Critical Energy Infrastructure and OT Security (NERC CIP and TSA Security Directives)

NARUC Cybersecurity Training for State Regulatory Commissions
March 23, 2023

Introduction

- Former utility staff (telecommunications, water & electric)
- First NERC CIP auditor in the US
- Former Manager, CIP Audits and Investigations - WECC
- Drafter of NERC CIP standards and formal interpretations
- NERC CIP Supply Chain Working Group contributor
- Former Principal Investigator US DOE National Electric Sector Cybersecurity Organization
- EnergySec Founder, Former Director, Former Instructor and President Emeritus
- SANS ISC456 Instructor: Essentials for NERC Critical Infrastructure Protection
- US Coordinator, Centro de Ciberseguridad Industrial (CCI)
- Cybersecurity Advisory Team for State Solar, NARUC/NASEO
- National Telecommunications and Information Administration (NTIA) and Idaho National Lab (INL) Software Bill of Materials (SBOM) Energy POC Stakeholders
- DOE Solar Energy Technology Office (SETO) and National Renewable Energy Lab (NREL) Industry Advisory Board (IAB) for the Securing Solar for the Grid (S2G)
- Advisor to multiple industrial hardware and software vendors
- GCIP, CISA, CRISC, CISSP-ISSAP, SSCP, NSA-IAM, CVI, TCP, SCP

OT CYBERSECURITY BASICS

OT Security - Sectors










pmiller@amperesec.com | @patrickcmiller | +15032721414 | www.amperesec.com

IT vs. OT

IT = Information Technology

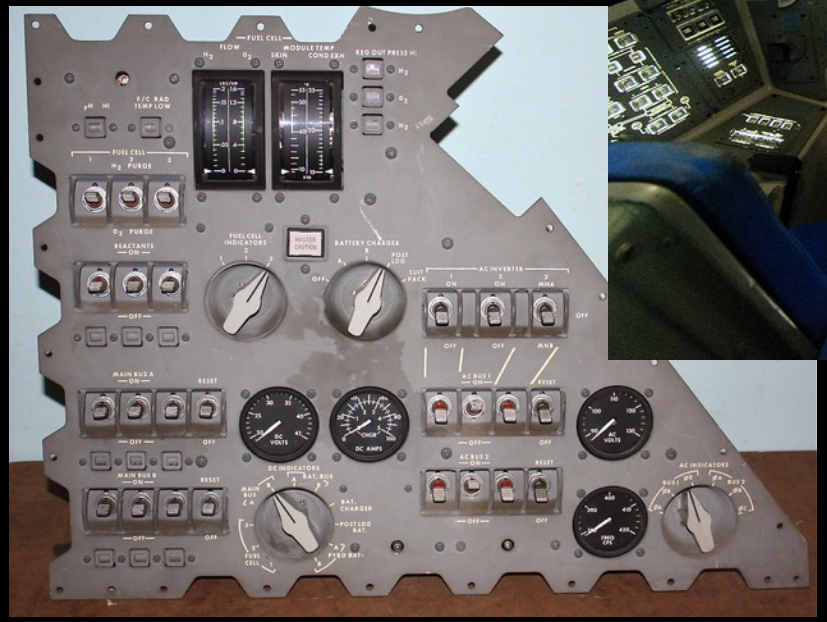
Ephemeral: data at rest, data in motion, data in use – electronic/virtual

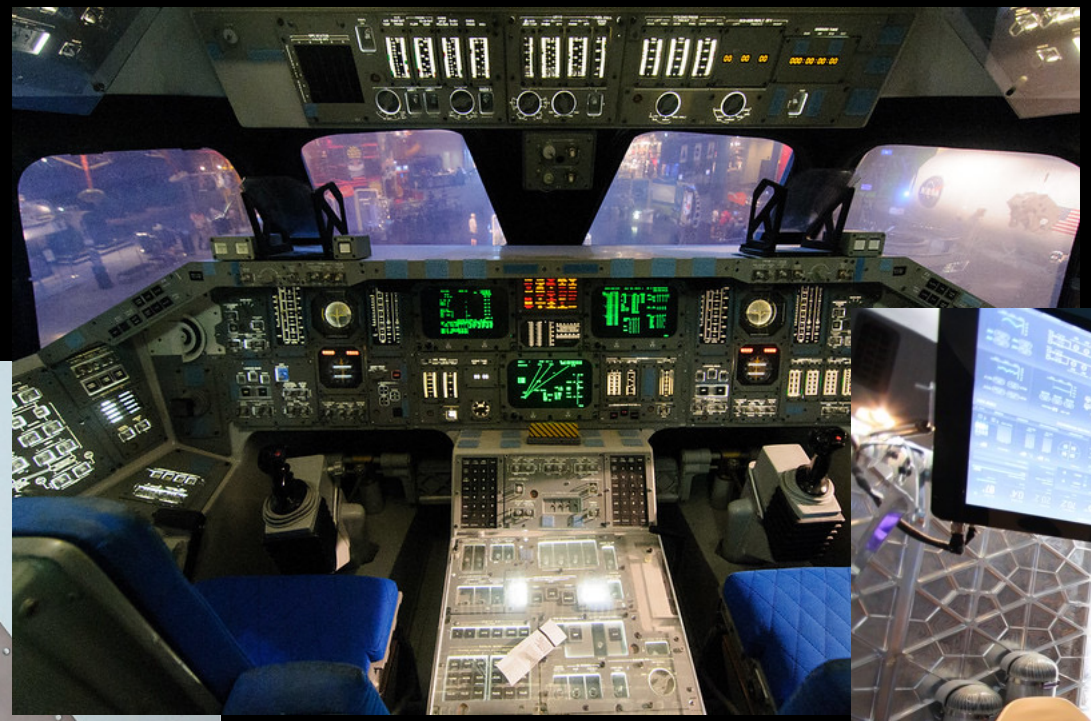
OT = Operational Technology

Physical: Data and systems that do something in the physical world – kinetic

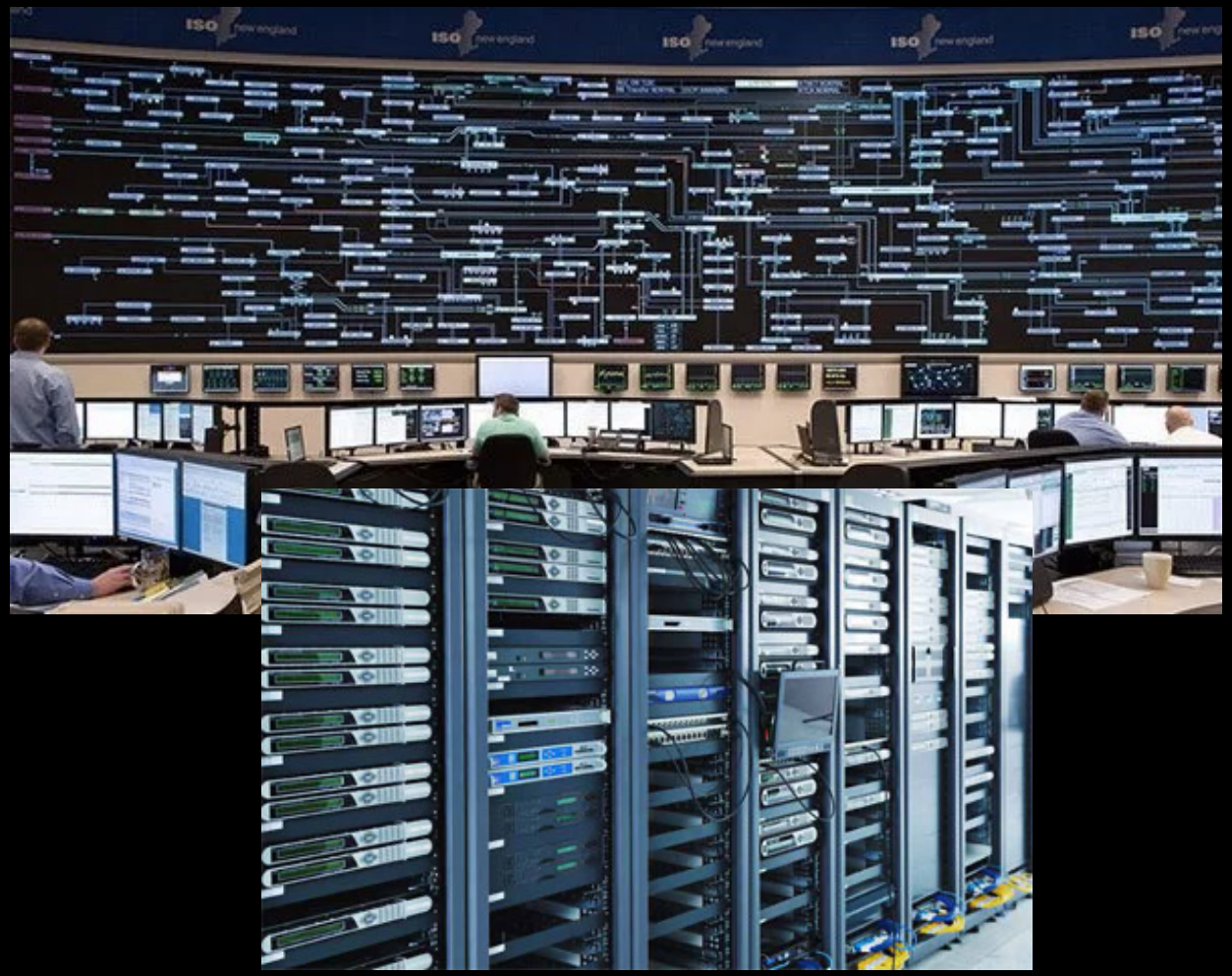
Origins of OT/ICS

OT Changes Over Time





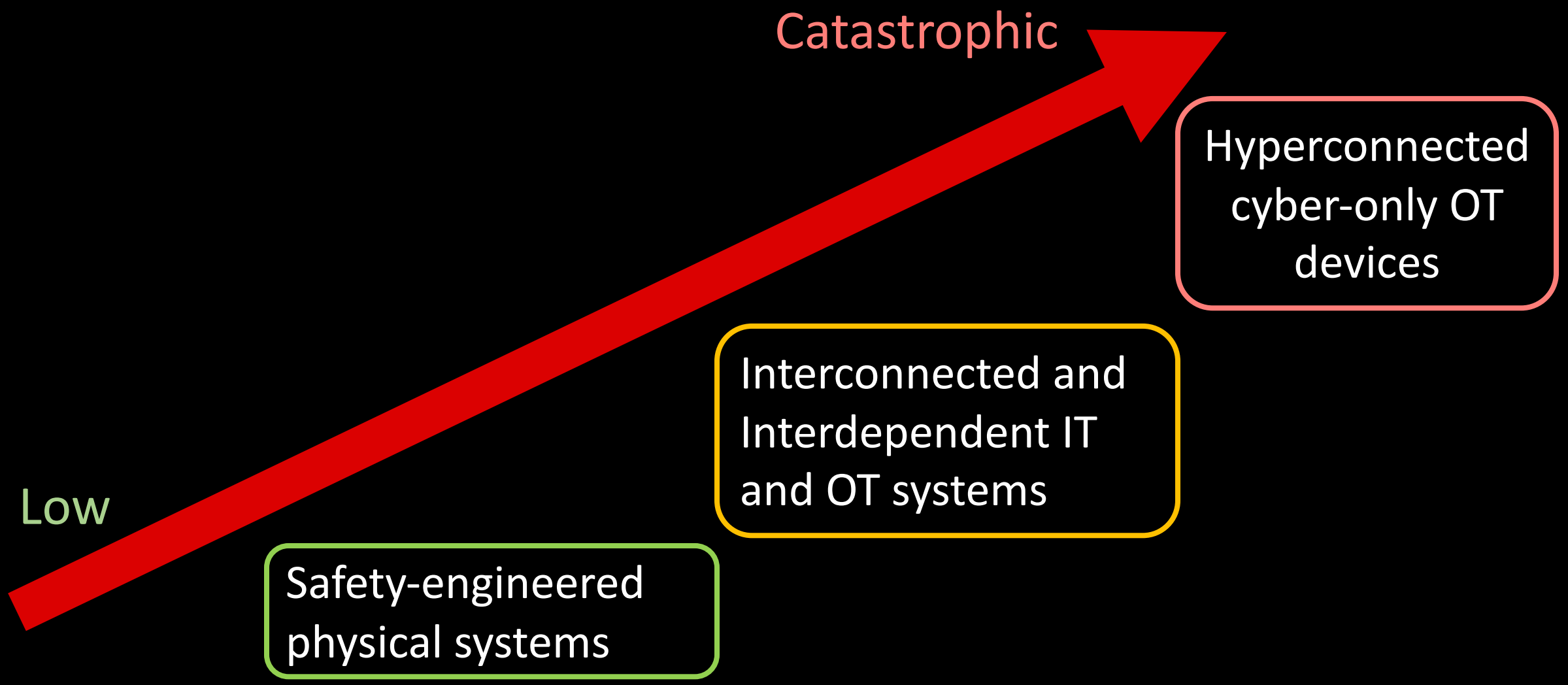
ICS/OT Technology Spectrum



Common Terms

- Cyber-Physical technology
- Operational Technology (OT)
- Industrial Control Systems (ICS)
- Instrumentation Automation and Control (IAC)
- Purpose-built (single purpose)
- SCADA – Supervisory Control and Data Acquisition
- DCS – Distributed Control System
- EMS – Energy Management System
- BMS – Building Management System
- PLC – Programmable Logic Controller
- RTU – Remote Telemetry/Terminal Unit

Risk Trends


Catastrophic
Hyperconnected cyber-only OT devices
Interconnected and Interdependent IT and OT systems
Low
Safety-engineered physical systems

Attacker Objectives

- Loss
  - Loss of view
  - Loss of control
- Denial
  - Denial of view
  - Denial of control
  - Denial of safety
- Manipulation
  - Manipulation of view
  - Manipulation of control
  - Manipulation of sensors and instruments
  - Manipulation of safety

We have well-practiced plans for loss of view or control at a site level or for short periods

Plans are not comprehensive (ready) for when systems are available but do not perform as designed/expected

Few plans are ready for events when systems are available, but someone else is controlling them (possibly maliciously)

Attacker Tactics vs. Defense

- ICS Opportunistic
  - Conficker, Petya/NotPetya, BlackEnergy 3
  - 2008, 2017, 2015
- ICS Focus
  - Dragonfly 2
  - 2016
- ICS Specific Access
  - BlackEnergy 2, Havex, Dragonfly 1
  - 2011, 2011, 2011

Governance, Standards, Regulation, Architecture, Cyber Hygiene

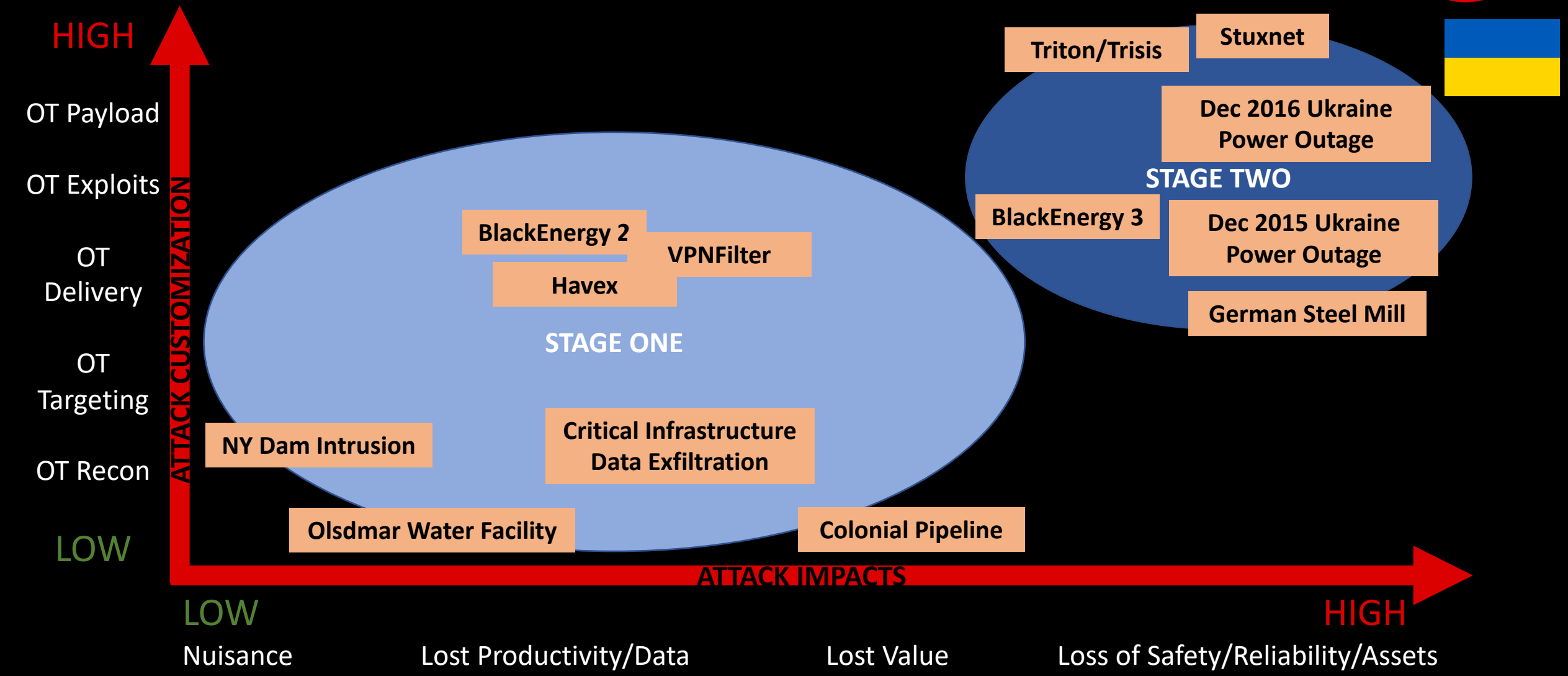
Passive Defense

- ICS Specific Effect
  - Stuxnet, CrashOverride, Triton/Trisis
  - 2009, 2016, 2017

Operations, Resilience, Cyber Engineering,

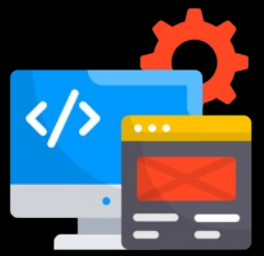
Active Defense

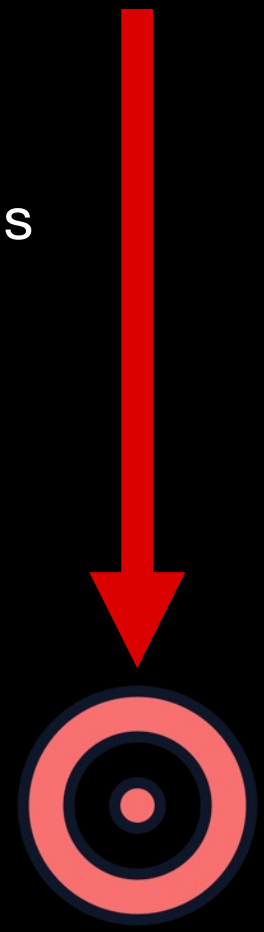
OT Incidents and Campaigns



Attack Paths and Options

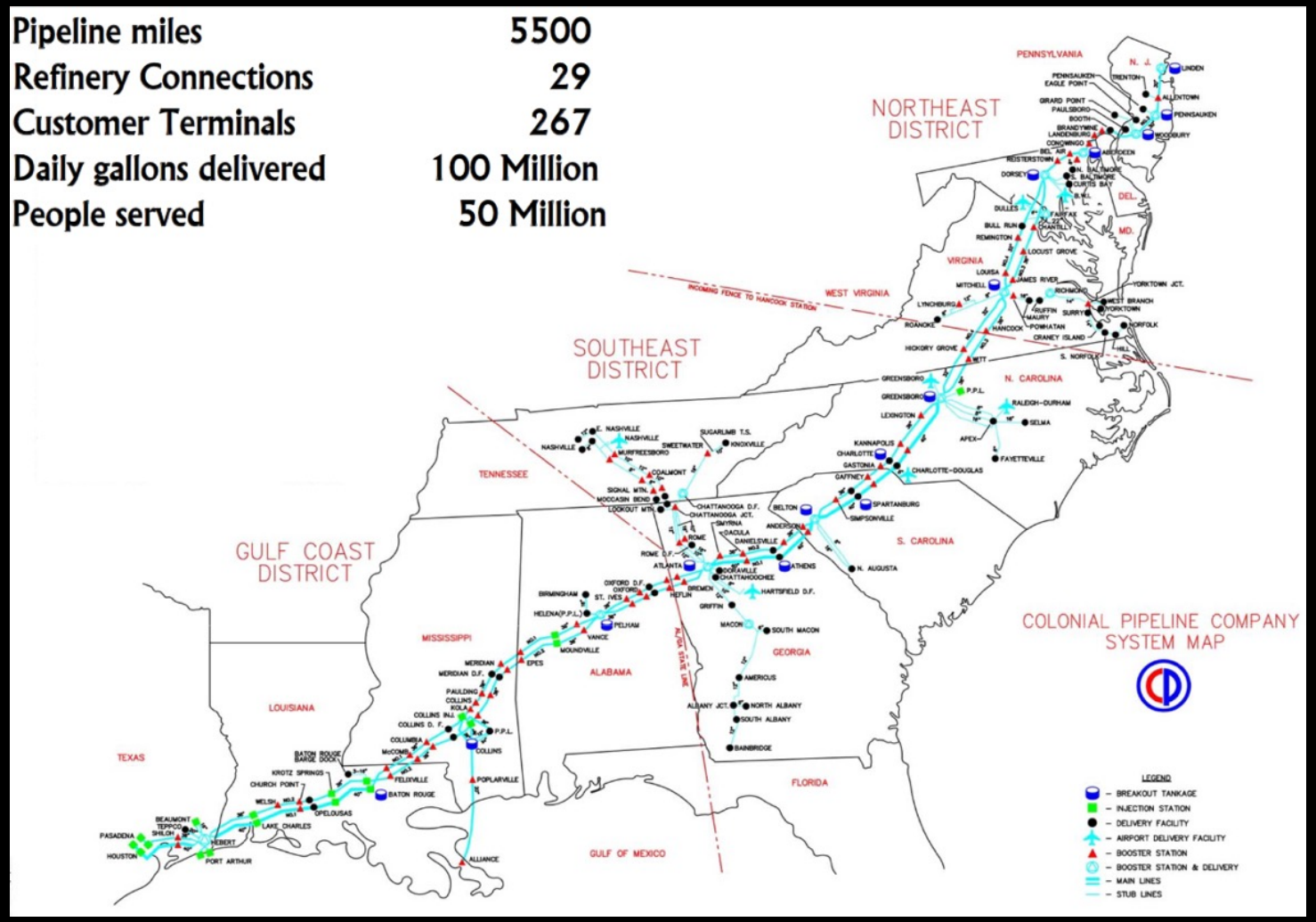
- Reconnaissance
  - Discovery about the target
  - Public/non-public
- Remote Access
  - Gain access however possible; phishing, Access Broker, weak credentials
- “Hunting and gathering”
  - Establishing presence and seeking paths to OT from IT
- OT Manipulation
  - What kind of control do you have (damage can you do)?
- Supply Chain
  - Hardware, software and services
- People
  - Humans are human; Hanlon’s razor





CASE STUDY: COLONIAL PIPELINE

Case Study - Colonial Pipeline

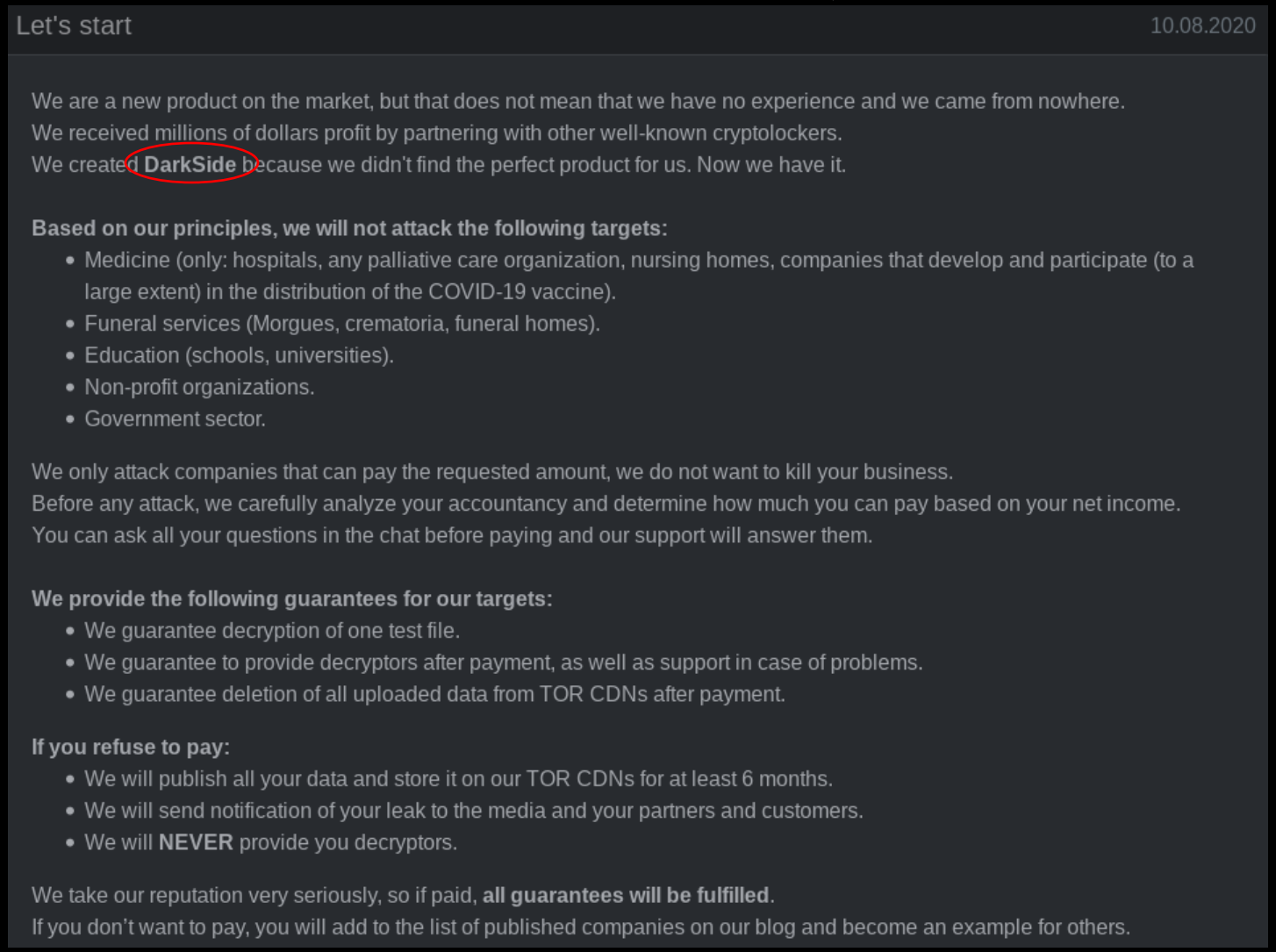


- Largest refined products pipeline in the US
- 45% of the fuel to the East Coast
- May 7 2021, operations were shut down due to a ransomware attack on the IT business systems (not OT)

Case Study – Colonial Pipeline

- 5 days after operations shut down, start up began on May 12, 5:11pm
- On May 13, product deliver started in most markets
- All markets receiving product by mid-day

Ransomware (As a Service)



Let's start 10.08.2020

We are a new product on the market, but that does not mean that we have no experience and we came from nowhere.
We received millions of dollars profit by partnering with other well-known cryptolockers.
We created **DarkSide** because we didn't find the perfect product for us. Now we have it.

Based on our principles, we will not attack the following targets:

- Medicine (only: hospitals, any palliative care organization, nursing homes, companies that develop and participate (to a large extent) in the distribution of the COVID-19 vaccine).
- Funeral services (Morgues, crematoria, funeral homes).
- Education (schools, universities).
- Non-profit organizations.
- Government sector.

We only attack companies that can pay the requested amount, we do not want to kill your business.
Before any attack, we carefully analyze your accountancy and determine how much you can pay based on your net income.
You can ask all your questions in the chat before paying and our support will answer them.

We provide the following guarantees for our targets:

- We guarantee decryption of one test file.
- We guarantee to provide decryptors after payment, as well as support in case of problems.
- We guarantee deletion of all uploaded data from TOR CDNs after payment.

If you refuse to pay:

- We will publish all your data and store it on our TOR CDNs for at least 6 months.
- We will send notification of your leak to the media and your partners and customers.
- We will **NEVER** provide you decryptors.

We take our reputation very seriously, so if paid, **all guarantees will be fulfilled**.
If you don't want to pay, you will add to the list of published companies on our blog and become an example for others.

- Ransomware-as-a-service
- Double extortion – payment for decryption and payment to delete stolen data
- Operates with affiliates
- Claims no geopolitical affiliation and claims only driver is financial
- Intends to provide moderation and review future targets

Case Study – Colonial Pipeline

On May 7, the Colonial Pipeline Company learned it was the victim of a cybersecurity attack. We have since determined that this incident involves ransomware. In response, we proactively took certain systems offline to contain the threat, which has temporarily halted all pipeline operations, and affected some of our IT systems.

- Attacker came through a legacy VPN with single factor authentication and a compromised password
- Even though the problem was on the IT side, the OT side was shut down as precaution, (known/unknown) interdependencies)

Case Study – Colonial Pipeline

Business or Plant Network

Supervisory Control Elements
(HMI, Historian, Engineering Workstation)

Sensing & Control Elements
(PLCs, RTUs, SIS, Sensors, Actuators)

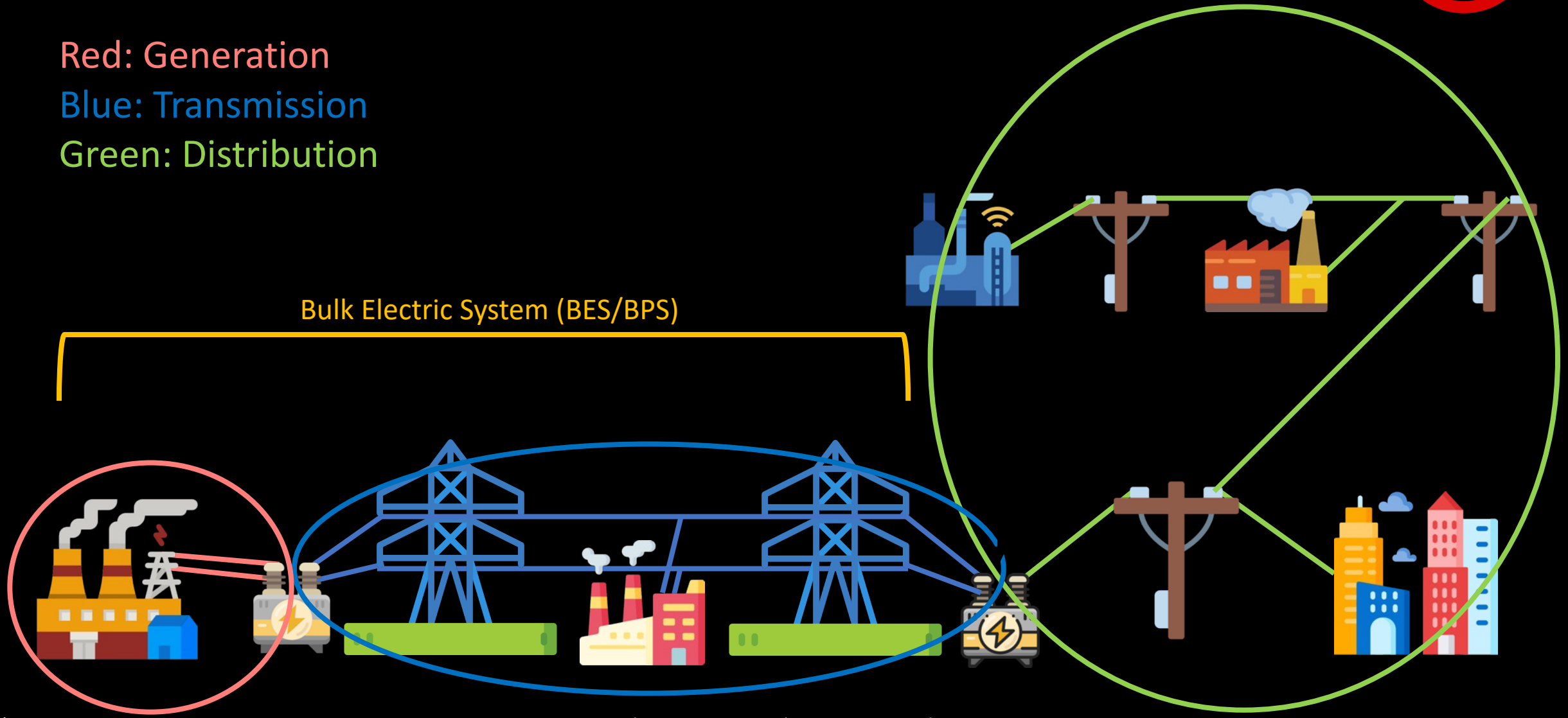
Ransomware and OT

- Currently, ransomware targets primarily IT computer systems, but not embedded systems like PLCs, RTUs, sensors, etc
- Ransomware can affect IT systems used in OT environments
- Effects include (for example):
  - No access to design and configuration tools on engineering workstations
  - Loss of process visibility (HMI) and alarm servers
  - Loss of historical data
  - Loss of quality assurance systems
  - Loss of analytical tools
  - Loss of SCADA functions
  - Inability to authenticate users to OT environment

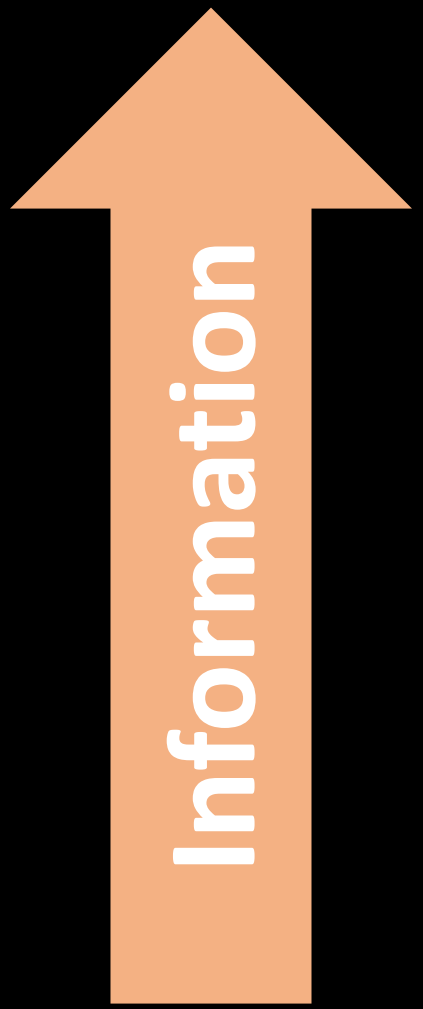
INTRO TO NERC CIP STANDARDS

Power System Basics

Red: Generation
Blue: Transmission
Green: Distribution



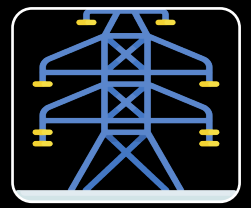
The Regulatory Stack



FERC

NERC/ERO

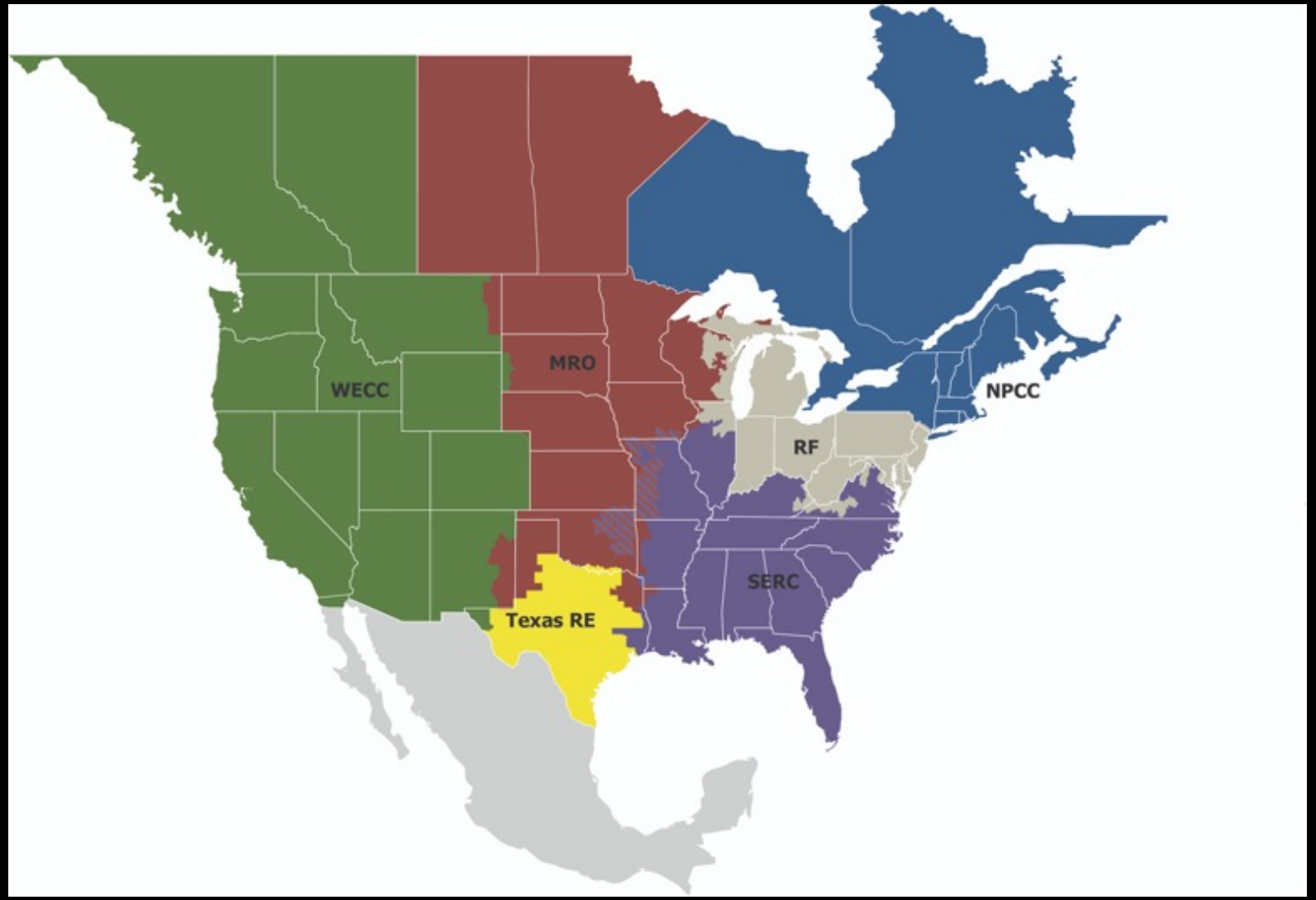
Regions



Utilities

pmiller@amperesec.com | @patrickcmiller | +15032721414 | www.amperesec.com

NERC Regional Entities



All 6 NERC Regions report to NERC for direction and budget

Utilities work directly with Region(s)

Each Region operates slightly different

Origins of NERC CIP

- 1998: Presidential Decision Directive (PDD) 63
- 9/11 Terrorist Attack
- FBI, NIPC, CIPAG
- FERC Standard Market Design (SMD) Appendix G
- NERC Urgent Action Standard (UAS) 1200
- NERC Urgent Action Standard (UAS) 1300
- Blackout of 2003
- Energy Policy Act of 2005 (Section 215)

Requirements designed to ensure physical and electronic security of Cyber Assets required for operating North America's Bulk Electric System (BES)

CIP Versions to Date

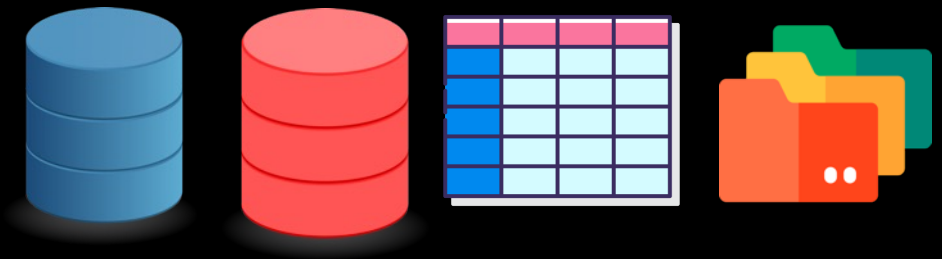
- Version 1
  - Approved in FERC Order 706 on Jan 18, 2008
  - Took effect on July 1, 2008
- Versions 2 and 3
  - Minor changes to address issues raised by FERC
  - Effective dates of Sep 30, 2010 and Oct 1, 2010, respectively
- Version 4
  - Approved, then later superseded by V5. Never went into effect
- Version 5
  - Approved in FERC Order 791 on November 26, 2013
  - Superseded by V6 on its effective date
- Version 6
  - Approved by FERC (Order 822) on January 21, 2016
  - Took effect beginning on July 1, 2016
- After V6, each standard took its own path and gets versioned individually

The NERC CIP Standards

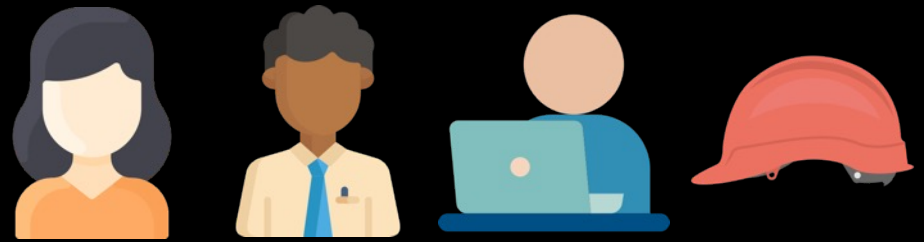
- NERC CIP: Critical Infrastructure Protection (current)
  - CIP-002 BES Cyber System Categorization
  - CIP-003 Security Management Controls
  - CIP-004 Personnel & Training
  - CIP-005 Electronic Security Perimeter(s)
  - CIP-006 Physical Security of BES Cyber Systems
  - CIP-007 System Security Management
  - CIP-008 Incident Reporting and Response Planning
  - CIP-009 Recovery Plans for BES Cyber Systems
  - CIP-010 Configuration Change Mgmt & Vulnerability Assessments
  - CIP-011 Information Protection
  - CIP-012 Communication Between Control Centers
  - CIP-013 Supply Chain Risk Management (coming soon to low impact)
  - CIP-014 Physical Security

NERC CIP Simplified

- Electronic Protection
- Physical Protection
- Lists of individual access



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



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

Sidebar: NERC O&P Standards

- (COM) Communications
- (EOP) Emergency Preparedness and Operations
- (FAC) Facilities Design, Connections, and Maintenance
- (IRO) Interconnection Reliability Operations and Coordination
- (MOD) Modeling, Data, and Analysis
- (PER) Personnel Performance, Training, and Qualifications
- (PRC) Protection and Control
- (TOP) Transmission Operations
- (TPL) Transmission Planning
- (VAR) Voltage and Reactive

The Important CIP Stuff

- Applicable Systems
  - Lists Cyber Asset categories in-scope for the respective Requirement
- Requirements
  - Lists what must be done or accomplished
  - Legal thing that must be done
- Measures
  - Lists examples of compliance evidence
- Attachments
  - Extensions of the Requirements, legally binding
- Violation Risk Factors (VRFs) & Violation Severity Levels (VSLs)
  - Influences enforcement (penalties)

Standards at a Glance

CIP-007-6 — Cyber Security – Systems Security Management

R2. Each Responsible Entity shall implement one or more documented process(es) that collectively include each of the applicable requirement parts in *CIP-007-6 Table R2 – Security Patch Management*. *[Violation Risk Factor: Medium] [Time Horizon: Operations Planning].*

M2. Evidence must include each of the applicable documented processes that collectively include each of the applicable requirement parts in *CIP-007-6 Table R2 – Security Patch Management* and additional evidence to demonstrate implementation as described in the Measures column of the table.

CIP-007-6 Table R2 – Security Patch Management

Part	Applicable Systems	Requirements	Measures
2.1	High Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA Medium Impact BES Cyber Systems and their associated: 1. EACMS; 2. PACS; and 3. PCA	A patch management process for tracking, evaluating, and installing cyber security patches for applicable Cyber Assets. The tracking portion shall include the identification of a source or sources that the Responsible Entity tracks for the release of cyber security patches for applicable Cyber Assets that are updateable and for which a patching source exists.	An example of evidence may include, but is not limited to, documentation of a patch management process and documentation or lists of sources that are monitored, whether on an individual BES Cyber System or Cyber Asset basis.

Enforcement Factors

R #	Time Horizon	VRF	Violation Severity Levels (CIP-010-2)			
			Lower VSL	Moderate VSL	High VSL	Severe VSL
R1	Operations Planning	Medium	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only four of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only three of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has documented and implemented a configuration change management process(es) that includes only two of the required baseline items listed in 1.1.1 through 1.1.5. (1.1)	The Responsible Entity has not documented or implemented any configuration change management process(es). (R1) OR The Responsible Entity has documented and implemented a configuration change management process(es) that includes only one of the required baseline items listed in 1.1.1 through 1.1.5. (1.1) OR The Responsible Entity does not have a process(es) that

Enforcement (Penalties/Fines)

Source	Existing maximum civil monetary penalty	New adjusted maximum civil monetary penalty
16 U.S.C. 8250-1(b), Sec. 316A of the Federal Power Act	$1,291,894 per violation, per day	$1,307,164 per violation, per day.
16 U.S.C. 823b(c), Sec. 31(c) of the Federal Power Act	$23,331 per violation, per day	$23,607 per violation, per day.
16 U.S.C. 825n(a), Sec. 315(a) of the Federal Power Act	$3,047 per violation	$3,083 per violation.
15 U.S.C. 717t-1, Sec. 22 of the Natural Gas Act	$1,291,894 per violation, per day	$1,307,164 per violation, per day.
15 U.S.C. 3414(b)(6)(A)(i), Sec. 504(b)(6)(A)(i) of the Natural Gas Policy Act of 1978	$1,291,894 per violation, per day	$1,307,164 per violation, per day.

Most Common CIP Acronyms/Terms

- BCA - BES Cyber Asset
- BCS - BES Cyber System
- BCSI - BES Cyber System Information
- BES - Bulk Electric System
- EACMS - Electronic Access Control or Monitoring System
- EAP - Electronic Access Point
- ERC - External Routable Connectivity
- ESP - Electronic Security Perimeter
- PACS - Physical Access Control System.
- PCA - Protected Cyber Asset
- PSP - Physical Security Perimeter
- TFE - Technical Feasibility Exception
- CEC - CIP Exceptional Circumstance

CIP-002: What's in Scope?

- Cornerstone of the entire body of NERC CIP standards

- Identify in scope facilities (assets, sites, locations)
  - 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
- Determine High, Medium, Low Impact Rating

CIP-003: Governance & Low Impact

- High/Medium Impact
  - CIP Senior Manager (individual responsible for program)
  - Required cybersecurity policies (CIP-004 – CIP-011, CEC)
- Low Impact
  - Cybersecurity Awareness
  - Physical Security Controls
  - Electronic Access Controls
  - Cybersecurity Incident Response
  - Malicious code risk mitigation for Transient Cyber Assets (TCAs) & Removable Media (RM)
  - *Vendor remote access security controls (future effective date)*
  - Declaring & responding to CIP Exceptional Circumstances

CIP-004: Personnel & Access

Personnel & Training

- Access Management Program
  - Documented authorization for access
  - Quarterly verification
  - Annual privilege review
  - Access to BCSI storage locations
- Access Revocation
  - Remove access for terminations within 24 hours
  - Remove access for reassignments next calendar day
  - Remove access to BCSI storage locations

CIP-005: Electronic Boundary

Electronic Security Perimeter

- Typically, a firewall but anything that can enforce ACLs
- If you have routable traffic traversing firewall, it must go through an identified interface (Electronic Access Point)
- ACLs are required, and must be justified, documented
- Method for detecting malicious communications
- If Interactive Remote Access, then jump host with MFA is required
- Vendor remote access detection & kill switch

CIP-006: Physical Security

Physical Security of BES Cyber Systems

- Have a Physical Security Plan
- Define physical controls to restrict access
  - Locks, Keys, Badges
  - Monitor and alert for unauthorized access to perimeters and PACS
  - Log all entry at the unique individual level with date/time; keep for 90 days
- Visitor Control Program
  - Require continuous escort for visitors
  - Log of all visitors, entry and exit
  - Retain logs for 90 days
- Maintenance & testing of PACS & all hardware every 24 months

CIP-007: System Security

Systems Security Management

- Ports and services (logical and physical)
- Patch Management
  - 35 days to identify, 35 days to patch or mitigate
- Malicious Code Prevention
  - Mitigate threat of malicious code
- Security Event Monitoring
  - Log, alert, review
- System Access Control
  - Account and Password Management

CIP-008: Incident Response

Incident Reporting & Response Planning

- Incident Response Plan (IRP) Testing
  - Test incident response plan every 15 calendar months
  - Use the plan when responding to a CSI
  - Document deviations from the plan taken during response
  - Retain records related to R-CSI
- IRP Review, Update and Communication
  - Document lessons learned (90 days)
  - Update IRP with lessons learned (90 days)
  - Update IRP if technology change (60 days)
  - Notify all roles of updates (60/90 days)

CIP-009: Disaster Recovery

Recovery Plans for BES Cyber Systems

- Recovery Plan Specifications
  - Conditions for activation of the recovery plan
  - Roles and responsibilities of responders
  - Process for backup and storage of info required to recovery
  - Verify successful completion of backups
  - Preserve CSI forensic data if recovery plan is triggered
- Recovery Plan Testing
- Recovery Plan Review, Update and Communication

CIP-010: Change Management

Config Change Mgmt & Vulnerability Assessments

- Develop a baseline
  - Operating system or firmware if no OS exists
  - COTS, open-source or custom software intentionally installed
  - Logical network accessible ports
  - Security patches applied
- 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

Information Protection

- Identify BES Cyber System Information (BCSI)
- Procedures for secure handling of BCSI
  - Storage, transit and use
- BES Cyber Asset Reuse and Disposal
  - Prevent unauthorized retrieval of BCSI from the Cyber Asset

CIP-012: Control Center Comms

Communication Security Between Control Centers

- 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

CIP-013: Supply Chain Security

Supply Chain Risk Management Plan

- Processes used in planning for procurement of BCS+
  - Identify and assess cyber security risks
- Processes used in procuring BCS+
  - Notification by vendor of vendor-identified incidents
  - Coordination of responses to vendor-identified incidents
  - Notification by vendors when remote/onsite access no longer needed
  - Vendor disclosure of known vulnerabilities
  - Verification of software integrity and authenticity
  - Coordination of controls for vendor remote access (interactive or system-to-system)

CIP-014: Transmission Security

Transmission Facility Physical Security

- Identify and protect Transmission stations and Transmission substations, and their associated primary control centers
- Risk assessment
- Verification of the risk assessment by third party
- Evaluation of the potential threats and vulnerabilities of a physical attack against Transmission and Control Center
- Physical security plan
- Verification of the physical security plan by third party

NERC CIP “Greatest Hits”

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

NERC CIP Lessons Learned

- Interpretation inconsistencies
- The stronger the internal controls program, the more violations
- Regulatory lag
- Potential innovation impacts
- TFE process
- Fear of the auditor over the attacker
- Can lead toward document-driven compliance
- Predictive targets for adversaries
- Compliance/audit economies demand funding and resources
- Need for funding and incentives

NERC CIP Crystal Ball

- Legislators, regulators and agencies are getting educated
- Drifting toward NIST
- Focus on monitoring, incident response, and recovery
- Supply Chain
  - Coming to a Low Impact asset near you
- Cloud (BCSI and BCS)
- Virtualization
  - Biggest shift in CIP since v3 to v5
- Global adoption is picking up steam

CI Regulatory Crystal Ball

- Each “catalytic event” creates a cyber-avalanche
- NERC CIP moved the needle for electric sector, everyone noticed
- Legislators, regulators and commissions are educated and aware
  - MANY new cybersecurity bills introduced in this session
  - On pace for even more next session
- Regulation is always considered as a response
- So many federal motions in so many government and industry verticals it’s hard to understand them all…

BUT WAIT…
THERE'S MORE!

National Cybersecurity Strategy

National Cybersecurity Strategy

- White House issued National Cybersecurity Strategy (3/1/2023)
  - Companion Fact Sheet
- Ambitious; very well constructed; input from many parties
- Not a law, not an executive order, closer to a memorandum
- Five pillars
  - Defend Critical Infrastructure
  - Disrupt and Dismantle Threat Actors
  - Shape Market Forces to Drive Security and Resilience
  - Invest In a Resilient Future
  - Forge International Partnerships to Pursue Shared Goals
- Implementation (call to action)

“Fundamental Shifts”

- “We must rebalance the responsibility to defend cyberspace by shifting the burden for cybersecurity away from individuals, small businesses, and local governments, and onto the organizations that are most capable and best-positioned to reduce risks for all of us.”

- “We must realign incentives to favor long-term investments by striking a careful balance between defending ourselves against urgent threats today and simultaneously strategically planning for and investing in a resilient future.”

NCS Highlights

- Last one was in 2018; very different approach
- Name and shame nation states as biggest threat
- Critical infrastructure sectors that don’t have regulation, probably will soon
- Shifting liability to software makers vs. consumers
- OT gets multiple (legitimate) mentions
- Cyber-Informed Engineering (CIE, CCE)
- Cyber workforce
- Lighter on incident response, but CSRB is mentioned

NCS Challenges

- “…work with Congress…”
  - Vegas wouldn’t take these odds
- New regulation, legislation will be needed
  - Even reversal of some existing legal standing
- Stretching jurisdiction and capacity of existing agencies with any regulatory authority
- Lean on State regulatory functions
- Administration may change in 2 years
  - What if we do a bunch of hard work and spend a lot of money and everything gets unwound in 2 years?

National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems

National Security Memorandum

- Not a law/regulation – voluntary collaborative initiative (for now)
- Baseline security controls across all critical infra sectors
- Some controls will be common with existing frameworks (CIP)
- NIST 800-53/82 are being promoted (expected) to be the set
- Measurement (no enforcement) will be DHS CISA and SSA
- Unclear how measurement will happen (audit, assessment?)
- Will apply first to electricity subsector, then gas, chemical, water
  - Unclear if "National Security" banner will loop in Distribution
- Final framework to be completed by July 28, 2022 (*it's late*)
- Clear signaling that participation is expected, or else…

NSM – to do list

- "…deployment of technologies and systems that provide threat [and anomaly] visibility, indications, detection, and warnings…"
- "…response capabilities for cybersecurity in essential control system and operational technology networks…"
- …" Government and industry to collaborate to take immediate action…"
- "…baseline cybersecurity goals that are consistent across all critical infrastructure sectors…"

NSM – Recommended Actions

- Gap assessment of current CIP controls against 800-53/82
  - CIP has already been mapped, use existing tools
- Create action plan to remediate any control gaps
  - Owners, actions, dates, budget
- Begin any architecture/system modifications needed for increased monitoring, detection, response and recovery
- Procure and/or tune network anomaly detection software
  - CRISP, Neighborhood Keeper, Essence or other commercial tool
- Establish trained and resourced security operations function
  - Can be outsourced or insourced
  - Process, analyze, respond and tune new tools
- Perform REAL incident and recovery response exercises

NSM – voluntary vs. mandatory

- PR incentives/hit – public perception minimum bar has been set
- Cyber insurance impacts can be very real
- Business partnerships – upstream/downstream; M&A, contracts
- Constrained markets over time
- Earlier adopter bonus points with oversight body
- Easier to demonstrate proactive continuous improvement vs. late-stage, time-constrained, forced, and reactive efforts
- Given the situational gravity, it may be inevitable
- If not the NSM, then any one of the other “influences”

Direct signaling

"...defend US critical infrastructure by encouraging & facilitating deployment of tech & systems that provide threat visibility, indications, detection, & warnings, & that facilitate response capabilities for cybersecurity in essential control system & operational tech networks."

"We're committed to addressing it. We're starting with voluntary, as much as we can, because we want to do this in full partnership. And — but we're also pursuing all options we have in order to make the rapid progress we need."

"...multiple administrations have recognized that there are no mandated authorities to mandate cybersecurity requirements for critical infrastructure... in the context of our openly saying that we really are committed to addressing the limited and piecemeal regulation..."

"The President is essentially saying, 'We expect responsible owners and operators to meet these performance goals. We will look to you to implement this.'"

- National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, The White House

June 28, 2021

Biden 100-day Plan Plan to Address Cybersecurity Risks to the U.S. Electric System

100-day Plan for electricity ss

The initiative modernizes cybersecurity defenses and:

- Encourages owners and operators to implement measures or technology that enhance their detection, mitigation, and forensic capabilities
- Includes concrete milestones over the next 100 days for owners and operators to identify and deploy technologies and systems that enable near real time situational awareness and response capabilities in critical industrial control system (ICS) and operational technology (OT) networks;
- Reinforces and enhances the cybersecurity posture of critical infrastructure information technology (IT) networks; and
- Includes a voluntary industry effort to deploy technologies to increase visibility of threats in ICS and OT systems.

100-day plan for Electricity ss

- Internal network anomaly detection
- External network anomaly detection
  - CRISP, Neighborhood Keeper, Essence, MANY others
- Boundary or electronic perimeter-level detection
  - UTM, firewall, NIDS
- Asset or system-level detection
  - Tripwire (integrity monitoring)
  - HIDS
  - Antivirus
  - Application whitelisting
- SOC/SIEM analytics capacity
- Information Sharing…
- 100 days has passed with no public release from ESSC

100 day plan for…

All sectors mentioned in the National Security Memo will be getting 100 day plans/sprints…

- Natural Gas…
- Water/Wastewater…
- Chemical…

Relevant Executive Orders

Executive order 13873

“Securing the Information and Communications Technology and Services Supply Chain"

- Issued by Trump, May 15 2019
- Unprecedented authority to prevent or modify transactions involving information and communications technology and services (“ICTS”) originating in countries designated as “foreign adversaries” which pose an undue risk to critical infrastructure or the digital economy in the United States, or an unacceptable risk to US national security

Executive order 13920

“Securing the United States Bulk-Power System”

- Issued by Trump, May 1 2020
- Declared a National Emergency for BPS
- Issued a Prohibition Order; primarily a supply chain motion
- No-buy list of countries and vendors
- Task force on Federal Energy Infrastructure Procurement Policies Related to National Security
- Pre-approved list of countries and vendors
- Paused for 90 days by Biden on Jan 20, 2021
- Biden Admin revoked the Prohibition Order on April 20, 2021

Executive order 14017

“America’s Supply Chains”

- Issued by Biden February 24, 2021
- Wide-ranging evaluation of America’s supply chains over 1 year with two tracks:
- 100-day review
  - semiconductors and advanced packaging;
  - high-capacity batteries;
  - critical minerals and other identified strategic materials; and
  - active pharmaceutical ingredients
- Year long review
  - defense industrial base;
  - public health and biological preparedness industrial base;
  - information and communications technology (ICT) industrial base;
  - energy sector industrial base;
  - transportation industrial base;
  - agricultural commodities and food products

Executive order 14028

“Improving the Nation's Cybersecurity”

- Issued by Biden, May 12 2021
- Remove barriers to threat information sharing between government and the private sector
- Modernize and implement stronger cybersecurity standards in the federal government
- Improve software supply chain security
- Establish a cybersecurity safety review board (Cyber NTSB)
- Create a standard playbook for responding to cyber incidents
- Improve detection of cybersecurity incidents on federal government networks
- Improve investigative and remediation capabilities
- Labeling programs related to the Internet of Things (IoT) and software to inform consumers

DHS CISA Cross-Sector Cyber Performance Goals

CISA Cross-Sector CPGs

DHS CISA Cross-Sector Cybersecurity Performance Goals (CPGs) Common Baseline

- Account Security
- Device Security
- Data Security
- Governance & Training
- Vulnerability Management
- Supply Chain / Third Party
- Resilience
- Network Segmentation
- Physical Security

"…baseline cybersecurity goals that are consistent across all critical infrastructure sectors…"

DHS CISA CPG Sample Table

1.0 Account Security

ID	Controls	Risk	Measurement	Scope	External References
1.1	Automatic account lockout after 5 or fewer failed login attempts should be enabled on all password protected IT and OT assets to reduce the risk of brute force attacks. This control should be verified by the implementation of system enforced policies to prevent login after a predetermined number of failed attempts.				
	Automatic account lockout after failed login attempts	Brute force attacks Password spraying	System-enforced policy that prevents future logins (for some minimum time, or until re-enabled by a privileged user) after 5 or fewer failed login attempts. This configuration should be enabled when available on an asset.	All password protected IT and OT assets, where technically capable	NIST CSF: PR.AC ISA 62443-2-1

CPG Direction

- Controversial origin; went through significant ”discussion” with all interested parties
  - CISA vs. NCSD (and other agencies)
  - CISA vs. Industry
  - CISA vs. CISA
- These are “voluntary” *for now*…
- Have been mapped to NIST CSF, NERC CIP and others
- Updated several times already since adoption
- Becoming *de facto* for comparing different sectors on key security baseline elements

TSA PIPELINE SECURITY DIRECTIVES

TSA Pipeline Security Directive #1

- May 27, 2021 – Security Directive-Pipeline-2021-01
- Within 30 calendar days, conduct a detailed gap assessment of their cybersecurity programs using the TSA's Guidelines; remediation measures
- Report information and physical security incidents affecting their IT or operational technology OT systems to CISA within 12 hours of identification. Reportable incidents include:
  - Unauthorized access;
  - Discovery of malicious software;
  - Denial of service (DoS) attacks;
  - Physical attacks against network infrastructure; and
  - Any other cybersecurity incident that disrupts systems or facilities, "or otherwise has the potential to cause operational disruption that adversely affects the safe and efficient transportation of liquids and gases including, but not limited to impacts to a large number of customers, critical infrastructure or core government functions, or impacts national security, economic security or public health and safety" or have the potential to disrupt system or facility operations
- Designate a Cybersecurity Coordinator

TSA Pipeline Security Directive #2

- Known:
  - Implement specific mitigation measures to protect against ransomware attacks and other known threats to IT & OT
  - Develop and implement a cybersecurity contingency and recovery plan
  - Conduct a cybersecurity architecture design review
- Reported/rumored:
  - Password updates
  - Disabling Microsoft macros
  - Programmable logic controller (PLCs) protections
  - Antivirus/malware protection
  - Detection technologies
  - Ingress and egress communications
  - System segmentation
  - Multi-factor authentication (MFA)
  - Zero trust

Direct Signaling

"For over a decade, the Federal Energy Regulatory Commission (FERC), in coordination with the North American Electric Reliability Corporation, has established and enforced mandatory cybersecurity standards for the bulk electric system. However, there are no comparable mandatory standards for the nearly 3 million miles of natural gas, oil, and hazardous liquid pipelines that traverse the United States.

"It is time to establish mandatory pipeline cybersecurity standards similar to those applicable to the electricity sector. Simply encouraging pipelines to voluntarily adopt best practices is an inadequate response to the ever-increasing number and sophistication of malevolent cyber actors. Mandatory pipeline security standards are necessary to protect the infrastructure on which we all depend.

"Therefore, I am pleased that Commissioner Clements is joining me today in my longstanding calls for mandatory cybersecurity standards for our nation's pipeline infrastructure."

- FERC Chairman Richard Glick, May 10, 2021

TSA SD Lessons Learned

- IT cybersecurity concepts applied to OT were not effective or even possible in many cases
- Unachievable incident response notification/reporting window
- Not based or part of any existing standard or framework
- Lack of transparency; work with industry stakeholders before imposing standard
- Lack of OT experience for assessors/auditors; not enough of them
- Confusing and questionable monitoring and enforcement method
- Revised SD2 mid-2022 - movement toward a “performance-based model that will enhance security and provide the flexibility needed to ensure cybersecurity advances with improvements in technology.”
- Suggested to adopt API 1164 as long-term replacement

COMMON THREADS

Regulatory/Standards Context

- Global trend…
  - ISO 27001, NIS-2, CAF, BSI, 62443, NIST 800-53/82/CSF, NERC CIP and many more
- FERC RFI seeking to align with NIST (and incentives)
- DOE RFI seeking information on possible additional security controls
- 100-day Plan to Address Cybersecurity Risks
- ES-C2M2 (new version) and ONG C2-M2
  - Both are being used by commissions and underwriters
- TSA Pipeline Security Guidelines updated, Security Directives (x2), updated
  - Possible shift to API 1164?
- Recent updates to CFATS
- Too many Executive Orders to list
- Strong National Security Memorandum and National Cybersecurity Strategy
- Renewed interest in AWWA G430 and J100 standards
- DHS CISA Cyber Performance Goals (CPGs)

Para-Regulatory Forecast

- Whether direct regulation (CIP, TSA, CFATS, EPA) or indirect "transitive" or "para"-regulation (NIST, EO, NSM), new normal is:
  - Buy only "trusted" hardware, software, services
  - Know all cyber assets in your environment
  - Know the security posture for all cyber assets
  - Segment and restrict access (zero trust, MFA)
  - Monitoring and detection at asset and network level
  - Strong incident response capability
  - "Intelligent islanding" (turtle mode)
  - Strong recovery capability
- Less "guessing" - aligns with most guidelines, regulation, Executive Orders, National Security comms, etc. in peer sectors

Assets and Architecture

- Do you have an asset inventory?
  - Not everything, but even just the critical stuff
  - Back it with change control or expect drift (waste time/money)
- Do you have an environment you can defend?
  - Segmented networks
  - One-way traffic
  - MFA and strict remote access controls
  - Shear-away networks, “crumple zones,” intelligent islanding
- Interdependencies can be your Achilles heel
  - Runs converse to many current approaches

Situational Awareness

- Would you know – with sufficient confidence – if there was (or was not) an adversary in your system?
- Monitoring is in every federal conversation now
  - CRISP, Neighborhood Keeper, Essense…
- "Smoke detectors" will be required in the "building code"
- Regulation, insurance, diligence, reporting (data breach)
- Start where you can, tune, then lather, rinse, repeat
- Based on solid asset inventory and feeds response and/or recovery

Supply Chain Risk Management

- NERC CIP-013 is the tip of the iceberg
  - Adding new asset types and moving to low impact
- Multiple Executive Orders, probably more to come
- ”No-buy” lists, rip/replace, legacy risk often unaddressed
- “Made in” often means “assembled in”
- How far do you go? Was it far enough?
- HBOM, SBOM, FBOM
- “CyberStar,” transparency centers, certification, validation
- Frustration and costs go up for everyone

Practice Like Game Day

- When was the last time you did a **real** incident response exercise?
  - Did it include a recovery drill?
  - Did it include IT impacting OT through business process?
- Everything else leads up to this
  - Asset inventory, supply chain, segmentation, monitoring
- Borrow from operations (and safety)
  - Can you really go to manual? For how long?
- Expect "oversight" and media when it happens
  - Cyber NTSB, CISA, E-ISAC, FBI, Commerce, State…
- What happens to one utility will affect all others…

Common Solutions

- For organizations already subject to NERC CIP, TSA, CFATS, much can be borrowed
- Other controls frameworks also exist for an “overlay” (mapping) approach to managing compliance risk
  - Focus on NIST 800-53 and 800-82
- Portable skill sets across sector types in OT
  - IT already has common skill pool
- Some common solutions exist for IT and OT
  - Hardware
  - Software

Controls vs. Performance

- How are you going to be measured?
- Performance
  - Much less on the how, more on the what
  - Strict focus on proof that you did what the requirement says
  - Very subjective
- Controls
  - Control objective defined, control designed, control test performed
  - Ensures all controls are functioning as expected
  - Preventive or detective (pick one)
  - Procedural or technical (pick one)
  - Much less subjective

Good Evidence Practices

- Performance-based audits/assessments
  - Policy, program, procedure, process stating “why” and “how”
  - At least one piece of evidence with proof requirement was performed
  - Word documents, Excel, PDF (everything else)
  - Strong consistency is very important
- Controls-based audits/assessments
  - Well-defined control objective that maps to existing standard/framework
    - What you are trying to control and why
  - Well-defined control that maps to existing standard/framework
    - How you are applying the control objective controlling the process/thing
  - Documented control test that demonstrates the control is functioning as expected

Questions?

Email: pmiller@amperesec.com

Web: www.amperesec.com

LinkedIn: https://www.linkedin.com/in/millerpatrickc/

Twitter: @patrickcmiller

Mastodon: @patrickcmiller@infosec.exchange

Podcast: Critical Assets Podcast