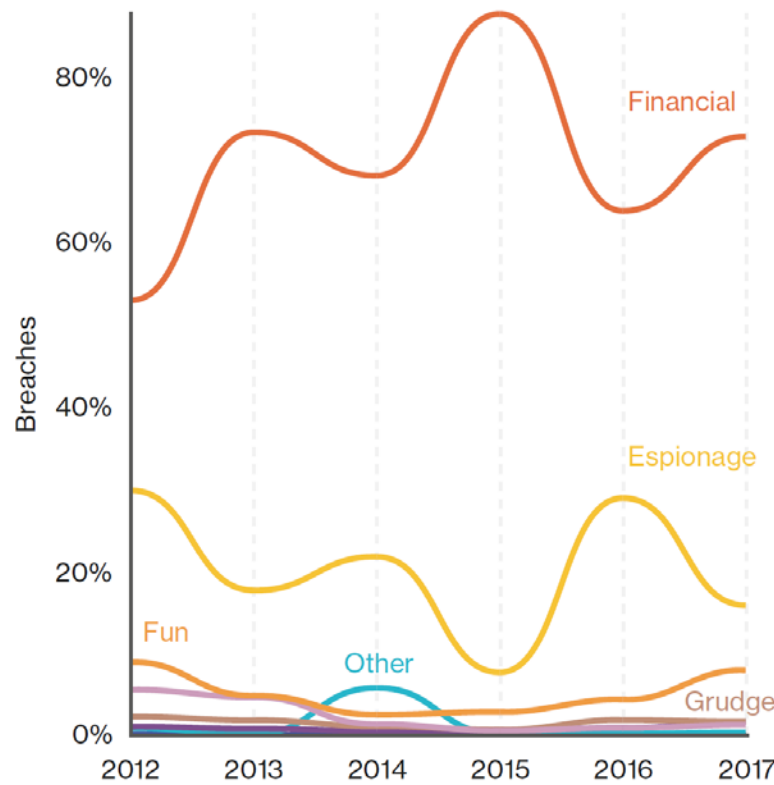
Verizon Data Breach Investigations Report

Reference

- Verizon. (2018, May 16). Verizon 2018 Data Breach Investigations Report. Retrieved from Verizon:
<http://www.verizonenterprise.com/verizon-insights-lab/dbir/>

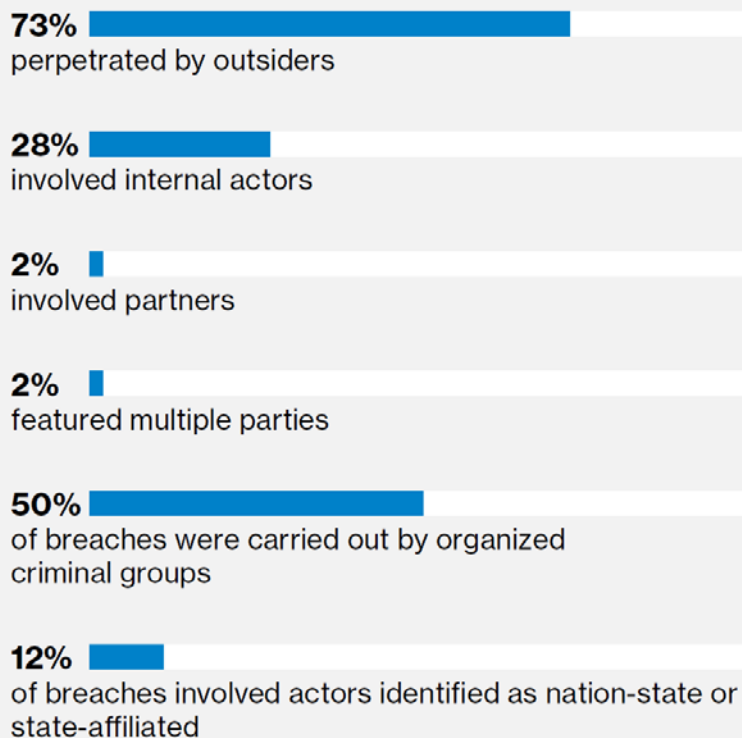
Verizon Data Breach Investigations Report

Actor motives in breaches



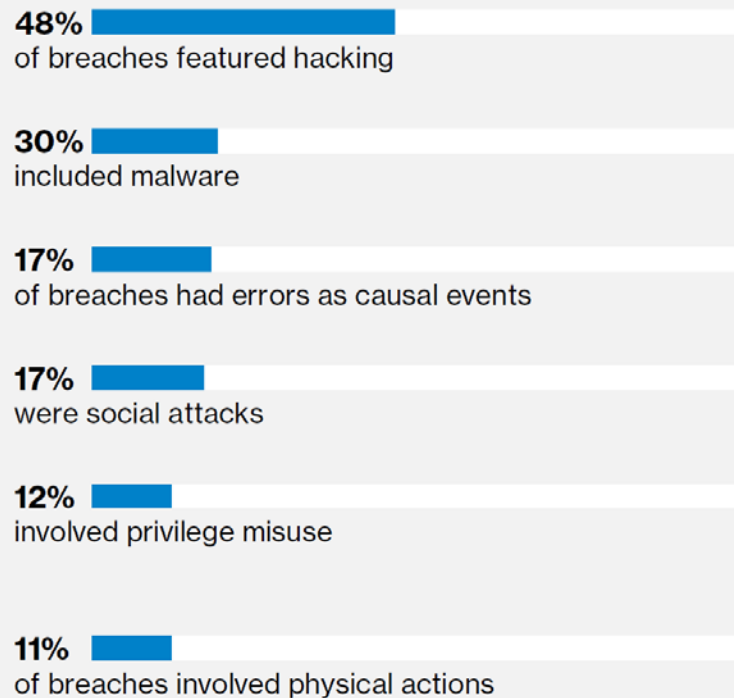
Verizon Data Breach Investigations Report

Who's behind the breaches?



Verizon Data Breach Investigations Report

What tactics are utilized?



Verizon Data Breach Investigations Report

What are other commonalities?

49% 
of non-POS malware was installed via malicious email¹

76% 
of breaches were financially motivated

13% 
of breaches were motivated by the gain of strategic advantage (espionage)

68% 
of breaches took months or longer to discover

Verizon Data Breach Investigations Report

Top 20 action varieties in breaches

Use of stolen credentials (hacking)

399

RAM scraper (malware)

312

Phishing (social)

236

Privilege abuse (misuse)

201

Misdelivery (error)

187

Use of backdoor or C2 (hacking)

148

Theft (physical)

123

Phishing

- Training / Awareness
 - Test your ability to detect a campaign, identify infected hosts, look for existence of data exfiltration.
- Identify the clickers
 - Give them a tablet or sandboxed OS
 - Segment clients from critical assets
 - Use strong authentication (i.e., more than a keylogger is needed to compromise)

Information Handling

- What information is provided to Vendors
 - Full databases (troubleshooting)
 - Obfuscate data where possible or use test data
 - Ensure vendor knows if data is sensitive
 - Logs
 - Redact usernames and passwords
 - Passwords
 - Have secure method, don't keep a full spreadsheet of unencrypted passwords within your vendor's portal

NPCC Cyber Outreach

- Voluntary program
- 1-2 day Cyber Assessment
 - High level network architecture review
 - CIS Critical Security Controls review
 - Onsite debrief and confidential non-public report
- Compliance with CIP Standards is NOT reviewed as part of this assessment

Questions?

Jenifer Wallace Farrell, CISSP, CISA

Senior CIP Analyst

jwallace@npcc.org

PRC-027-1

Coordination of Protection Systems for Performance During Faults

A stylized white 'H' logo is positioned on an orange background. The 'H' is composed of two vertical bars and a horizontal bar, with a small gap in the top left of the first vertical bar.

10.08.18

PRC-027-1 Requirements

-All reference material for this presentation was pulled from NERC PRC-027-1 Standards Subject to Future Enforcement.

Applicability

- Transmission Owners (TOs),
- Generator Owners (GOs), and
- Distribution Providers (DPs) with Protection Systems installed to detect and isolate Faults on BES Elements

Purpose

- To maintain the coordination of Protection Systems installed to detect and isolate Faults on Bulk Electric System (BES) Elements, such that those Protection Systems operate in the intended sequence during Faults.

Effective Date: 10/1/2020

- PRC-001-1.1(ii) will be retired on this effective date

Key Points:

- The coordination of Protection description is from the pending revision of IEEE Standard C37.113-1999 (Reaffirmed: 2004), Guide for Protective Relay Applications to Transmission Lines, which reads:

“The process of choosing current or voltage settings, or time delay characteristics of protective relays such that their operation occurs in a specified sequence so that interruption to customers is minimized and least number of power system elements are isolated following a system fault.”

- The Standard Supplement Material points out that a single definition or criterion for “Protection System coordination” is **not** practical.



PRC-027-1 Requirements Continued

R1. Must be developed and documented by 10/1/20

Key Points:

- For GOs and DPs will need to request fault current data from Transmission Planners, Planning Coordinators, or Transmission Owners.
- Short-Circuit Model Reviews could include but are not limited to:
 - A review of applicable BES line, transformer, and generator impedances and fault currents.
 - A review of the network model to confirm the network in the study accurately reflects the configuration of the actual System, or how the System will be configured when the proposed relay settings are installed.
 - A review, where applicable, of interconnected Transmission Owner, Generator Owner, and Distribution Provider Information.
- A review of developed Protection System settings is any systematic process of verifying the developed settings meet the technical criteria of the entity (i.e.. Peer reviews, automated checking programs, and entity-developed review processes).
- Establish a process for communicating protection system changes and reviews with neighboring entities (TOs, GOs, and DPs).
- Establish a process for verifying any identified coordination issues are resolved prior to implementation.
- Requirement R1 part 1.3 does not apply to Protection Systems applied on individual dispersed generation resources. It does apply to Protection Systems applied on the BES elements that electrically join Facilities owned by separate functional entities.

- R1.** Each Transmission Owner, Generator Owner, and Distribution Provider shall establish a process for developing new and revised Protection System settings for BES Elements, such that the Protection Systems operate in the intended sequence during Faults. The process shall include: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*
- 1.1.** A review and update of short-circuit model data for the BES Elements under study.
 - 1.2.** A review of the developed Protection System settings.
 - 1.3.** For Protection System settings applied on BES Elements that electrically join Facilities owned by separate functional entities (Transmission Owners, Generator Owners, and Distribution Providers), provisions to:
 - 1.3.1.** Provide the proposed Protection System settings to the owner(s) of the electrically joined Facilities.
 - 1.3.2.** Respond to any owner(s) that provided its proposed Protection System settings pursuant to Requirement R1, Part 1.3.1 by identifying any coordination issue(s) or affirming that no coordination issue(s) were identified.
 - 1.3.3.** Verify that identified coordination issue(s) associated with the proposed Protection System settings for the associated BES Elements are addressed prior to implementation.
 - 1.3.4.** Communicate with the other owner(s) of the electrically joined Facilities regarding revised Protection System settings resulting from unforeseen circumstances that arise during implementation or commissioning, Misoperation investigations, maintenance activities, or emergency replacements required as a result of Protection System component failure.
- M1.** Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation to demonstrate that the responsible entity established a process to develop settings for its Protection Systems, in accordance with Requirement R1.



PRC-027-1 Requirements Continued

Must be developed and documented by 10/1/20

Key Points:

- For R2 (Coordination Study)....For all R2 options, the 6 calendar year time frame to perform either the Option 1 study or the Option 2 study **starts on 10/1/20. It expires on 12/31/26.**
- If you choose Option 1: Initial protection system coordination study **must be complete by 12/31/26.** As soon as the initial study is done, you **must follow 6 calendar years for updates.**
- However, if you choose Option 2: **Must complete the establishment of the initial fault current baseline by 10/1/20.** Then, the comparison to the present fault current values and any needed Protection System Coordination **Study must both be done by 12/31/26; then follow the 6 calendar years.**

R2. Each Transmission Owner, Generator Owner, and Distribution Provider shall, for each BES Element with Protection System functions identified in Attachment A: *[Violation Risk Factor: Medium] [Time Horizon: Long-term Planning]*

- Option 1: Perform a Protection System Coordination Study in a time interval not to exceed six-calendar years; or
- Option 2: Compare present Fault current values to an established Fault current baseline and perform a Protection System Coordination Study when the comparison identifies a 15 percent or greater deviation in Fault current values (either three phase or phase to ground) at a bus to which the BES Element is connected, all in a time interval not to exceed six-calendar years;¹ or,
- Option 3: Use a combination of the above.

PRC-027-1 Requirements Continued

Must use the developed process from R1 at all times after 10/1/20

Key Points:

- For GOs and DPs will need to request fault current data from Transmission Planners, Planning Coordinators, or Transmission Owners.
- Reviews could included but are not limited to:
 - A review of applicable BES line, transformer, and generator impedances and fault currents.
 - A review of the network model to confirm the network in the study accurately reflects the configuring of the actual System, or how the System will be configured when the proposed relay settings are installed.
 - A review, where applicable, of interconnected Transmission Owner, Generator Owner, and Distribution Provider Information.

- R3.** Each Transmission Owner, Generator Owner, and Distribution Provider shall utilize its process established in Requirement R1 to develop new and revised Protection System settings for BES Elements. *[Violation Risk Factor: High] [Time Horizon: Operations Planning]*
- M3.** Acceptable evidence may include, but is not limited to, dated electronic or hard copy documentation to demonstrate that the responsible entity utilized its settings development process established in Requirement R1, as specified in Requirement R3.

PRC-027-1 Concepts

- Establish Documented protection philosophies for how you set your relay elements (21, 50, 51, and 67).
 - You may need to establish multiple philosophy documents depending on the variability in your systems.
- Establish a Documented Protection System Setting Change Process.
- Verify and Document that in-service Protection System Settings in the field match the record copy you will utilize for your coordination studies & analysis.
- Verify and Document that your Short-Circuit Model aligns with the field installations.
- Establish and Document a Communication Protocol with all of your neighboring Entities that interface your BES elements.





WWW.IRONHOUSEINC.COM

Compliance Portal (CDAA) and CMEP Tool Update

Scott Nied

snied@npcc.org

CDAA

- Stands for what?
- Maintain!
- Entity Administrator
- Primary Compliance Contacts (PCCs) are used for:
 - NERC Alerts
 - NPCC Compliance Webinars/Emails
 - Compliance matters
- Updated User Guide Posted

CDAA Questions?

- Send to jwang@npcc.org
- Desk Number: 212-205-7068

CMEP Technology Tool

- What this presentation will address:
 - What is it?
 - When can the ERO expect it going live?
 - Can a registered entity participate and provide feedback?

CMEP Technology Tool

- All compliance related activities will now be consolidated into the CMEP tool
 - One tool amongst all regions
 - Self-Reports, Audits, Self-Certifications, Mitigation Plans
- Will replace all regional compliance portals (CDAA, WebCDMS)
- Will replace NPCC's CITS (Compliance Information Tracking System)

Timeline – Process Harmonization

Process (No Stakeholders yet)	Start	End (Vendor can Implement)	Status
Self-Reports and Self-Logging	March 2018	June	UAT
Enforcement Processing (PNC, CE/FFT, Disposition and Settlement)	May	July	Building
Mitigation Plan Creation and Tracking	May	September	Building
Self-Certification, Periodic Data Submittals, TFE	September	November	Process Harmoni
Compliance Audit and Spot Check; Compliance Investigations, Complaints	October	March 2019	Process Harmoni
Compliance Planning (Risk Elements, IP, IRA, ICE, COP)	November	April 2019	

CMEP Tool – Entity Participation

- Each Process Harmonization will identify Regional differences. Real Example:
 - Self Logging Entities :
 - Are there issues submitting self-logs through an excel spreadsheet? Good/Bad? Why/Why Not?
 - What are your thoughts on submitting issues ad hoc versus within the quarterly timeframe?
 - Is there a preference? Why?
- Testing/Deployment will involve stakeholder feedback before going operational

CMEP Tool – Canadian Provinces

- What types of data segregation will need to be implemented related to International Entities?
- NERC welcomes Canadians to use the tool
- Carve outs can be discussed by Province
- Data Centers in U.S. and Canada?
- FERC will not get Canada data

CMEP Tool – Unanswered

- Deployment – will the tool be released simultaneously or staggered?
- CEI data within the tool?

CMEP Tool Questions?

- Send to jwang@npcc.org
 - Desk Number: 212-205-7068
- Want to Participate? Go through the NERC CCC AWG
 - consistency@nerc.net
 - Lunch Time! See you at 1 PM.