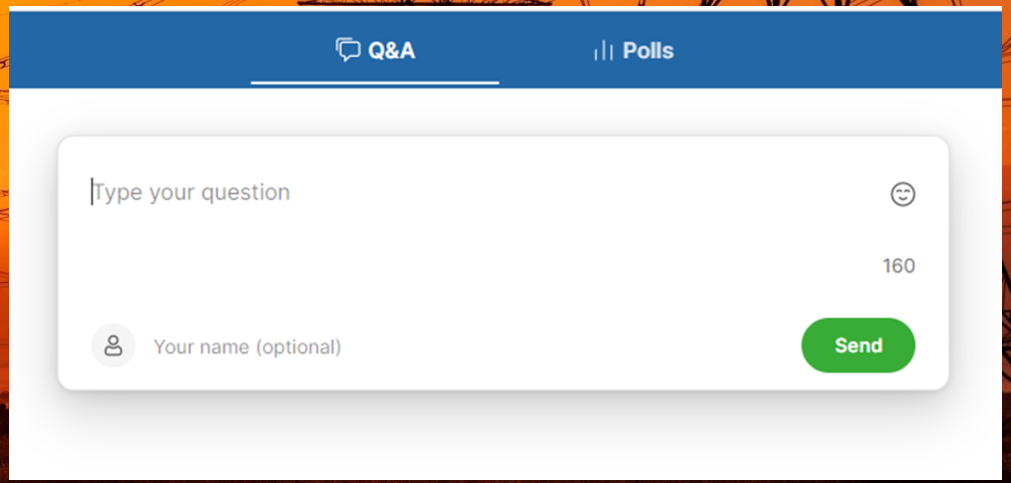
Texas RE Fall Standards, Security, & Reliability Workshop

November 20, 2024

AGENDA

- Kick-off and Instructions
- Executive Welcome
- CISA Update
- NIST Cybersecurity Framework
- Threat Briefing
- Lonestar Infrastructure Protection Act
- Physical Security
- ITCS
- Large Loads in the Texas Interconnection
- Root Cause Analysis and Cause Codes
- 2025 CMEP IP
- Common and High Risk Violations

To submit questions during the workshop, please visit **slido.com** and enter today's participant code: **TXRE**



Welcome & Instructions

Thad Crow
Texas RE
Communications & Training Coordinator

STANDARDS, SECURITY, & RELIABILITY
FALL WORKSHOP

Antitrust Admonition

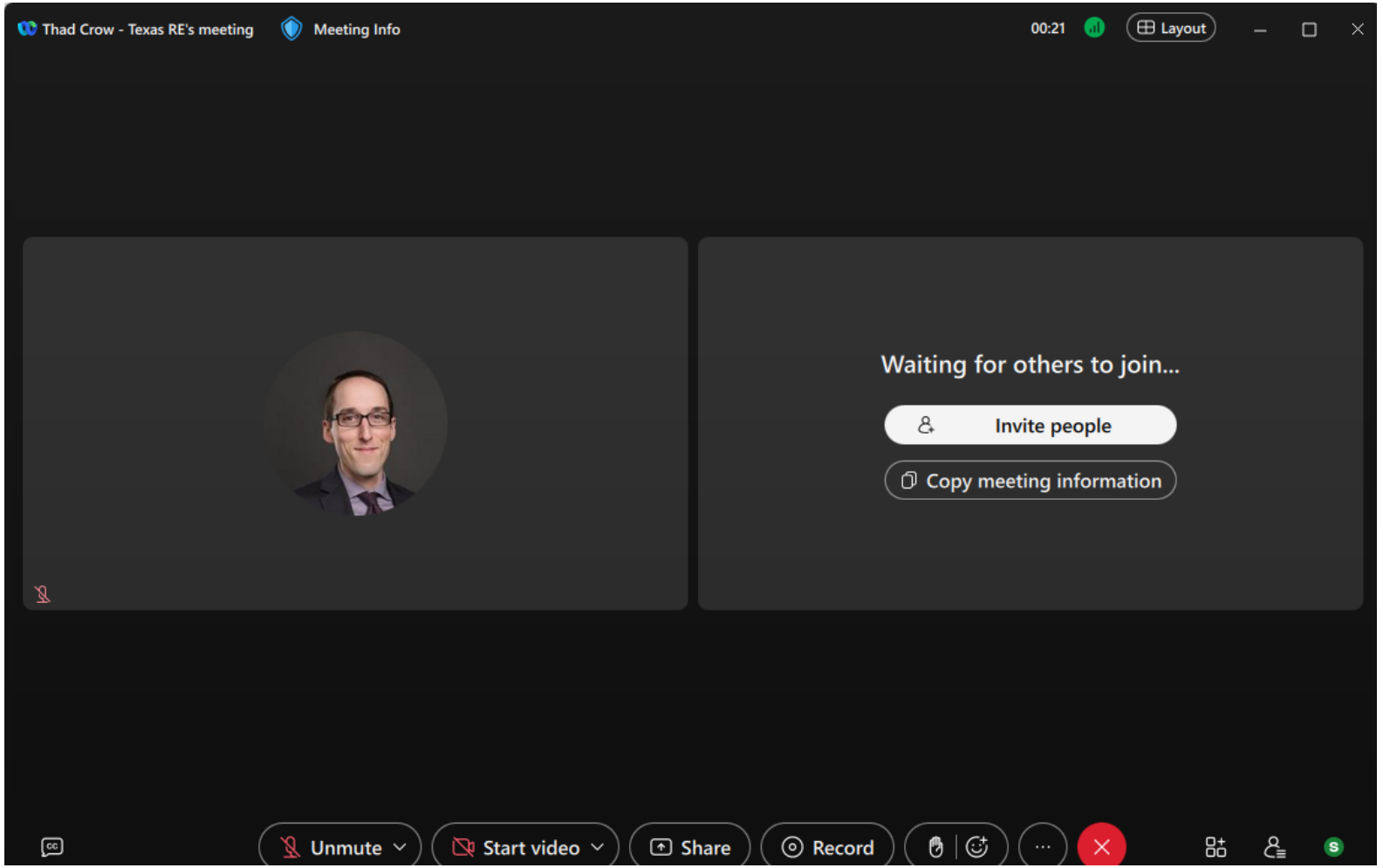
Texas Reliability Entity, Inc. (Texas RE) strictly prohibits persons participating in Texas RE activities from using their participation as a forum for engaging in practices or communications that violate antitrust laws. Texas RE has approved antitrust guidelines available on its website. If you believe that antitrust laws have been violated at a Texas RE meeting, or if you have any questions about the antitrust guidelines, please contact the Texas RE General Counsel.

Notice of this meeting was posted on the Texas RE website and this meeting is being held in public. Participants should keep in mind that the listening audience may include members of the press, representatives from various governmental authorities, and industry stakeholders.

Safety Moment

In case of emergency

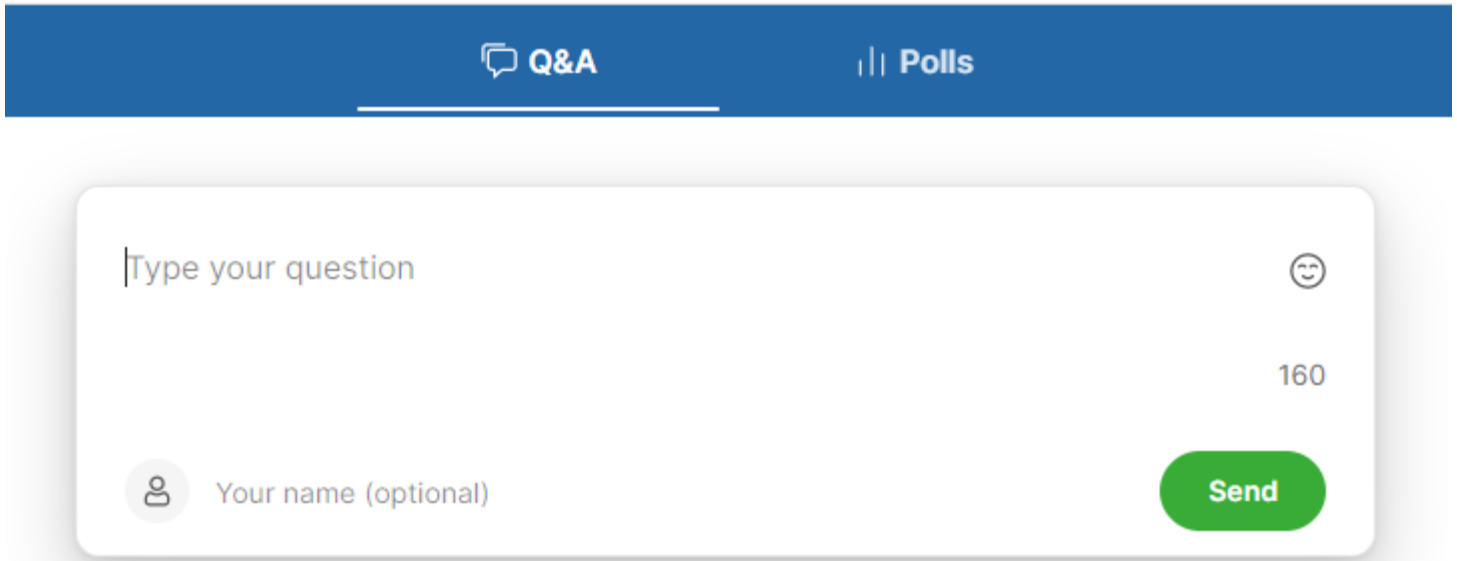
Leave the WebEx



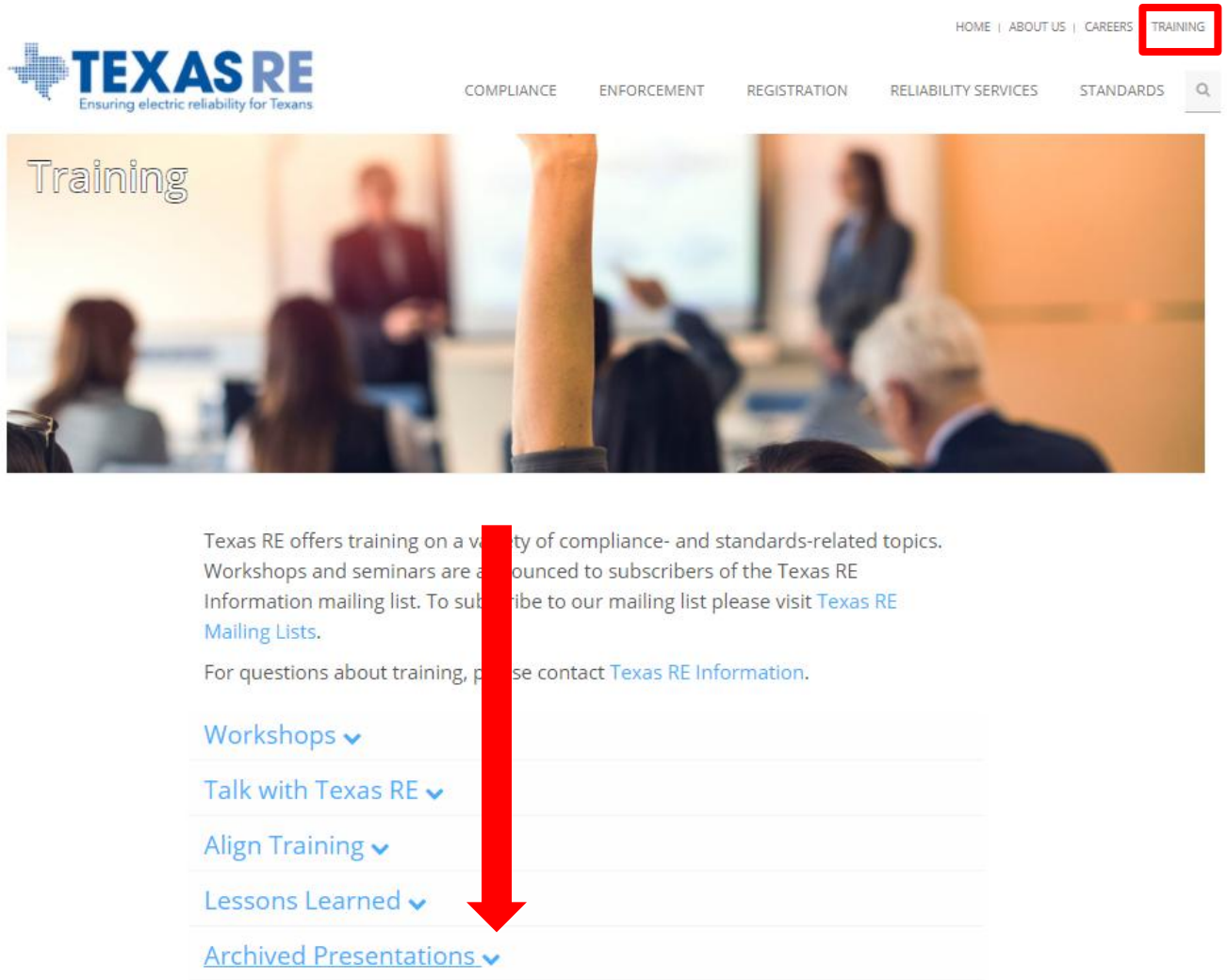
Questions

To submit questions during the workshop, please visit **slido.com** and enter today's participant code: **TXRE**

slido



Training Page



Archived Presentations

All of Texas RE's outreach activities are free and open to the public. Past presentations delivered by Texas RE staff are available here. Please be aware that presentations will not be available indefinitely, and may be removed to comply with Texas RE's document retention policy.

ALIGN

Align Release 1 Training | Recording

Align Release 2 Periodic Data Submittal Training | Recording

Align Release 2 TFE and Self-Certification Training | Recording

Align Release 3 Training | Recording

Align Release 4 & 4.5 Training | Recording

Workshops

Women's Leadership in Grid Reliability and Security Conference | Recording

2024 Cyber and Physical Security Workshop | Keynote | Panels: Critical Infrastructure, Threat Assessment, Grid Technologies, Security Posture

Understanding New Generator Obligations | Recording

Fall Standards, Security, and Reliability Workshop

2024 Fall Standards, Security, and Reliability Workshop

MCLE Credit

This workshop is accredited for 5 MCLE hours. To receive credit you may either:

- **Self-report the MCLE course number**
  - *174257186*

OR

- **Email Information@texasre.org your attendee information**
  - Name
  - Bar Card Number
  - Hours Attended

Upcoming Texas RE Events

Social Media

/texas-reliability-entity-inc

@Texas_RE_Inc

/TexasReliabilityEntity

Executive Welcome

Joseph Younger
Texas RE
Vice President & Chief Operating Officer

STANDARDS, SECURITY, & RELIABILITY
FALL WORKSHOP

SHIELDS READY

PLANNING FOR NEAR AND LONG-TERM CYBER RESILIENCE BEST PRACTICES, RESOURCES, AND SERVICES FOR ENERGY

TEXAS RELIABILITY ENTITY, INC.

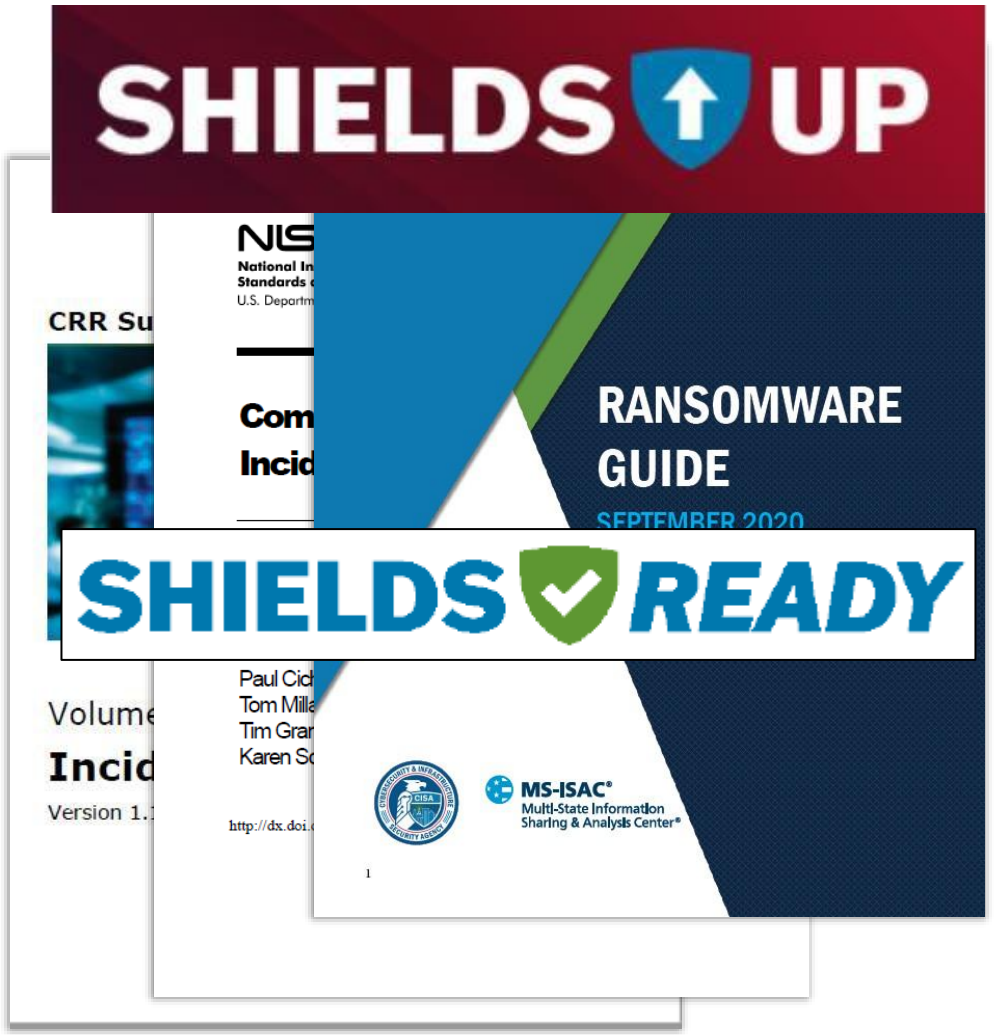
FALL STANDARDS, SECURITY, AND RELIABILITY WORKSHOP

Ernesto Ballesteros, JD, MS, CISSP, CISA, Security+
Cybersecurity State Coordinator | State of Texas
CISA | Region 6

Shields Up/Ready: Building Cyber Resilience

Presentation Sections

- **Introductory Briefing**
- **Part 1: Cyber Resilience | Prepare**
  - Prepare for Cyber Incidents
- **Part 2: Cyber Resilience | Defend**
  - Identify and Mitigate Attack Vectors
- **Part 3: Cyber Resilience | Respond & Recover**
  - Detect, Contain, Eradicate, and Recover
- **Part 4: Cyber Resilience | Next Steps**
  - CISA's No-Cost Resources and Services
  - How to Get Started



CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient infrastructure for the American people.

MISSION

CISA partners with industry and government to understand and manage risk to our Nation's critical infrastructure.

OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent threats and hazards

seconds days weeks

GOAL 2

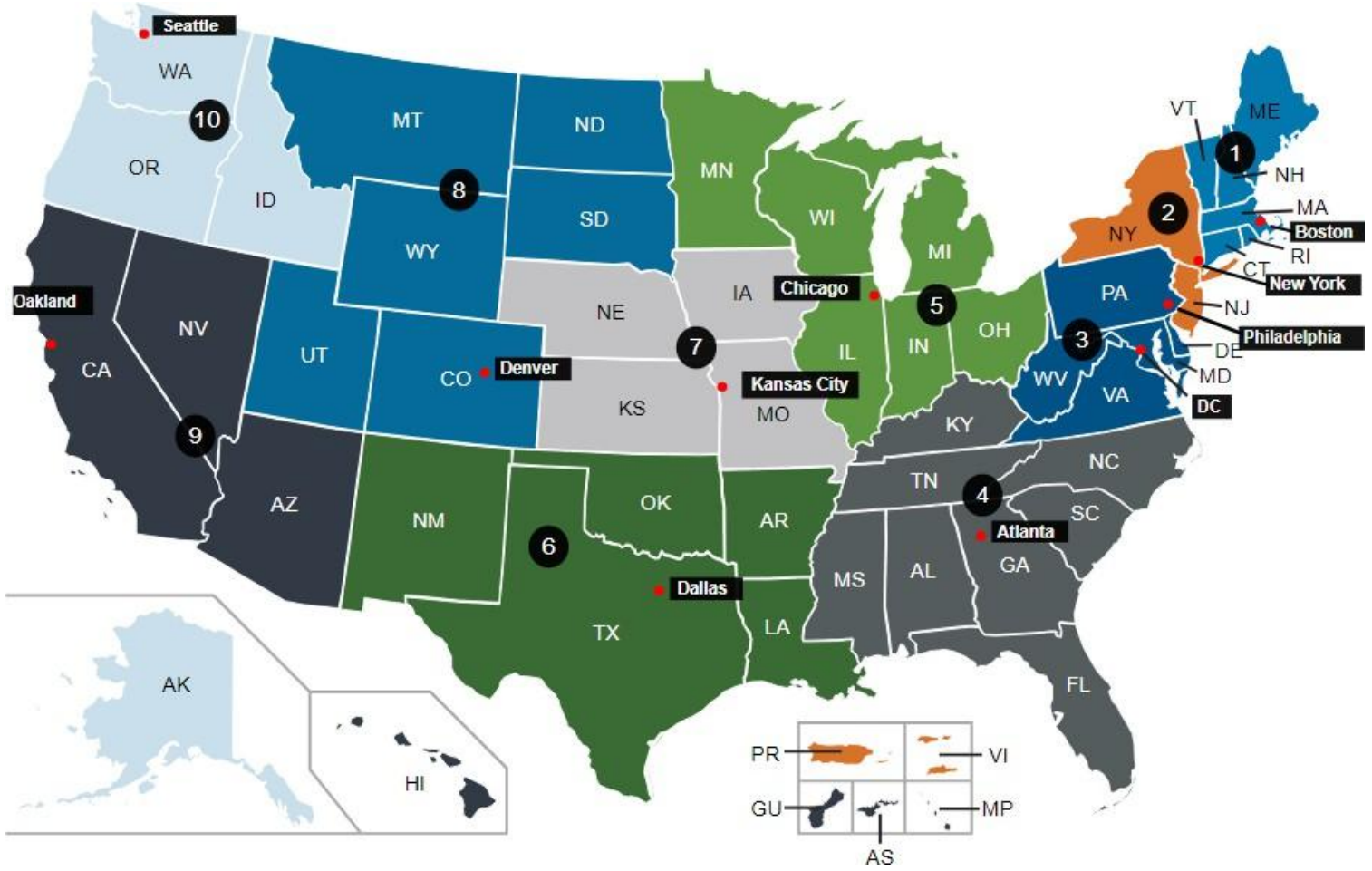
SECURE TOMORROW

Strengthen critical infrastructure and address long-term risks

months years decades

CISA Regions

Region	Location
1	Boston, MA
2	New York, NY
3	Philadelphia, PA
4	Atlanta, GA
5	Chicago, IL
6	Dallas, TX
7	Kansas City, MO
8	Denver, CO
9	Oakland, CA
10	Seattle, WA



https://www.cisa.gov/cisa-regions

Cybersecurity State Coordinator | State of Texas

§665c. Cybersecurity State Coordinator

6 United States Code, Section 665(c) (2021)

(a) Appointment

The Director shall appoint an employee of the Agency in each State, with the appropriate cybersecurity qualifications and expertise, who shall serve as the Cybersecurity State Coordinator.

(b) Duties

The duties of a Cybersecurity State Coordinator appointed under subsection (a) shall include-

(1) building strategic public and, on a voluntary basis, private sector relationships, including by advising on establishing governance structures to facilitate the development and maintenance of secure and resilient infrastructure;

(2) serving as the Federal cybersecurity risk advisor and supporting preparation, response, and remediation efforts relating to cybersecurity risks and incidents;

(3) facilitating the sharing of cyber threat information to improve understanding of cybersecurity risks and situational awareness of cybersecurity incidents;

(4) raising awareness of the financial, technical, and operational resources available from the Federal Government to non-Federal entities to increase resilience against cyber threats;

(5) supporting training, exercises, and planning for continuity of operations to expedite recovery from cybersecurity incidents, including ransomware;

(6) serving as a principal point of contact for non-Federal entities to engage, on a voluntary basis, with the Federal Government on preparing, managing, and responding to cybersecurity incidents;

(7) assisting non-Federal entities in developing and coordinating vulnerability disclosure programs consistent with Federal and information security industry standards;

(8) assisting State, local, Tribal, and territorial governments, on a voluntary basis, in the development of State cybersecurity plans;

(9) coordinating with appropriate officials within the Agency; and

(10) performing such other duties as determined necessary by the Director to achieve the goal of managing cybersecurity risks in the United States and reducing the impact of cyber threats to non-Federal entities.

(c) Feedback

The Director shall consult with relevant State, local, Tribal, and territorial officials regarding the appointment, and State, local, Tribal, and territorial officials and other non-Federal entities regarding the performance, of the Cybersecurity State Coordinator of a State.

(Pub. L. 107–296, title XXII, §2217, formerly §2215, as added Pub. L. 116–283, div. A, title XVII, §1717(a)(1)(B), Jan. 1, 2021, 134 Stat. 4099 ; renumbered §2217 and amended Pub. L. 117–81, div. A, title XV, §1547(b)(1)(A)(iv), Dec. 27, 2021, 135 Stat. 2061 .)

Ernesto Ballesteros, JD, MS, CISSP, CISA
Cybersecurity State Coordinator of Texas
Email: ernesto.ballesteros@cisa.dhs.gov

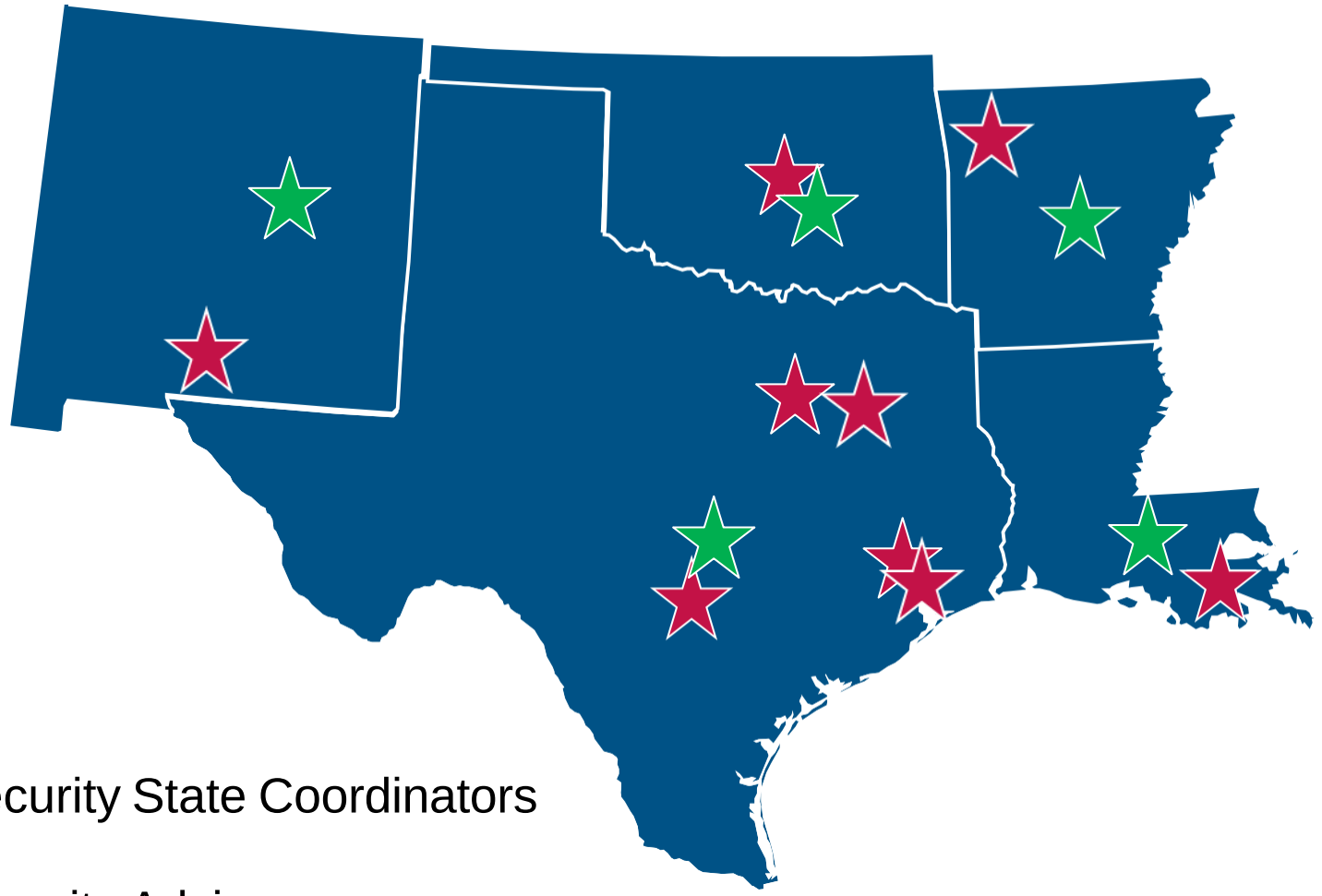
Cybersecurity Advisors (CSAs)

Cybersecurity Advisors (CSAs)

Provide direct coordination, outreach, and regional support in order to protect cyber components essential to the sustainability, preparedness, and protection of the Nation's Critical Infrastructure and Key Resources (CIKR) and State, Local, Tribal, and Territorial (SLTT) governments.

- **Assess**: Evaluate critical infrastructure cyber risk.
- **Promote**: Encourage best practices and risk mitigation strategies.
- **Build**: Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate**: Inform and raise awareness.
- **Listen**: Collect stakeholder requirements.
- **Coordinate**: Bring together incident support and lessons learned.

Region 6 | Cybersecurity Personnel



Cybersecurity State Coordinators

Cybersecurity Advisors

CISA's No-Cost Cybersecurity Resources

NO-Cost/Federally Funded

- **Cybersecurity Assessments**
  - Baseline Assessments
    - Ransomware Readiness Assessment (RRA)
    - Cybersecurity Performance Goals (CPG)
  - Intermediate Assessments
    - Cyber Infrastructure Survey (CIS)
    - Cyber Resilience Essentials (CRE)
  - Advanced Assessments
    - External Dependencies Management (EDM)
    - Incident Management Review (IMR)
    - Cyber Resilience Review (CRR)
- **Cyber Hygiene Services**
  - External Vulnerability Scanning Service
  - Web Application Scanning Service

- **Workshops & Exercises**
  - Asset Management Workshop (AMW)
  - Cyber Resilience Workshop (CRW)
  - Incident Management Workshop (IMW)
  - Vulnerability Management Workshop (VMW)
  - Digital Forensics Workshop I (DFW I)
  - Digital Forensics Workshop II (DFW II)
  - Cyber Tabletop Exercise (CTTX)
- **Technical Assessments***
  - Remote Penetration Test (RPT)
  - Risk and Vulnerability Assessment (RVA)
  - Validated Architecture Design Review (VADR)

***Note:** Eligibility for technical assessments is contingent upon assessment of the stakeholder's capabilities by their Cybersecurity Advisor (CSA).

Today's Risk Landscape

America remains at risk from a variety of threats:

INSIDER THREAT

ACTS OF TERRORISM

CYBER ATTACKS

EXTREME WEATHER

PANDEMICS

ACCIDENTS OR TECHNICAL FAILURES

Critical Infrastructure Cyber Risk Landscape Summary

Critical infrastructure is continuously targeted by a variety of threat actors, including opportunists, hacktivists, nation-state sponsored threat actors—such as groups back by the People's Republic of China (PRC), Russia, and Iran—advanced persistent threats (APTs), financially motivated actors, and insider threats.

Goals:

- Disrupt national critical functions;
- Obtain and ransom sensitive data;
- Undermine U.S. global standing;
- Sow discord inside the U.S.; and
- Undermine public confidence in U.S. institutions.

In recent years malicious cyber actors have targeted vulnerable infrastructure with a variety of cyber-based attacks, including DDoS attacks, phishing attacks, ransomware attacks, and more.

This trend is likely to continue due to the sector's limited cybersecurity resources, push for technology integration, and significant third-party dependencies.

ODNI 2023 Annual Threat Assessment

Russia - Remains a top cyber threat as it refines and employs its espionage, influence, and attack capabilities.

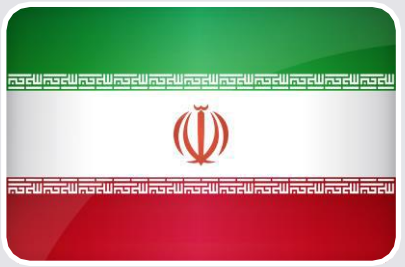
- Continues to target critical infrastructure, including underwater cables and industrial control systems.

- Considers cyber attacks an acceptable option to deter adversaries, control escalation, and prosecute conflicts.

China - Presents a prolific and effective cyber-espionage threat, possesses substantial cyber-attack capabilities, and presents a growing influence threat.

- Cyber pursuits and proliferation of related technologies increase the threats of cyber attacks against the US.

- Can cause localized, temporary disruptions to critical infrastructure within the US.



Iran - Expertise and willingness to conduct aggressive cyber operations make it a significant threat to the security of US networks and data.

- Has the ability to conduct attacks on critical infrastructure, as well as to conduct influence and espionage activities.

- Responsible for multiple cyber attacks against Israeli water facilities.

North Korea - Cyber program poses a growing espionage, theft, and attack threat.

- Possesses the expertise to cause temporary, limited disruptions of some critical infrastructure networks and disrupt business networks.

- Conducted cyber theft against financial institutions and cryptocurrency exchanges worldwide.

ODNI 2023 Annual Threat Assessment

Russia - Remains a top cyber threat as it refines and employs its **espionage**, influence, and attack capabilities.

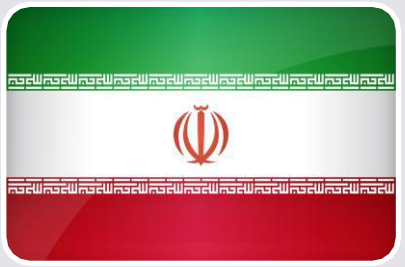
- Continues to target critical infrastructure, including underwater cables and industrial control systems.

- **Considers cyber attacks an acceptable option to deter adversaries, control escalation, and prosecute conflicts.**

China - Presents a prolific and effective **cyber-espionage threat**, possesses substantial cyber-attack capabilities, and presents a growing influence threat.

- Cyber pursuits and proliferation of related technologies increase the threats of cyber attacks against the US.

- Can cause localized, temporary **disruptions to critical infrastructure** within the US.



Iran - Expertise and willingness to conduct aggressive cyber operations make it a significant threat to the security of US networks and data.

- Has the **ability to conduct attacks on critical infrastructure**, as well as to conduct influence and espionage activities.

- **Responsible for multiple cyber attacks against Israeli water facilities.**

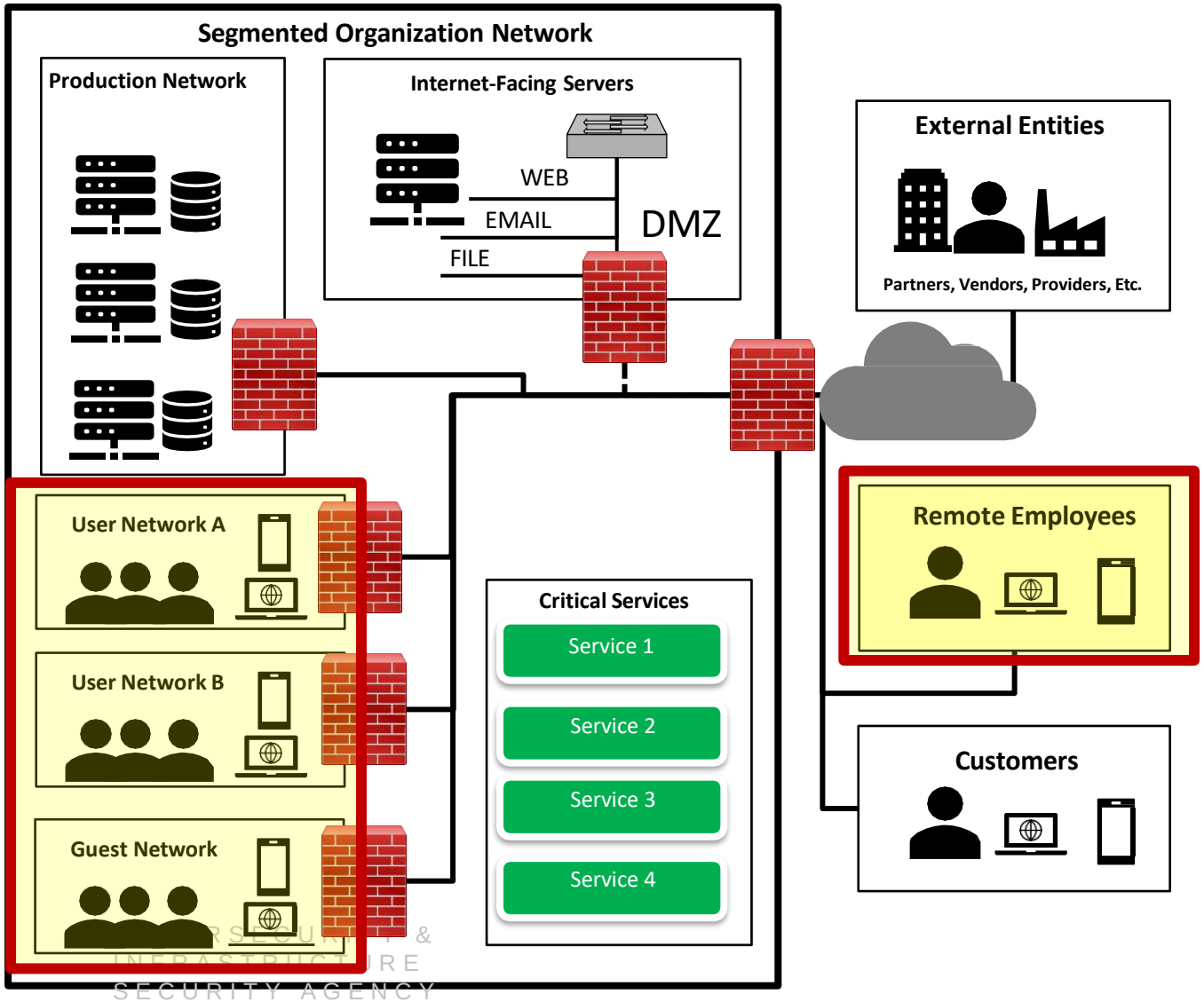
North Korea - Cyber program poses a growing espionage, theft, and attack threat.

- Possesses the expertise to cause temporary, limited disruptions of some critical infrastructure networks and disrupt business networks.

- Conducted **cyber theft against financial institutions** and cryptocurrency exchanges worldwide.

How Attackers Gain Initial Access

Common Attack Vectors: How Hackers Gain Access

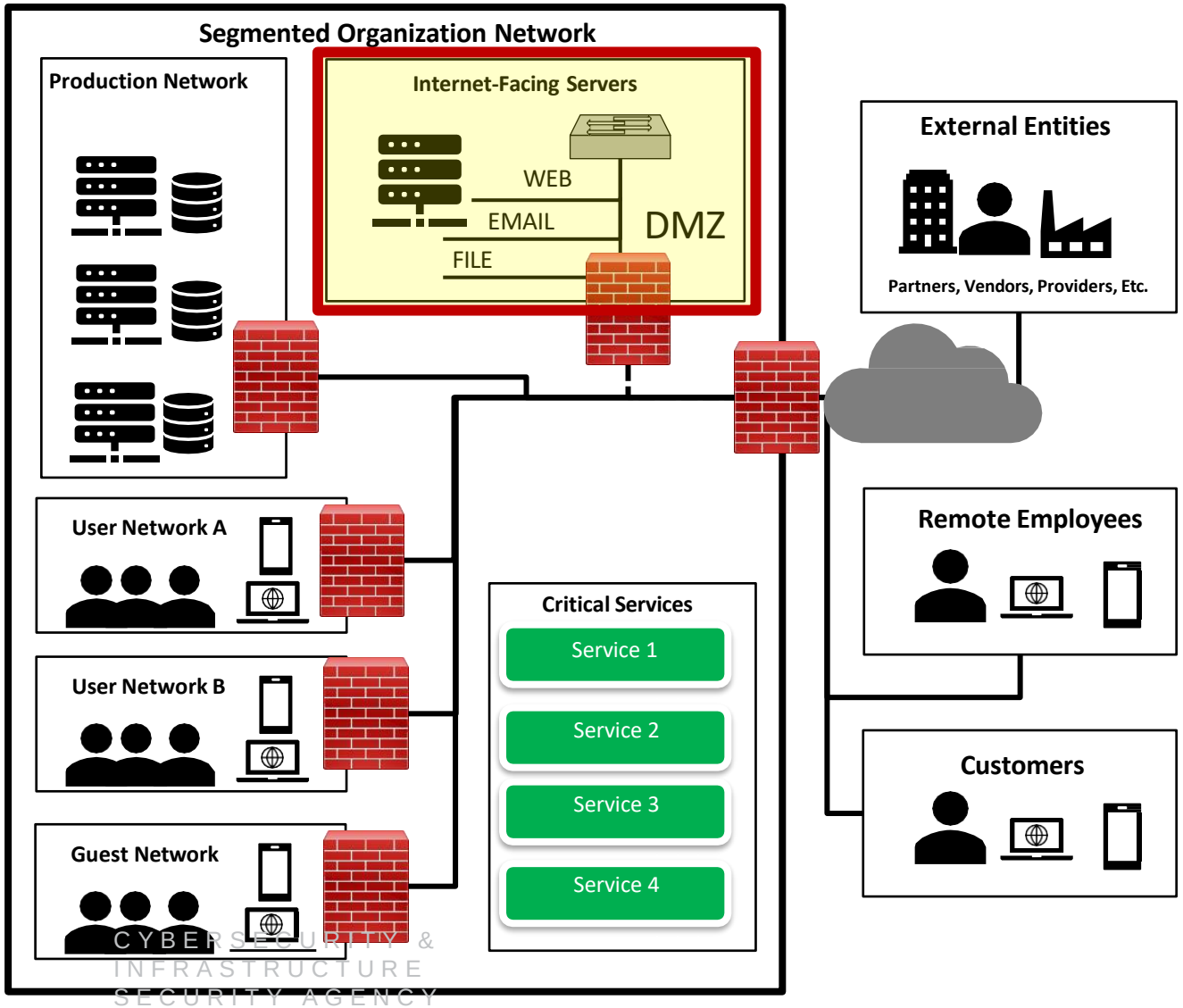


Common Vectors Threat Actors Use to Gain Access to Your Organization

Common Targets/Vectors:

1. **Vulnerable Users**
   a. Users have vulnerabilities that can be easily exploited
   b. Users are only an email or phone call away

Common Attack Vectors: How Hackers Gain Access

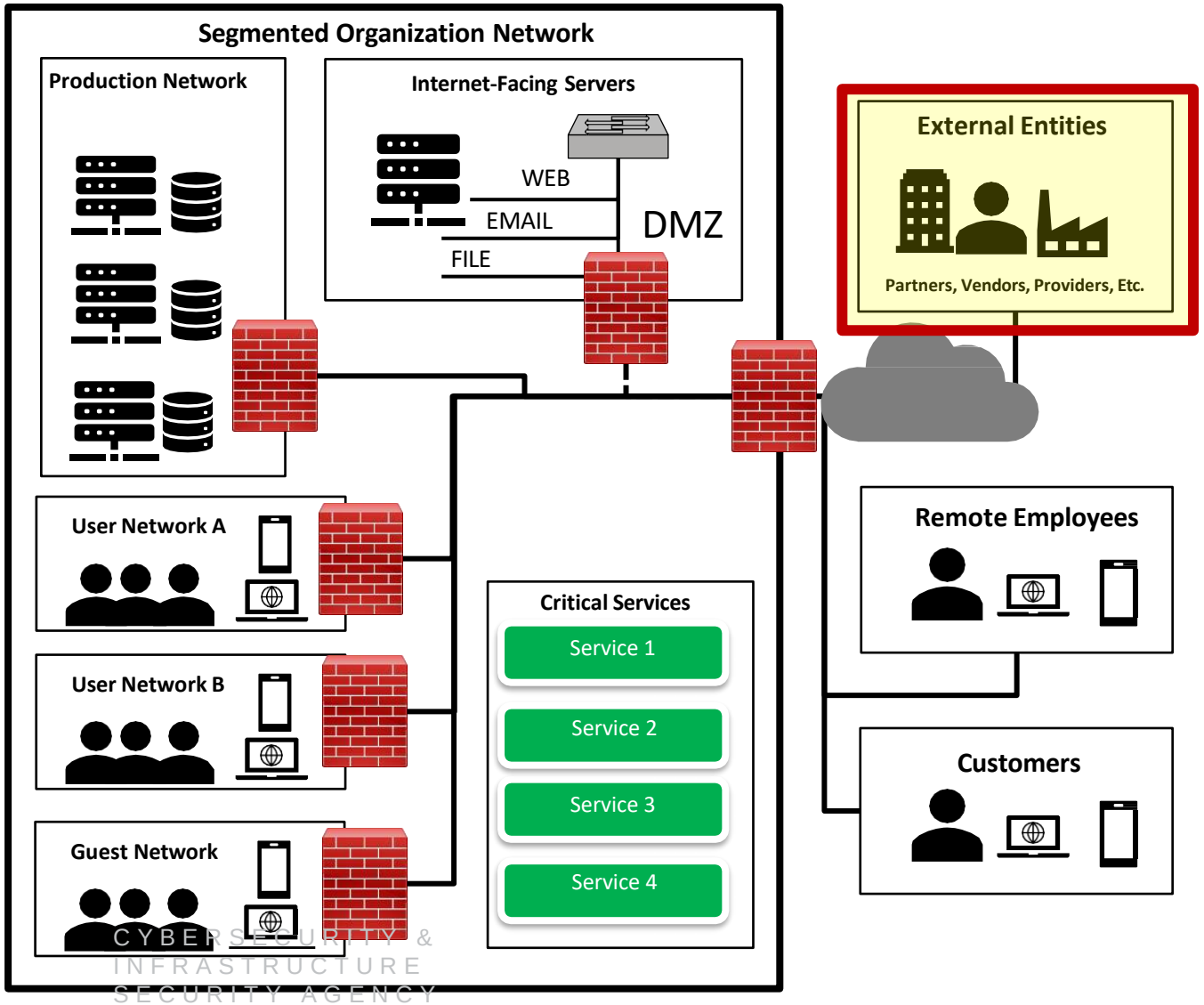


Common Vectors Threat Actors Use to Gain Access to Your Organization

Common Targets/Vectors:

1. **Vulnerable Users**
   a. Users have vulnerabilities that can be easily exploited
   b. Users are only an email or phone call away
2. **Vulnerable Internet-Facing Devices**
   a. These are accessible to anyone with an internet connection
   b. They may be vulnerable due to a misconfiguration or outdated software that can be exploited by a threat actor

Common Attack Vectors: How Hackers Gain Access



Common Vectors Threat Actors Use to Gain Access to Your Organization

Common Targets/Vectors:

1. **Vulnerable Users**
   a. Users have vulnerabilities that can be easily exploited
   b. Users are only an email or phone call away
2. **Vulnerable Internet-Facing Devices**
   a. These are accessible to anyone with an internet connection
   b. They may be vulnerable due to a misconfiguration or outdated software that can be exploited by a threat actor
2. **Vulnerable External Entities**
   a. Vendors may have vulnerable users
   b. Vendors may also have vulnerable internet-facing devices
   c. Each may be exploited by threat actors

Common Attacks

Social Engineering Attacks

Social Engineering Attacks

- **Description**:
  - According to NIST, **social engineering** refers to *"[t]he act of deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust."* **Source:** NIST SP 800-63-3 Digital Identity Guidelines
- **Threat Vector:**
  - Vulnerable users
- **Threat Actor Objective**:
  - Manipulate a target (i.e., a user) into providing unauthorized access to personnel, information, technology, and facilities.
- **Common Threat Actor Techniques**:
  - Phishing (generalized email-based social engineering attack)
  - Spear Phishing (targeted email-based social engineering attack)
  - SMISHING (SMS-based social engineering attack)
  - VISHING (Voicemail-based social-engineering attack)
  - Masquerading (In-Person/Physical)

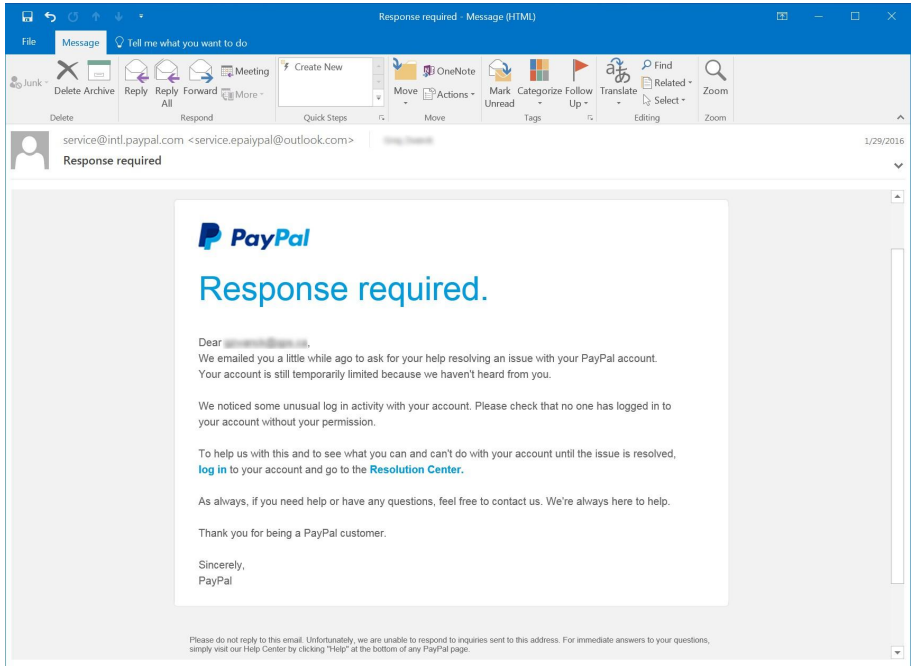


Image Source: knowbe4.com

Phishing Indicators

Common Indicators of Phishing

- **Suspicious sender's address** that may imitate a legitimate business
- **Generic greetings and signature** and a lack of contact information in the signature block
- **Spoofed hyperlinks and websites** that do not match the text when hovering over them
- **Misspelling**, poor grammar or sentence structure, and inconsistent formatting
- **Suspicious attachments** or requests to download and open an attachment

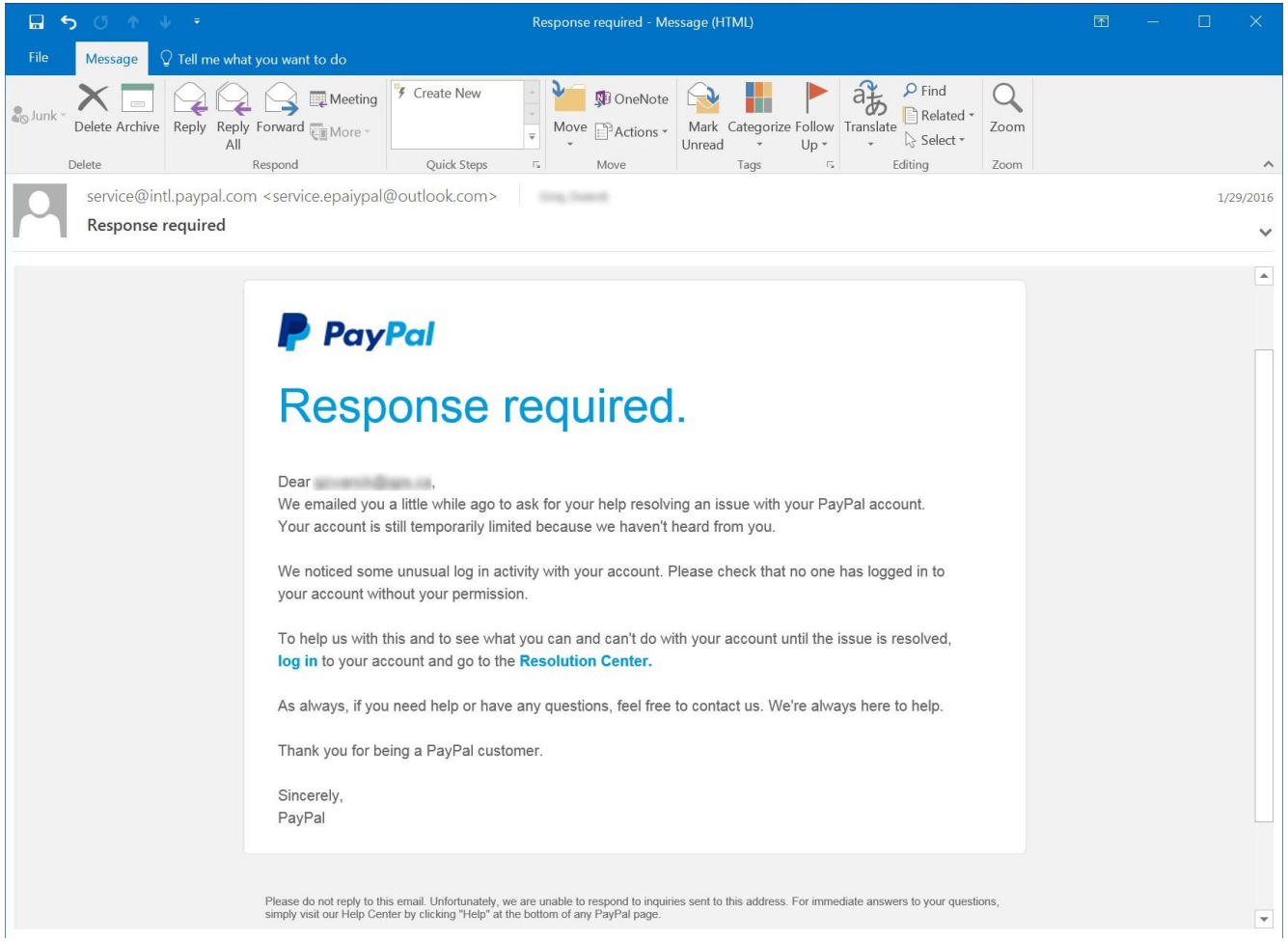


Image Source: knowbe4.com

Note: For more details on how to defend against phishing attacks, see CISA's *Phishing Guidance: Stopping the Attack Cycle at Phase One*.

Business Email/Email Account Compromise Attack

Business Email Compromise/Email Account Compromise Attacks

- **Description**:
  - According to the FBI, a **Business Email Compromise/Email Account Compromise (BEC/EAC)** attack is *"Business Email Compromise/Email Account Compromise (BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests… frequently carried out when an individual compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds."* **Source**: FBI IC3 Alert Number: I-050422
- **Threat Vector:**
  - Vulnerable users
- **Threat Actor Objective**:
  - Gain unauthorized access to a victim's email account.
  - Use compromised account to abuse trusted relationships with account contacts to:
    - Induce fraudulent transfer of funds (via wire transfer)
    - Target additional victims in the compromised account's contact list
- **Common Threat Actor Techniques**:
  - Brute force password guessing (e.g., password spraying);
  - Social engineering (phishing) to acquire unauthorized access to victim's accounts; and
  - Malware (e.g., keyloggers) to acquire a victim's account credentials.

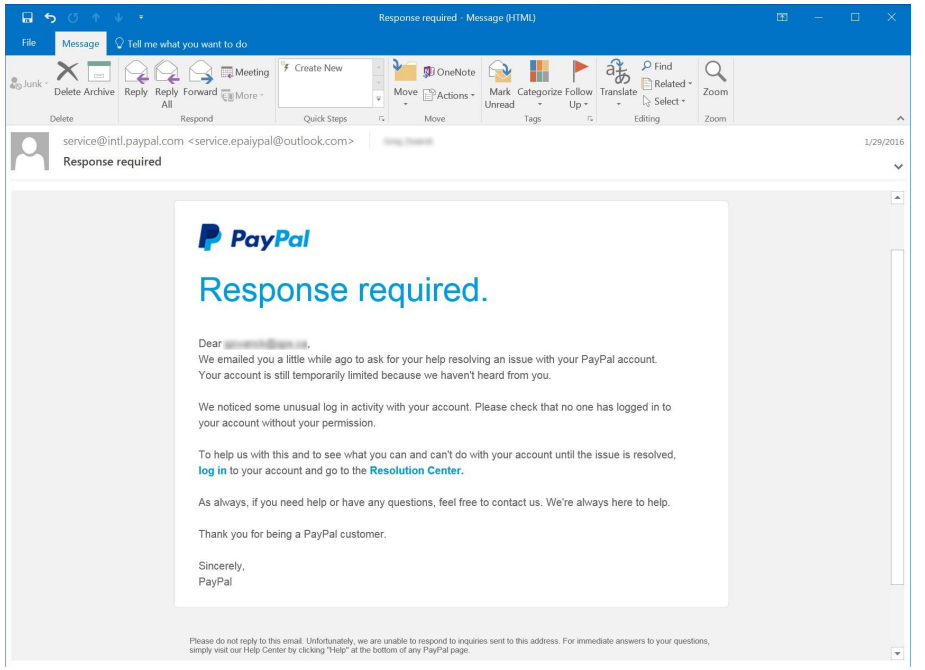


Image Source: knowbe4.com

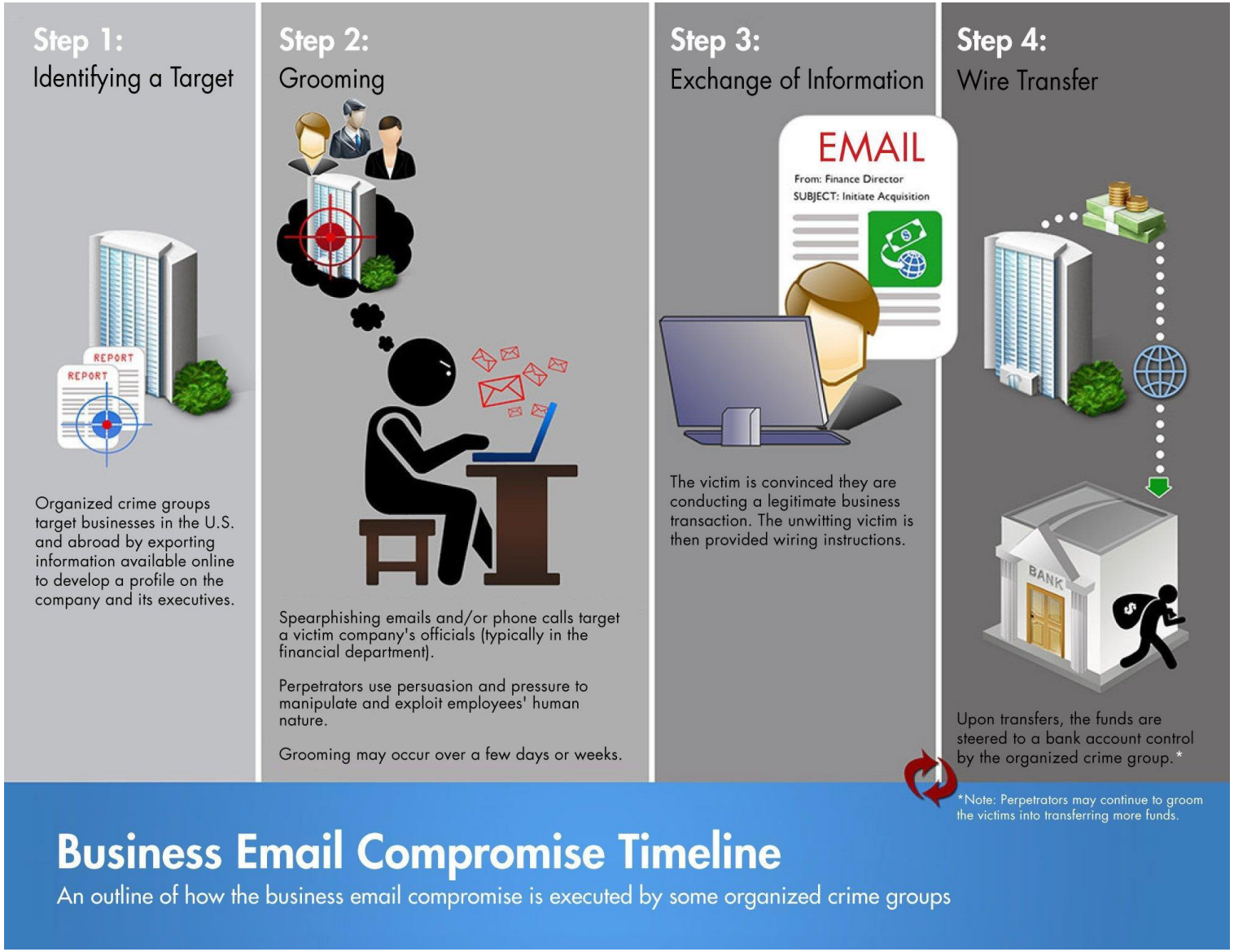
Business Email/Email Account Compromise (cont.)

How Criminals Carry Out BEC Scams

A scammer might:

- **Spoof an email account or website.** Slight variations on legitimate addresses (john.kelly@examplecompany.com vs. john.kelley@examplecompany.com) fool victims into thinking fake accounts are authentic.
- **Send spearphishing emails.** These messages look like they're from a trusted sender to trick victims into revealing confidential information. That information lets criminals access company accounts, calendars, and data that gives them the details they need to carry out the BEC schemes.
- **Use malware.** Malicious software can infiltrate company networks and gain access to legitimate email threads about billing and invoices. That information is used to time requests or send messages so accountants or financial officers don't question payment requests. Malware also lets criminals gain undetected access to a victim's data, including passwords and financial account information.

Source: Business Email Compromise — FBI

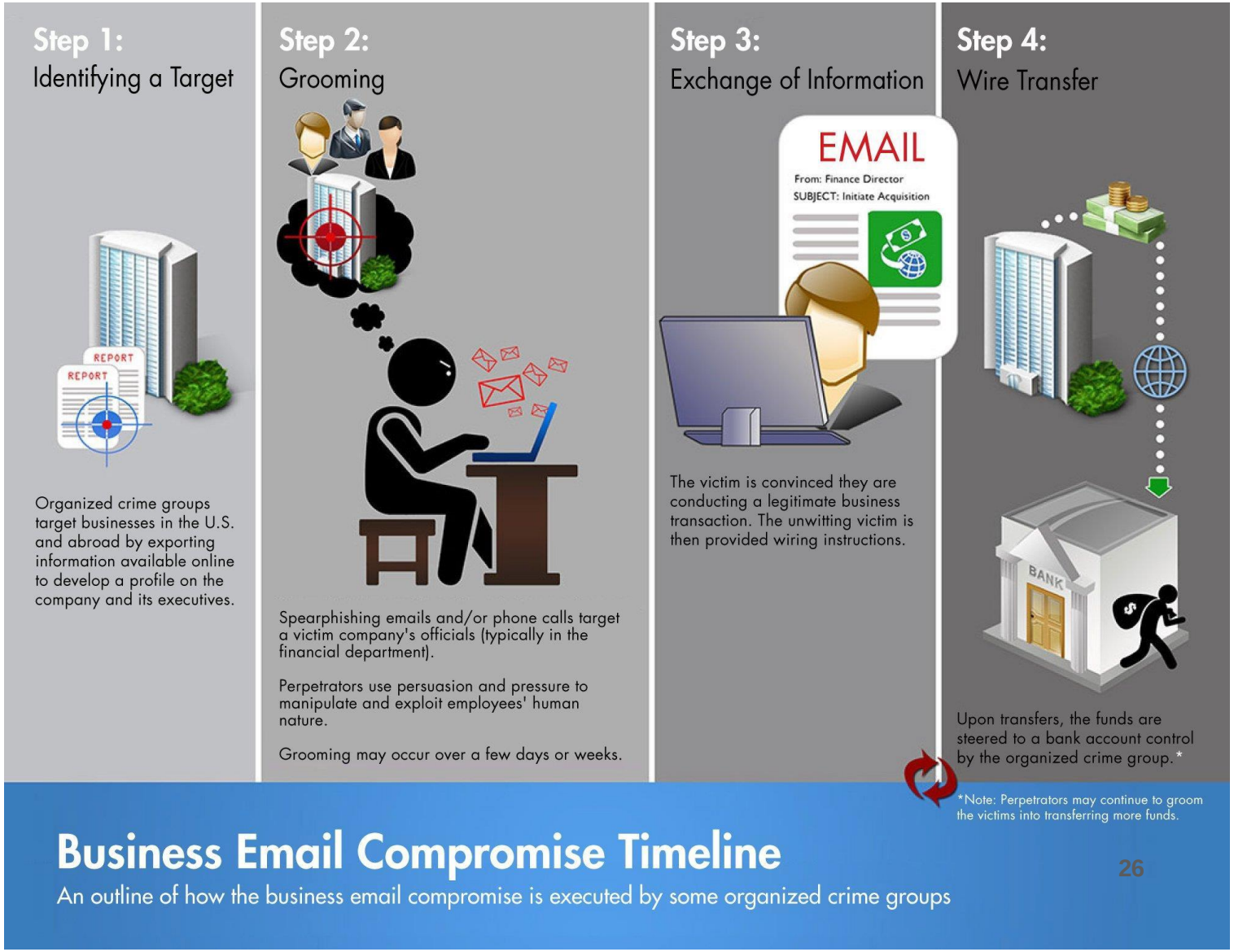


Business Email/Email Account Compromise (cont.)

How to Protect Yourself

- **Don’t overshare information online**:
  - Sharing things like pet names, schools attended, family members, and birthdays give attackers information they can use to guess passwords or account security questions.
- **Scrutinize emails/text messages**:
  - Carefully examine the email address, URL, and spelling used in any correspondence.
- **Email attachments**:
  - Never open an email attachment from someone you don’t know and be wary of email attachments forwarded to you.
- **Email/text message links**:
  - Don’t click on links in unsolicited emails or text messages asking you to update or verify account information.
- **Two-factor authentication**:
  - Setup two-factor authentication for any account that allows it.
- **Verifying payment and purchase requests**:
  - Verify payment and purchase requests in person, if possible, or by calling the person to make sure it is legitimate.
  - Verify any change in account number or payment procedures with the person making the request.
- **Pressure tactics**:
  - Be especially wary if the requestor is pressing you to act quickly.

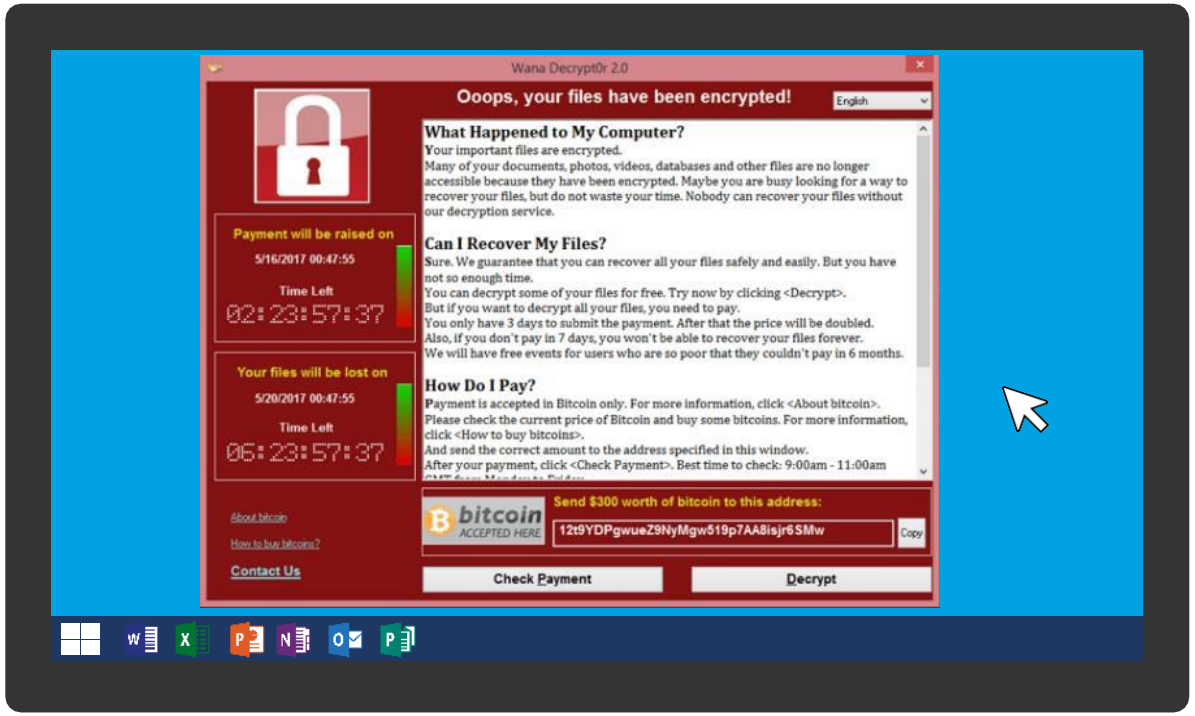
Source: Business Email Compromise — FBI



Ransomware Attack

Ransomware Attack

- **Description:**
  - The term "**ransomware**" refers to *"a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption."* **Source**: CISA Ransomware Guide 2020
- **Threat Vector:**
  - Vulnerable users and technology
- **Threat Actor Objective**:
  - Hold your data for ransom
- **Common Threat Actor Techniques**:
  - Gain unauthorized access to your network
    - Compromise vulnerable users via social engineering
    - Compromise vulnerable systems via technical exploit
  - Compromise accounts
  - Establish a foothold in victim network
  - Encrypt and exfiltrate victim data
  - Hold the data for ransom

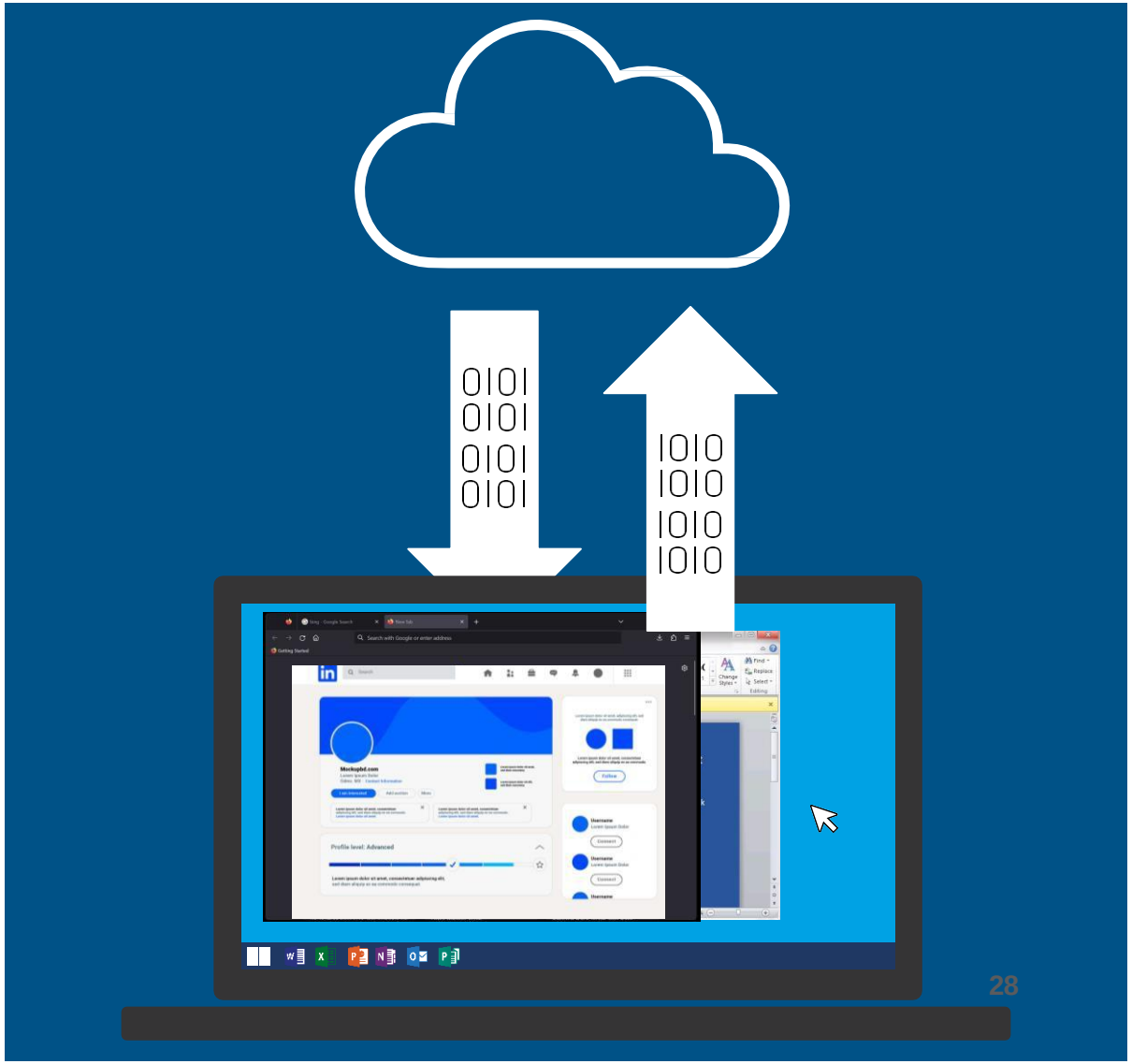


Ransomware Attacks (cont.)

How Ransomware Works (simplified phishing scenario)

Threat Actor

- Plans
  - Identify target organization
- Identifies
  - Identify target users, internet-facing systems, and known external partners
  - Identify vulnerabilities in users, systems, and partners
  - Identify potential exploits
- Attacks
  - Phishing email with malicious attachment sent to target
  - Target opens malicious attachment
    - Macro opens command line
    - Runs PowerShell script that downloads malware from an external system
    - Malware is executed on victim machine, creating remote access infrastructure for executing ransomware attack
  - Attacker identifies:
    - Information to encrypt, exfiltrate and hold for ransom
    - Systems to disrupt
  - Attacker launches ransomware attack:
    - Information is encrypted and exfiltrated
    - System backups are wiped
    - Demands ransom in exchange for decryption key

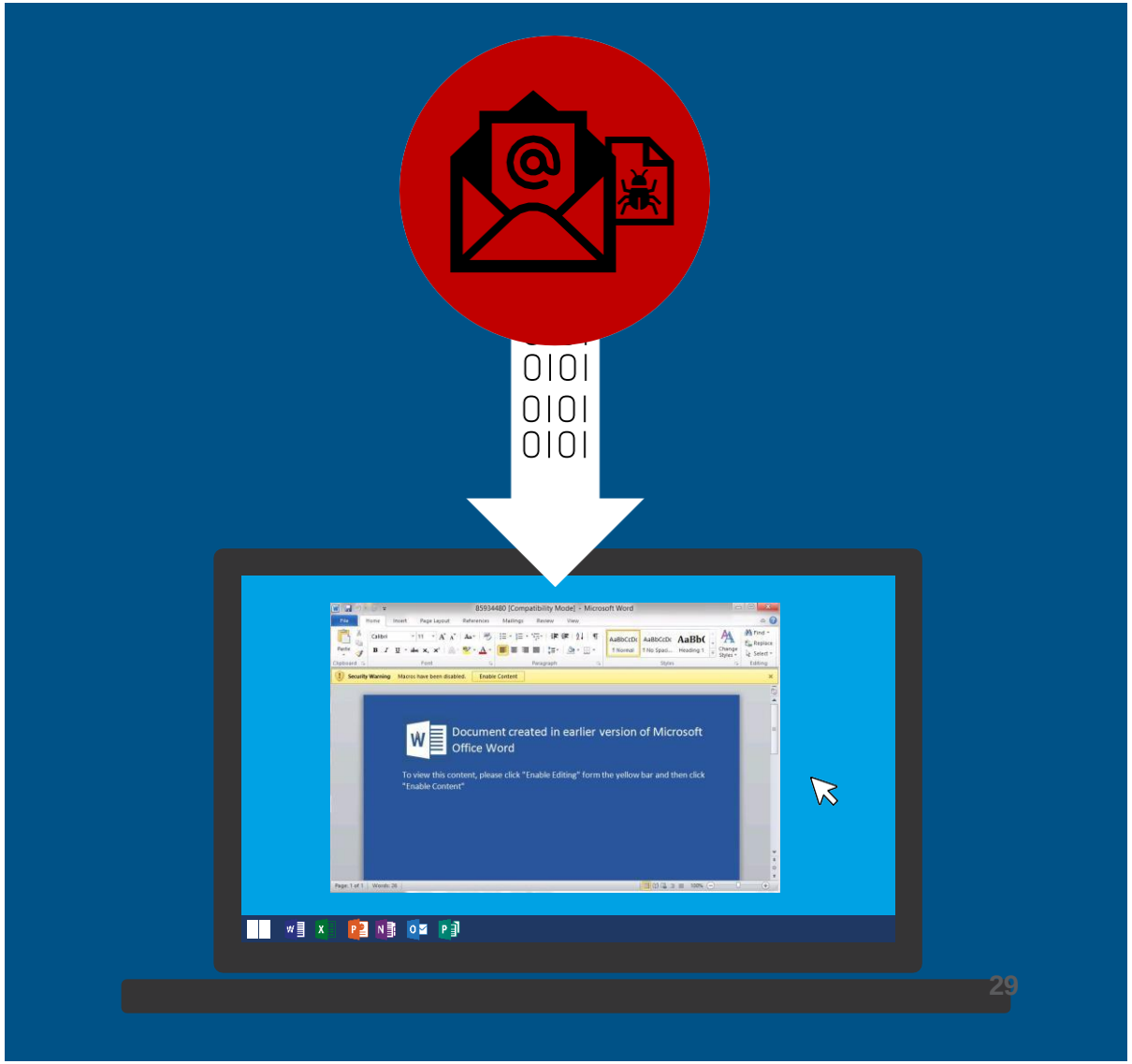


Ransomware (cont.)

How Ransomware Works (simplified)

Threat Actor

- Identifies
  - Identify target organization
  - Identify target users, internet-facing systems, and known external partners
  - Identify vulnerabilities in users, systems, and partners
  - Identify potential exploits
- Attacks
  - Phishing email with malicious attachment sent to target
  - Target opens malicious attachment
    - Macro opens command line
    - Runs PowerShell script that downloads malware from an external system
    - Malware is executed on victim machine, creating remote access infrastructure for executing ransomware attack
  - Attacker identifies:
    - Information to encrypt, exfiltrate and hold for ransom
    - Systems to disrupt
  - Attacker launches ransomware attack:
    - Information is encrypted and exfiltrated
    - System backups are wiped
    - Demands ransom in exchange for decryption key

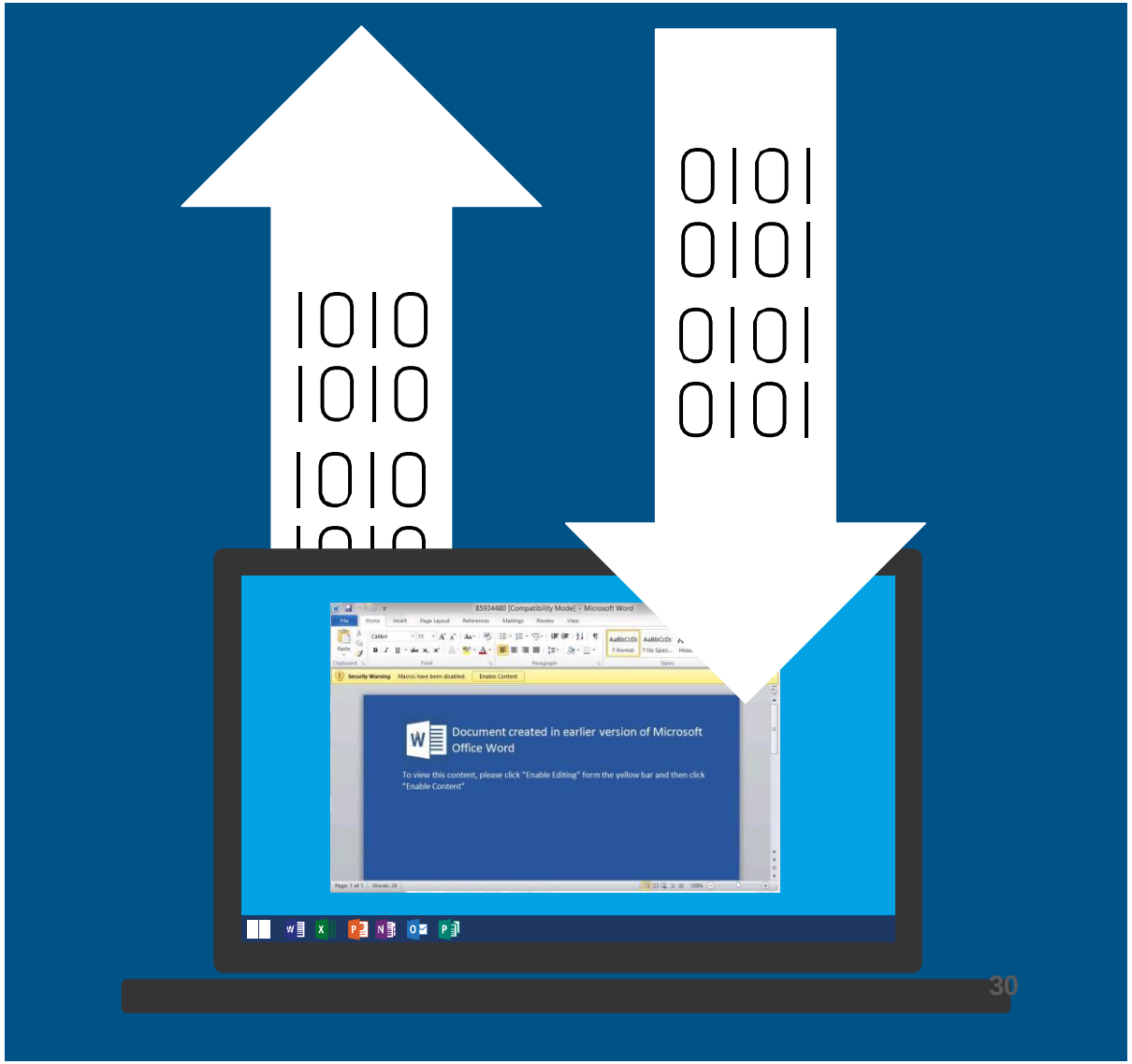


Ransomware (cont.)

How Ransomware Works (simplified)

Threat Actor

- Identifies
  - Identify target organization
  - Identify target users, internet-facing systems, and known external partners
  - Identify vulnerabilities in users, systems, and partners
  - Identify potential exploits
- Attacks
  - Phishing email with malicious attachment sent to target
  - Target opens malicious attachment
    - Macro opens command line in the background
    - Runs PowerShell script that downloads malware from an external system
    - Malware is executed on victim machine, creating remote access infrastructure for executing ransomware attack
  - Attacker identifies:
    - Information to encrypt, exfiltrate and hold for ransom
    - Systems to disrupt
  - Attacker launches ransomware attack:
    - Information is encrypted and exfiltrated
    - System backups are wiped
    - Demands ransom in exchange for decryption key

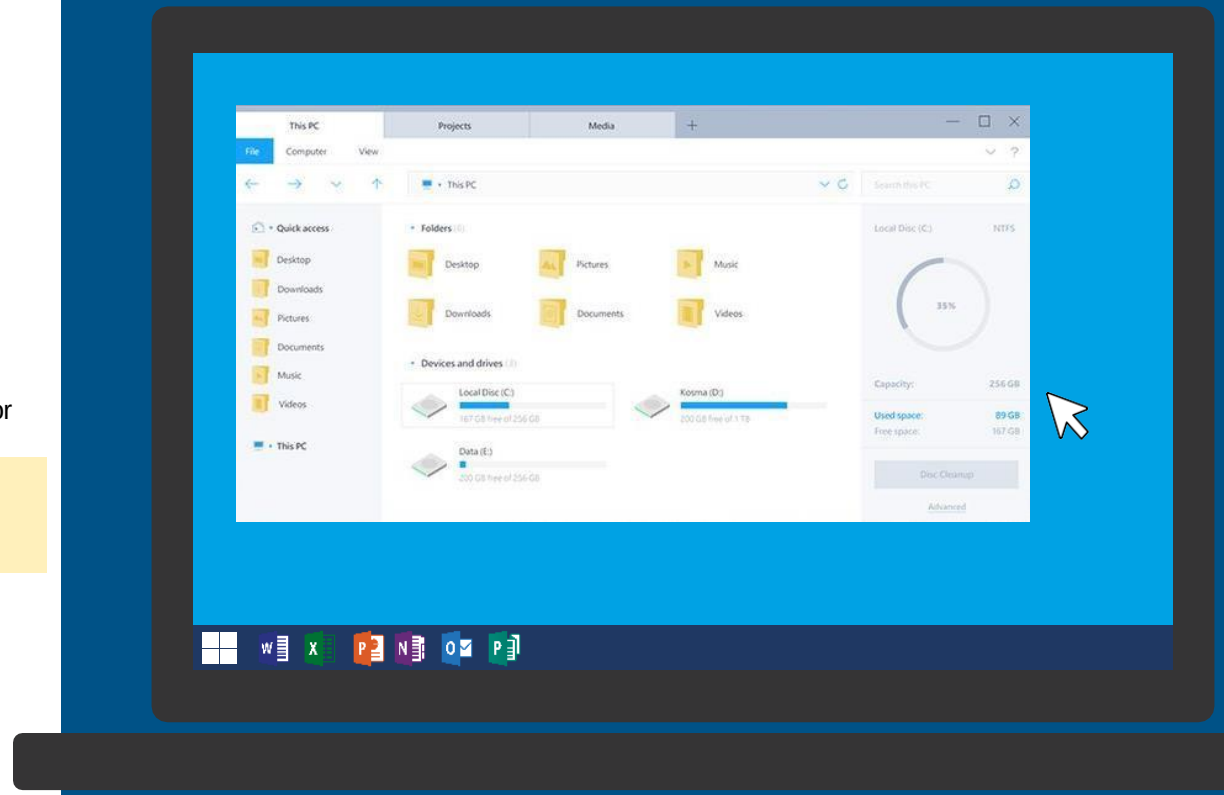


Ransomware (cont.)

How Ransomware Works (simplified)

Threat Actor

- Identifies
  - Identify target organization
  - Identify target users, internet-facing systems, and known external partners
  - Identify vulnerabilities in users, systems, and partners
  - Identify potential exploits
- Attacks
  - Phishing email with malicious attachment sent to target
  - Target opens malicious attachment
    - Macro opens command line in the background
    - Runs PowerShell script that downloads malware from an external system
    - Malware is executed on victim machine, creating remote access infrastructure for executing ransomware attack
  - Attacker identifies:
    - Information to encrypt, exfiltrate and hold for ransom
    - Systems to disrupt
  - Attacker launches ransomware attack:
    - Information is encrypted and exfiltrated
    - System backups are wiped
    - Demands ransom in exchange for decryption key

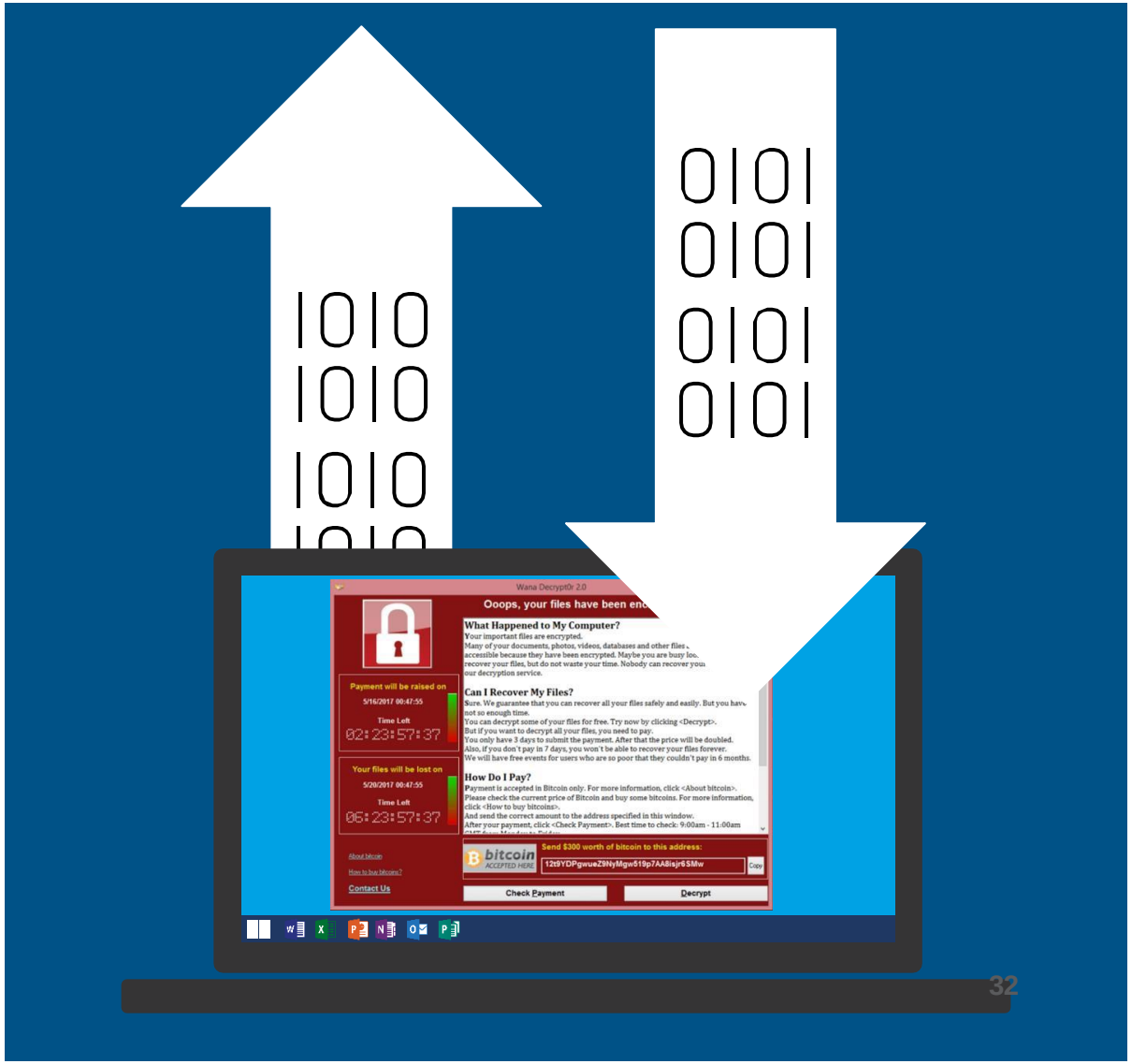


Ransomware (cont.)

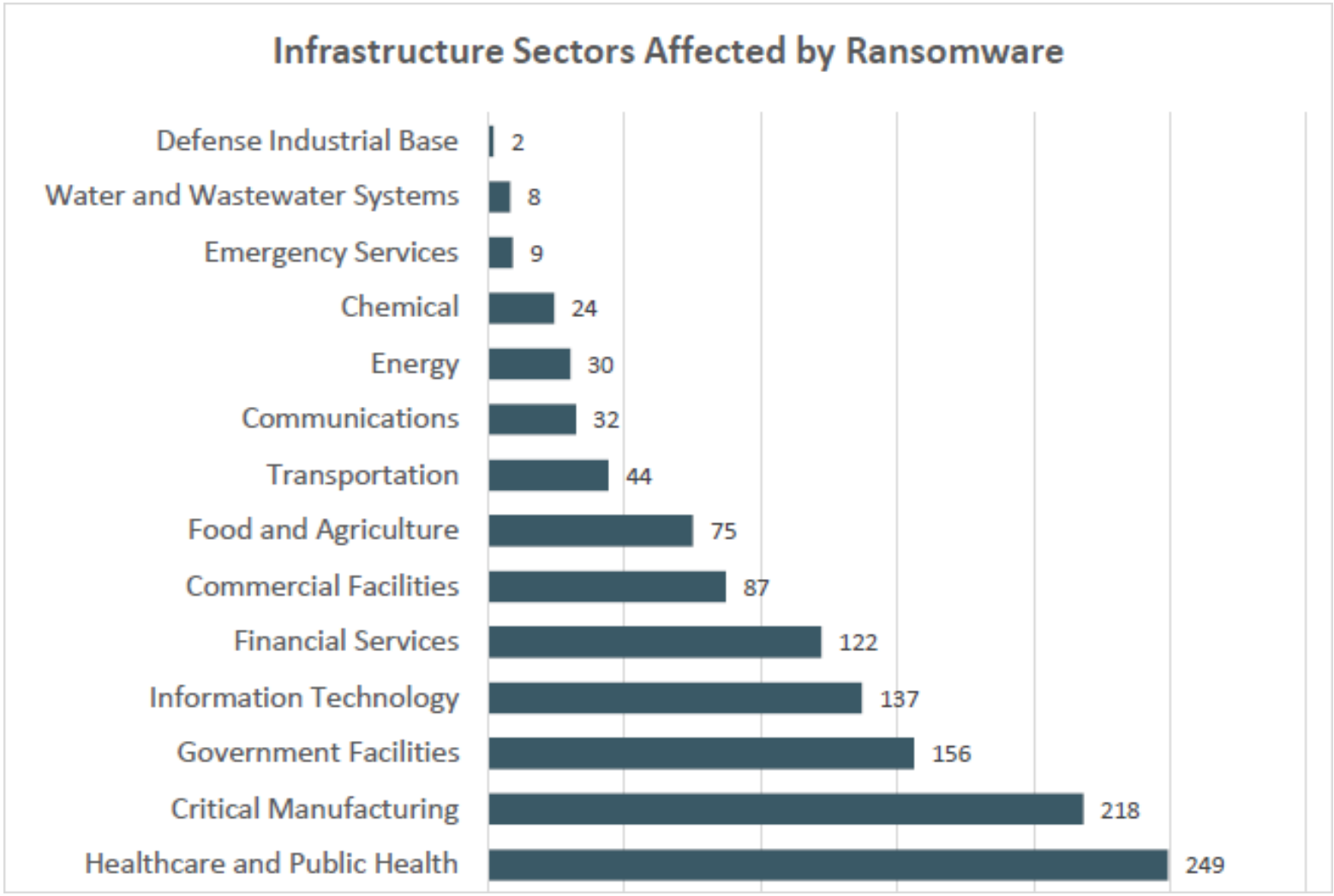
How Ransomware Works (simplified)

Threat Actor

- Identifies
  - Identify target organization
  - Identify target users, internet-facing systems, and known external partners
  - Identify vulnerabilities in users, systems, and partners
  - Identify potential exploits
- Attacks
  - Phishing email with malicious attachment sent to target
  - Target opens malicious attachment
    - Macro opens command line in the background
    - Runs PowerShell script that downloads malware from an external system
    - Malware is executed on victim machine, creating remote access infrastructure for executing ransomware attack
  - Attacker identifies:
    - Information to encrypt, exfiltrate and hold for ransom
    - Systems to disrupt
  - Attacker launches ransomware attack:
    - Information is encrypted and exfiltrated
    - System backups are wiped
    - Demands ransom in exchange for decryption key

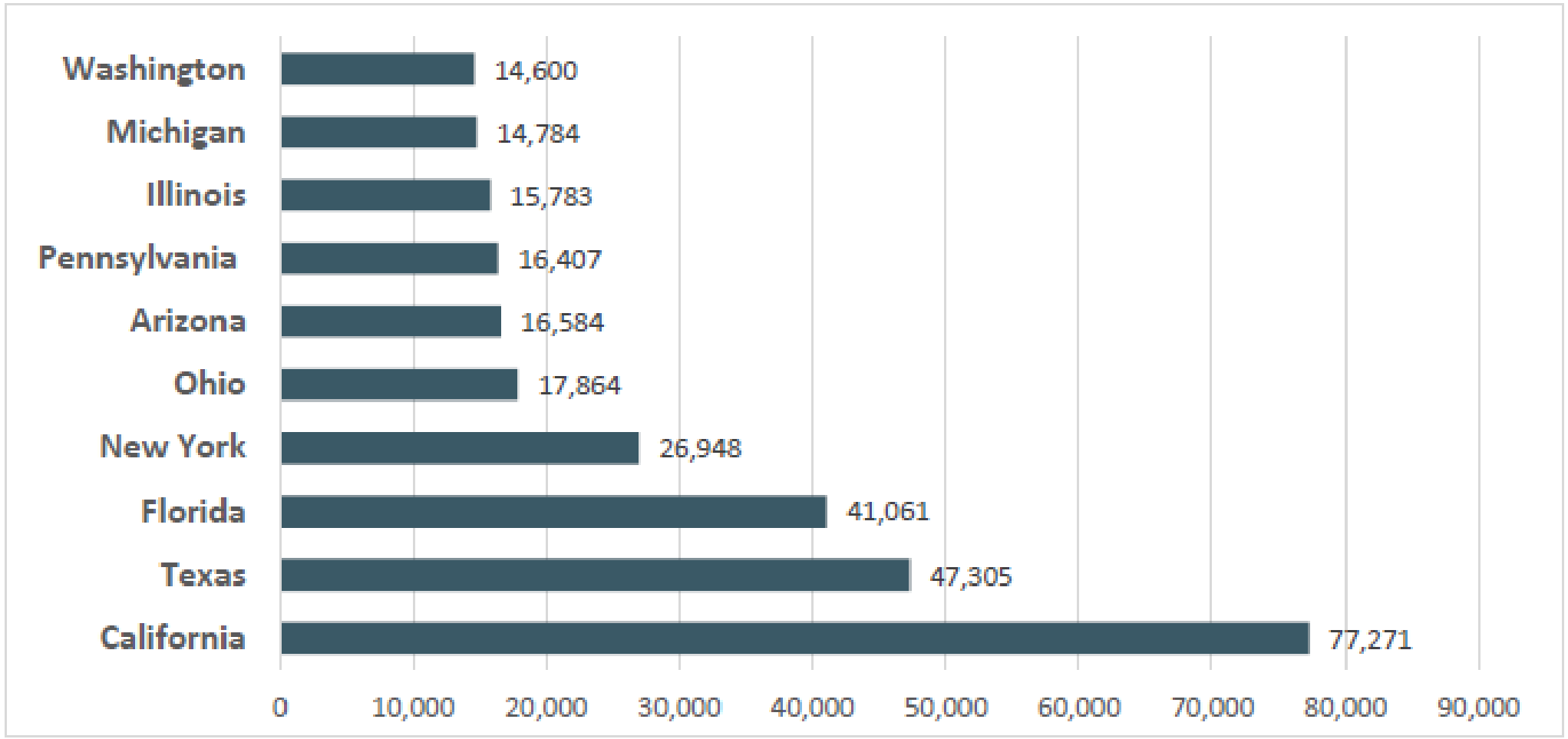


2023 – Infrastructure Sectors Victimized by Ransomware



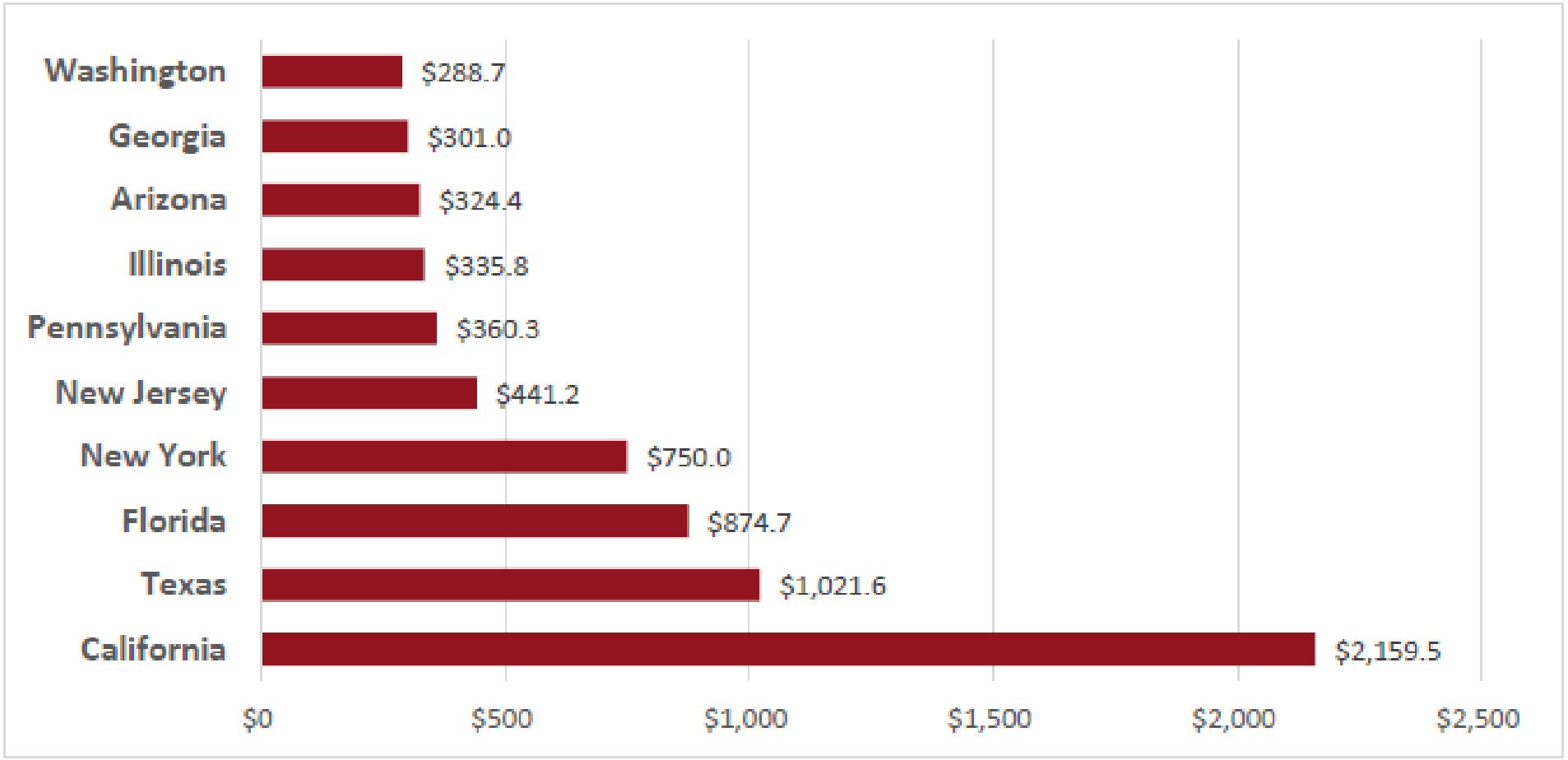
Source [FBI IC3 2023 Annual Report]

2023 – Top 10 States by Number of Victims



Source [FBI IC3 2023 Annual Report]

2023 – Top 10 States by Victim Loss (in Millions)



Source [FBI IC3 2023 Annual Report]

Recent Cyber Attacks in Texas

North Texas Municipal Water District hit by 'cybersecurity incident'

Nov 28, 2023

WYLIE, Texas — The North Texas Municipal Water District was hit by a "cybersecurity incident," but water services have not been impacted, officials said Tuesday. The Wylie-based district, which serves water to 13 North Texas cities mostly north and northeast ...

Cyber-attack closes hospital emergency rooms in three US states

Nov 25, 2023

A cyber-attack has shut down emergency rooms in at least three states, a hospital operator warned on Monday, forcing the organization to divert patients to other facilities. Ardent Health, which oversees 30 hospitals in states across the US, including New .....

Cyberattack at Harris Center for Mental Health causes delays

Nov 6, 2023

Police are investigating a cyberattack against the Harris Center for Mental Health and IDD that was discovered on Tuesday. Authorities reported that the ransomware attack encrypted employee files, making them inaccessible to Harris Center staff. To prevent ...

Dallas County cyberattack claim to have stolen sensitive data

Oct 19, 2023

An international cyber hacker group is threatening to publish sensitive information it claims it stole from the Dallas County computer system unless the county pays a ransom by Friday. County officials confirmed a cyber incident was detected on Oct. 19. The county ...

City of Harlingen recovering from cyber attack

Oct 17, 2023

Phone services were restored Monday after the city of Harlingen was hit by a cyberattack that caused phone and internet services to be knocked out across all city departments. As the city works to restore service, a cybersecurity expert offers a warning to the

Cyber Attack on Greater Dallas Healthcare Enterprises, TX

Oct 2, 2023

On October 2, 2023, Greater Dallas Healthcare Enterprises ("GDHE") filed a notice of data breach with the Attorney General of Texas after discovering that an unauthorized third party gained access to an employee's email account. In this notice, GDHE .....

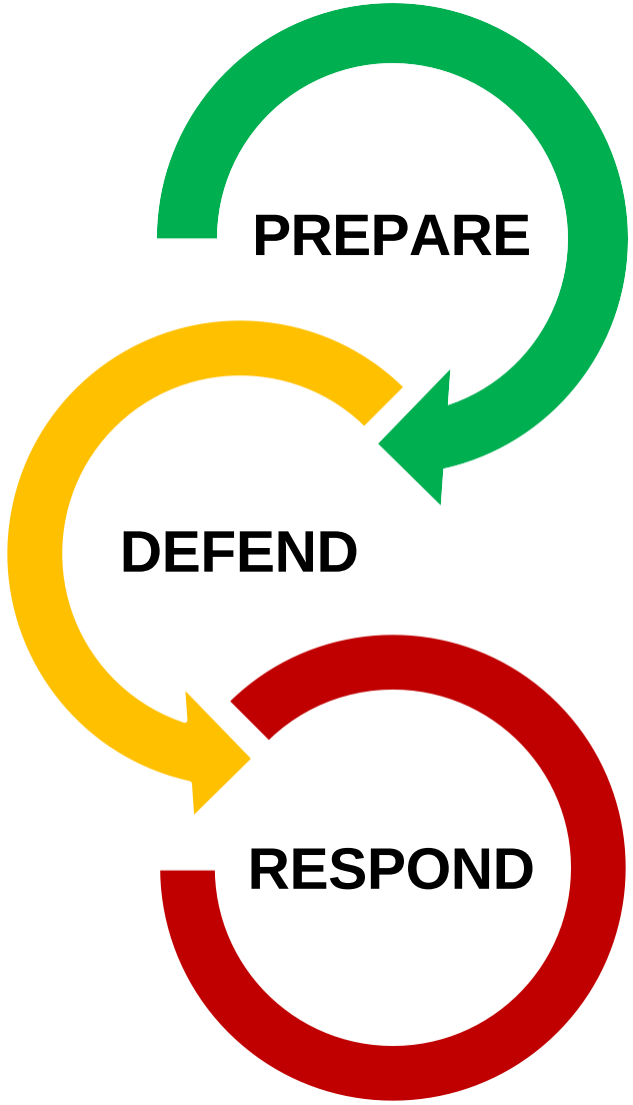
Source [FBI IC3 2023 Annual Report]

Building Cyber Resilience | Near-Term Strategies

Shields Up/Ready: Building Cyber Resilience

Cyber Resilience | Near-Term Strategies

- **Part 1: Cyber Resilience | Prepare**
  - Prepare for Cyber Incidents
- **Part 2: Cyber Resilience | Defend**
  - Identify and Mitigate Attack Vectors
- **Part 3: Cyber Resilience | Respond & Recover**
  - Detect & Analyze
  - Contain & Eradicate
  - Recover
  - Improve

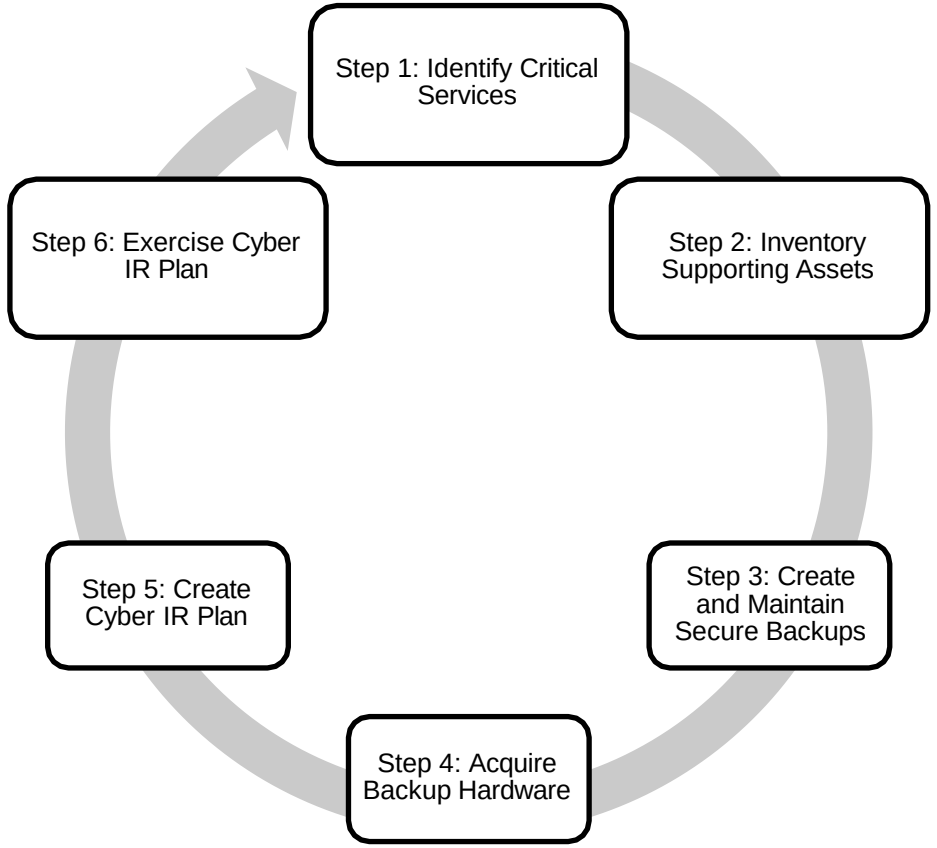


Cyber Resilience
Part 1 | Prepare

Cyber Resilience Part 1 | Prepare

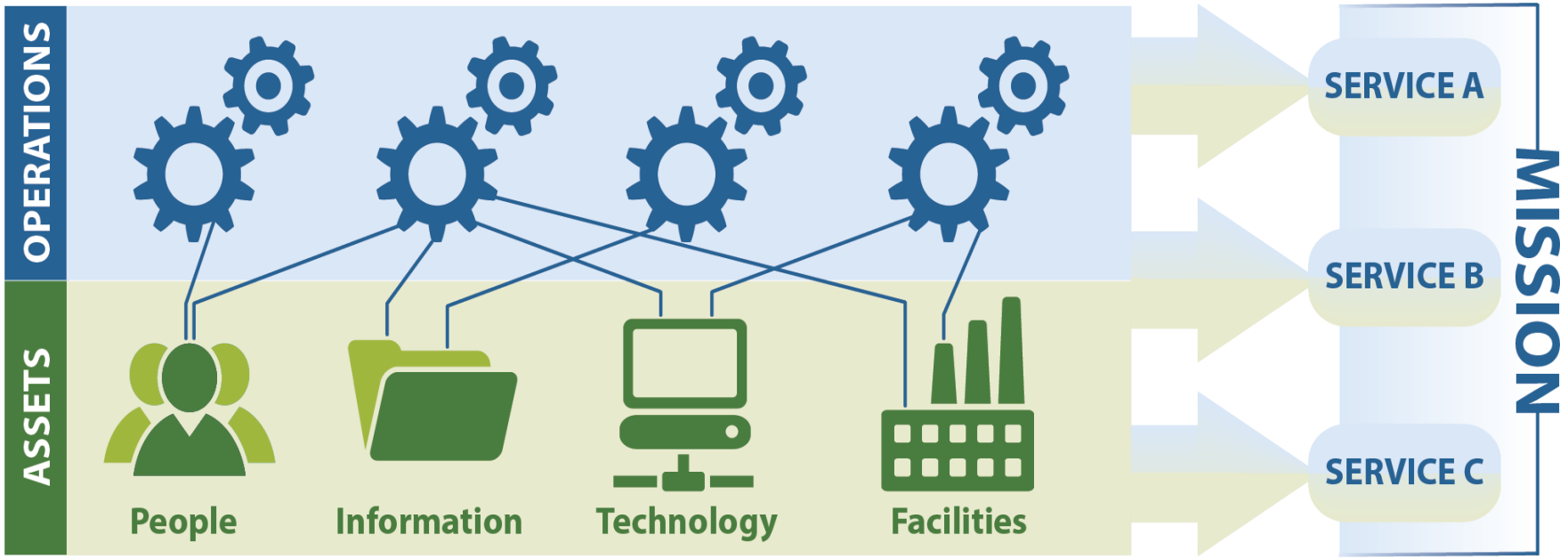
Cyber Resilience Part 1 | Prepare

- Step 1: Identify your organization's critical services
- Step 2: Create an inventory of the assets that support each critical service
- Step 3: Create encrypted and offline backups of essential software and configuration baselines for your technology assets
- Step 4: Acquire backup hardware for critical systems
- Step 5: Create a cyber incident response plan
- Step 6: Exercise your cyber incident response plan



Critical Services and Supporting Assets

"**Critical service**" is defined as *"[a] set of activities that the organization carries out in the production of a product or while providing services to its customers, that are so **important to the success of the organization** that **disruption to the service would severely impact** the organization's **operation or business**."*



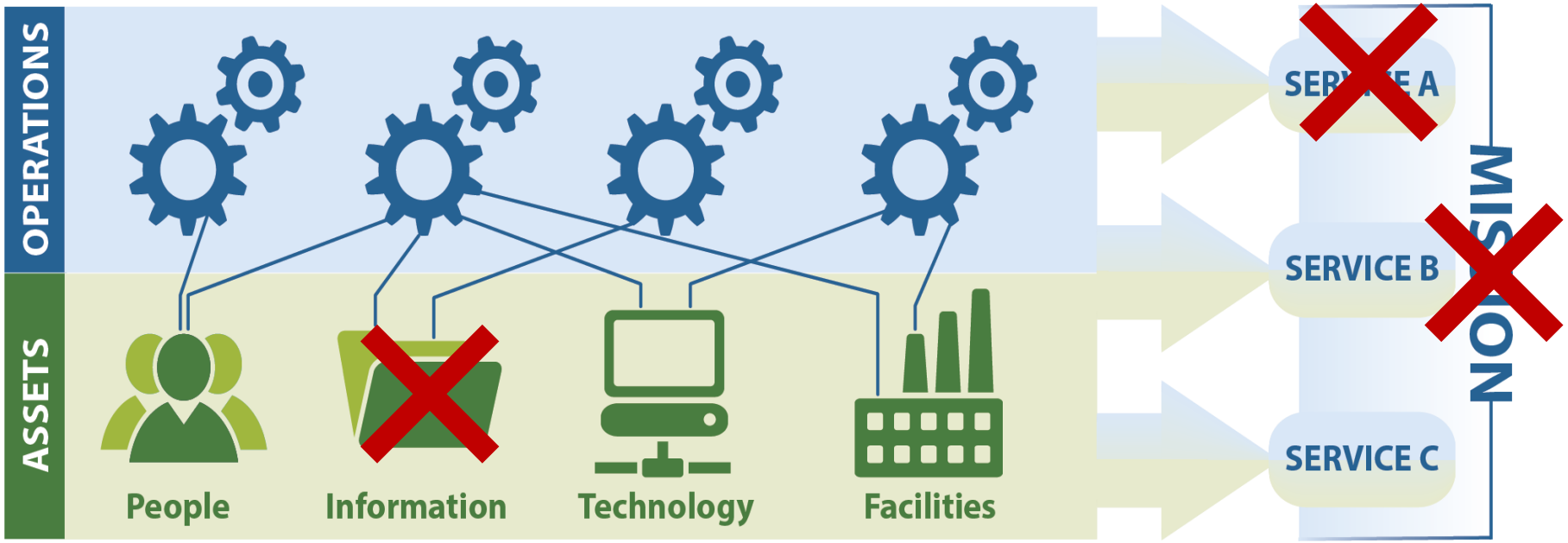
Organizations use **assets (people, information, technology, and facilities)** to provide operational **services** and accomplish **missions.**

An organization uses its **assets** to perform productive activities to provide operational services and accomplish its mission.

- **People** – Those who operate and monitor the service (e.g., system administrators)
- **Information** – Data associated with the service (e.g., configuration files, logs, or other)
- **Technology** – Systems and software that automate and support the service (e.g., hardware and software)
- **Facilities** – Where the service is performed (e.g., data centers, recovery sites, or other)

Critical Services and Supporting Assets

"**Critical service**" is defined as *"[a] set of activities that the organization carries out in the production of a product or while providing services to its customers, that are so **important to the success of the organization** that **disruption to the service would severely impact** the organization's **operation or business**."*

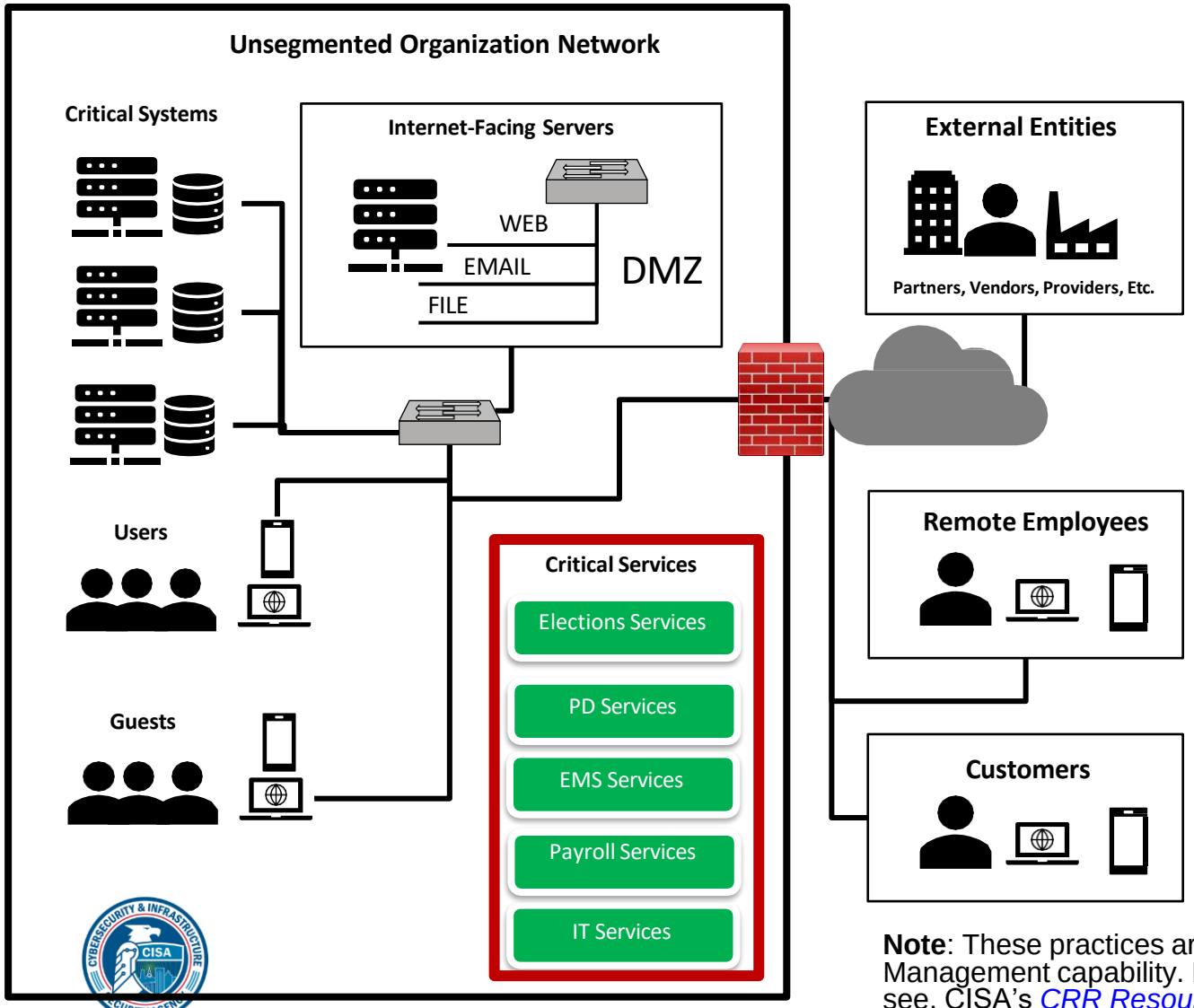


An organization uses its **assets** to perform productive activities to provide operational services and accomplish its mission.

- **People** – Those who operate and monitor the service (e.g., system administrators)
- **Information** – Data associated with the service (e.g., configuration files, logs, or other)
- **Technology** – Systems and software that automate and support the service (e.g., hardware and software)
- **Facilities** – Where the service is performed (e.g., data centers, recovery sites, or other)

Organizations use **assets (people, information, technology, and facilities)** to provide operational **services** and accomplish **missions.**

Cyber Resilience Part 1 | Prepare



Step 1: Identify Critical Services

County Example

Purpose: To establish a prioritized list of services, which will help inform incident response, recovery, and continuity efforts.

Actions:

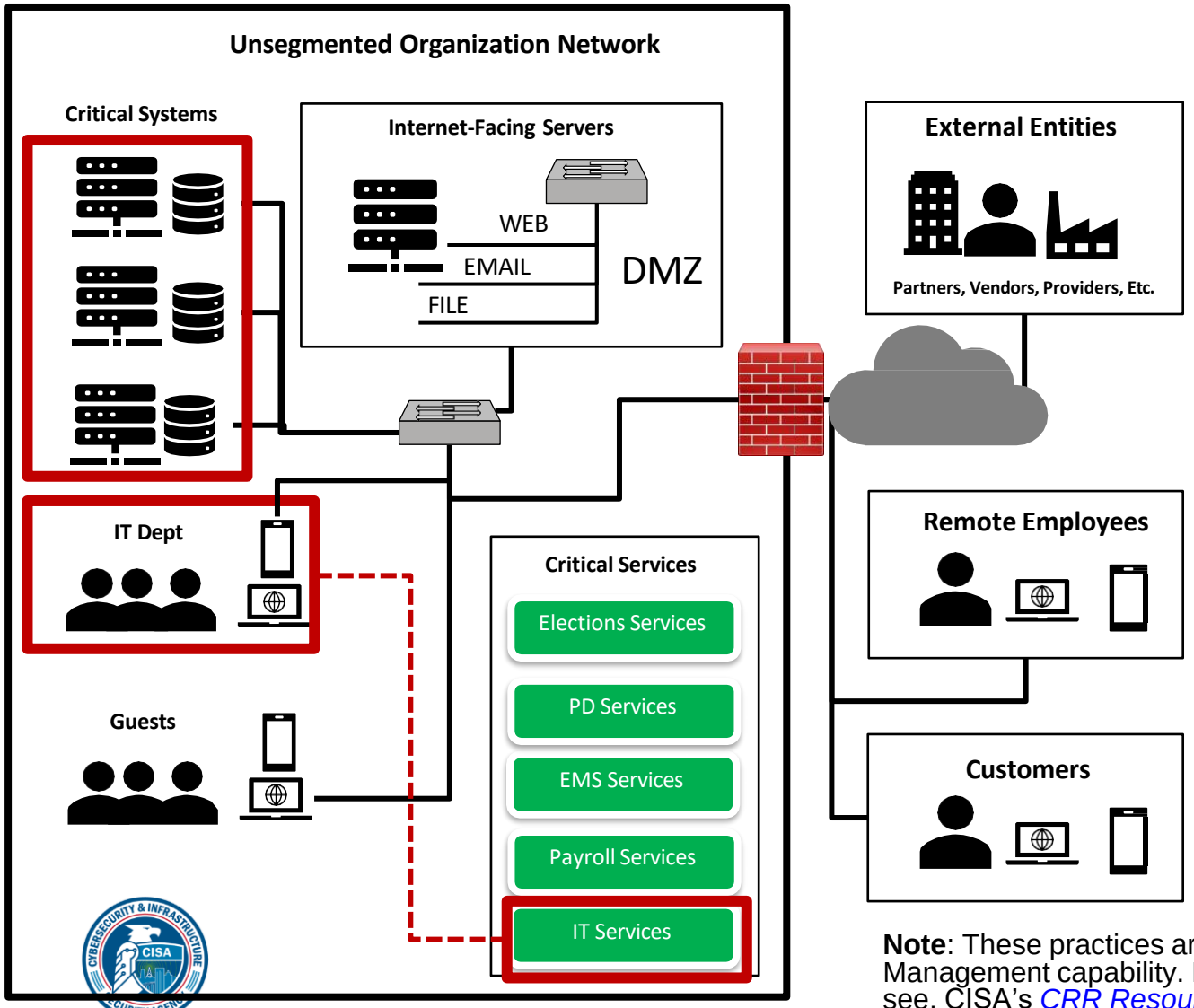
- Identify and inventory the following:
  - External services provided to external customers/stakeholders
    - Elections Services
    - PD Services
    - EMS Services
    - Etc.
  - Internal services provided to internal stakeholders
    - Payroll
    - Information Technology Services
  - Create a prioritized list of services based on impact to your organization's mission.

Deliverable/Result:

- A prioritized list of internal and external services essential to the organization's mission

Note: These practices are non-exhaustive and should be incorporated into a larger Asset Management capability. For more details on how to develop an Asset Management capability, see, CISA's *CRR Resource Guide: Asset Management*.

Cyber Resilience Part 1 | Prepare



Step 2: Create Critical Service Asset Inventory

IT Services Example

Purpose: To establish an inventory of assets supporting a critical service, to help prioritize incident response and service continuity

Actions:

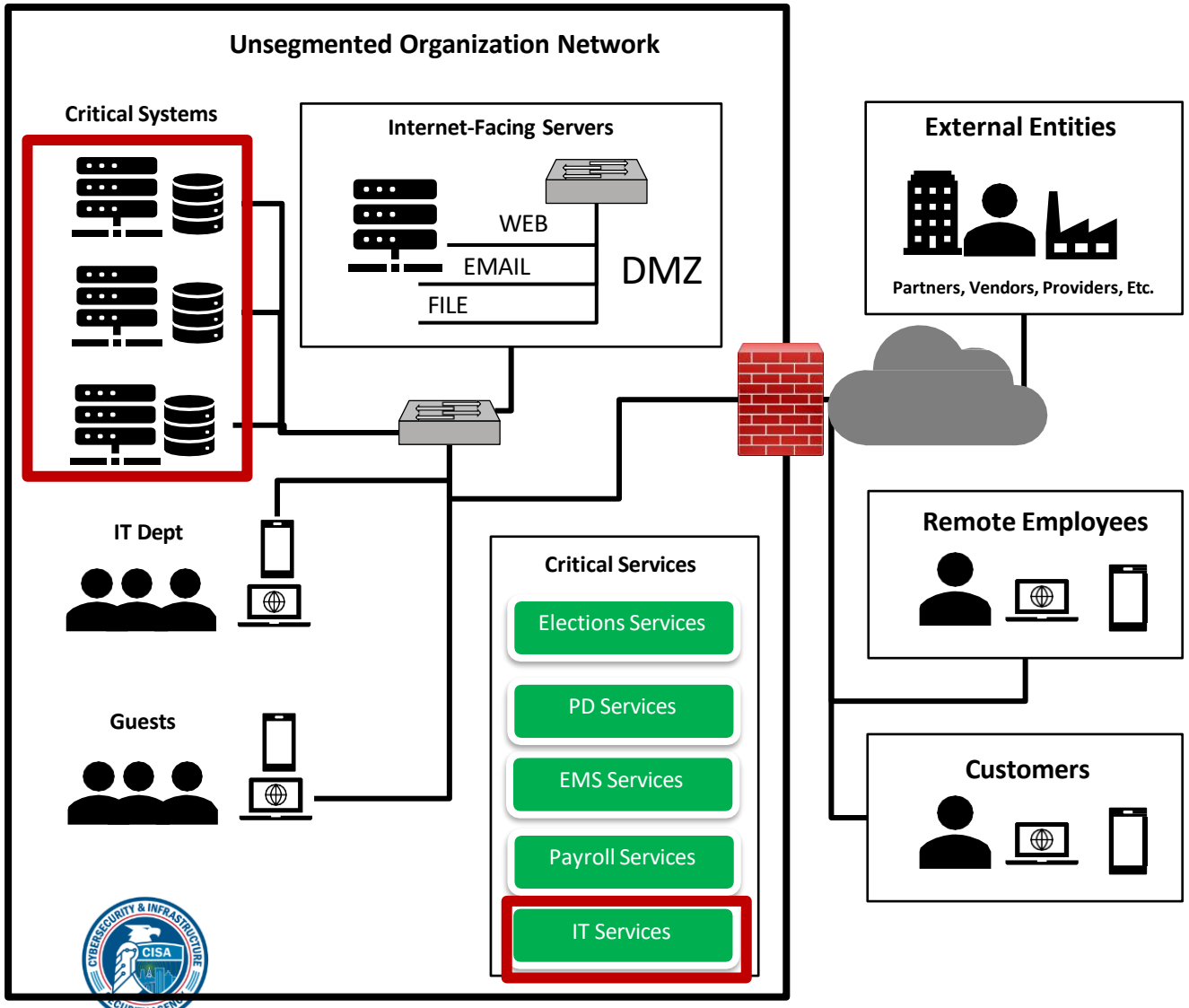
- Identify and inventory the following:
  - Personnel essential for delivery of IT services (e.g., system admin, network admin, etc.)
  - Information or data essential for delivery of IT services (e.g., databases, config files, etc.)
  - Technology assets (hardware/software) essential for delivery of IT services (e.g., servers, workstations, routers, switches, applications, OSs)
  - Third-party services essential for delivery of IT services? (e.g., ISP, managed service providers, etc.)
  - Facilities essential for delivery of IT services? (e.g., datacenter, secondary disaster recovery site, etc.)

Deliverable/Result:

- A comprehensive inventory of assets that support the critical service [IT Services in this example]

Note: These practices are non-exhaustive and should be incorporated into a larger Asset Management capability. For more details on how to develop an Asset Management capability, see, CISA's *CRR Resource Guide: Asset Management*.

Cyber Resilience Part 1 | Prepare



Step 3: Create Secure Backups of Critical Service Information Assets

IT Services Example

Purpose: To create backups of critical information assets that support the critical service to quickly restore service when recovering from an incident

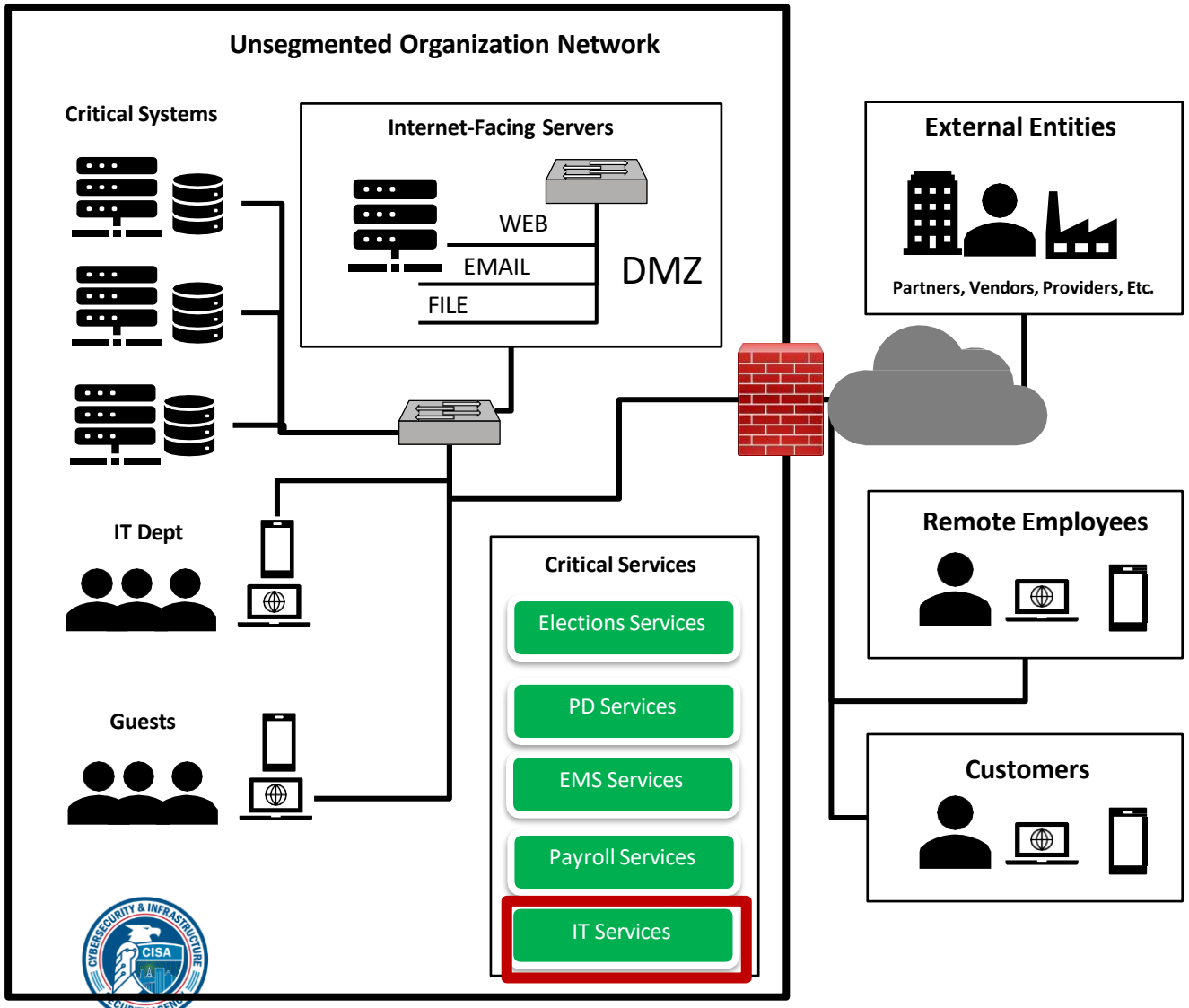
Actions:

- Establish baseline configurations of:
  - Network devices
  - Servers
  - Endpoints
- Create backups of each baseline:
  - Encrypt
  - Store off-line
  - Validate backup and restoration process
- Create backups of essential databases, software, and operating systems:
  - Encrypt
  - Store off-line
  - Validate backup and restoration process

Deliverable/Result:

- System baselines, applications, operating systems, and databases that can be used to restore infected systems to pre-incident state

Cyber Resilience Part 1 | Prepare



Step 4: Acquire Redundant Critical Service Technology Assets

IT Services Example

Purpose: To acquire redundant hardware that will be essential to quickly resume service in the event of a hardware failure

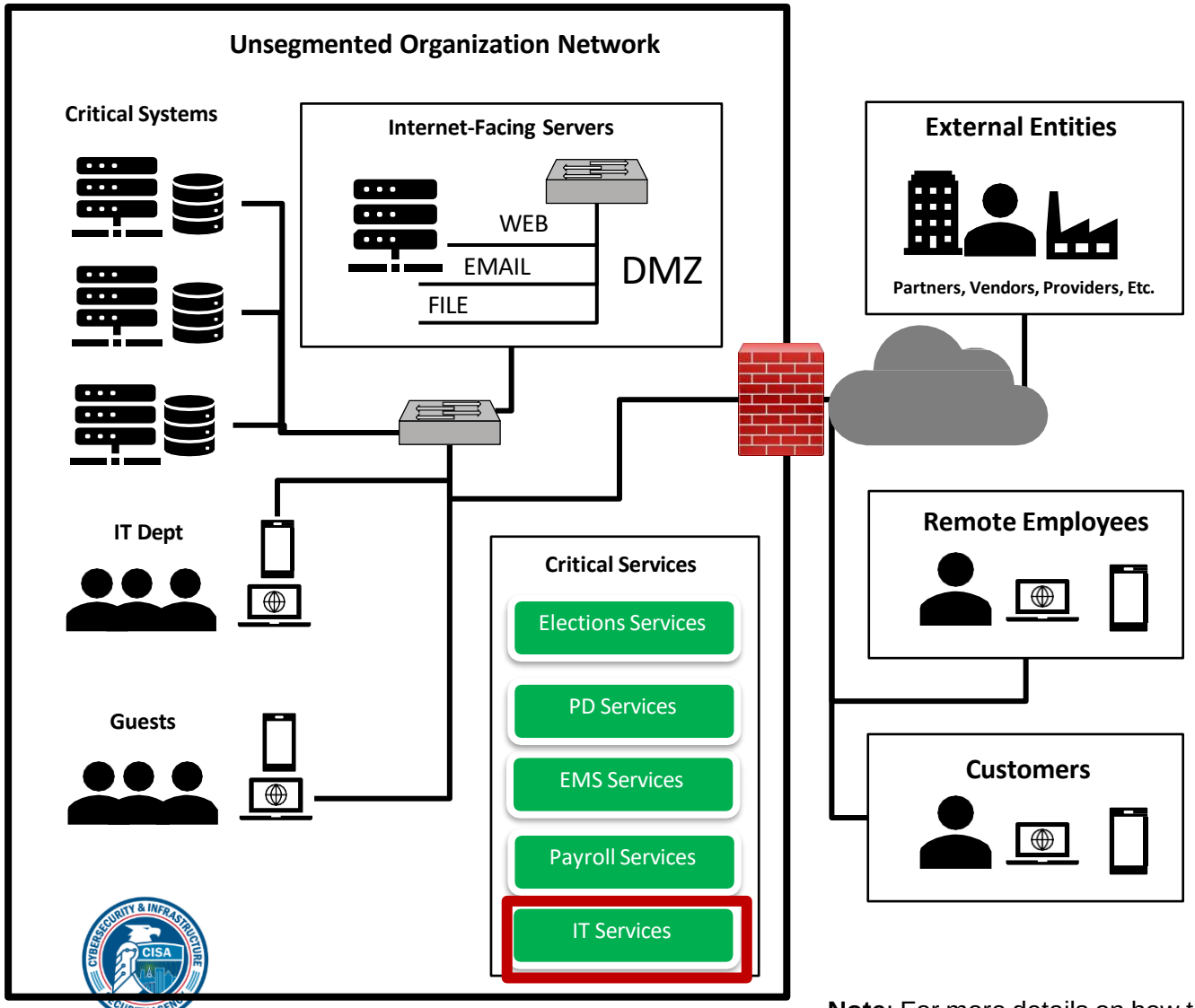
Actions:

- Refer to the asset inventory
- Determine which technology assets you should purchase redundant solutions for
  - Considerations
    - Whether the asset is a single point of failure
    - Whether the asset is nearing it's known life-expectancy
    - Whether the asset is known to fail often
    - Whether the asset is scarce and has few (if no) alternatives
- Identify "trusted suppliers"
- Acquire redundant equipment

Deliverable/Result:

- Backup/redundant equipment that can be used to replace hardware that fails

Cyber Resilience Part 1 | Prepare



Step 5: Create an Incident Response Plan

IT Services Example

Purpose: To create an incident response plan that will inform how the organization will respond to and recover from cyber incidents

Actions:

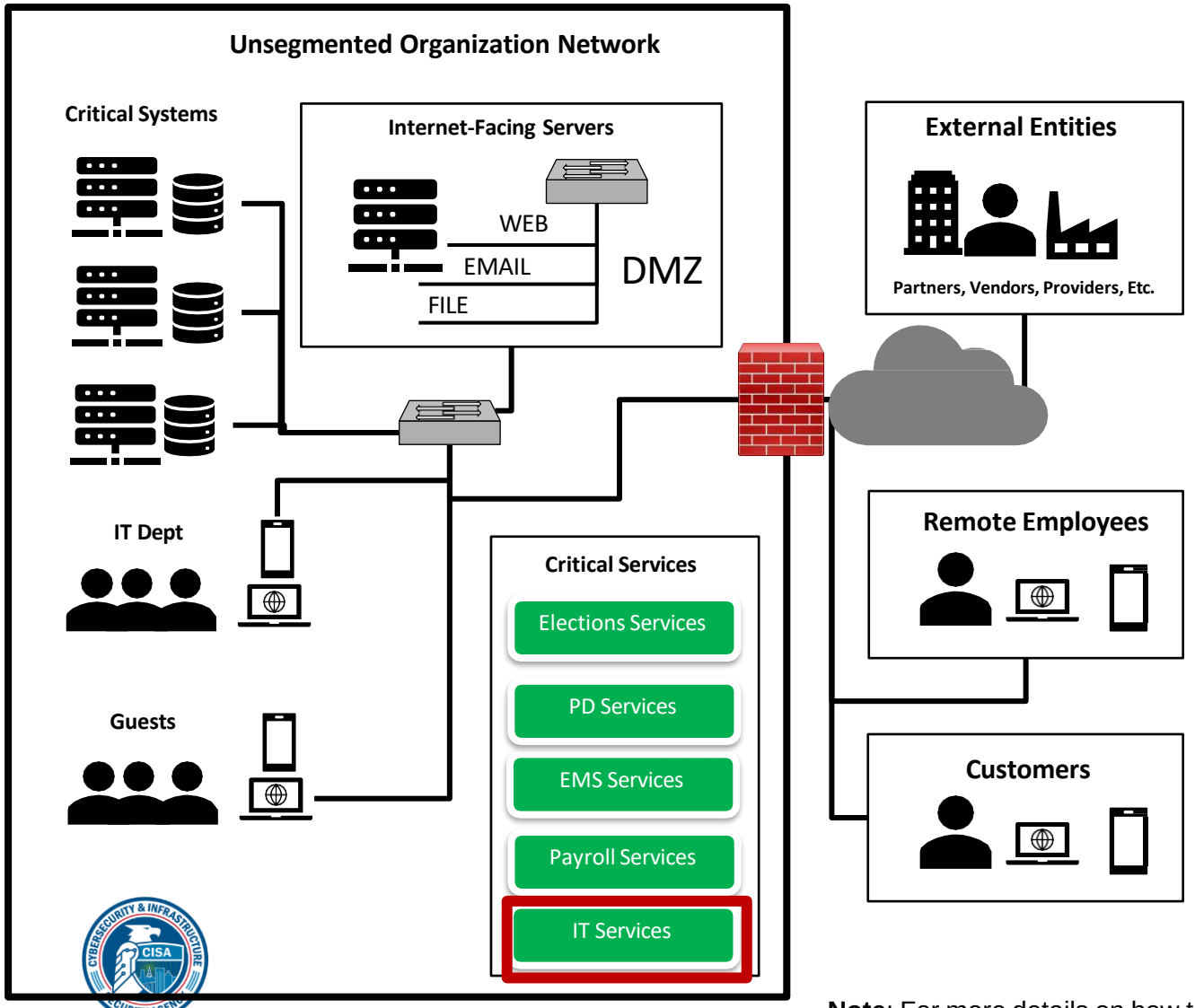
- Create a plan that defines how to detect, analyze, respond to, and recover from incidents
- Define an incident management process
  - Detect events
  - Analyze and triage events
  - Respond and recover from incident
  - Analyze and improve incident management process
- Define the roles of the plan
  - Incident Manager – leads response
  - Tech Manager – technical subject matter expert (response, recovery, and/or liaison to external assistance)
  - Communications Manager – interacts with media, customers, other external stakeholders
- Identify and assign internal/external stakeholders to the roles
  - Internal: IT/cyber, legal counsel, Public Information Officer (PIO), executive leadership (CEO/President), etc.
  - External: Cyber insurance, incident response service providers, state/federal regulators and law enforcement, etc.

Deliverable/Result:

- An initial incident response plan that can be improved post-incident or exercise

Note: For more details on how to develop an incident response plan, see *NIST SP 800-34 Rev.1 Contingency Planning Guide for Federal Information Systems* and CISA's *CRR Resource Guide: Service Continuity, Revision 2*.

Cyber Resilience Part 1 | Prepare



Step 6: Exercise the Incident Response Plan

IT Services Example

Purpose: To ensure the organization is familiar with the incident response plan and identify opportunities for improving it

Actions:

- Create or acquire a cyber tabletop exercise
- Identify all relevant stakeholders to participate in the exercise
- Execute the exercise
  - Ensure that all stakeholders understand their role and know how to use the plan
  - Identify opportunities to improve the plan or other capabilities (e.g., asset management, change/configuration management, vulnerability management, etc.)
- Develop an after-action report that summarizes the findings of exercise and assigns responsibility for any follow-on tasks

Deliverable/Result:

- Validation of the incident response plan
- An after-action report outlining exercise findings and a plan for addressing any follow-on tasks

Note: For more details on how to develop an incident response plan, see *NIST SP 800-34 Rev.1 Contingency Planning Guide for Federal Information Systems* and CISA's *CRR Resource Guide: Service Continuity, Revision 2*.

Cyber Resilience
Part 2 | Defend

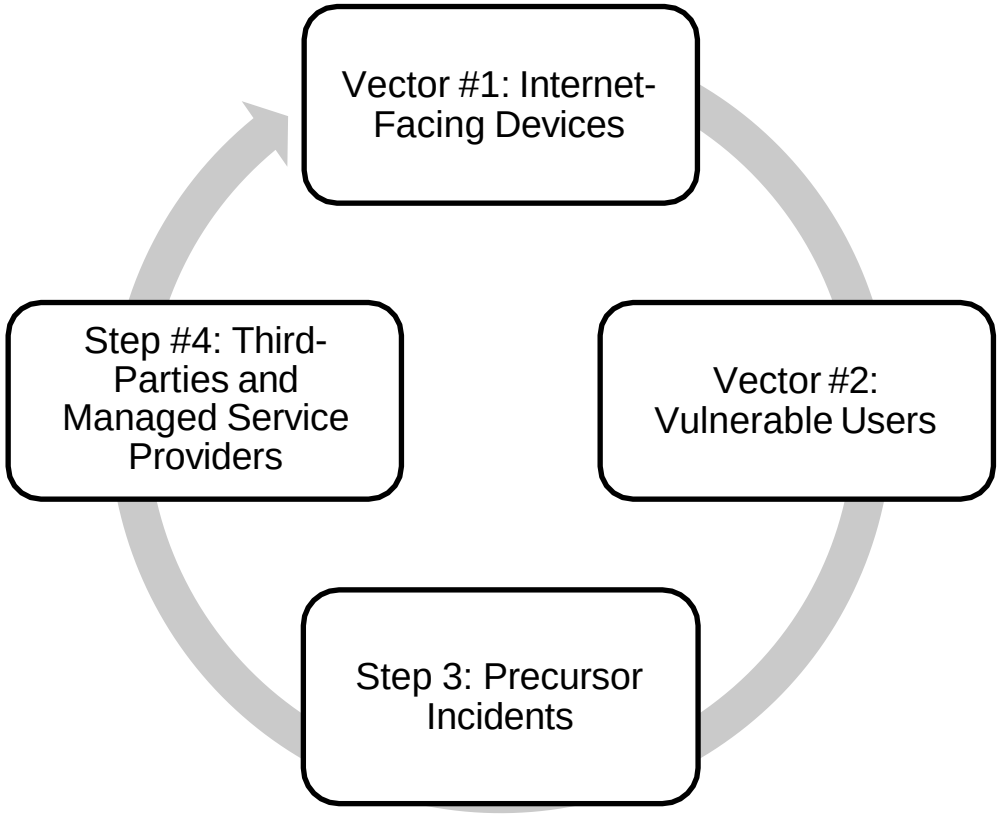
Cyber Resilience Part 2 | Defend

Cyber Resilience Part 2 | Defend

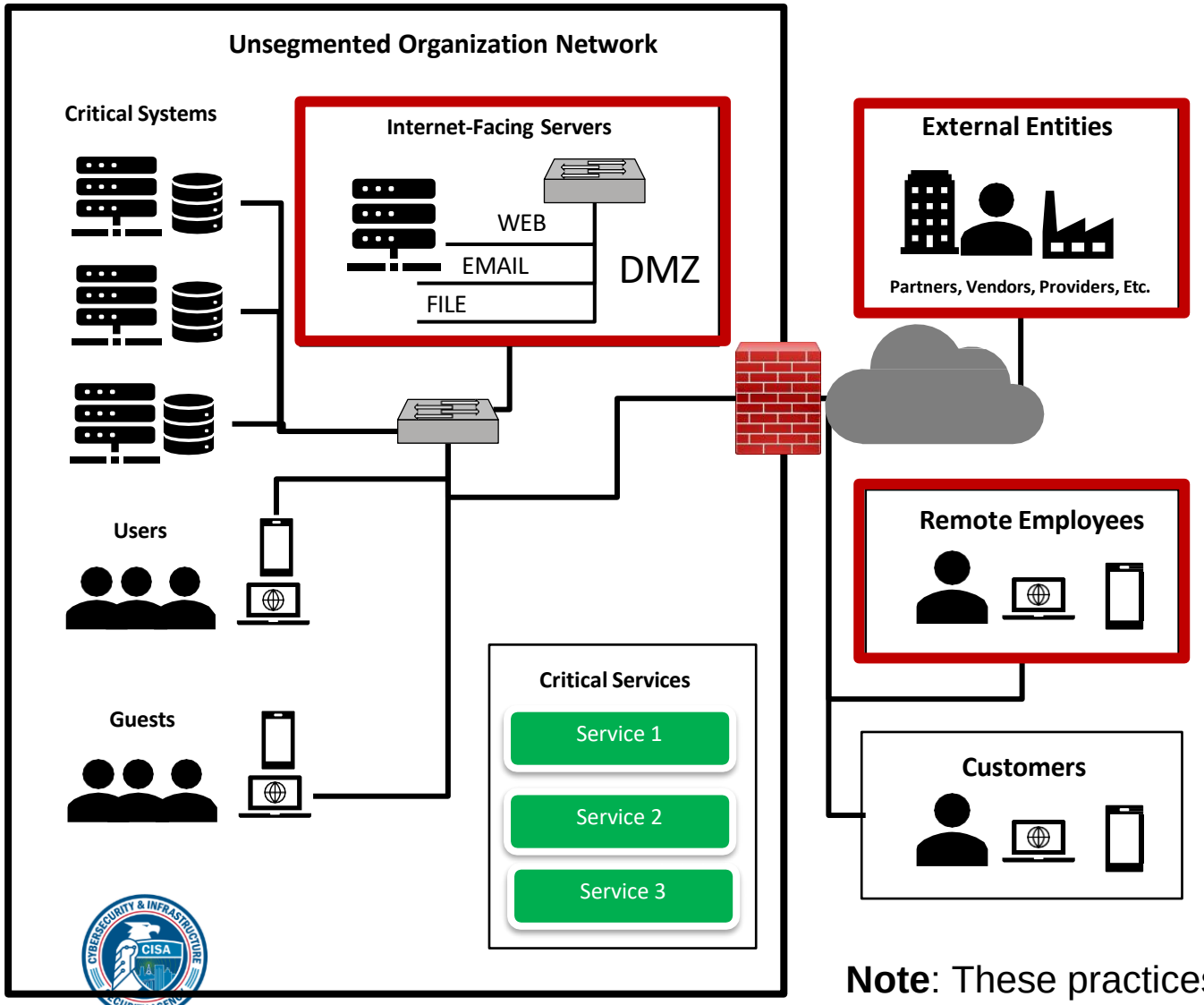
Identify and Address Common Infection Vectors

- Vector #1: Internet-Facing Devices With Vulnerabilities and Misconfigurations
- Vector #2: Phishing Attacks
- Vector #3: Precursor Malware Infections/Network Compromises
- Vector #4: Third-Parties and Managed Service Providers

Additional Hardening Considerations



Vector 1: Internet-Facing Vulnerabilities



Identify and Address Common Infection Vectors

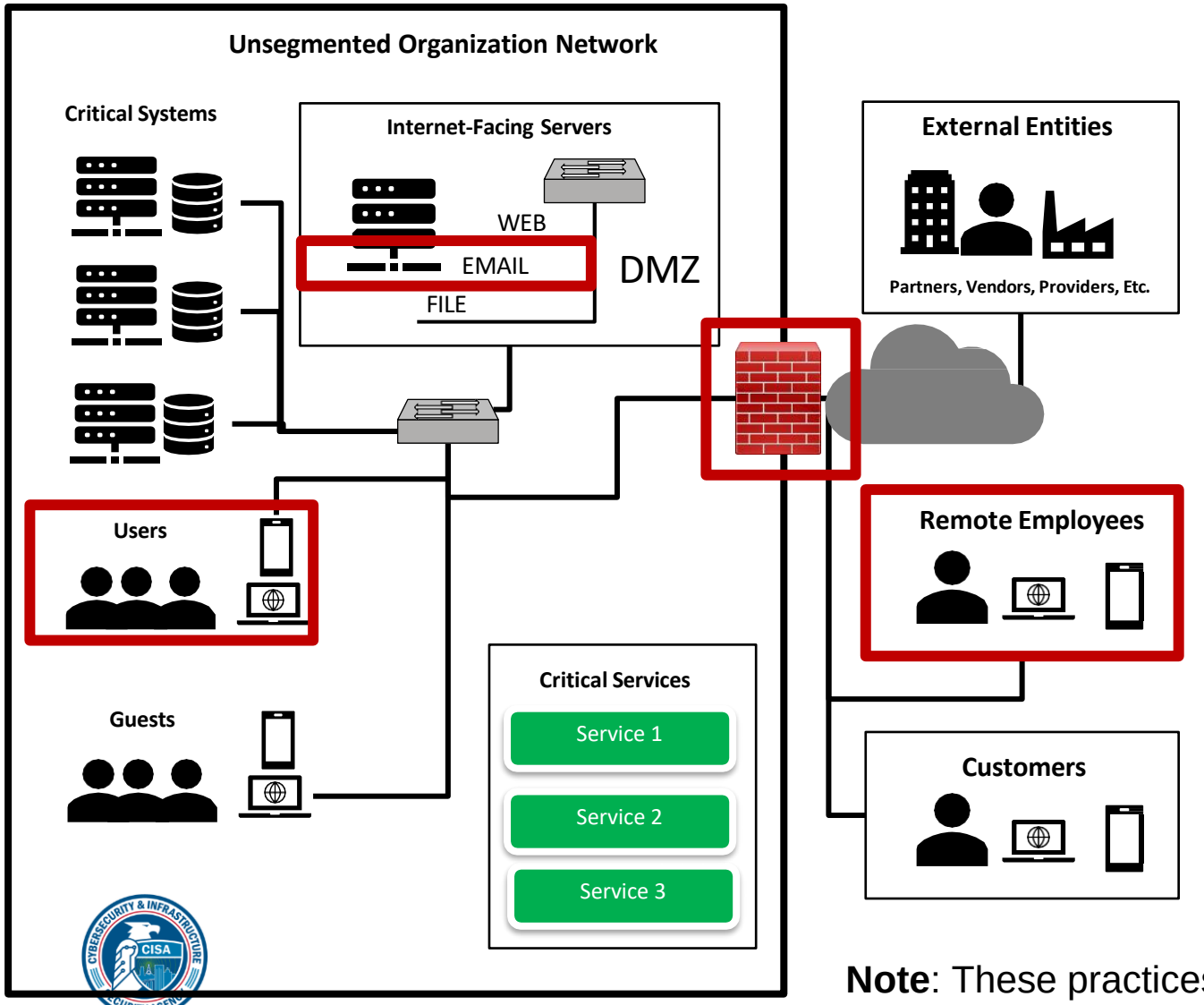
Vector #1: Internet-Facing Devices With Vulnerabilities and Misconfigurations

Recommended Actions

- Conduct Regular Vulnerability Scans
  - External or internet-facing (device) IPs (DMZ)
  - Internal (device) IPs
- Manage Vulnerability
  - Update and properly configure firmware, operating systems, and applications
- Systems Hardening
  - Enable security features
  - Remove unnecessary ports and services
- Remote Access Protocol Hardening
  - Control and monitor use of RDP services
  - Log and monitor all RDP logins and sessions
  - Apply Multi-Factor Authentication (MFA)

Note: These practices should be incorporated into your organization's Vulnerability Management Program and Controls Management Program.

Vector 2: Phishing Attacks



Identify and Address Infection Vectors

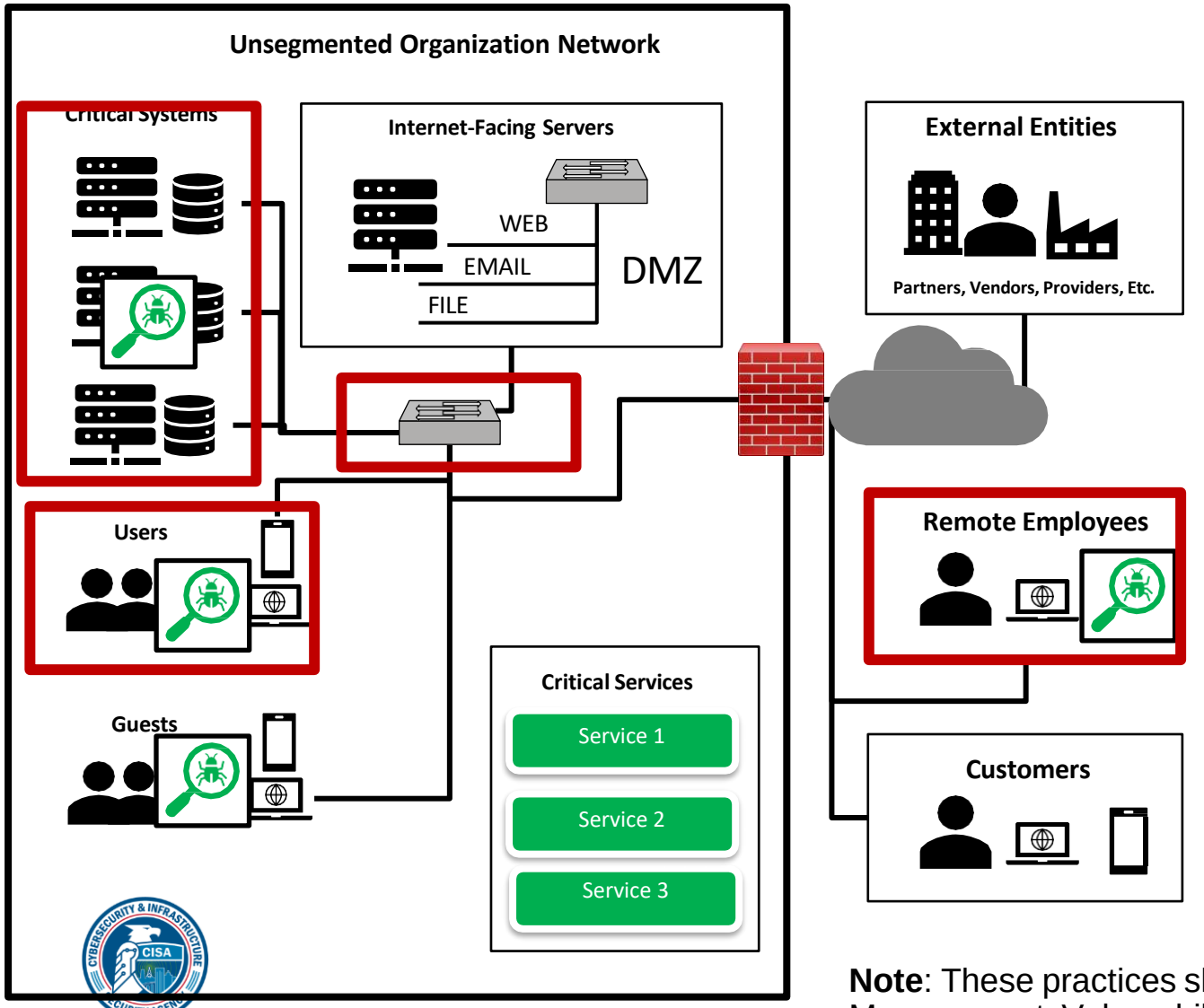
Vector #2: Phishing Attacks

Recommended Actions

- Conduct User Cyber Awareness and Training
  - Annualized
  - Required by FTEs and Contractors before access to network
  - Know how to spot phishing attacks
  - Know how to report phishing attacks
- Conduct Phishing Campaigns
  - Assess effectiveness of cyber awareness/training program
- Deploy Email Controls
  - Filter Email With Known Malicious Indicators
  - Employ Domain-Based Message Authentication, Reporting and Conformance (DMARC)
  - Disable macro scripting for MS Office files sent via email
- Block Known Malicious IPs at Firewall

Note: These practices should be incorporated into your organization's Education and Awareness Program and Controls Management Programs.

Vector 3: Precursor Malware/Intrusions



Identify and Address Infection Vectors

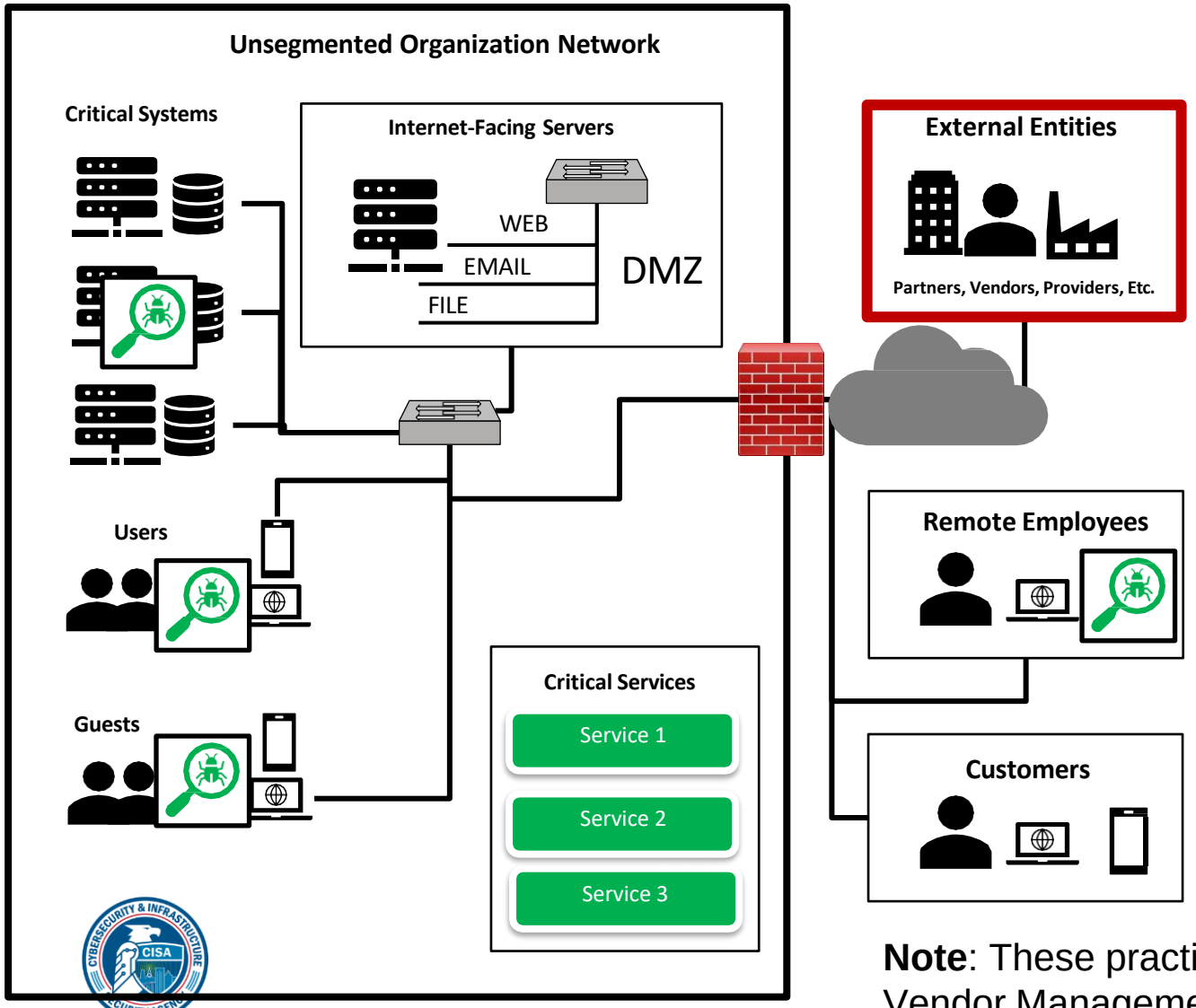
Vector #3: Precursor Malware Infections/Network Compromises

Recommended Actions

- Deploy Network and Host Event Monitoring Capabilities
  - Enables logging and visibility of events occurring in your network
- Deploy Antivirus/Antimalware Solutions
  - Automatically detect and stop malware on your technology assets
  - Ensure signatures are updated
- Deploy Intrusion Detection and Prevention Solutions
  - Automatically detect and prevent malicious events from occurring in your network
- Employs allowlisting
  - Ensure only authorized software is installed on technology assets

Note: These practices should be incorporated into your organization's Controls Management, Vulnerability Management, and Incident Management Programs.

Vector 4: Third-Parties and Managed Services



Identify and Address Infection Vectors

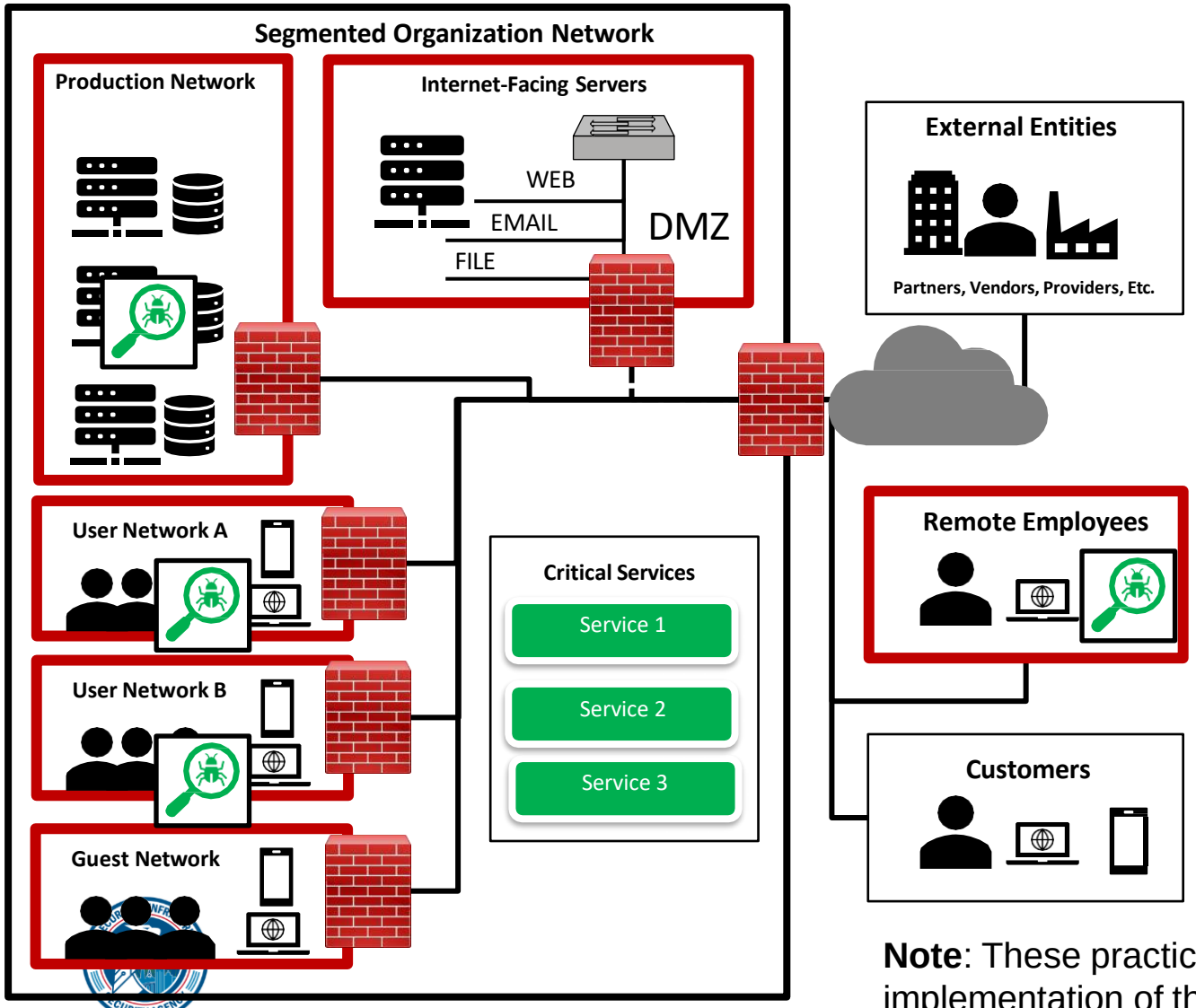
Vector #4: Third-Parties and Managed Service Providers

Recommended Actions

- Pre-Execution of Contract
  - Consult with your cyber and legal personnel to identify privacy and security requirements
  - Communicate these security requirements with prospective third-parties/service providers
  - Request security questionnaires from prospective third-parties/service providers
  - Request independent audit reports of prospective third-parties/service providers
  - Negotiate to incorporate security requirements into contract language
- Post-Execution of Contract
  - Implement safeguards to control risk from security requirements not incorporated into the contract
  - Control and monitor third-party/service provider access to your assets
  - Monitor third-party/service provider performance/non-performance

Note: These practices should be incorporated into your organization's Vendor Management Program.

General Network Hardening Considerations



General Network Hardening Considerations

Near-Term Practices to Adopt a Heightened Security Posture Internally

Recommended Actions

- Restrict use of PowerShell and monitor its use
- Limit, control, and log use of administrative accounts
- Employ Multi-Factor Authentication (MFA) and strong password policies where feasible
- Secure your domain controllers and limit access to administrators only – these are targets for propagation
- Baseline and analyze network and host activity to detect anomalous behavior
- Employ principle of least privileges for users – reduces risk of an attacker compromising an account with excessive privileges
- Segment your networks to limit threat actor lateral movement
- Ensure no OT devices are accessible from the Internet
- More

Note: These practices are non-exhaustive. Also, for more details regarding implementation of these actions, refer to CISA's #StopRansomware Guide.

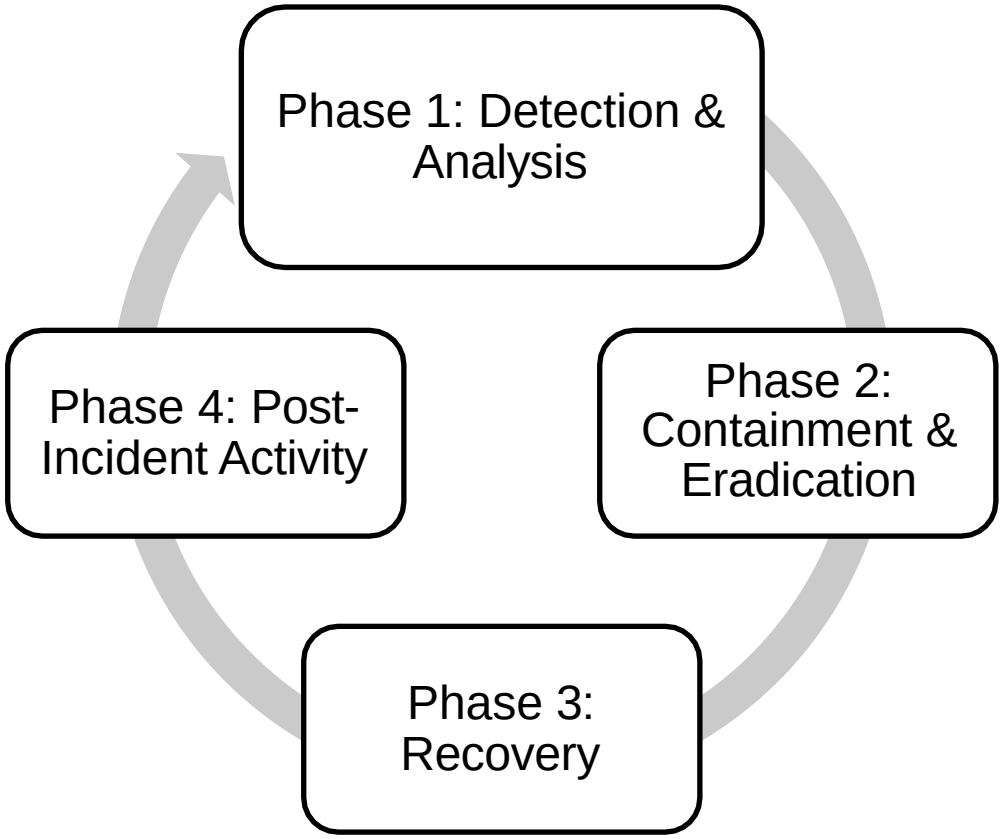
Cyber Resilience
Part 3 | Respond & Recover

Cyber Resilience Part 3 | Respond

Cyber Resilience Part 3 | Respond

The Incident Management Cycle

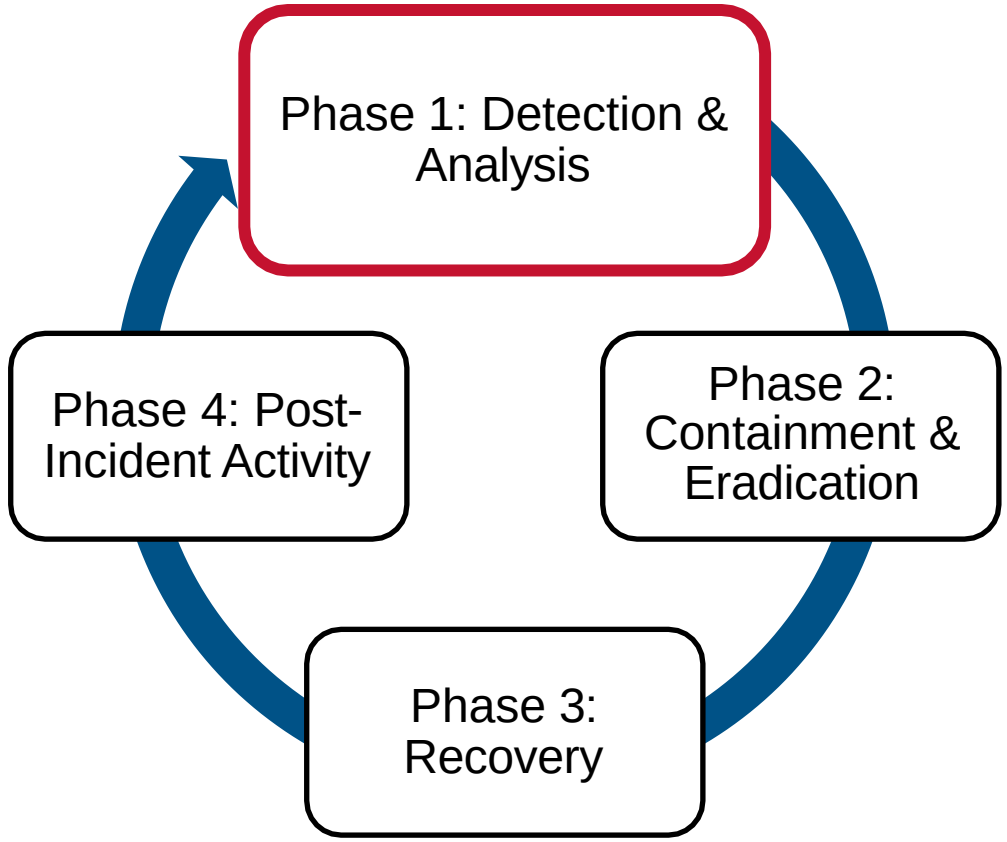
- Phase 1: Detection & Analysis
- Phase 2: Containment & Eradication
- Phase 3: Recovery
- Phase 4: Post-Incident Activity



Phase 1: Detection and Analysis

Phase 1: Detection & Analysis

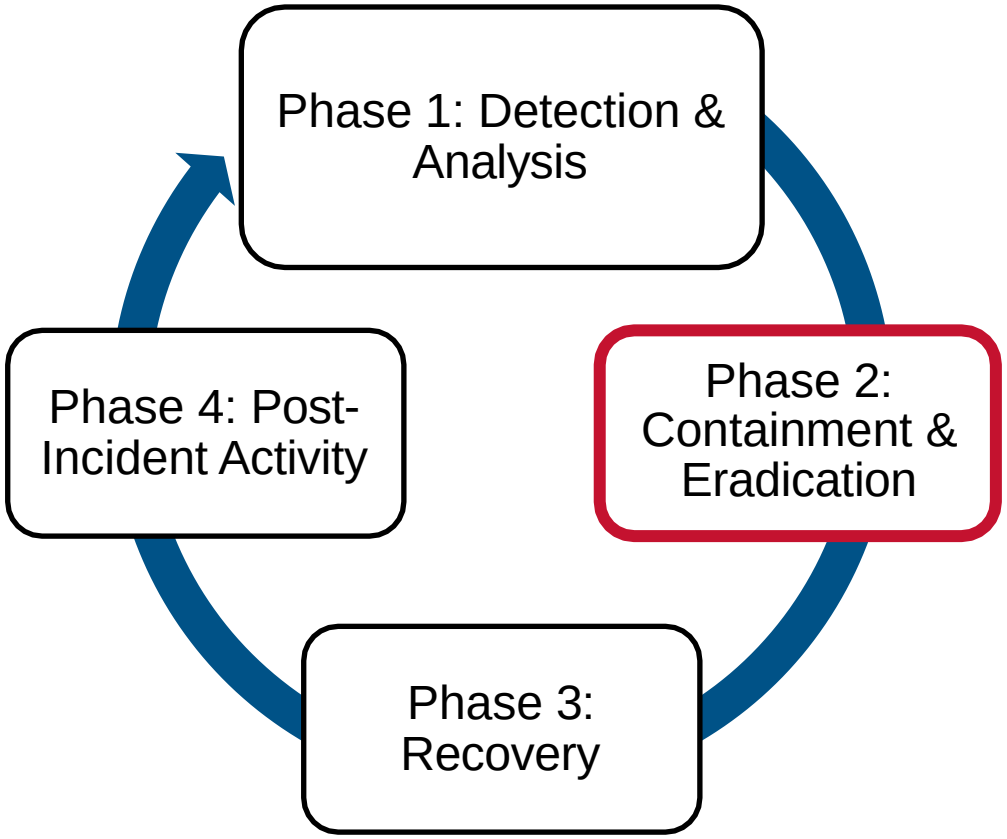
- Step 1: Identify and isolate impacted devices
- Step 2: If you are unable to disconnect from the network, power them down
- Step 3: Triage devices for restoration and recovery efforts
- Step 4: Confer with incident response team
- Step 5: Engage internal/external stakeholders



Phase 2: Containment & Eradication

Phase 2: Containment & Eradication

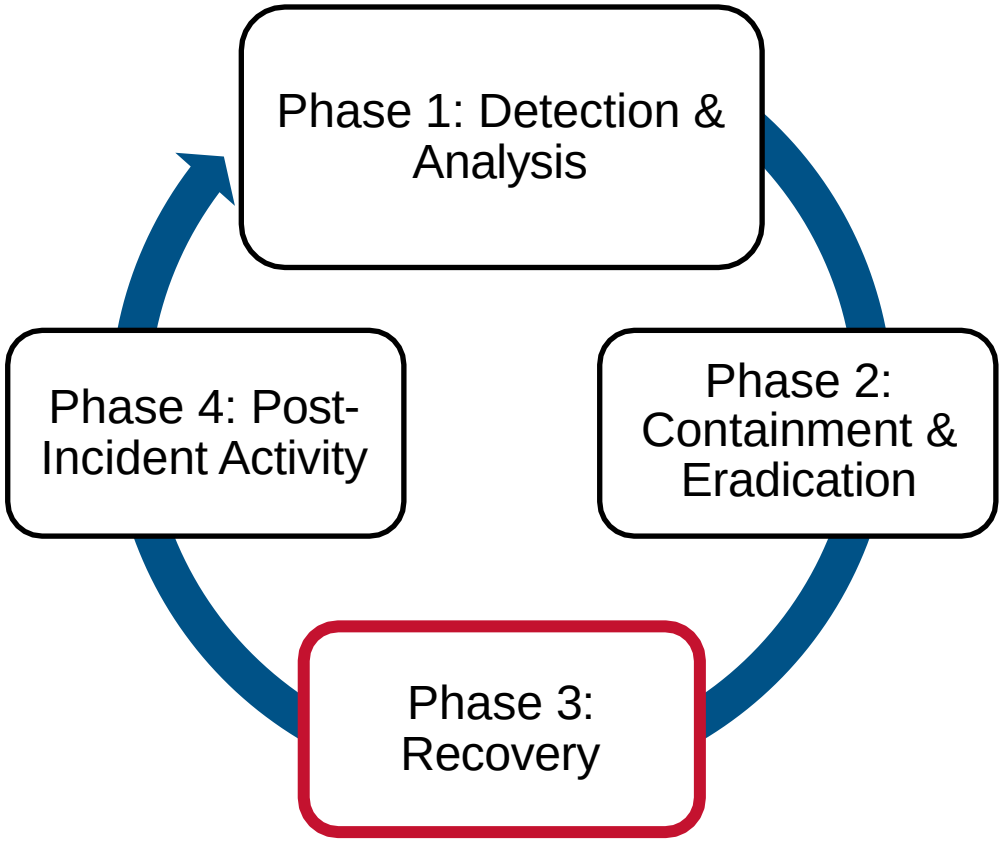
- Step 1: Take a system image and memory capture of an affected device – identify the variant
  - Collect any potentially relevant artifacts (observables/indicators) for investigation purposes
- Step 2: Contact law enforcement for assistance with variant decryptors
- Step 3: Research trusted guidance on the ransomware variant
- Step 4: Identify systems and accounts involved in the initial breach
- Step 5: Contain any associated systems that may be used for continued unauthorized access
- Step 6: Identify and eradicate any outside-in and inside-out persistence mechanisms



Phase 3: Recovery

Phase 3: Recovery

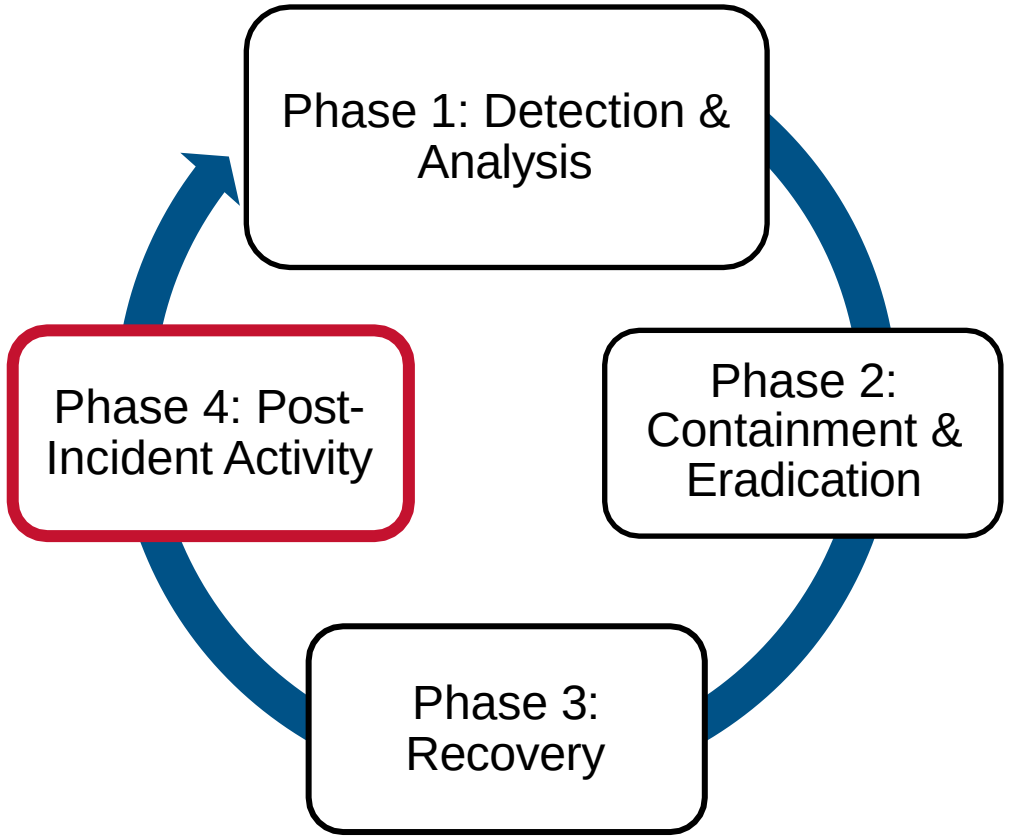
- Step 1: Rebuild systems using pre-configured images
- Step 2: Issue password resets for all affected systems and accounts
- Step 3: Reconnect systems and restore data from offline, encrypted backups



Phase 3: Recovery

Phase 4: Post-Incident Activity

- Step 1: Schedule a post-incident meeting with all relevant stakeholders involved
- Step 2: Document lessons-learned and improve on your incident response plan
  - Why did the incident occur? (root cause)
  - Was our plan effective?
  - What needs to be changed/added to our plan and/or other capabilities?
- Step 3: Assign stakeholders to implement changes identified in the after-action report
- Step 4: Track progress of each change to closure
- Step 5: Implement changes
- Step 6: Consider sharing your lessons-learned with trusted communities, such as ISACs, ISAOs, and CISA



Next Steps

Partnering with CISA on Cybersecurity Matters
No-Cost/Federally-Funded Resources and Services

CISA's No-Cost Cybersecurity Resources

NO-Cost/Federally Funded

- **Cybersecurity Assessments**
  - Baseline Assessments
    - Ransomware Readiness Assessment (RRA)
    - Cybersecurity Performance Goals (CPG)
  - Intermediate Assessments
    - Cyber Infrastructure Survey (CIS)
    - Cyber Resilience Essentials (CRE)
  - Advanced Assessments
    - External Dependencies Management (EDM)
    - Incident Management Review (IMR)
    - Cyber Resilience Review (CRR)
- **Cyber Hygiene Services**
  - External Vulnerability Scanning Service
  - Web Application Scanning Service
- **Workshops & Exercises**
  - Asset Management Workshop (AMW)
  - Cyber Resilience Workshop (CRW)
  - Incident Management Workshop (IMW)
  - Vulnerability Management Workshop (VMW)
  - Digital Forensics Workshop I (DFW I)
  - Digital Forensics Workshop II (DFW II)
  - Cyber Tabletop Exercise (CTTX)
- **Technical Assessments***
  - Remote Penetration Test (RPT)
  - Risk and Vulnerability Assessment (RVA)
  - Validated Architecture Design Review (VADR)

***Note:** Eligibility for technical assessments is contingent upon assessment of the stakeholder's capabilities by their Cybersecurity Advisor (CSA).

CISA's No-Cost Cybersecurity Resources

NO-Cost/Federally Funded

STRATEGIC (HIGH-LEVEL)

- **Cybersecurity Assessments**
  - Baseline Assessments
    - Ransomware Readiness Assessment (RRA)
    - Cybersecurity Performance Goals (CPG)
  - Intermediate Assessments
    - Cyber Infrastructure Survey (CIS)
    - Cyber Resilience Essentials (CRE)
  - Advanced Assessments
    - External Dependencies Management (EDM)
    - Incident Management Review (IMR)
    - Cyber Resilience Review (CRR)

Request CISA's cybersecurity assessments to assess your cyber program and identify opportunities to improve it.

Contact your CISA Cybersecurity State Coordinator (CSC) or Cybersecurity Advisor (CSA) to schedule these.

TECHNICAL (LOW-LEVEL)

Cyber Resilience Review (CRR)

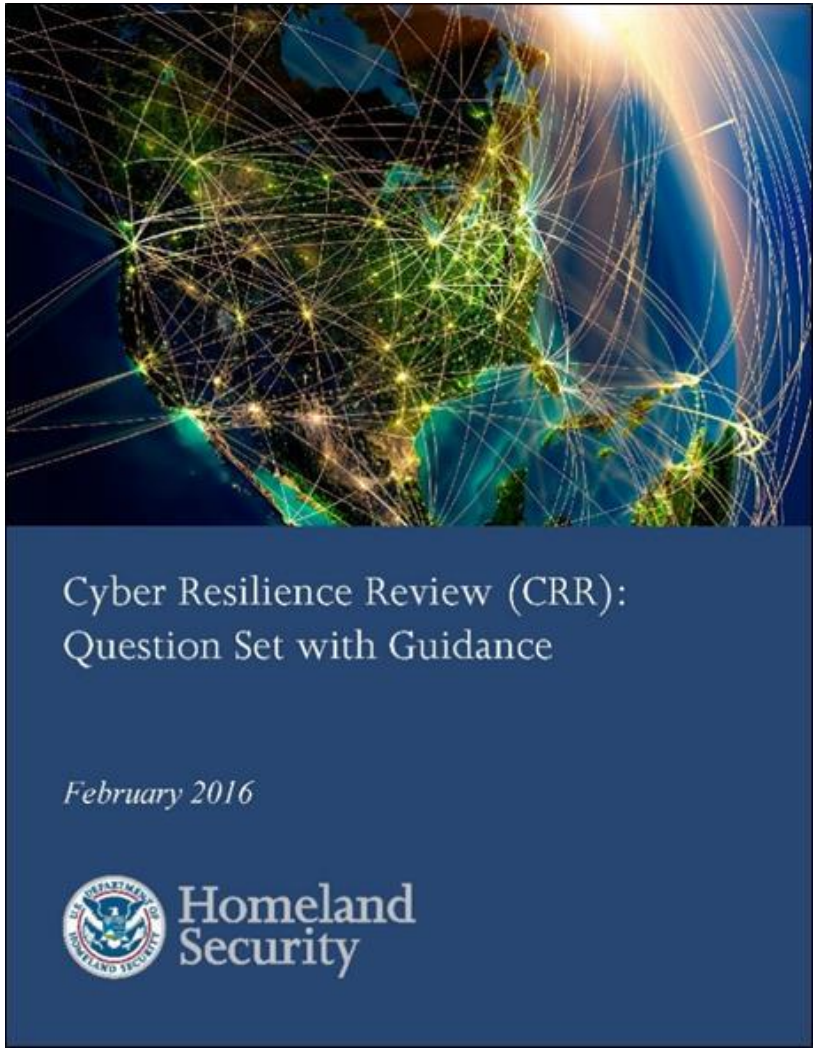
Purpose: The CRR is an assessment intended to evaluate an organization's operational resilience and cybersecurity practices of its critical services

Delivery: The CRR can be

- Facilitated by CISA Cybersecurity Advisor/Coordinator

CRR Self-Assessment Package is available on the C-Cubed Voluntary Program website.

- Helps public and private sector partners understand and measure cyber security capabilities as they relate to operational resilience and cyber risk
- Based on the CERT ® Resilience Management Model (CERT® RMM)



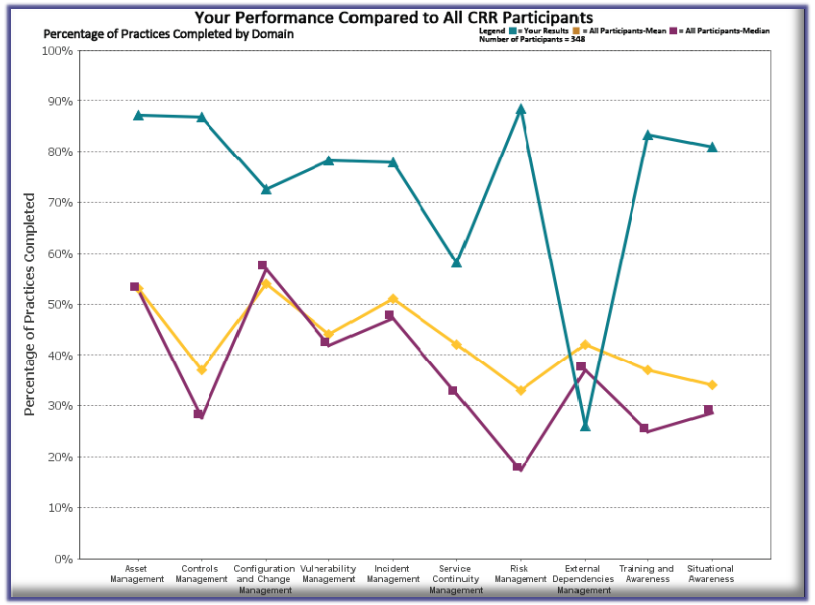
Cyber Resilience Review (CRR) | Domains

These represent key areas that typically contribute to an organization's cyber resilience— each domain focuses on:

- Documentation in place, and periodically reviewed & updated
- Communication and notification to all those who need to know
- Execution/Implementation & analysis in a consistent, repeatable manner
- Alignment of goals and practices within and across CRR domains

AM	**Asset Management** *identify, document, and manage assets during their life cycle*	SCM	**Service Continuity Management** *ensure continuity of IT operations in the event of disruptions*
CCM	**Configuration and Change Management** *ensure the integrity of IT systems and networks*	RISK	**Risk Management** *identify, analyze, and mitigate risks to services and IT assets*
CNTL	**Controls Management** *identify, analyze, and manage IT and security controls*	EXD	**External Dependency Management** *manage IT, security, contractual, and organizational controls that are dependent on the actions of external entities*
VM	**Vulnerability Management** *identify, analyze, and manage vulnerabilities*	TRNG	**Training and Awareness** *promote awareness and develop skills and knowledge*
IM	**Incident Management** *identify and analyze IT events, detect cyber security incidents, and determine an organizational response*	SA	**Situational Awareness** *actively discover and analyze information related to immediate operational stability and security*

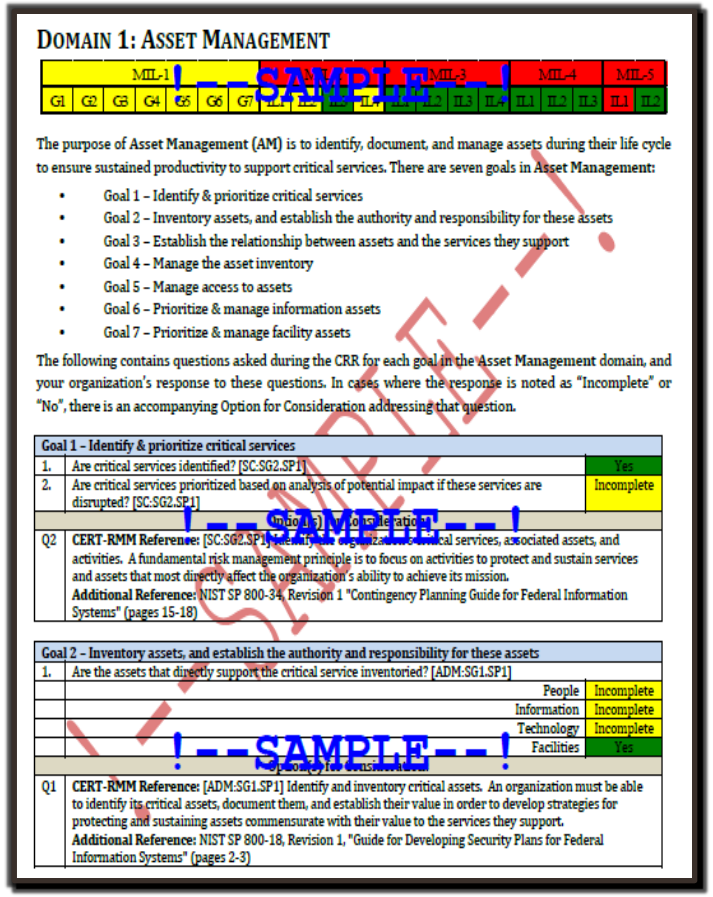
Cyber Resilience Review Outcomes



Cyber capability maturity analysis

A summary “snapshot” graphic, related to the **NIST Cyber Security Framework**

Domain performance of existing cybersecurity capability and options for consideration for all responses



DOMAIN 1: ASSET MANAGEMENT

MIL-1			MIL-2				MIL-3				MIL-4		MIL-5	
G1	G2	G3	G4	G5	G6	G7	IL1	IL2	IL3	IL4	IL1	IL2	IL3	IL1	IL2

The purpose of **Asset Management (AM)** is to identify, document, and manage assets during their life cycle to ensure sustained productivity to support critical services. There are seven goals in **Asset Management:**

- Goal 1 – Identify & prioritize critical services
- Goal 2 – Inventory assets, and establish the authority and responsibility for these assets
- Goal 3 – Establish the relationship between assets and the services they support
- Goal 4 – Manage the asset inventory
- Goal 5 – Manage access to assets
- Goal 6 – Prioritize & manage information assets
- Goal 7 – Prioritize & manage facility assets

The following contains questions asked during the CRR for each goal in the **Asset Management** domain, and your organization's response to these questions. In cases where the response is noted as "Incomplete" or "No", there is an accompanying Option for Consideration addressing that question.

Goal 1 – Identify & prioritize critical services		
1.	Are critical services identified? [SC:SG2.SP1]	Yes
2.	Are critical services prioritized based on analysis of potential impact if these services are disrupted? [SC:SG2.SP1]	Incomplete
	Option(s) for Consideration	
Q2	**CERT-RMM Reference:** [SC:SG2.SP1] Identify the organization's critical services, associated assets, and activities. A fundamental risk management principle is to focus on activities to protect and sustain services and assets that most directly affect the organization's ability to achieve its mission. **Additional Reference:** NIST SP 800-34, Revision 1 "Contingency Planning Guide for Federal Information Systems" (pages 15-18)	

Goal 2 – Inventory assets, and establish the authority and responsibility for these assets		
1.	Are the assets that directly support the critical service inventoried? [ADM:SG1.SP1]	
	People	Incomplete
	Information	Incomplete
	Technology	Incomplete
	Facilities	Yes
	Option(s) for Consideration	
Q1	**CERT-RMM Reference:** [ADM:SG1.SP1] Identify and inventory critical assets. An organization must be able to identify its critical assets, document them, and establish their value in order to develop strategies for protecting and sustaining assets commensurate with their value to the services they support. **Additional Reference:** NIST SP 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems" (pages 2-3)	

CISA's No-Cost Cybersecurity Resources

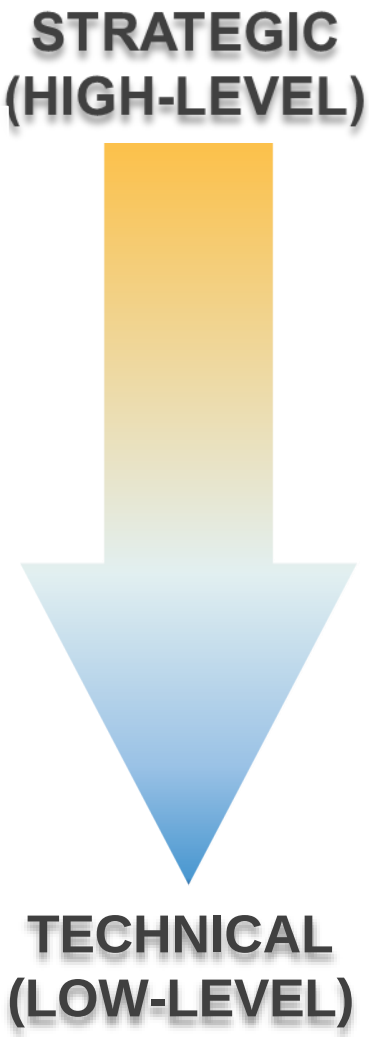
NO-Cost/Federally Funded

- **Cybersecurity Assessments**
  - Baseline Assessments
    - Ransomware Readiness Assessment (RRA)
    - Cybersecurity Performance Goals (CPG)
  - Intermediate Assessments
    - Cyber Infrastructure Survey (CIS)
    - Cyber Resilience Essentials (CRE)
  - Advanced Assessments
    - External Dependencies Management (EDM)
    - Incident Management Review (IMR)
    - Cyber Resilience Review (CRR)

- **Cyber Hygiene Services**
  - External Vulnerability Scanning Service
  - Web Application Scanning Service

Identify and mitigate vulnerabilities on your internet-facing systems and web applications with CISA's vulnerability and web application scanning services.

Contact your CISA Cybersecurity State Coordinator (CSC) or Cybersecurity Advisor (CSA) to schedule these.

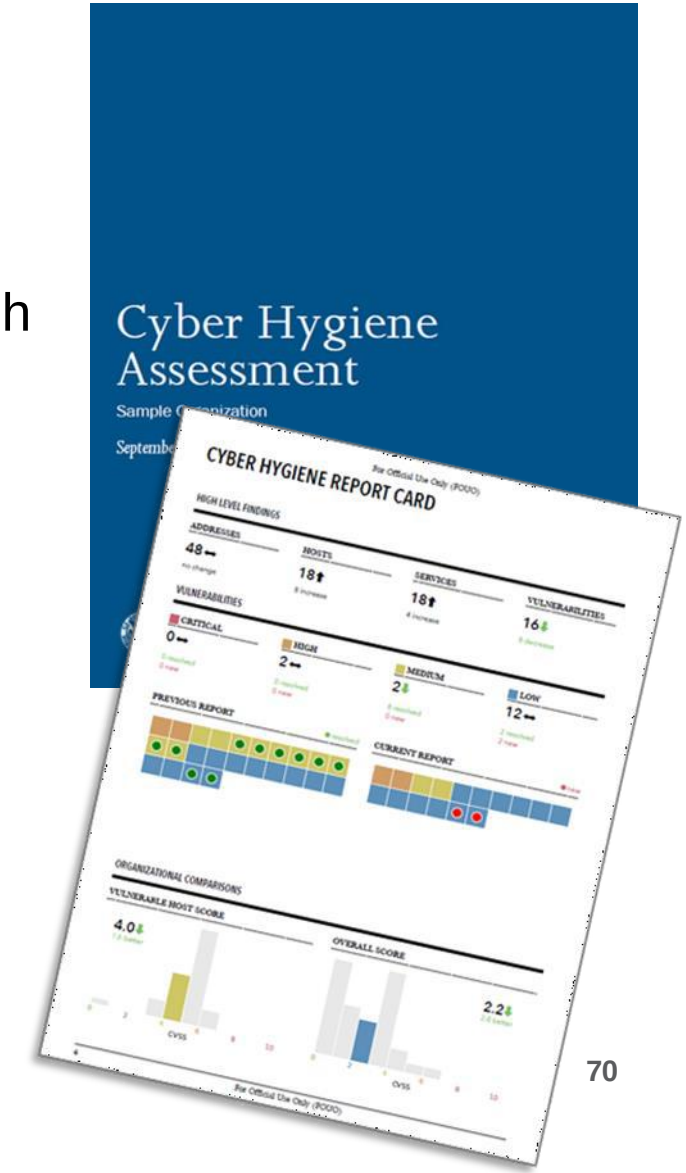


Vulnerability Scanning Service (CyHy)

CISA's Vulnerability Scanning (VS) is persistent "internet scanning-as-a-service". VS service continuously assesses the health of your internet-accessible assets by checking for known vulnerabilities, weak configurations—or configuration errors—and suboptimal security practices. VS service also recommends ways to enhance security through modern web and email standards.

VS service includes:

- **Target Discovery** identifies all active internet-accessible assets (networks, systems, and hosts) to be scanned.
- **Vulnerability Scanning** initiates non-intrusive checks to identify potential vulnerabilities and configuration weaknesses.
- **Weekly Report** of known vulnerabilities detected on Internet-facing hosts for your organization, as well as recommended remediations.



Web Application Scanning (WAS)

CISA's Cyber Hygiene Web Application Scanning is "internet scanning-as-a-service."

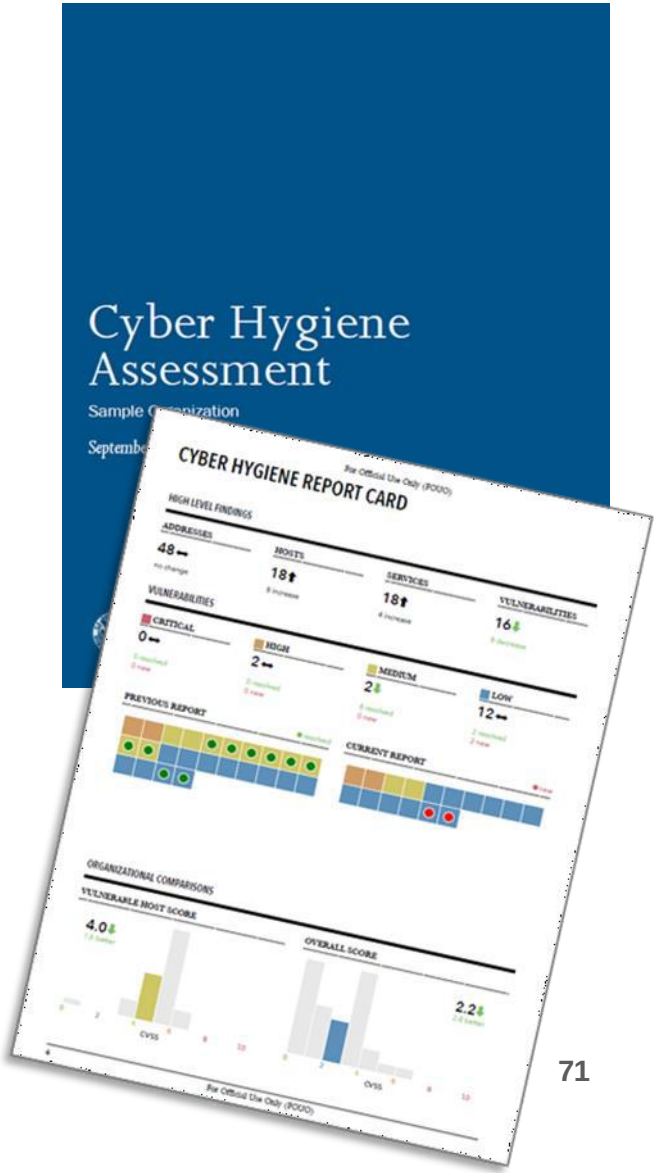
This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations and provide recommendations on how to remediate.

Scanning Objectives:

- Maintain enterprise awareness of your publicly accessible web-based assets
- Provide insight into how systems and infrastructure appear to potential attackers
- Drive proactive mitigation of vulnerabilities to help reduce overall risk

Scanning Phases

- Discovery Scanning: identify active, internet-facing web applications
- Vulnerability Scanning: Initiate non-intrusive checks to identify potential vulnerabilities and configuration weaknesses



CISA's No-Cost Cybersecurity Resources

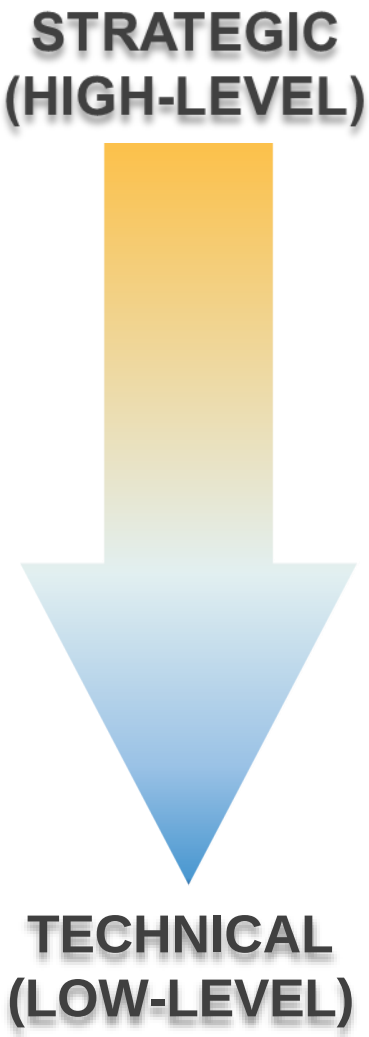
NO-Cost/Federally Funded

Build new or mature existing cyber capabilities with our workshops.

Exercise your incident response, business continuity, and disaster recovery plans with our Cyber Tabletop Exercise.

Contact your CISA Cybersecurity State Coordinator (CSC) or Cybersecurity Advisor (CSA) to schedule these.

- **Workshops & Exercises**
  - Asset Management Workshop (AMW)
  - Cyber Resilience Workshop (CRW)
  - Incident Management Workshop (IMW)
  - Vulnerability Management Workshop (VMW)
  - Digital Forensics Workshop I (DFW I)
  - Digital Forensics Workshop II (DFW II)
  - Cyber Tabletop Exercise



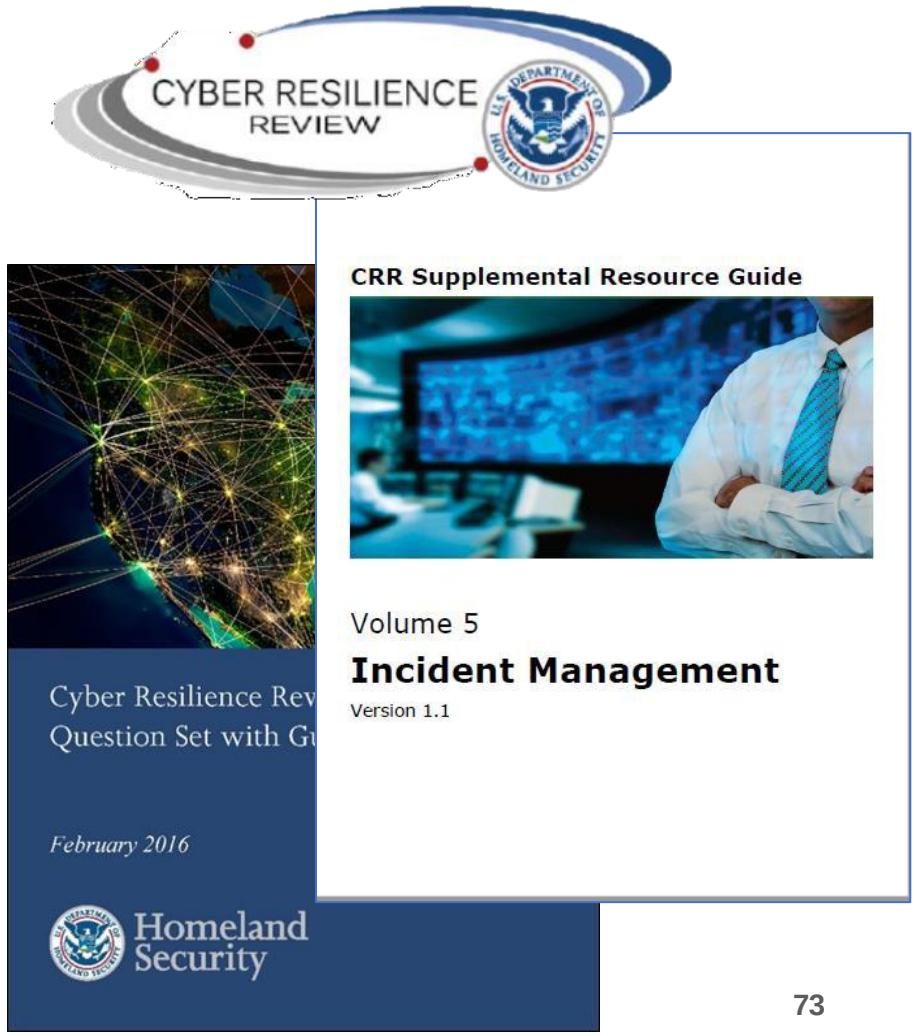
Incident Management Workshop (IMW)

Description: A 2-hour non-technical and informative session designed to help organizations understand incident management concepts, key elements, planning and implementation.

Goal: The goal of the workshop is to provide organizations with tangible, useful takeaway information on how to manage cybersecurity incidents effectively and, ultimately, achieve operational resilience.

Audience: Organizations that want to learn about an approach to developing a cyber incident management capability.

Format: In-Person or Virtual



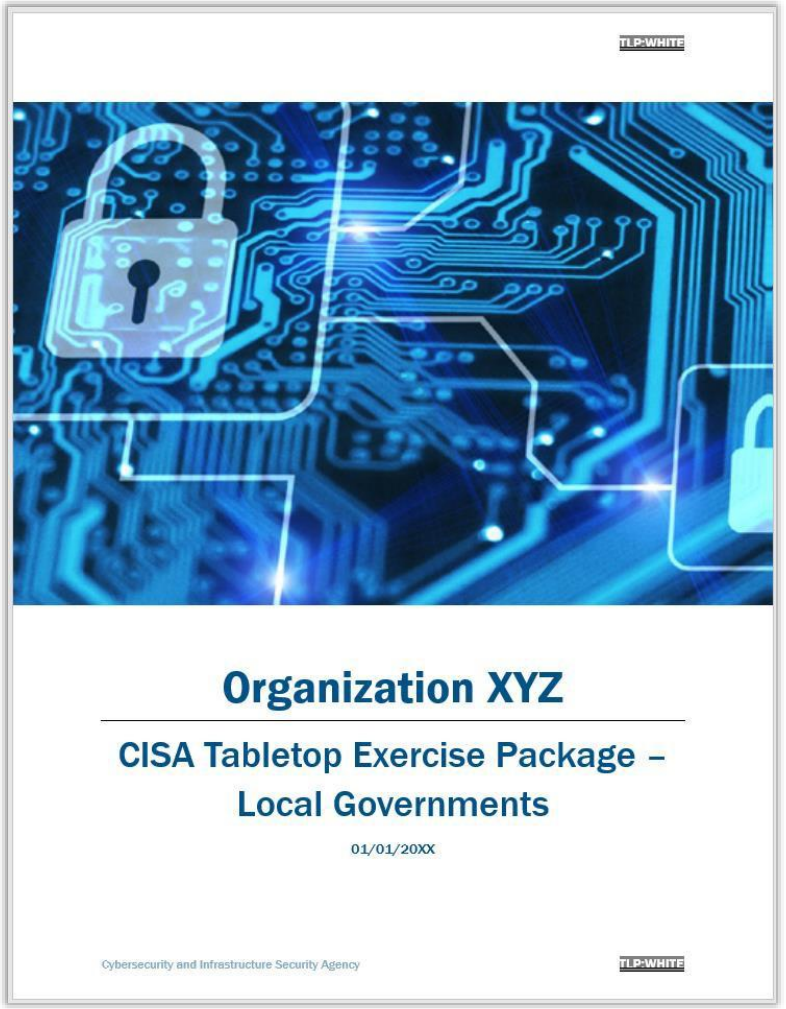
Cyber Tabletop Exercise (CTTX)

Description: A 2-hour or 4-hour facilitated cybersecurity tabletop exercise, where organizations are presented with a cyber threat-based scenario and are challenged to consider how their organization would respond, based on existing incident response plans.

Goal: The goal of the exercise is to provide organizations an opportunity to assess their level of readiness to respond to and recover from a cybersecurity incident impacting their operating environment.

Audience: Organizations that want to assess their level of readiness to respond to and recover from a cybersecurity incident.

Format: In-Person or Virtual



CISA's No-Cost Cybersecurity Resources

NO-Cost/Federally Funded

STRATEGIC (HIGH-LEVEL)

- **Cybersecurity Assessments**
  - Baseline Assessments
    - Ransomware Readiness Assessment (RRA)
    - Cybersecurity Performance Goals (CPG)
  - Intermediate Assessments
    - Cyber Infrastructure Survey (CIS)
    - Cyber Resilience Essentials (CRE)
  - External Vulnerability Scanning Service
  - Web Application Scanning Service

- **Workshops & Exercises**
  - Asset Management Workshop (AMW)
  - Cyber Resilience Workshop (CRW)
  - Incident Management Workshop (IMW)
  - Vulnerability Management Workshop (VMW)
  - Digital Forensics Workshop I (DFW I)
  - Digital Forensics Workshop II (DFW II)

Assess and validate your organization's architecture and controls with our technical assessments.

Technical Assessments*
- Remote Penetration Test (RPT)
- Risk and Vulnerability Assessment (RVA)
- Validated Architecture Design Review (VADR)

***Note:** Eligibility for technical assessments is contingent upon assessment of the stakeholder's capabilities by their Cybersecurity Advisor (CSA).

TECHNICAL (LOW-LEVEL)

Next Steps: CISA Cyber Partnership

Would you like to know more about CISA's no-cost cyber resources (cyber assessments, workshops, exercises, etc.) and partnership opportunities?

Next Steps:

1. Contact CISA Region 6's office (CISARegion6@cisa.dhs.gov) or your **Cybersecurity State Coordinator** (ernesto.ballesteros@cisa.dhs.gov);
2. Request an initial Cyber Protective Visit (CPV) from your **Cybersecurity Advisor (CSA)** or **Cybersecurity State Coordinator (CSC)**; and
3. Discuss how we can provide these assessments, workshops, exercises, and technical services for your organization.

Relevant Cyber Resources

General CISA Cyber Resources

General CISA Cyber Resources

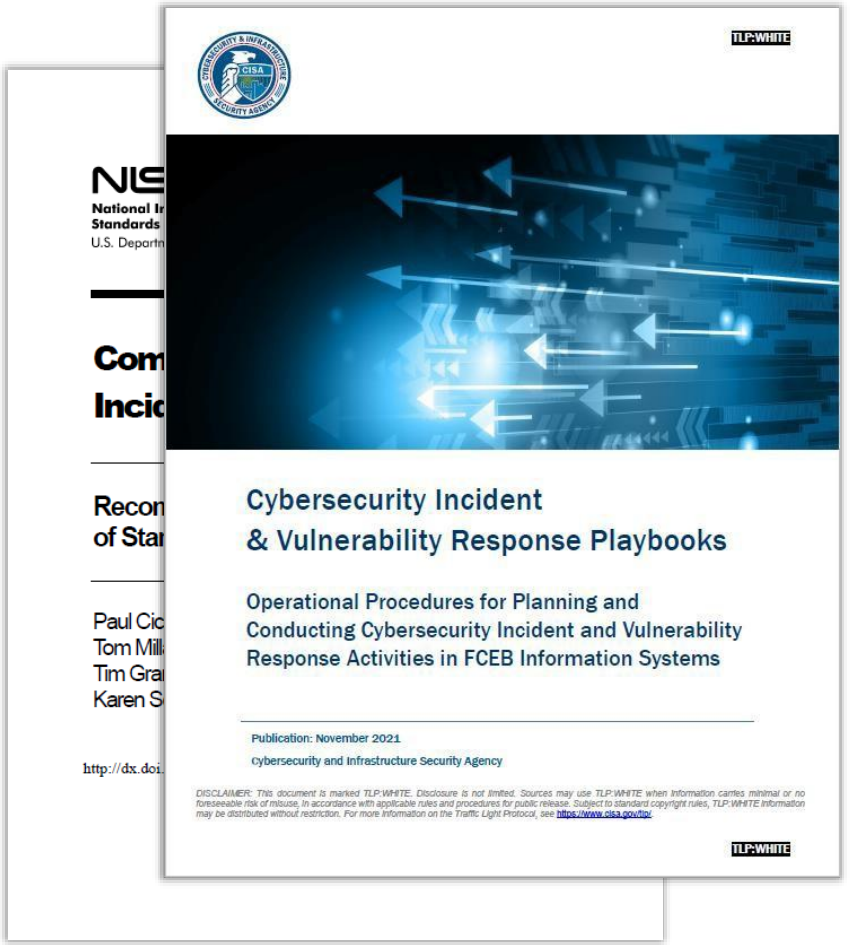
- Near-Term Actionable Information
  - CISA Shields Up Webpage
- Long-Term Actionable Information
  - CISA Shields Ready Webpage
- No-Cost Cyber Services
  - CISA Catalog of Free Cybersecurity Services
  - CISA Cyber Resource Hub
  - CISA's Free Cybersecurity Services and Tools Webpage
- Situational Awareness
  - CISA's Alerts and Advisories

https://www.cisa.gov/free-cybersecurity-services-and-tools

Cyber Incident Response Resources

General Cyber Incident Response Guidance and Training

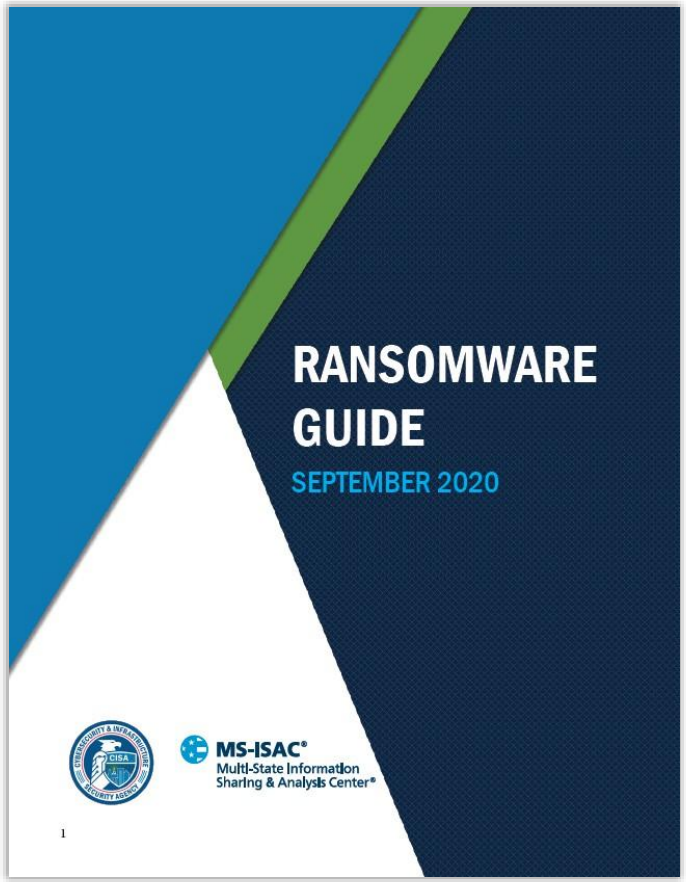
- Guidance
  - Federal Government Cybersecurity Incident & Vulnerability Response Playbooks
  - CISA's Water and Wastewater Sector – Incident Response Guide
  - CISA's CRR Resource Guide: Incident Management
  - NIST SP 800-61, Computer Security Incident Handling Guide Revision 2
- Training
  - CISA's Incident Response Training



Ransomware Readiness Resources

Ransomware Prevention Guidance, Best Practices and Tips

- Guidance
  - #StopRansomware Guide
- Best Practices and Tips
  - Identifying assets that are searchable via online tools and take steps to reduce that exposure
  - Understanding patches and software updates
  - Using caution with email attachments
  - SMB security best practices
  - Website security



CISA REGION 6

Ernesto Ballesteros, JD, MS, CISSP, CISA, Security+
Cybersecurity State Coordinator of Texas, Region 6
Cybersecurity and Infrastructure Security Agency
EMAIL: ernesto.ballesteros@cisa.dhs.gov
CELL: (210) 202-6646

CISA Region 6
CISARegion6@cisa.dhs.gov

MS-ISAC SOC INCIDENT REPORTING
866-787-4722; soc@cisecurity.org

CISA INCIDENT REPORTING SYSTEM
https://us-cert.cisa.gov/forms/report

CISA CENTRAL - 24/7 Watch
(888) 282-0870; report@cisa.gov

FBI's 24/7 Cyber Watch (CyWatch)
(855) 292-3937; CyWatch@fbi.gov

NIST Cybersecurity Framework (CSF) 2.0: Overview & Resources

Jeff Marron, NIST

November 2024

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

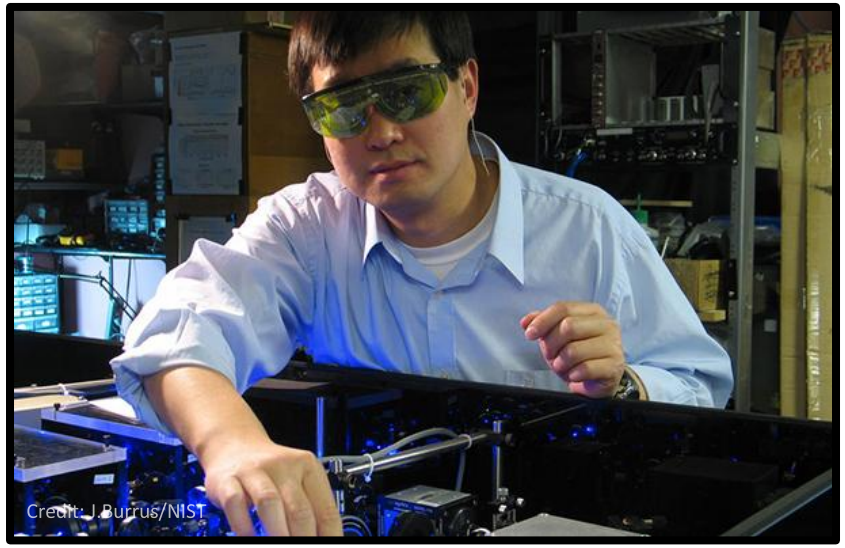
Agenda

- Introduction
- Brief Overview of NIST CSF
- What Has Changed with CSF 2.0
- Suite of CSF 2.0 Resources – including those for Energy sector
- Q&A

NIST's Mission

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

To promote U.S. innovation and industrial competitiveness by advancing **measurement science, standards, and technology** in ways that enhance economic security and improve our quality of life



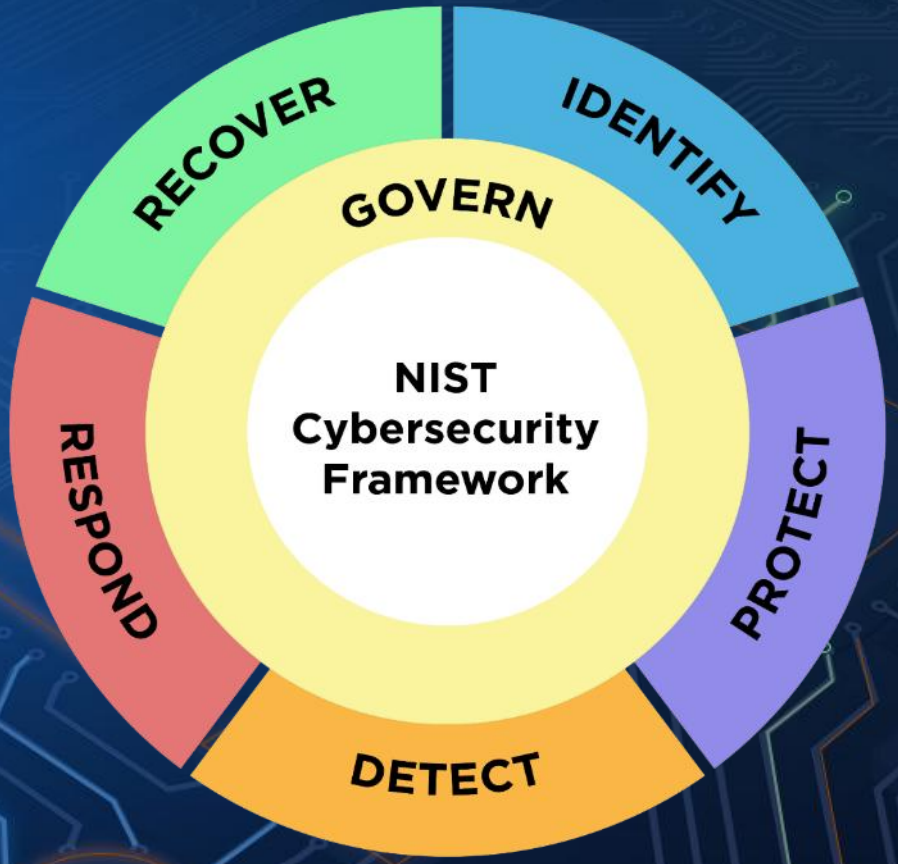
NIST's Priority Areas in Cybersecurity and Privacy

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Enhancing risk management	Privacy	Strengthening cryptographic standards and validation
Cybersecurity awareness, training, and education and workforce development	Metrics and measurements	Identity and access management
Trustworthy networks	Trustworthy platforms	Securing emerging technologies

Source: "*2021: What's Ahead from NIST in Cybersecurity and Privacy?*" By Kevin Stine, https://www.nist.gov/blogs/cybersecurity-insights/2021-whats-ahead-nist-cybersecurity-and-privacy

Brief Overview of CSF 2.0



NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

https://www.nist.gov/cyberframework

NIST Cybersecurity Framework

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

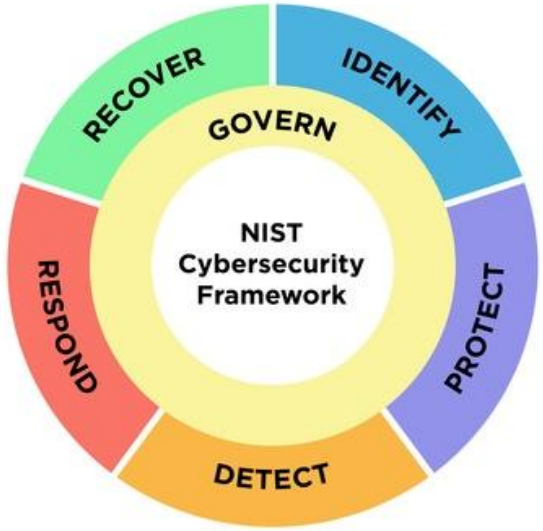
The NIST Cybersecurity Framework (CSF) helps organizations reduce their cybersecurity risks and is widely recognized as foundational to securing organizations & technology.

What is it?

- Comprehensive list of cybersecurity outcomes to reduce cybersecurity risks to an organization – the “what”, not “how” or “who”
- Based on and mapped to international standards and resources
- Adaptable to many technologies, sectors, maturity levels, and uses

How is it used?

- **Understand and Assess:** Describe the current or target cybersecurity posture of part or all of an organization, determine gaps, and assess progress toward addressing those gaps.
- **Prioritize:** Identify, organize, and prioritize actions for managing cybersecurity risks that align with the organization’s mission, legal and regulatory requirements, and risk management and governance expectations.
- **Communicate:** Provide a common language for communicating inside and outside the organization about cybersecurity risks, capabilities, needs, and expectations.



NIST Cybersecurity Framework 2.0

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

Voluntary guidance that helps organizations—regardless of size, sector, or maturity— better **understand, assess, prioritize**, and **communicate** their cybersecurity efforts.

**not a one-size-fits-all approach to managing cybersecurity risks.*

CSF Core	CSF Organizational Profiles	CSF Tiers
The nucleus of the CSF. **A taxonomy of high-level cybersecurity outcomes** that can help any organization manage its cybersecurity risks. Functions>Categories>Subcategories	A mechanism for describing an organization's **current and/or target cybersecurity posture** in terms of the CSF Core's outcomes.	Characterize the **rigor** of an organization's cybersecurity risk governance and management practices. Tiers can also provide **context** for how an organization views cybersecurity risks and the processes in place to manage those risks.

https://www.nist.gov/cyberframework

Global Impact of CSF 2.0

- The CSF is used widely **internationally**.
- NIST's work with the **International Organization for Standardization (ISO)**, in conjunction with the **International Electrotechnical Commission (IEC)**, over the last 11 years has been expansive.
- The resources allow organizations to build cybersecurity frameworks and organize controls using the CSF Functions.

Translations:

- CSF 1.1 and 1.0 – **13 languages**
- CSF 2.0 – **Portuguese** and **Spanish**
- The Small Business (SMB) Quick-Start Guide – **Portuguese**, **Spanish**, and **French**

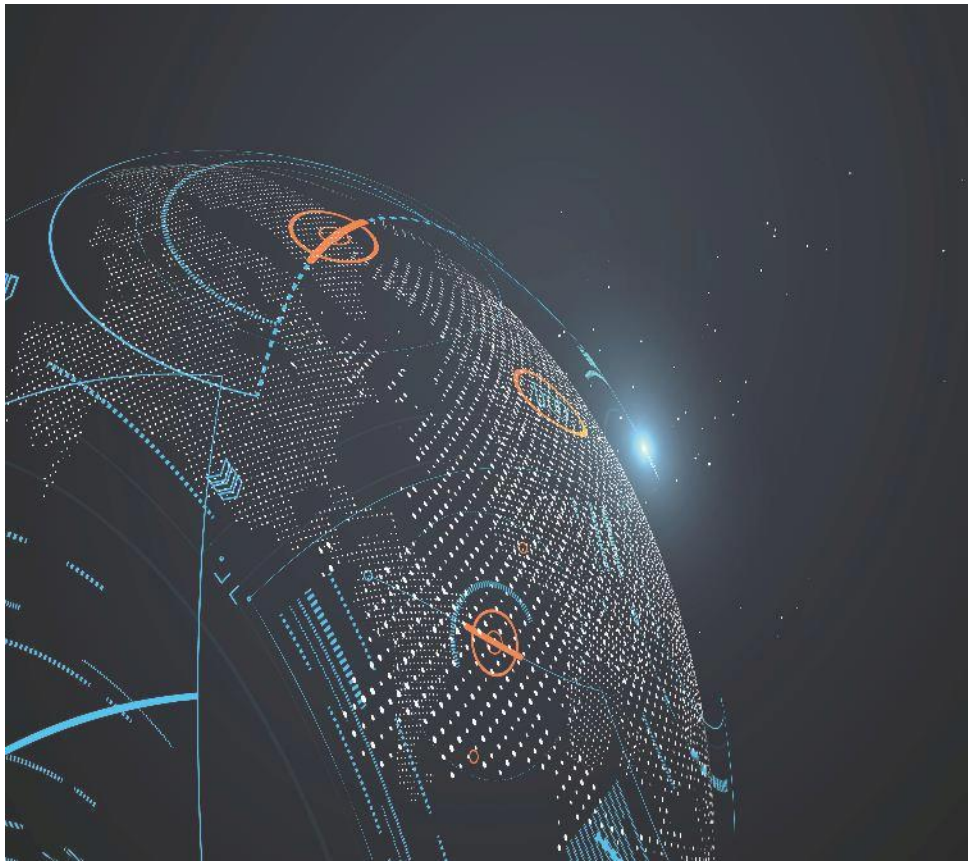
Learn more about our global impact: www.nist.gov/cyberframework

Governmental Policies on CSF

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

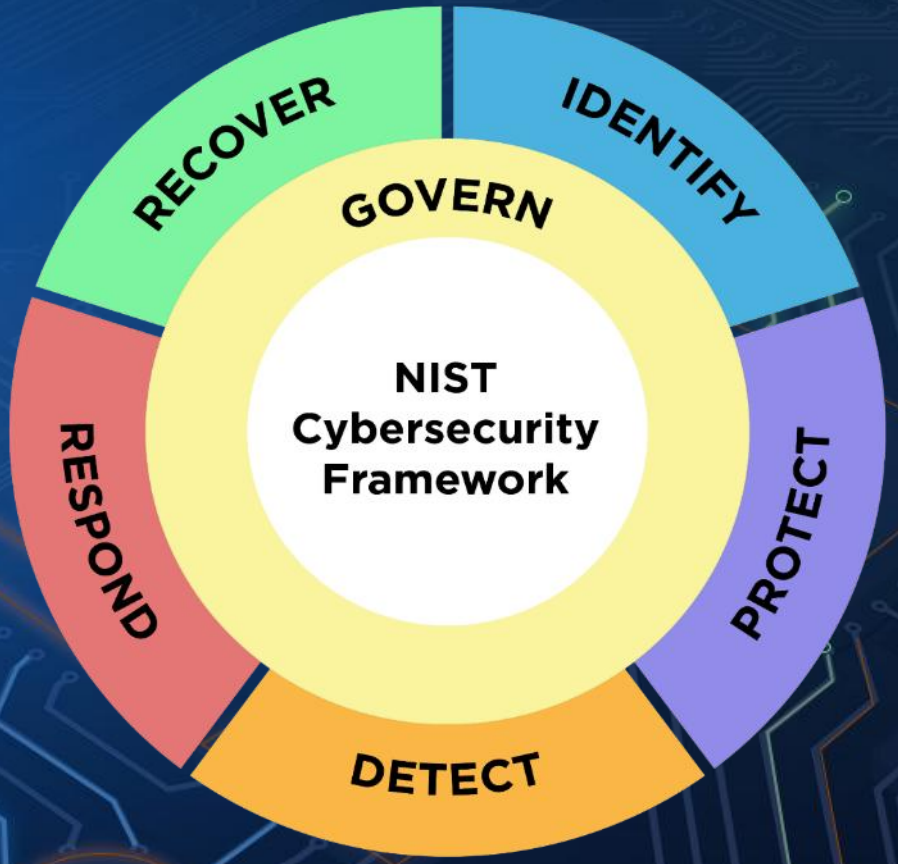
Adapted in several countries and regions

- United States (federal and state)
  - **The White House National Cybersecurity Strategy (March 2023): https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf**
    - "Regulations should be performance-based, leverage existing cybersecurity frameworks, voluntary consensus standards, and guidance – including the Cybersecurity and Infrastructure Security Agency (CISA)'s Cybersecurity Performance Goals and the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity – …"
- Italy, Poland, Israel, Japan, Uruguay, Australia, and more



Examples highlighted on the NIST International Cybersecurity and Privacy Resource Site:
https://www.nist.gov/cybersecurity/international-cybersecurity-and-privacy-resources

CSF 2.0



NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

https://www.nist.gov/cyberframework

How Did We Get Here?

The CSF has been developed through an iterative, community-driven process since 2013.

CSF 2.0 | What is Driving Change?

Stakeholder Insights – What *You* Needed!

Shifting Threat & Technology Environment

Evolving Enterprise Risk Management

The Existing Roadmap & Sector Profile Inputs

Changes in CSF 2.0

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Applies to ***all organizations*** – not just those in critical infrastructure.	Regardless of an organization's size or resources, there is a framework in place to help ensure safe and reliable power production and distribution.
Incorporates an entirely new function to address ***"Governing" risk management*** processes.	Provides an opportunity to align organizational goals and compliance requirements (e.g., NERC CIP).
Integrates Supply Chain throughout!	Focuses on third-party vendors and partners.
Focuses on ***continual improvement***.	Recognizes that cybersecurity is an evolving field and should adapt to new threats and technologies.
Provides a ***suite of resources*** (not one document).	Offers more guidance to help small businesses and specific use cases.
Encourages ***global*** use and collaboration.	Provides a collaborative approach to cybersecurity risk management.

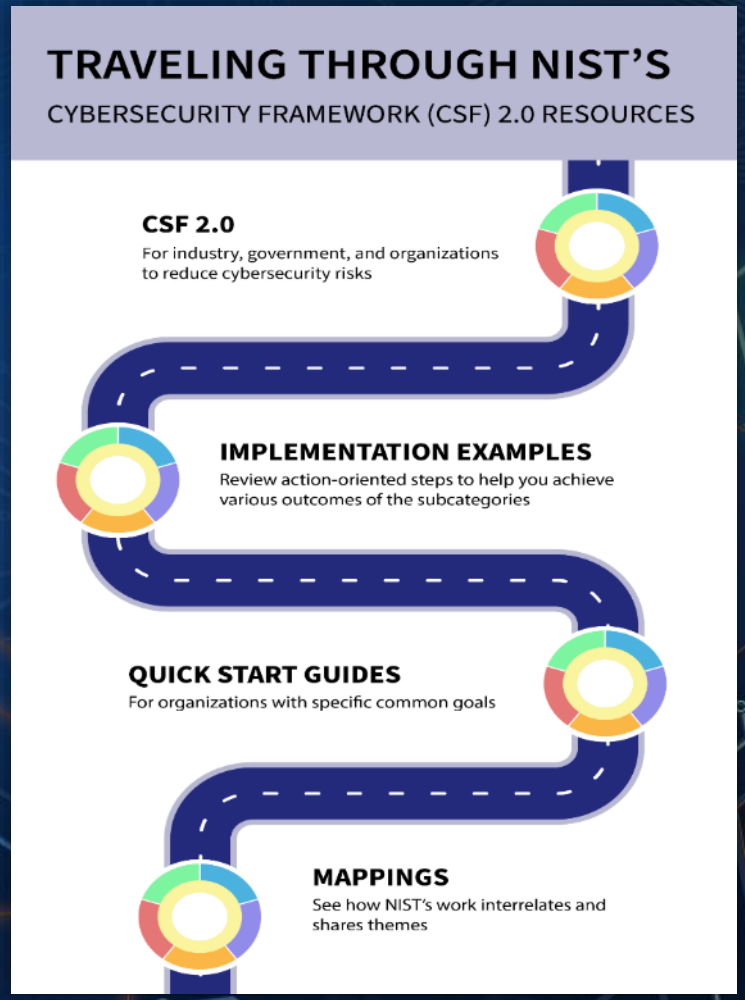
CSF 2.0 Core

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Table 1. CSF 2.0 Core Function and Category names and identifiers

Function	Category	Category Identifier
Govern (GV)	Organizational Context	GV.OC
	Risk Management Strategy	GV.RM
	Roles, Responsibilities, and Authorities	GV.RR
	Policy	GV.PO
	Oversight	GV.OV
	Cybersecurity Supply Chain Risk Management	GV.SC
Identify (ID)	Asset Management	ID.AM
	Risk Assessment	ID.RA
	Improvement	ID.IM
Protect (PR)	Identity Management, Authentication, and Access Control	PR.AA
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Platform Security	PR.PS
	Technology Infrastructure Resilience	PR.IR
Detect (DE)	Continuous Monitoring	DE.CM
	Adverse Event Analysis	DE.AE
Respond (RS)	Incident Management	RS.MA
	Incident Analysis	RS.AN
	Incident Response Reporting and Communication	RS.CO
	Incident Mitigation	RS.MI
Recover (RC)	Incident Recovery Plan Execution	RC.RP
	Incident Recovery Communication	RC.CO

NIST CSF 2.0 Resources

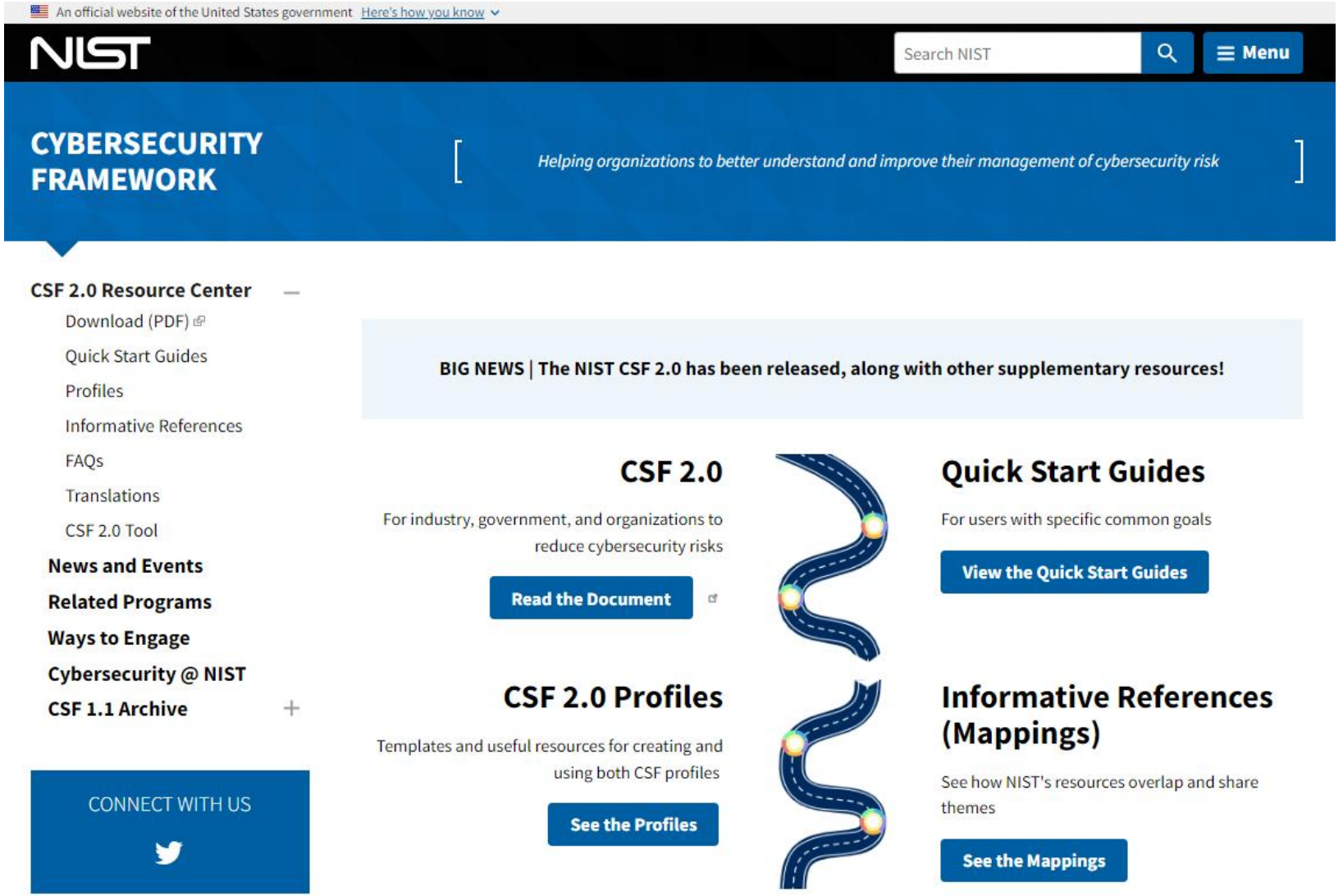


NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

https://www.nist.gov/cyberframework

CSF 2.0 Resource Library

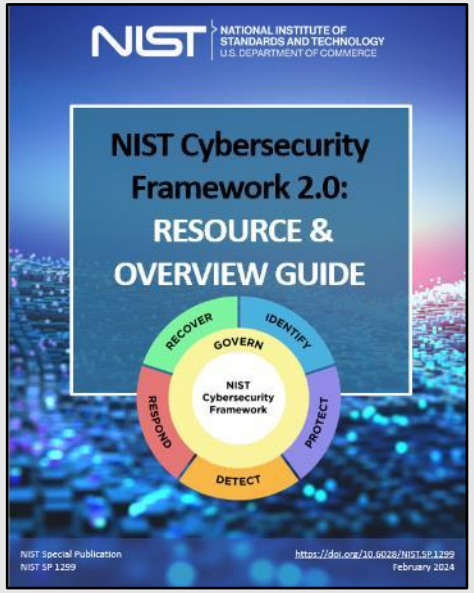
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

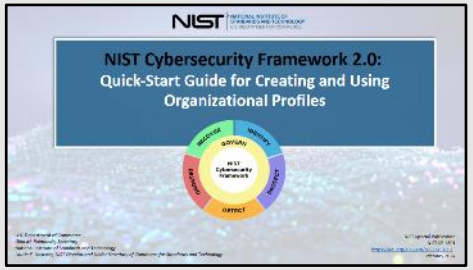


https://www.nist.gov/cyberframework

Suite of CSF 2.0 Resources

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE





Navigating NIST's CSF 2.0 Quick Start Guides

Resource and Overview Guide

Understand the basics and learn about the many available helpful CSF 2.0 resources

Download

The below targeted guides will help you with specific topics.

CSF 2.0 Organizational Profiles
Guidance for organizations, with considerations for creating and using spreadsheets called *Profiles*, to implement the CSF 2.0.

Download

CSF 2.0 Community Profiles
This guide provides considerations for creating and using Community Profiles to implement the CSF 2.0 and support the needs of organizations in communities that share common priorities.

Download

Small Business
Resources specifically tailored to small businesses with modest or no cybersecurity plans currently in place.

Download

C-SCRM
Helps organizations become smarter acquirers and suppliers of technology products and services.

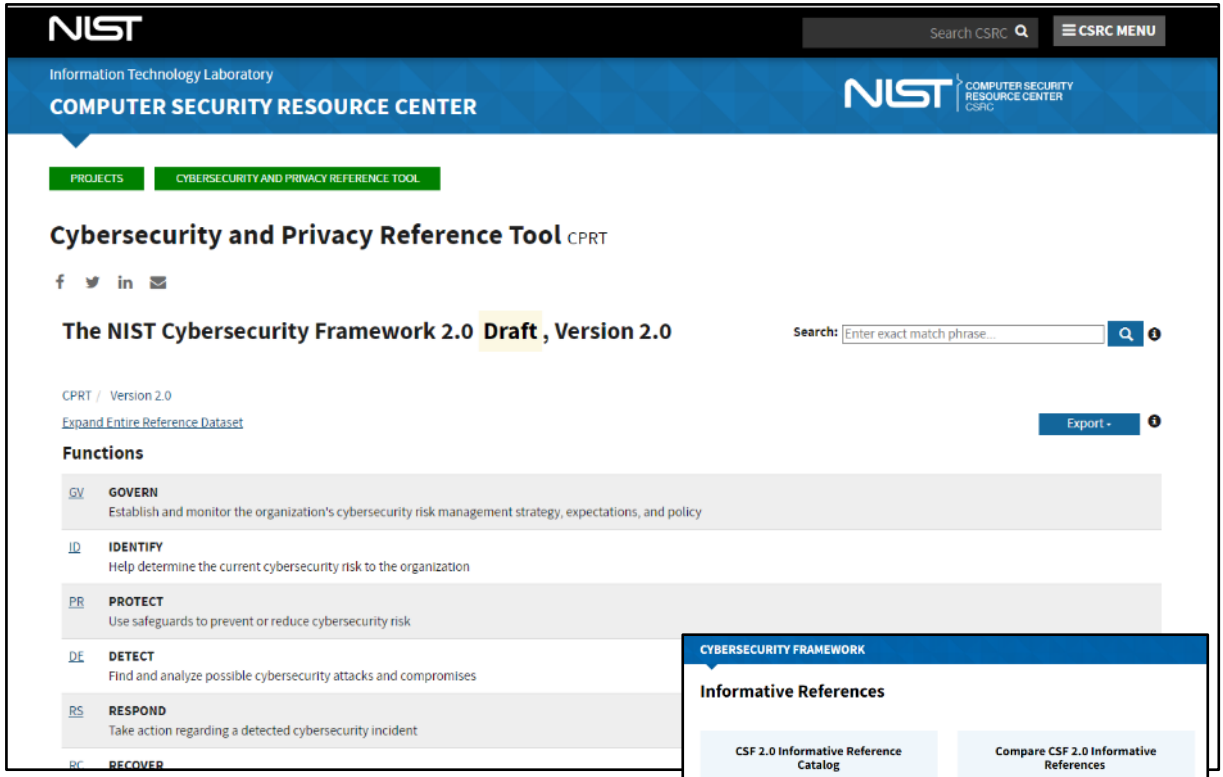
Download

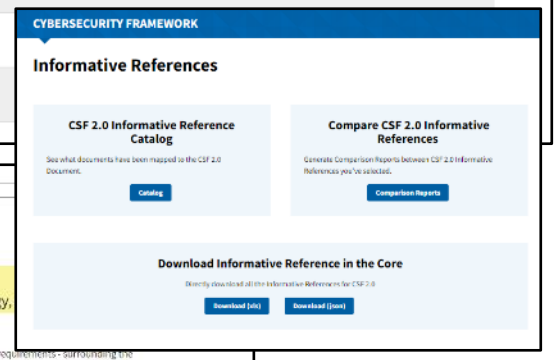
Tiers
Organizations can use these to apply the CSF 2.0 Tiers to Profiles to characterize the rigor of their cybersecurity risk governance and management outcomes.

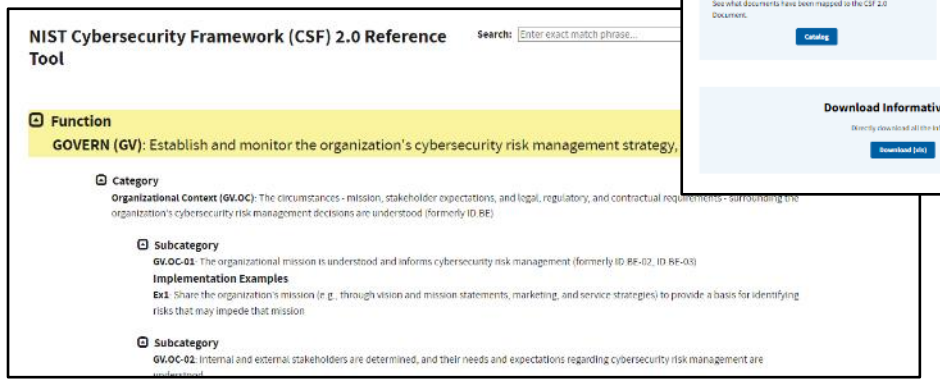
Download

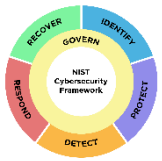
Enterprise Risk Management
How ERM practitioners can utilize the outcomes provided in the CSF 2.0 to improve organizational cybersecurity risk management.

Download









CSF Resources for Energy

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

OLIR Mapping of NERC CIP to CSF 1.1

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Download Informative Reference Resource

https://www.nerc.com/comm/RSTC_Reliability_Guidelines/NIST%20CSF%20to%20NERC%20CIP%20OLIR%20Mapping.xlsx

Informative Reference Information

Status:
Final

Informative Reference Version:
1.0.0

Focal Document Version:
CSF v1.1

Summary:
The purpose of this OLIR is to provide the relationship between NIST Cybersecurity Framework (CSF) v1.1 and the NERC Critical Infrastructure Protection (CIP) Standards.

Target Audience:
The intended audience are NERC registered entities of the Energy Sector Critical Infrastructure, electric segment, seeking to enhance the cyber security of the bulk electric system.

More details: Online Informative References (OLIR) | NERC CIP <-> CSF 1.1

OLIR Mapping of C2M2 to CSF 1.1

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Download Informative Reference Resource

https://www.nccoe.nist.gov/sites/default/files/2023-03/DOE-C2M2V2_1-CSF-mapping.xlsx

Informative Reference Information

Status:
Final

Informative Reference Version:
1.0.0

Focal Document Version:
CSF v1.1

Summary:
A mapping of Cybersecurity Capability Maturity Model version 2.1 practices to NIST Cybersecurity Framework version 1.1 Core.

Target Audience:
Energy sector entities seeking to evaluate their cybersecurity capabilities and optimize security investments.

More details: Online Informative References (OLIR) | C2M2 <-> CSF 1.1

NCCoE Energy Work Leveraging CSF

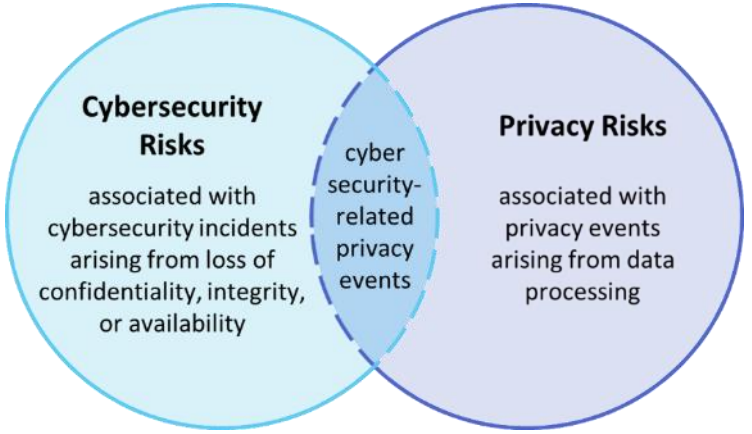
NIST SP 1800-7: Situational Awareness for the Energy Sector

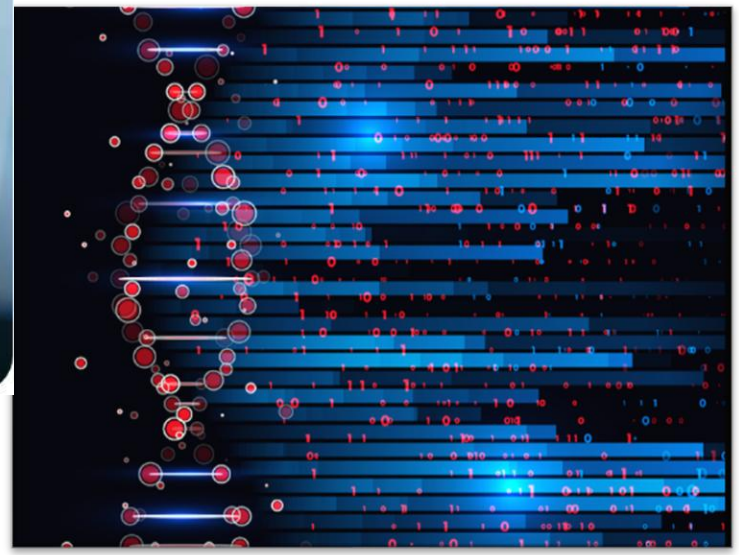
NIST SP 1800-23: Asset Management for the Energy Sector

NIST SP 1800-2: Identity and Access Management (IdAM) for the Energy Sector

NIST SP 1800-32: Securing Distributed Energy Resources

Upcoming: NIST IR 8498 Cybersecurity for Smart Inverters: Guidelines for Residential and Light Commercial Solar Energy Systems





Key Takeaways

- NIST standards and guidance help safeguard the nation's critical infrastructure, including energy.
- Anyone can download our freely available cybersecurity guidance and resources.
- Organizations can use our reference architectures to implement secure technology solutions.
- We are forward-looking – we incorporate technology concepts influencing the energy sector into our cybersecurity guidance.
- None of our cybersecurity guidance would be applicable without the expertise of our project collaborators.
- Cybersecurity risk management is always a journey – and the CSF 2.0 is a navigational guide that can help make that journey more successful.

Share with us your experiences with the CSF – we continue to encourage candid, constructive discussions around the CSF.

List of Resources

Quick Links	Contact Information
CSF 2.0 Website: https://www.nist.gov/cyberframework **CSF 2.0 FAQs:** https://www.nist.gov/faqs	cyberframework@nist.gov
NCCoE Community Profiles: https://www.nccoe.nist.gov/framework-resource-center https://www.nccoe.nist.gov/projects/guide-creating-community-profiles	framework-profiles@nist.gov
CSF 2.0 Small Business Quick Start Guide: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf	smallbizsecurity@nist.gov
Cybersecurity and Privacy Reference Tool (CPRT): https://csrc.nist.gov/Projects/cprt -	cprt@nist.gov
NCCoE Energy Portfolio: https://www.nccoe.nist.gov/energy	energy_nccoe@nist.gov

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

STAY IN TOUCH

CONTACT US

nist.gov
nccoe.nist.gov

@NISTcyber

Email us: cyberframework@nist.gov or nccoe@nist.gov

Energy Sector Threat Update – Nov 2024

Matt Tompkins, Federal Senior Intelligence Coordinator

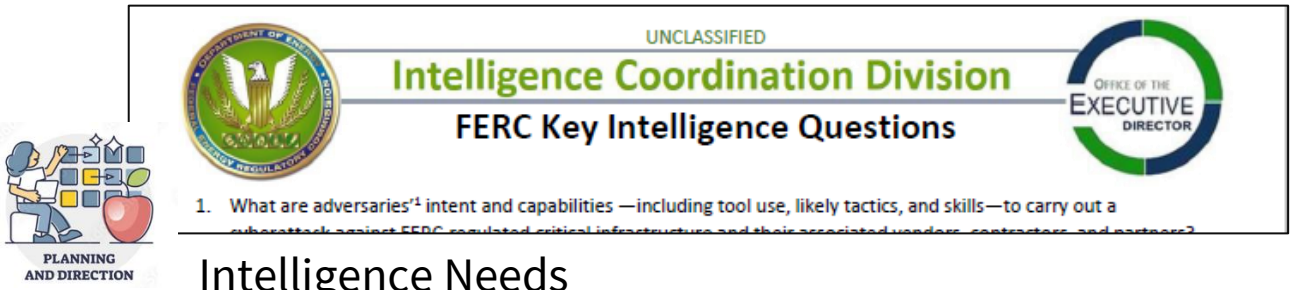
Agenda

- Intro to FERC's Intelligence Coordination Division
- Threat Update
  - Cyber Threats
  - Extremism
  - Espionage

All material is Unclassified

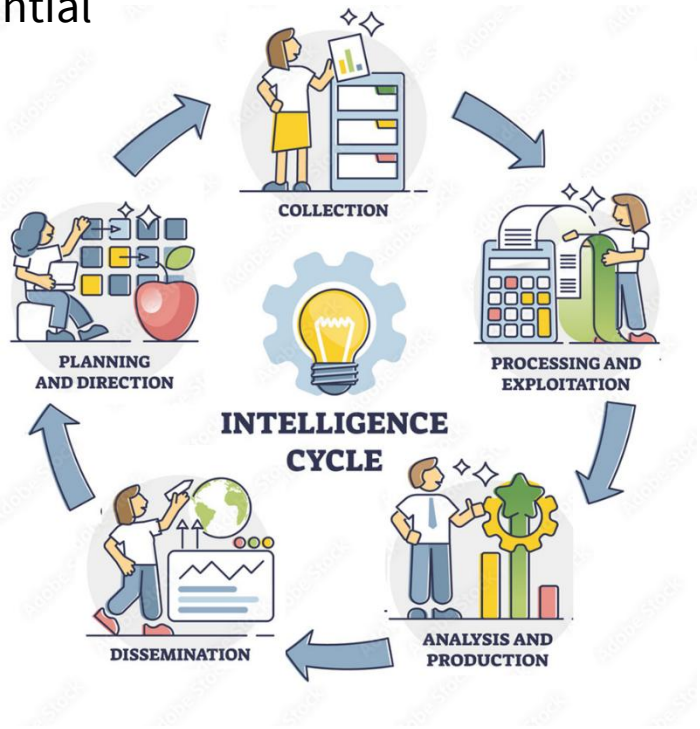
The material shared in this briefing does not necessarily represent the position of the Federal Energy Regulatory Commission, its Chairman, or individual Commissioners, and is not binding on the Commission.

FERC's Intelligence Coordination Division



Intelligence Needs

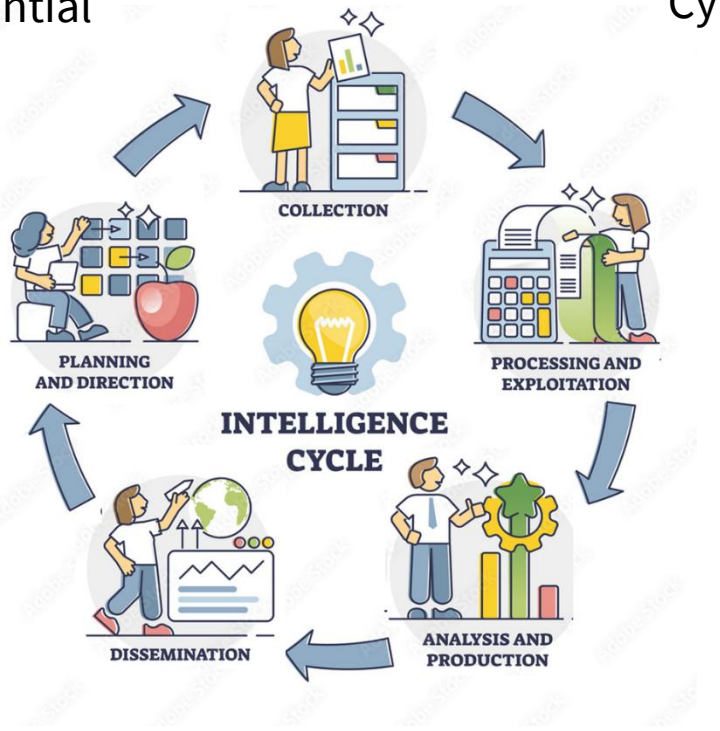
- Cyber Threats to Operational Technology (OT)
- General Cyber Threats with Disruptive Potential
- Physical Attack & Extremism Threats
- Espionage/Insider Threats & Sabotage
- Disruptive Technologies (UAS, AI, etc.)
- Supply Chain (Hardware, Software, inputs)



FERC's Intelligence Coordination Division

Intelligence Needs

- Cyber Threats to Operational Technology (OT)
- General Cyber Threats with Disruptive Potential
- Physical Attack & Extremism Threats
- Espionage/Insider Threats & Sabotage
- Disruptive Technologies (UAS, AI, etc.)
- Supply Chain (Hardware, Software, inputs)



Intelligence Partners & Resources

Intelligence Community (IC)

DOE ODNI FBI DHS NSA etc.

Info Sharing Environment

Fusion Centers ISACs Local LE

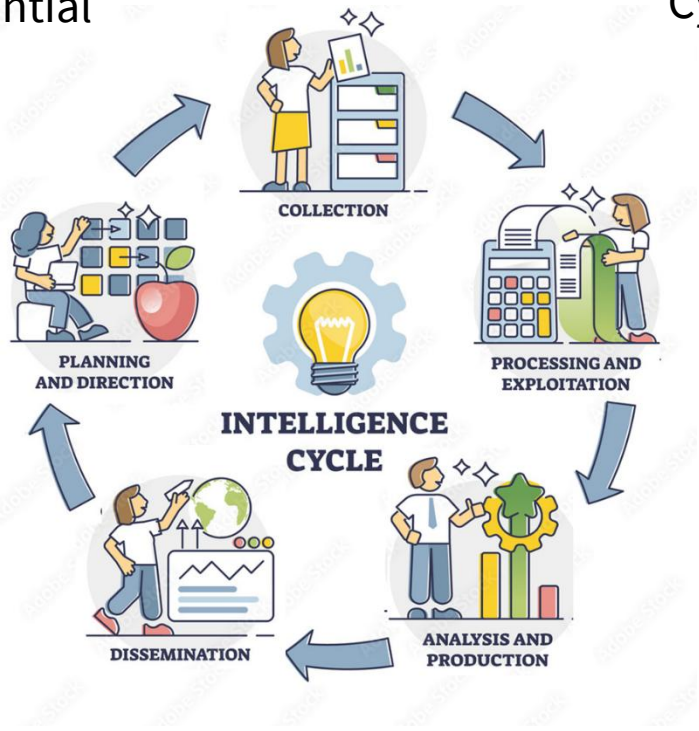
Additional Resources

Cybersecurity Vendors Foreign Partners

FERC's Intelligence Coordination Division

Intelligence Needs

- Cyber Threats to Operational Technology (OT)
- General Cyber Threats with Disruptive Potential
- Physical Attack & Extremism Threats
- Espionage/Insider Threats & Sabotage
- Disruptive Technologies (UAS, AI, etc.)
- Supply Chain (Hardware, Software, inputs)



Intelligence Partners & Resources

Intelligence Community (IC)

DOE ODNI FBI DHS NSA etc.

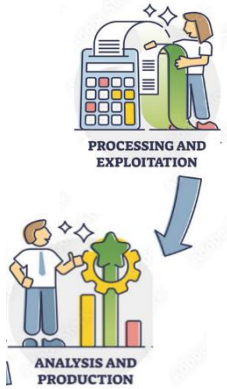
Info Sharing Environment

Fusion Centers ISACs Local LE

Additional Resources

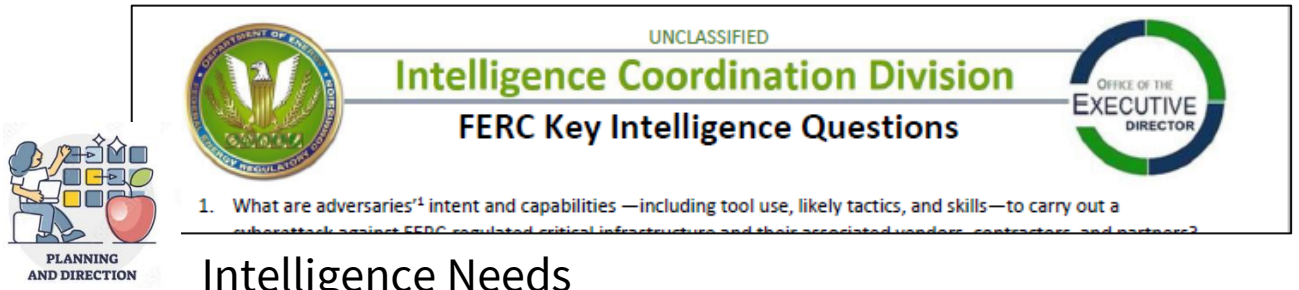
Cybersecurity Vendors Foreign Partners

Engagement, Processing & Production



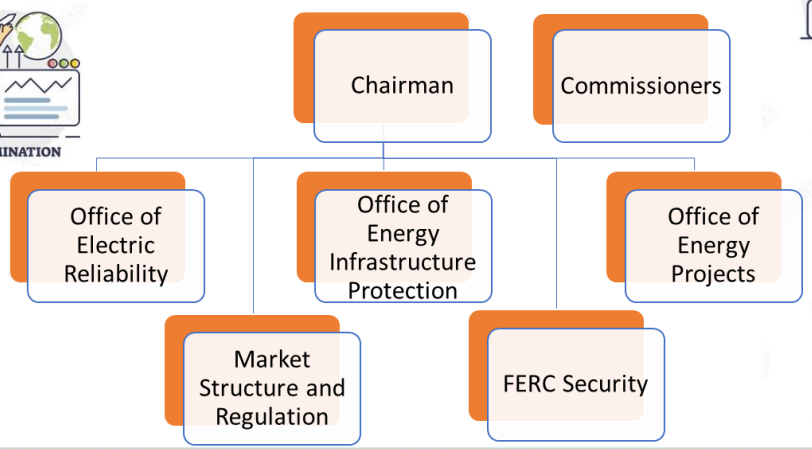
- FERC-specific insights on general reporting & analysis
- All levels of classification
- From incident reporting to routine updates to strategic analysis
- Intelligence utilization consultants for FERC NatSec novices
- Facilitate FERC subject matter expert insights for intelligence partners

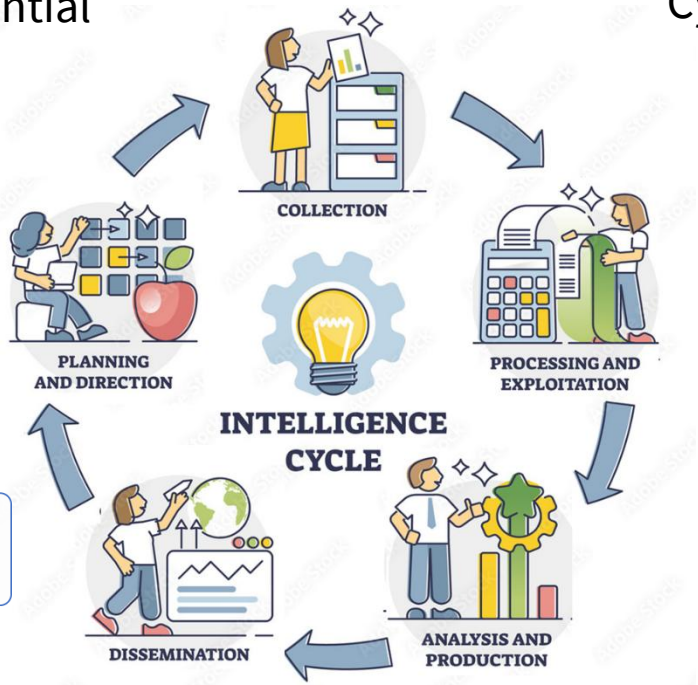
FERC's Intelligence Coordination Division



Intelligence Needs

- Cyber Threats to Operational Technology (OT)
- General Cyber Threats with Disruptive Potential
- Physical Attack & Extremism Threats
- Espionage/Insider Threats & Sabotage
- Disruptive Technologies (UAS, AI, etc.)
- Supply Chain (Hardware, Software, inputs)





Intelligence Partners & Resources

Intelligence Community (IC)

DOE ODNI FBI DHS NSA etc.

Info Sharing Environment

Fusion Centers ISACs Local LE

Additional Resources

Cybersecurity Vendors Foreign Partners

Engagement, Processing & Production

- FERC-specific insights on general reporting & analysis
- All levels of classification
- From incident reporting to routine updates to strategic analysis
- Intelligence utilization consultants for FERC NatSec novices
- Facilitate FERC subject matter expert insights for intelligence partners

Threat Update Materials

- Recent, specific updates on general topics

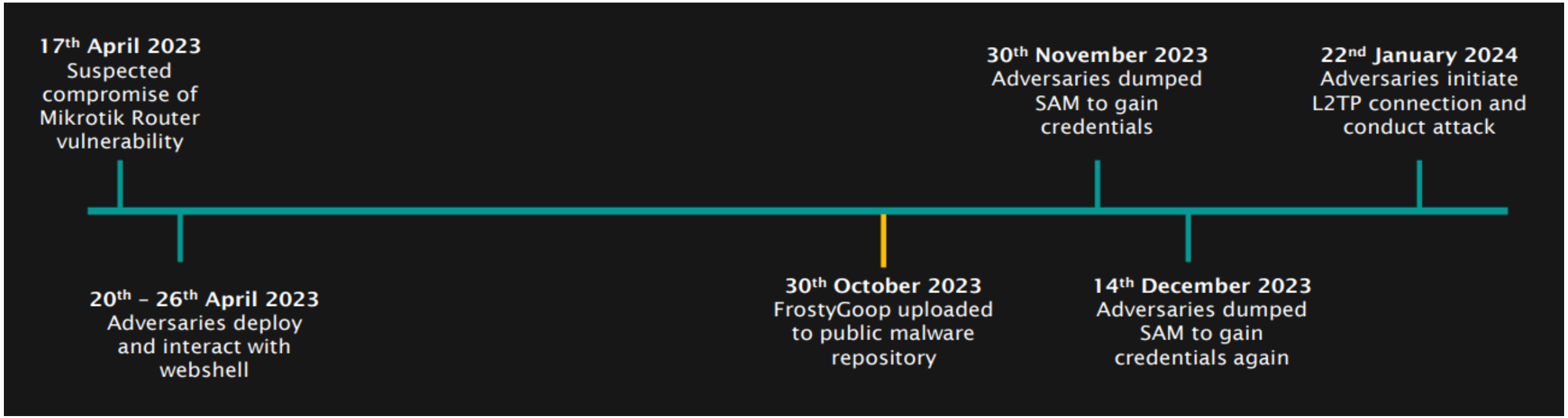
- Unrestricted material, often based on “Official Use Only” products
  - ➢Details provided to follow up for more information

Russian Cyber Activity Targeting Control Systems (Dragos, Mandiant)

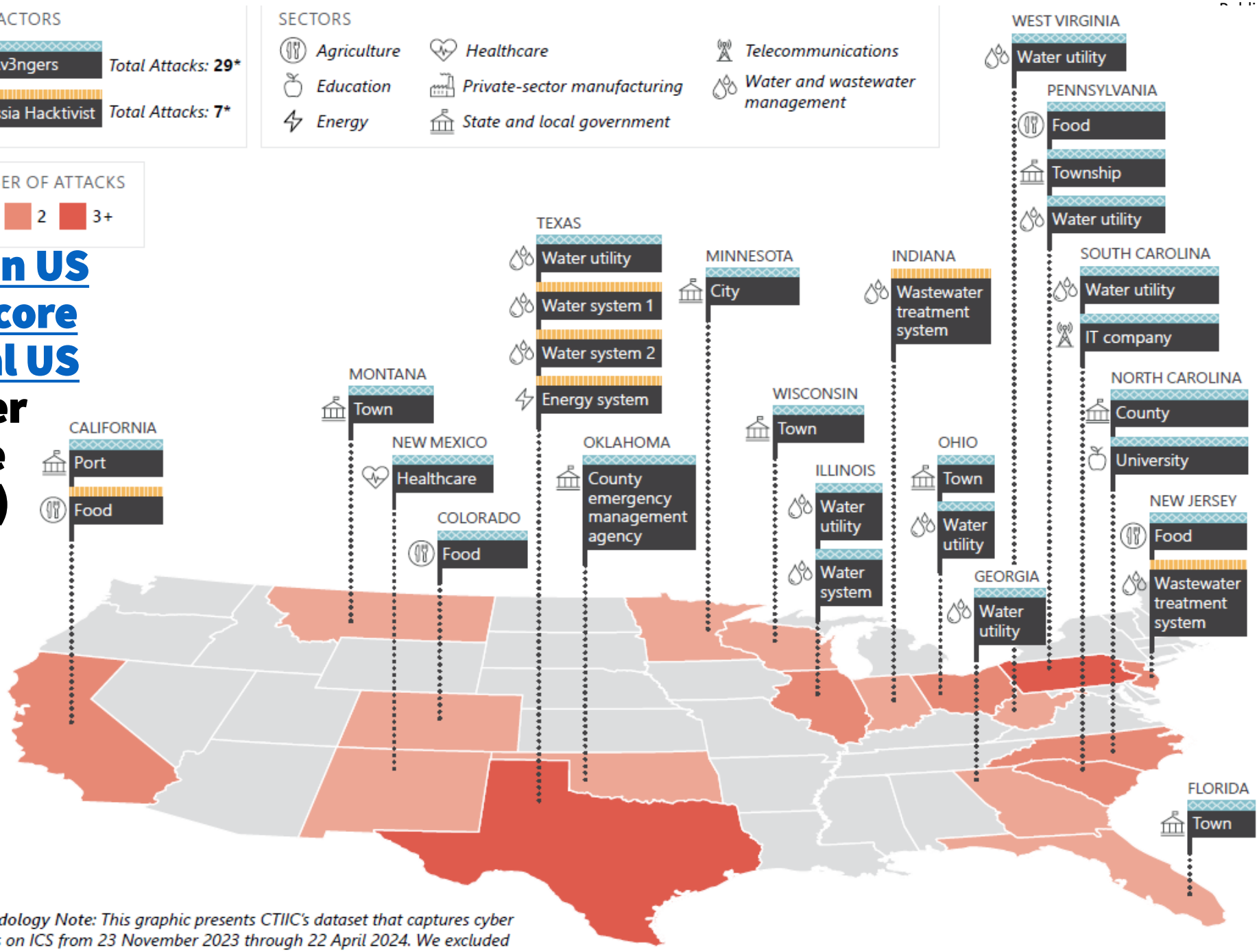
- **FrostyGoop**: newest industrial control system (ICS) specific malware
- **First ICS-specific malware** that directly interacts with industrial control systems (ICS) using Modbus Transmission Control Protocol (TCP) over port 502
- **Ukraine cyber attack**: during sub-zero temperatures, the attack disrupted municipal heating services to customers

What is Modbus TCP?

Modbus TCP is a communication protocol that enables devices to exchange data over a network.



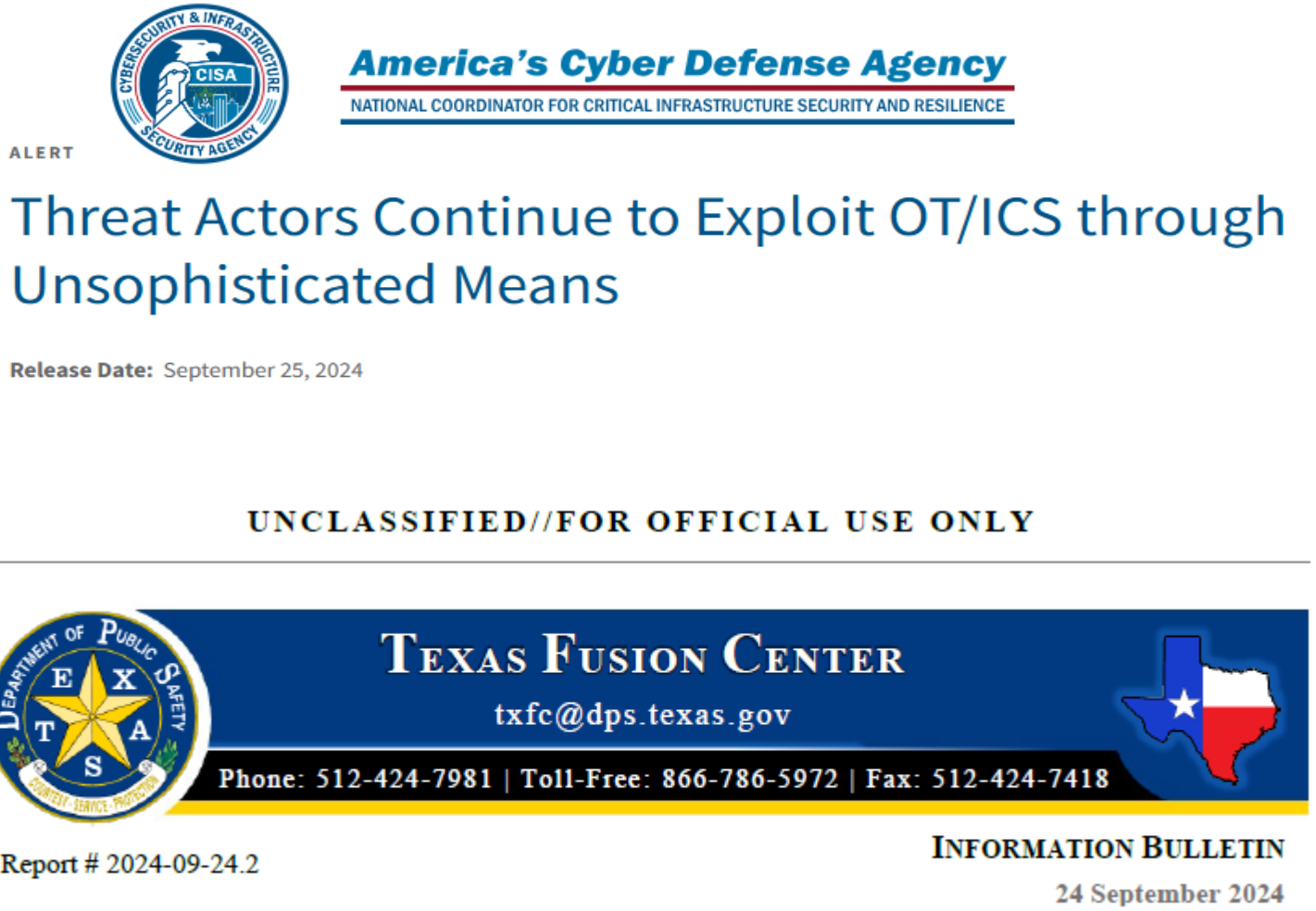
Recent Cyber Attacks on US Infrastructure Underscore Vulnerability of Critical US Systems (ODNI Cyber Threat Intelligence Integration Center)



Methodology Note: This graphic presents CTIIC's dataset that captures cyber attacks on ICS from 23 November 2023 through 22 April 2024. We excluded ransomware attacks on critical infrastructure entities.

*Including seven attacks at additional US locations.

Continued Hacktivist Activity Targeting TX Infrastructure



America's Cyber Defense Agency
NATIONAL COORDINATOR FOR CRITICAL INFRASTRUCTURE SECURITY AND RESILIENCE

ALERT

Threat Actors Continue to Exploit OT/ICS through Unsophisticated Means

Release Date: September 25, 2024

UNCLASSIFIED//FOR OFFICIAL USE ONLY

TEXAS FUSION CENTER
txfc@dps.texas.gov
Phone: 512-424-7981 | Toll-Free: 866-786-5972 | Fax: 512-424-7418

Report # 2024-09-24.2

INFORMATION BULLETIN
24 September 2024

- **Aug 2024:** Russian hacktivist compromise of West TX Wastewater System (WWS), with manipulation of control systems
- **Apr 2024:** Pro-Palestinian breach of North Texas municipal water district
- **Jan 2024:** Cyber Army of Russia Reborn (CARR) manipulated WWS in two Northwest TX municipalities
- **Nov 2023:** Financially-motivated cyber group targeted North TX municipal water facility in ransomware attack

U.S. Department of JUSTICE

Extremist Plots Targeting Energy Infrastructure

New Jersey Man Charged with Soliciting Destruction of Energy Facilities

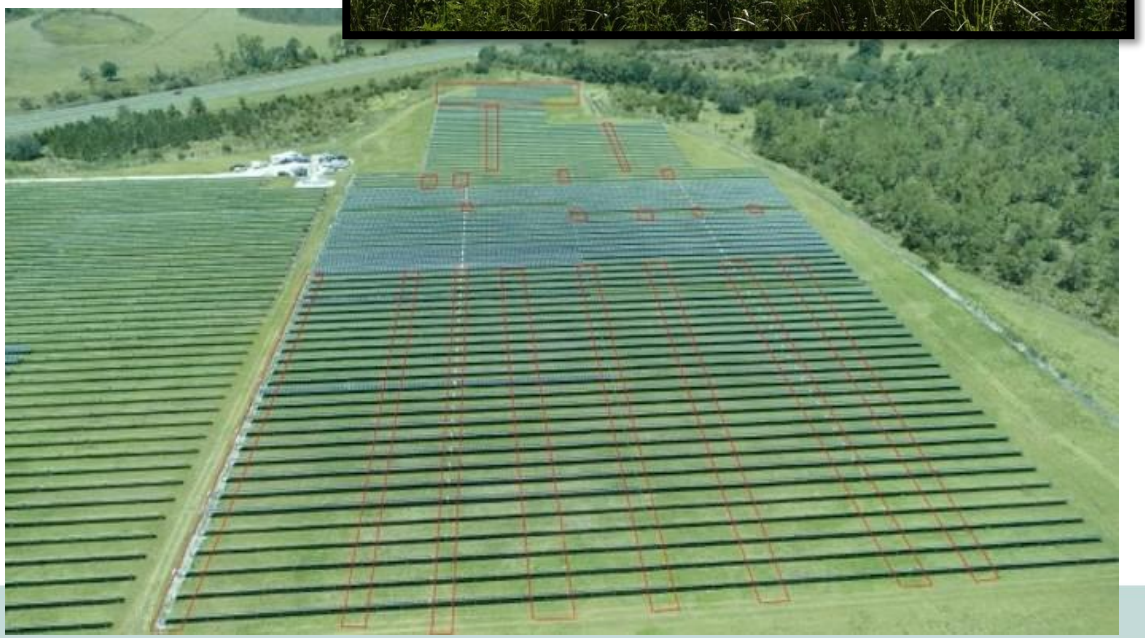
Thursday, July 11, 2024

Man Arrested for Explosives Threats and Attack on Energy Facility

Thursday, August 15, 2024

Man Arrested and Charged with Attempting to Use a Weapon of Mass Destruction and to Destroy an Energy Facility in Nashville

Monday, November 4, 2024



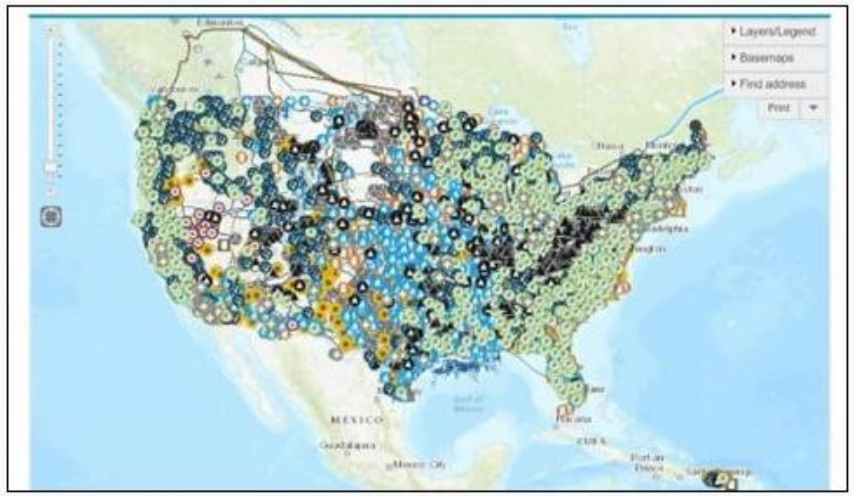
Two US citizens charged for "Terrorgram Collective" illegal activities, including attack guidance to target US energy infrastructure (DOJ)

Neo-Nazi Telegram Channel Provides Instructions for Making Improvised Explosive Devices

On December 12, a neo-Nazi Telegram channel posted instructions for building improvised explosive devices with commercially available items. The post was viewed approximately 900 times within four days. The channel has over 2,100 subscribers, and at least five previous versions of the channel have been removed by Telegram for violating the platform's Terms of Service. The specific set of instructions has previously been posted to iFunny, 4chan, and Reddit.

White Supremacist Forum on the Dark Web Shares U.S. Infrastructure Map, Encourages Attacks

CEP researchers located posts discussing attacks on U.S. electrical infrastructure on a white supremacist forum on the dark web. One user posted a link to an energy map on the U.S. Energy Information Administration website. Other users advised caution when accessing the site and offered advice on viewing the infrastructure map while remaining anonymous.



U.S. energy infrastructure map, the link to which was posted on a white supremacist site on the dark web.

TERRORGRAM Background/Refresher:

COUNTER EXTREMISM PROJECT

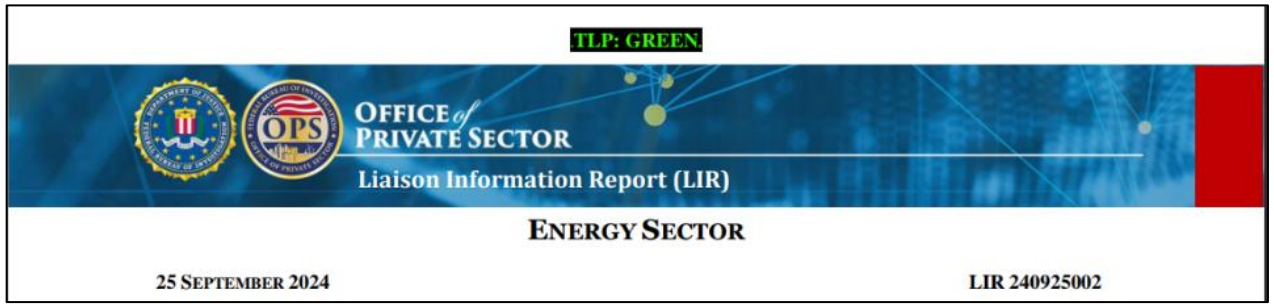
Extremist Content Online: White Supremacists Call For Acts Of Terrorism In New Book Released On Telegram

Monday, December 20, 2021

Security Camera Footage of US Energy Sector Attacks Benefit Law Enforcement Response (FBI)

States where incidents occurred at electrical substations cited in the report:

- Idaho (June 2023 – Cameras + Eyewitnesses)
- **Washington State (December 2022 – Cell Phone Data + Surveillance Video)**
- Oregon (November 2022 – IR, Motion, and local business camera)
- California (January 2023 – local business cameras)


TLP: GREEN

OFFICE of PRIVATE SECTOR

Liaison Information Report (LIR)

ENERGY SECTOR

25 SEPTEMBER 2024

LIR 240925002

DHS Assessments on Domestic Violent Extremist (DVE) Tactics

Exploring Cyber Tactics

Activities Observed	*and Discussed*
Website defacements	Reconnaissance
Data theft	Taking security systems offline
	Overwhelming control systems
	Intercepting credentials


UNCLASSIFIED//FOR OFFICIAL USE ONLY

OFFICE of INTELLIGENCE and ANALYSIS

INTELLIGENCE IN FOCUS

10 OCTOBER 2024 DHS-IA-IF-2024-05033

TERRORISM

Unmanned Aircraft Systems

Activities Observed	*and Discussed*
Surveillance	Lessons learned
Smuggling	Weaponization
Trespassing	


UNCLASSIFIED//FOR OFFICIAL USE ONLY

OFFICE of INTELLIGENCE and ANALYSIS

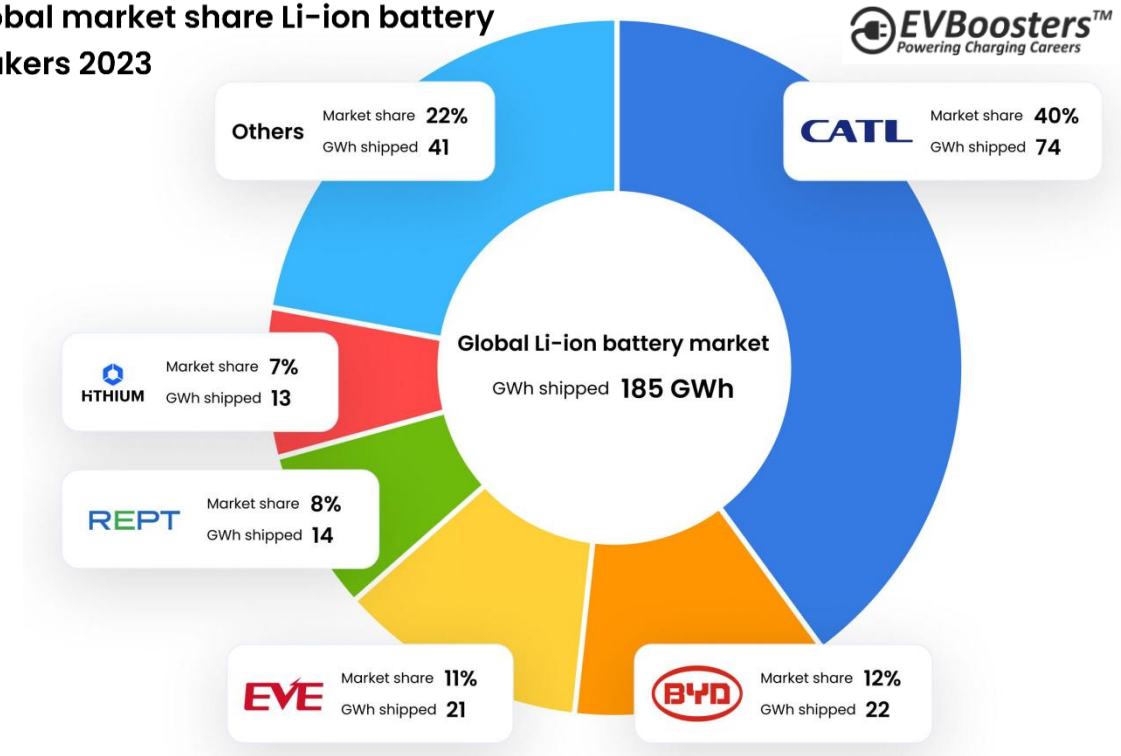
INTELLIGENCE IN FOCUS

23 AUGUST 2024 DHS-IA-IF-2024-10689

Chinese Mercantilism & Espionage Targeting of Energy Sector

China State-Supported Firms Likely Hindering US Utility Battery Energy Storage Security (DHS)

Global market share Li-ion battery makers 2023



UNCLASSIFIED//FOR OFFICIAL USE ONLY

OFFICE of INTELLIGENCE and ANALYSIS

INTELLIGENCE IN FOCUS

16 AUGUST 2024 DHS-IA-IF-2024-00021-A

PRC Positioned to Exploit US Green Energy Transition (FBI)

Green technology risks

EUROPEAN COUNCIL ON FOREIGN RELATIONS ecfr.eu

Economic dimension	Supply chain risk	The degree to which the production of a finished product or component is imported from a single source.
	Competitiveness risk	The degree to which domestic European industries are threatened in their existence by competition from foreign industry in the relevant sector.
	Weaponisation risk	The degree to which the producing country can use dependencies to coerce a recipient country into a desired action.
Climate dimension	Climate risk	The degree to which de-risking policies contribute to or hinder emissions reductions and the realisation of the EU's decarbonisation goals by 2050.
Security dimension	Energy security risk	The degree to which the EU is dependent on technology, materials, or components to ensure its energy security.
	National security risk	The degree to which a particular industry or product involves access to sensitive data or critical infrastructure that constitute a threat to national security.

TLP: GREEN

OFFICE of PRIVATE SECTOR

Liaison Information Report (LIR)

CROSS-SECTOR

20 AUGUST 2024 LIR 240820007-2

Russian Agents Continue to Escalate Sabotage Campaign in Europe, Including Energy Infrastructure (CSCE.gov)

The Marywilska 44 Shopping Center in Warsaw, Poland, burning during a potential sabotage attack.

"We've seen arson, sabotage and more dangerous actions conducted with increasing recklessness…the GRU in particular is on a sustained mission to generate mayhem on British and European streets"– Ken McCallum, Director General, MI5

"Russian intelligence services have gone a bit feral, frankly." – Sir Richard Moore, Chief, MI6

Selected sabotage incidents with suspected links to Russia in NATO countries , 2024 *The Economist*

1 Leonid Volkov attacked outside his home in Vilnius
2 Arson attack on Ukraine-linked business in London
3 Disruption of Czech rail-signalling systems **4** Planned sabotage against military installations in Germany
5 Reconnaissance at Rzeszow airport **6** Fire at Diehl Metall factory **7** Preparations for sabotage in Western Norway **8** Warsaw shopping-centre fire
9 Plot to bomb store north of Paris **10** Plot to assassinate CEO Armin Papperger revealed

Questions & Conversation

Matt Tompkins, FSIC

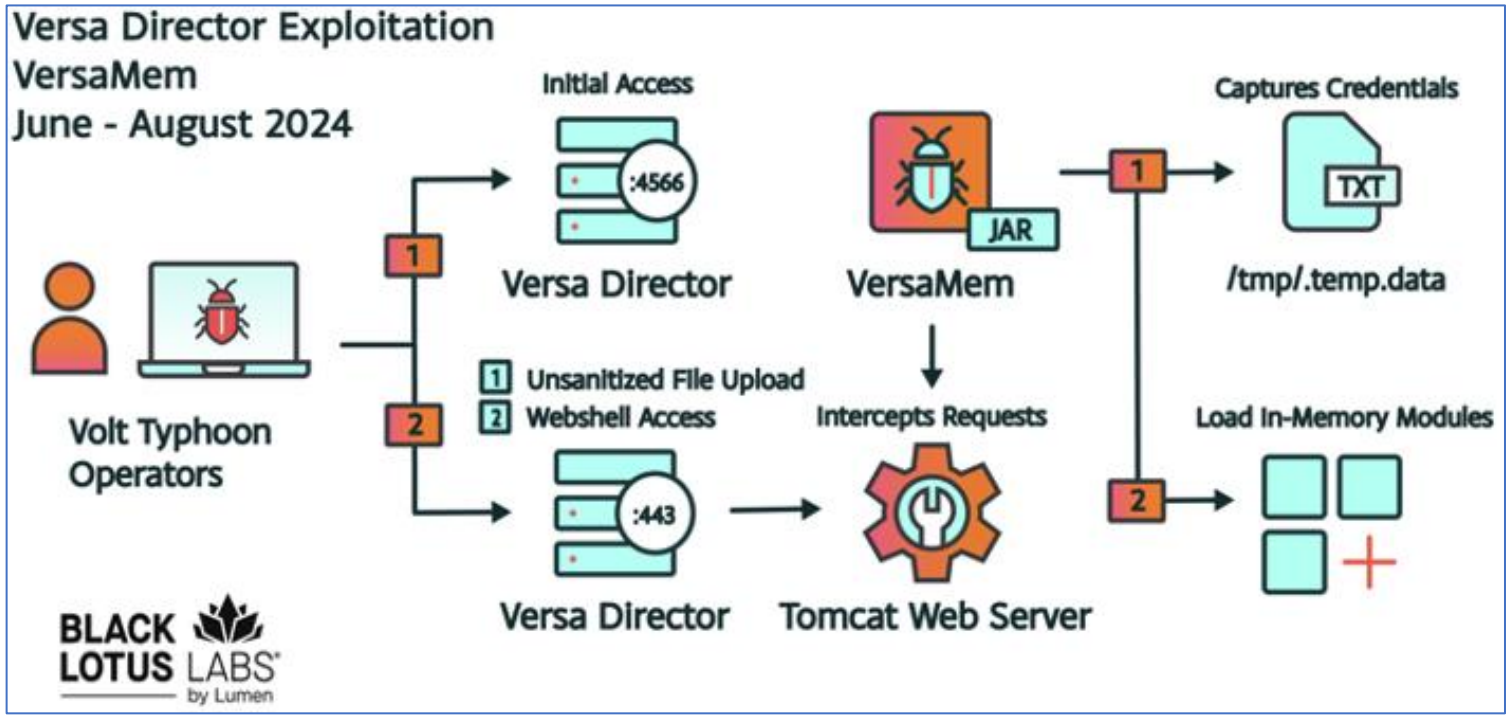
matthew.tompkins@ferc.gov

Backup / If Asked

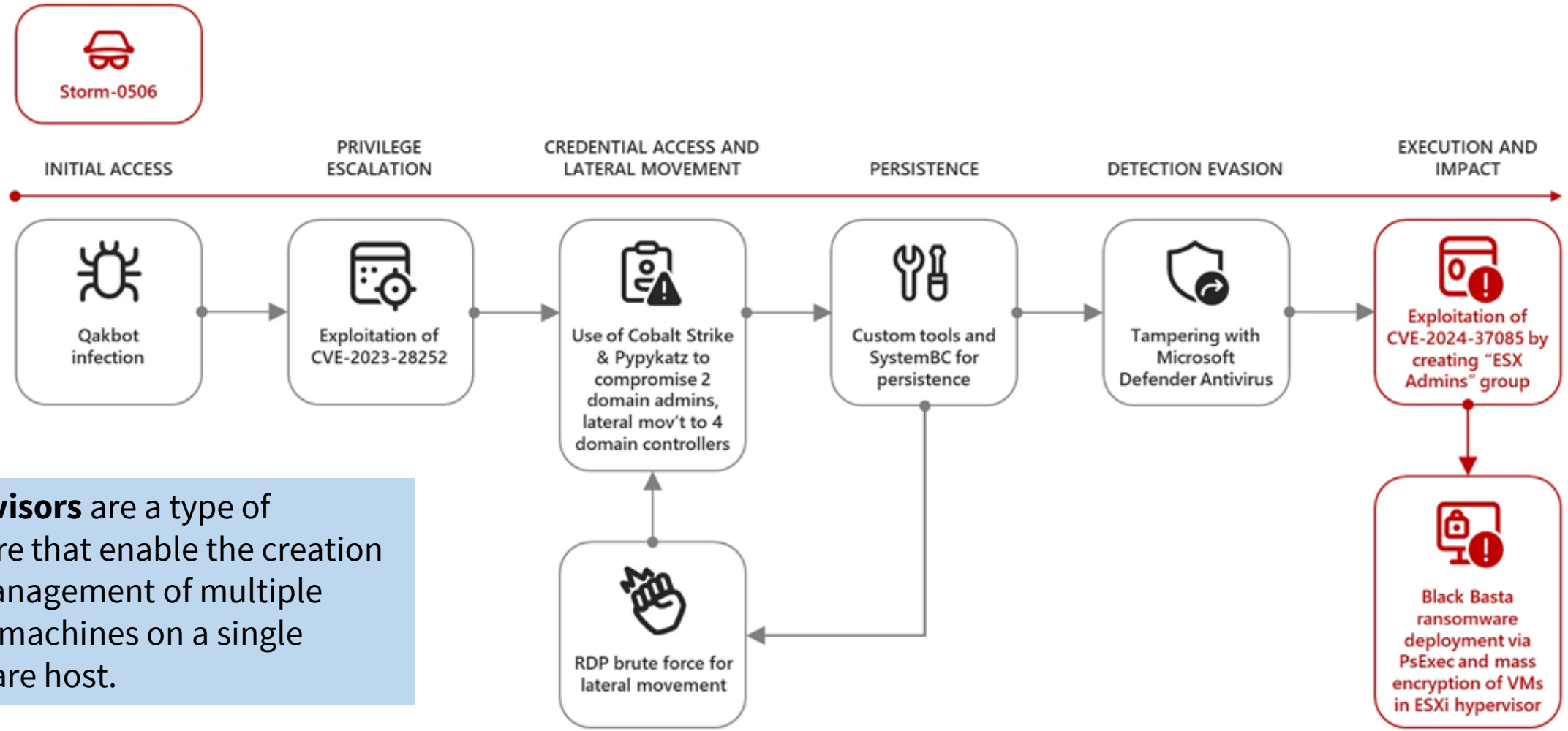
Chinese APT *Volt Typhoon* Exploiting Versa Zero-Day

- Active Zero-Day Exploitation
- Attributed to Volt Typhoon
- Targeting: ISPs/MSPs

…with the goal of accessing their customers



Ransomware Operators Exploit ESXi Hypervisor Vulnerability for Mass Encryption (Microsoft, E-ISAC)



Hypervisors are a type of software that enable the creation and management of multiple virtual machines on a single hardware host.

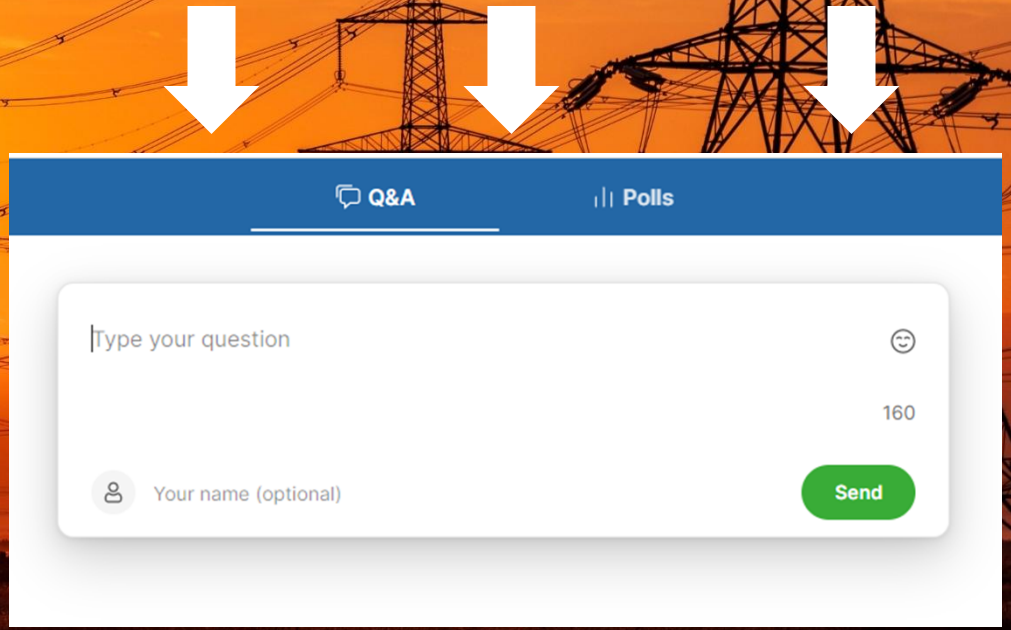
Texas RE Fall Standards, Security, & Reliability Workshop

AGENDA

- Kick-off and Instructions
- Executive Welcome
- CISA Update
- NIST Cybersecurity Framework
- Threat Briefing
- Lonestar Infrastructure Protection Act
- Physical Security
- ITCS
- Large Loads in the Texas Interconnection
- Root Cause Analysis and Cause Codes
- 2025 CMEP IP
- Common and High Risk Violations

Return at 10:55 a.m.

To submit questions during the workshop, please visit **slido.com** and enter today's participant code: **TXRE**



Texas Reliability Entity's Fall Standards, Security, and Reliability Workshop

Lone Star Infrastructure Protection Act

Chad Seely
ERCOT Senior Vice President, General Counsel and Corporate Secretary

November 20, 2024

What is the Lone Star Infrastructure Protection Act (LSIPA)?

- Lone Star Infrastructure Protection Act
  - State of Texas regulations regarding access to and security of critical infrastructure
- Originally adopted June 18, 2021
  - 87th Legislature via SB 2116
- Amended June 9, 2023
  - 88th Legislature via SB 2013

SB 2116 (87th Regular Session, effective June 18, 2021)

- SB 2116 amended Chapter 117, Title 5, Business and Commerce Code
  - Prohibits Texas businesses from **entering into agreements** relating to critical infrastructure with a company:
    - If the company would be **granted direct or remote access to or control of "critical infrastructure"** in Texas
      - **"Critical infrastructure" includes an "electric grid"**
      - Does not apply to access specifically allowed for product warranty and support purposes
    - And if it is known that the company is either:
      - **Owned by or the majority of stock or other ownership interest is held or controlled by**:
        - Citizens of, or directly controlled by the government of, **China, Iran, North Korea, Russia**, or a designated country, or
        - A company or other entity owned or controlled by citizens of or is directly controlled by the government of **China, Iran, North Korea, Russia**, or a designated country
      - Or headquartered in **China, Iran, North Korea, Russia**, or a designated country
  - Designated Country:
    - A country designated by the governor as a threat to critical infrastructure (See Section 117.003)
    - There are currently no additional designated countries
  - Applies only to a contract or agreement entered into, on or after the effective date of the LSIPA

ERCOT Rules/Procedures Adopted to Meet Requirements Under SB 2116

- ERCOT Requests for Information (RFIs) sent to Interconnecting Entities (December 2021)
  - **RFIs** sent to all Entities that had a proposed Resource **project seeking to interconnect with ERCOT**
  - RFIs asked Entities questions regarding citizenship, ownership, and headquarters
  - RFIs were sent to take **immediate action** regarding the LSIPA while rulemaking (Planning Guide Revision Request (PGRR) 99) was underway for ERCOT Planning Guide
- PGRR 99 (April 2022)
  - PGRR 99 incorporated similar questions to RFI into a **permanent attestation form** in ERCOT's Planning Guide (Planning Guide Section 8, Attachment D)
  - **Required new projects seeking interconnection to submit an attestation** (Planning Guide Section 5.2.2)
- Nodal Protocol Revision Request (NPRR) 1155 (June 2023)
  - While PGRR 99 adopted rules applicable to proposed Resources seeking to interconnect with ERCOT in the future, **NPRR 1155 established LSIPA rules for Market Participant registration**
  - Required all Market Participants to submit an **attestation** reflecting compliance with LSIPA rules on **MP citizenship, ownership, and headquarters**

Cybersecurity Impacts – Procurement/Contracting Policies for Vendors

- Supply Chain
  - Required Suppliers to identify ties to China, Iran, North Korea, Russia, or a designated country, consistent with LSIPA criteria
  - Added the following question to ERCOT Supplier Questionnaire:

ERCOT Question	Explanation of risk we are seeking to identify (Risks that impact ERCOT's Bulk Electric System, Cyber Systems and their associated Electronic Access Control or Monitoring Systems, and Physical Access Control Systems)
Is the supplier, or its parent company, or any affiliate of the supplier or its parent company majority owned or controlled by individuals who are citizens of China, Iran, North Korea, Russia, or other country prohibited under law?	ERCOT seeks to confirm that no suppliers or their parent companies or affiliates are majority owned or controlled by citizens of any country designated under the Office of Foreign Assets Control (OFAC) or Lone Star Infrastructure Protection Act (LSIPA).

- Legal
  - Updated ERCOT standard form agreements to contain language requiring third-party service providers to represent, warrant, agree, and certify compliance with such LSIPA terms
    - *Contractor represents, warrants, agrees, and certifies that it is not owned by, nor is the majority of stock or other ownership interest of the company is held or controlled by (a) individuals who are citizens of China, Iran, North Korea, Russia, or other country prohibited under law or (b) a company or other entity, including a governmental entity, that is owned or controlled by citizens of or is directly controlled by the government of China, Iran, North Korea, Russia, or other country prohibited under law. Contractor further represents, warrants, agrees, and certifies that it is not headquartered in China, Iran, North Korea, Russia, or other country prohibited under law. If Contractor's ownership or management structure changes in a way that would make it ineligible to maintain compliance with the Lone Star Infrastructure Protection Act, it will promptly notify ERCOT of the change.*

SB 2013 (88th Regular Session, effective June 9, 2023)

- SB 2013 amended Section 39.360, Subchapter H, Chapter 39, Utilities Code
  - An Independent System Operator (ISO) **may not register or maintain the registration** of a business entity operating in the power region **unless the business entity attests that they comply with the LSIPA**
  - As a condition of registration, **Market Participants must report to the ISO the purchase of any *critical electric grid equipment* or *service* from a company described by the LSIPA**
  - For each reported purchase, **Market Participants must submit an attestation that the purchase will not result in access to or control of its critical electric grid equipment** by a company described by the LSIPA
  - ISO **may immediately suspend or terminate a company's registration or access to any ISO systems** if the ISO has reasonable suspicion that the company meets any of the criteria described by the LSIPA
  - **ISO may adopt guidelines or procedures** relating to the requirements in this section, including the qualification of electric grid equipment or services as critical
  - The Texas Attorney General may conduct **periodic audits** of LSIPA attestations for CEGE/CEGS

ERCOT Rules/Procedures Adopted to Meet Requirements Under SB 2013

- NPRR 1155 (June 2023)
  - Because NPRR1155 was adopted during SB 2013's passage, **no new rules were needed** to comply with SB2013's requirements regarding Market Participant (MP) registration
- NPRR 1199 (May 2024)
  - Addressed new requirements in SB 2013 regarding MP reporting on the purchase of "critical electric grid equipment services"
    - **Created definitions for Critical Electric Grid Equipment (CEGE) and Critical Electric Grid Services (CEGS)**
    - **Adopted procedures and created standard reporting form for CEGE/CEGS reporting**
- ERCOT Registration Policies
  - ERCOT purchased **software providing reports** on a MP's corporate family tree
  - ERCOT is implementing procedures for **pulling random samples** of existing and new MPs on a regular basis to run and analyze corporate family tree reports
  - **RFIs** sent to MPs **when questions arise** regarding their attestation
- ERCOT's Employment Policies
  - Reviewed and modified ERCOT hiring and contracting processes to identify relevant ERCOT employee and contractor positions that are deemed "critical to the security of the grid"
  - No other changes needed to existing employee/contractor background check policies due to current requirements

Definition of “Critical Electric Grid Equipment (CEGE)”

Critical Electric Grid Equipment (CEGE)

(1) Equipment accessible by means of **routable connectivity** that, as installed, **can be used to gain remote access to or control of ERCOT System Infrastructure, the ERCOT Wide Area Network (WAN), or Market Information System (MIS),** if such equipment, if destroyed, degraded, misused, or otherwise rendered unavailable would, **within 15 minutes or less** of its mis-operation, non-operation, or required operation, **adversely impact the reliable operation of ERCOT System Infrastructure**. Redundancy of affected facilities, systems, and equipment shall not be considered when determining adverse impact.

(2) **For Load Resources**, this definition only applies to **equipment used to send and receive ERCOT telemetry and ERCOT Dispatch Instructions.**

(3) For purposes of this definition, **“reliable operation of ERCOT System Infrastructure**” **means** operating elements of ERCOT System Infrastructure within equipment and electric system thermal, voltage, and stability limits so that instability, uncontrolled separation, or cascading failures of ERCOT System Infrastructure will not occur as a result of a sudden disturbance, including a cybersecurity incident, or unanticipated failure of system elements.

Definition of “Critical Electric Grid Services (CEGS)”

Critical Electric Grid Services (CEGS)

Services and software **provided by a vendor** for the **operation, control, monitoring, maintenance, or use** of Critical Electric Grid Equipment (CEGE), **excluding access specifically allowed by the purchaser for product warranty or support purposes**.

CEGE/CEGS – Reporting Deadlines for New and Past Purchases

- **New purchases of CEGE or CEGS** from a LSIPA Designated Company
  - Reports and attestations shall be submitted **within 180 days** of the date of purchase

- **Past purchases of CEGE or CEGS** must be reported by new and existing MPs
  - **New entities applying for registration as an MP** with ERCOT must report purchase(s) made within the 5 years preceding their registration;
  - **Existing MPs** must report past purchases as follows:

Purchase(s) Made	Report and Attestation Deadline
After June 18, 2021	October 28, 2024
Between June 8, 2018, thru June 18, 2021	December 15, 2024

CEGE/CEGS – Questions on the Report and Attestation (Form S)

- Section 23 Form S: Reporting and Attestation Regarding Purchase of Critical Electric Grid Equipment (CEGE) and Critical Electric Grid Services (CEGS) from a Lone Star Infrastructure Protection Act (LSIPA) Designated Company or LSIPA Designated Country
  - **Question 1:**
    - Did the Applicant/MP purchase CEGE or CEGS from a LSIPA Designated Company/Country?
  - **Question 2:**
    - List each purchase (type of equipment; date of purchase; seller; LSIPA country).
  - **Question 3:**
    - **Attest** whether or not the purchase **WILL or WILL NOT result in access to or control of CEGE** by an LSIPA Designated Company/Country.
  - **Question 4:**
    - **If purchase WILL** result in access to or control of CEGE by an LSIPA Designated Company/Country, then **describe the access or control and list any actions the MP has taken to mitigate the risks** associated with such access or control.

Sample Data from CEGE Reports

- ERCOT received approximately 1,000 CEGE reports for the October 28th CEGE reporting deadline
- From a sampling of 33 reports – 7 of the 33 reported CEGE – all CEGE purchases were from China

CEGE Reported
Cellular Modems
Computer Servers
GMS Workstation
SCADA Workstation
Battery Management System
Local Controller
Converter
Power Conversion System
Main Power Transformer
Computer/Laptops

Mitigating Efforts
Examples of mitigating efforts included: • Firewalls • Multi-factor Authentication • Limited/Restricted Remote Access

WECC

Physical Security Best Practices for Low Impact Facilities

November 20, 2024

Brady Phelps, CPP, PCI, PSP
EM Physical Security Lead

Agenda

- Introduction to Low Impact
- WECC's Monitoring Approach
  - Methodologies and Criteria for Assessing Compliance
- Preparing for a Monitoring Engagement: Expectation vs. Reality
- Holistic Security Principles
- Developing Comprehensive Security Plans
- Importance of a Proactive and Adaptive Security Strategy
- Common Monitoring Findings: Challenges and Gaps
- Best Practices Derived from Monitoring Experiences
- Risk Ranking Programs

Introduction to Low Impact

NERC CIP-003-8 R2 Attachment 1, Section 2:

- Establishes the requirement for a documented cybersecurity plan that addresses the physical security of the Bulk Electric System's cyber assets critical to its reliability.

WECC's Monitoring Approach

NERC CIP-003-8 R2 Attachment 1, Section 2

Part I

- WECC's monitoring approach ensures that the security objective of physically securing low impact BES assets is achieved by thoroughly reviewing documented evidence that outlines the criteria for need-based access control. This is complemented by on-site inspections to verify the effective implementation of these controls, as required by the standard.

WECC's Monitoring Approach

NERC CIP-003-8 R2 Attachment 1, Section 2

Part II

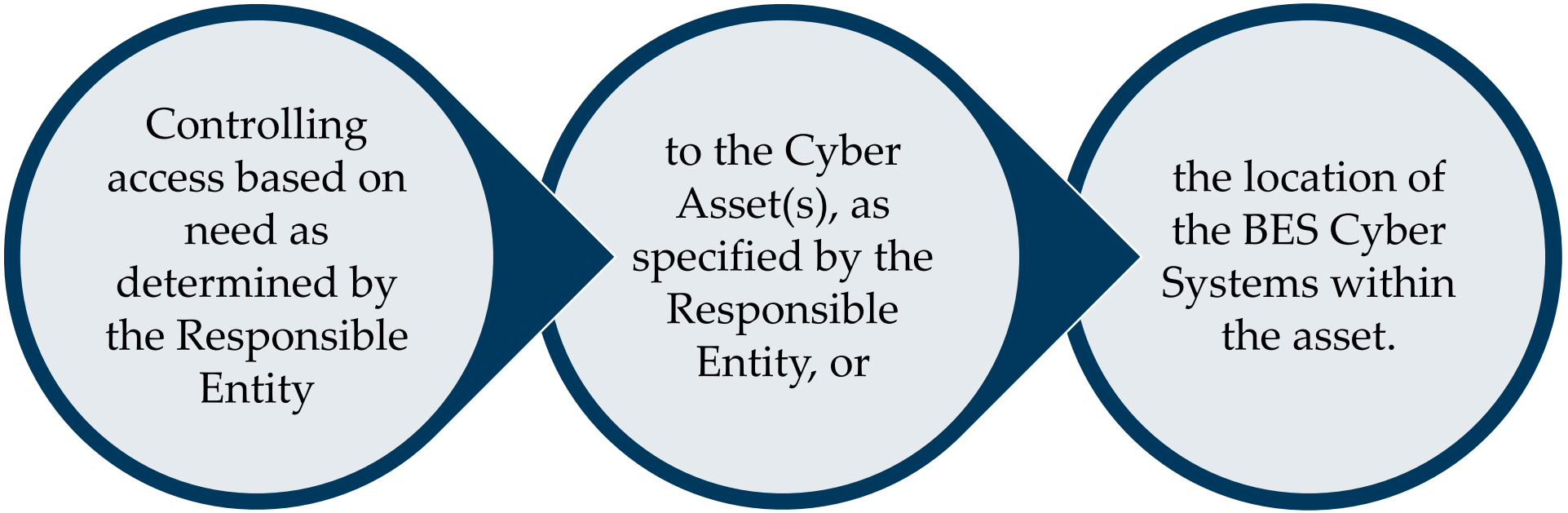
- WECC will evaluate the documented evidence and implementation of controls against industry best practices through a risk review. The findings from this review will be provided to WECC's Oversight Planning team to inform future Compliance Oversight Plans (COP).

WECC's Monitoring Approach

NERC CIP-003-8 R2 Attachment 1, Section 2

- Each Responsible Entity with at least one asset identified in CIP-002 containing low impact BES Cyber Systems shall implement one or more documented cybersecurity plan(s) for its low impact BES Cyber Systems that include the sections in Attachment 1.
- Physical Security Controls: Each Responsible Entity shall control physical access, based on need as determined by the Responsible Entity, to (1) the asset or the locations of the low impact BES Cyber Systems within the asset, and (2) the Cyber Asset(s), as specified by the Responsible Entity, that provide electronic access control(s) implemented for Section 3.1, if any.

WECC's Monitoring Approach



How do you effectively prepare for a monitoring engagement?

WECC's Monitoring Approach

Review of Documented Cybersecurity Plans

- Existence of Plans: Verify that the Responsible Entity has documented cybersecurity plans in place specifically for low impact BES Cyber Systems.
- Inclusion of Required Sections: Ensure that the cybersecurity plans include all required sections outlined in Attachment 1, particularly the Physical Security Controls.
- Plan Adequacy: Assess whether the documented plans are sufficiently detailed, outlining the physical security measures and access controls relevant to the identified assets.

WECC's Monitoring Approach

Assessment of Physical Security Controls

- Need-based Access: Evaluate whether the entity has implemented access controls that are based on a legitimate need, as determined by the Responsible Entity. This involves checking whether access to the locations of the low impact BES Cyber Systems and associated Cyber Assets is restricted appropriately.
- Access Control Mechanisms: Inspect the physical and electronic mechanisms in place (e.g., locks, keycards, biometric systems) to control access to critical areas and ensure they align with the documented security plan.

WECC's Monitoring Approach

Verification of Implementation

- On-site Inspection: Conduct on-site inspections to verify that the physical security controls described in the documented plans are implemented and operational.
- Access Logs and Records: Review access logs, security records, and other documentation to confirm that access controls are enforced consistently and that any breaches or exceptions are properly documented and addressed.

WECC's Monitoring Approach

Evaluation of Need Determination

- Process for Determining Access Need: Examine the process used by the Responsible Entity to determine who needs access to specific assets. Ensure that this process is documented, consistent, and aligned with the organization's security policies.
- Periodic Review: Check whether there is a process for regularly reviewing and updating access needs and controls, ensuring they remain appropriate as organizational needs and threat landscapes evolve.

WECC's Monitoring Approach

NERC CIP-003-8 R2 Attachment 1, Section 2

Verification of Implementation:

Did you achieve the Security Objective of CIP-003-8?

WECC's Monitoring Approach

NERC CIP-003-8 R2 Attachment 1, Section 2

- Did you properly document a need-based access program and security controls?
  - Does this documentation clearly identify whether the controls are to the asset or location of the asset?
  - Does the documentation clearly outline the controls being used?
- Did the site tours demonstrate an effective and reliable access control method of;
  - Barriers?
  - Locks?
  - Keys and key management (if used)?

Preparing for Monitoring: Expectations vs. Reality

Expectation:
Adversarial Audit

Entities often anticipate a confrontational audit process.

Reality:
Collaborative and Educational

Audits are professional, organized, and purpose-driven, focusing on sharing best practices, education, and outreach.

Preparing for Monitoring: Expectations vs. Reality

Expectation:
Strictly Formal Procedures

There's an assumption audits strictly follow formal procedures without flexibility.

Reality:
Dynamic Interaction

In addition to offsite reviews, on-site audits include impromptu interviews or "walk-and-talks," and real-time testing of security measures, offering a more comprehensive and engaging evaluation.

Preparing for Monitoring: Expectations vs. Reality

Expectation:
Sole Focus on Compliance

Entities might expect auditors to solely focus on compliance checklists.

Reality:
Holistic Approach

While compliance is key, auditors also assess the effectiveness of implemented security measures, ensuring entities are not just compliant but also effectively secured against threats.

Holistic Security Principles

Observation:

- Holistic physical security principles, in the context of compliance with NERC CIP physical security Standards, encompass a broad and integrated approach to ensuring the physical security of the BES. These principles are designed to not only meet specific regulatory requirements but also to promote a comprehensive, adaptive, and resilient security posture that protects against physical threats and vulnerabilities.

Holistic Security Principles

Integrated Security Framework

Low Impact	Holistic Principle
Emphasizes the importance of managing security as an integral part of the org's broader security framework. This includes identifying and documenting physical risks to BES Cyber Systems and applying appropriate security controls.	Ensures that physical security measures are not siloed but integrated into the overall security and risk management framework of the org, promoting a unified approach to protecting critical infrastructure.

Developing Comprehensive Security Plans

Risk Assessment

- Threat Identification: Identifying potential threats to the organization.
- Vulnerability Assessment: Evaluating the vulnerabilities of the organization's assets.
- Risk Analysis: Determining the likelihood and impact of identified threats.

Developing Comprehensive Security Plans

Security Objectives

- Goals: Defining what the organization aims to achieve with its physical security measures.
- Prioritization: Determining which assets are most critical and require the highest level of protection.

Developing Comprehensive Security Plans

Real-world Example

- Prioritization: Determining which assets are most critical and require the highest level of protection.

Developing Comprehensive Security Plans

Prioritization

Questions about your facility:

- Facility necessary for crank path, black start, or capability essential to restoring regional electricity service?
- Primary source of electrical service to a military installation?
- Installations necessary for the provision of regional drinking water supplies and wastewater services?

Developing Comprehensive Security Plans

Prioritization

Questions about your facility:

- Serve a regional public safety establishment?
- Serve a major transportation facility?
- Serve as a Level 1 Trauma Center?
- Serve over 60,000 meters?

Developing Comprehensive Security Plans

Security Policies and Procedures

- **Access Control:** Policies on who can access certain areas and how access is granted.
- **Incident Response:** Procedures for responding to security breaches or threats.
- **Monitoring and Surveillance:** Guidelines for using technologies like cameras and alarms.

Developing Comprehensive Security Plans

Security Measures and Technologies

- **Physical Barriers:** Use of locks, fences, gates, and barriers to secure premises.
- **Surveillance Systems:** Implementation of CCTV, alarm systems, and intrusion detection.
- **Access Control Systems:** Technologies such as keycards, biometric scanners, and visitor management systems.

Developing Comprehensive Security Plans

Response and Recovery Plans

- **Threat Response:** Step-by-step actions to take in the event of a security incident.
- **Business Continuity:** Strategies to maintain operations during and after a security event.
- **Post-incident Review:** Procedures for assessing the effectiveness of the response and making necessary adjustments.

Developing Comprehensive Security Plans

Training and Awareness

- **Employee Training:** Regular training on security procedures and threat response.
- **Awareness Programs:** Initiatives to keep security top-of-mind for all personnel.

Developing Comprehensive Security Plans

Documentation and Reporting

- **Security Audits**: Regular review and documentation of security measures and their effectiveness.
- **Incident Reports**: Detailed records of any security breaches and responses.

Proactive & Adaptive Strategies

Anticipate Emerging Threats

Proactively adapting security strategies under LI standards ensures that entities can anticipate and prepare for emerging threats, rather than react to incidents after they occur.

Enhance Security Posture

A proactive and adaptive approach allows continuous improvement in posture, using the latest technologies and best practices to protect cyber assets from threats, ensuring that security measures are current.

Compliance & Resilience

Adapting to shifts in regulatory requirements and threat landscapes is essential not only for compliance but also for building resilience against disruptions to the BES.

Real-world Findings and Lessons Learned

Common Monitoring Findings: Challenges & Gaps

- Entities often provide vague policies, such as stating they “will grant access based on need” without detailing the underlying process.
  - Insufficient detail leaves access procedures unclear, leading to potential inconsistency and misinterpretation.
  - Document the full access request process within the security plan.
  - Applying these best practices helps close documentation gaps, clarify access protocols, and strengthen CIP-003 R2 compliance.

Real-world Findings and Lessons Learned

Common Monitoring Findings: Challenges & Gaps

- Entities often lack comprehensive access management plans, specifically in the management of physical keys.
  - Reliance on traditional hard keys and padlocks without a detailed key management plan leaves low impact assets vulnerable and security measures unenforceable.
  - Follow best practices under Key Management strategies (listed in notes).

Real-world Findings and Lessons Learned

Real-world Example:

- Two types of access control: Physical Access Control Systems (PACS) and hard keys

Real-world Findings and Lessons Learned

Common Monitoring Findings: Challenges & Gaps

- Entities often fail to test site protections adequately before WECC monitoring team visits.
  - Oversights in alarms, perimeter security, or procedural adherence are frequently uncovered during effectiveness testing by the monitoring team, which could have been preemptively identified and rectified.

Takeaways

- Balancing Compliance and Security:
  - Minimal compliance with NERC CIP-003-8 may be sufficient, but a comprehensive physical security plan is preferable for robust protection and reduced risk.
- Importance of a Comprehensive Physical Security Plan:
  - A full plan should include risk assessments, security objectives, policies, procedures, response plans, and training, not just a list of controls.
- Risk-based Monitoring Approach:
  - Entities with only minimal controls may be considered higher risk, requiring more scrutiny during audits compared to those with comprehensive security plans.
- Monitoring Expectations:
  - WECC's audit approach will review both documented evidence and on-site implementation of physical security controls to ensure compliance and security effectiveness.
- Informing Future Risk Management:
  - Results from audits and risk reviews will feed into WECC's Risk Department, guiding future Compliance Oversight Plans (COPs) and enhancing overall security strategies.

WECC

Electric Reliability and Security for the West

www.wecc.org

Interregional Transfer Capability Study

Mark Henry
Chief Engineer & Director, Reliability Outreach

ITCS Objectives

Congress directed NERC to perform an Interregional Transfer Capability Study (ITCS) in the Fiscal Responsibility Act of 2023. ITCS aligns with ERO's obligations to perform reliability assessments.

- Independent and objective
- System-wide perspective
- Reliability focus
- Collaboration and coordination
- Strategic planning
- Repeatable process

ITCS Scope: Fiscal Responsibility Act of 2023

Part I: Calculate current total transfer capability

Part II: Recommend prudent additions to transfer capability

Part III: Recommend how to meet and maintain transfer capability

ITCS Timeline Overview

Fiscal Responsibility Act of 2023
June 3, 2023

Study Cases Prepared and Initial Actions Complete
January 31, 2024

2024/2025 Transfer Analysis Complete
August 2024

Recommendation for Prudent Additions Complete
October 2024

Parts II and III Report
October 2024

Final Report submitted to FERC
December 2, 2024

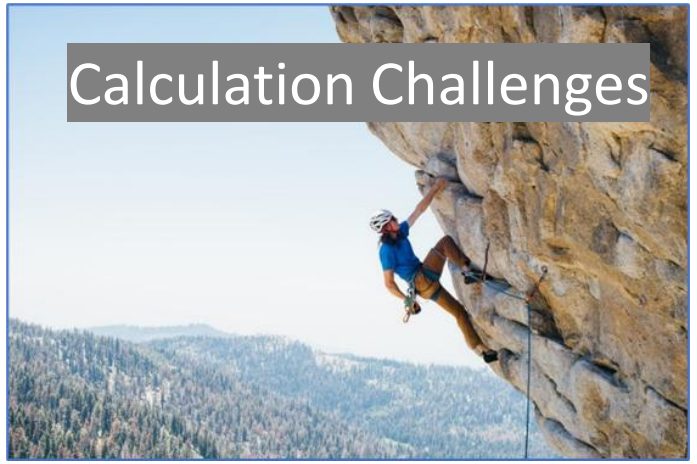
FERC Posts Report for Public Comments

FERC files its report to Congress

Canadian Analysis Q1 2025

Part I Transfer Analysis—Scope

- **Total Transfer Capability = Base Transfers + FCITC (First Contingency Incremental Transfer)**
- **Transfer Directions**
  - Non-simultaneous and simultaneous transfer analysis performed between the neighboring regions
  - Transfers into or between Canadian provinces will be included as part of the Canadian Analysis to be published in early 2025
- **Modeling of Transfer Participation**
  - Each transfer simulated until a valid thermal limit is reached
  - A voltage screening performed for each transfer direction at the FCITC limit



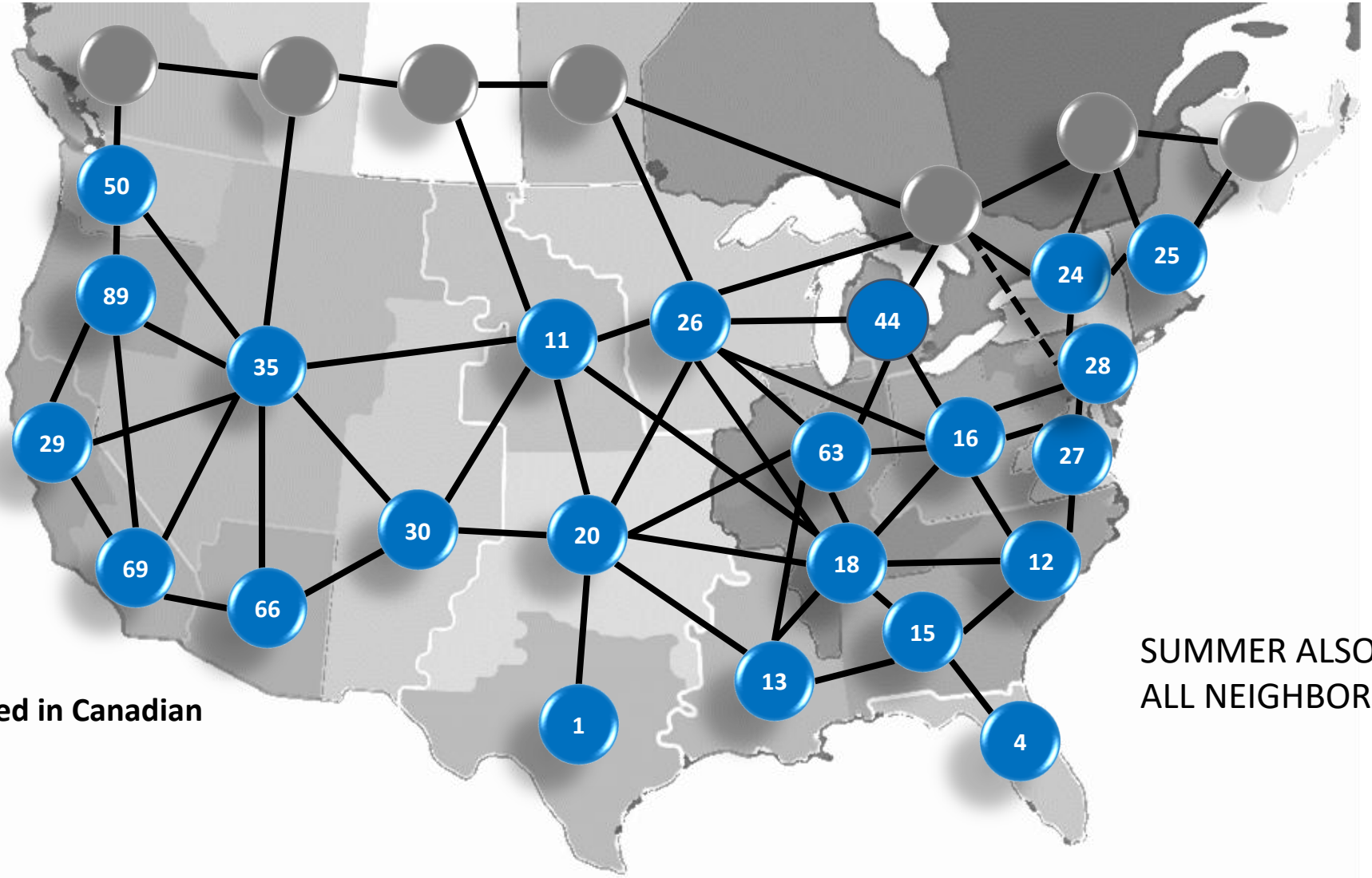
Congress required region-to-region transfer capability

Simultaneous import capability analysis required

Transfer capability is not always a single constant number

Enhancements needed to cases for future studies

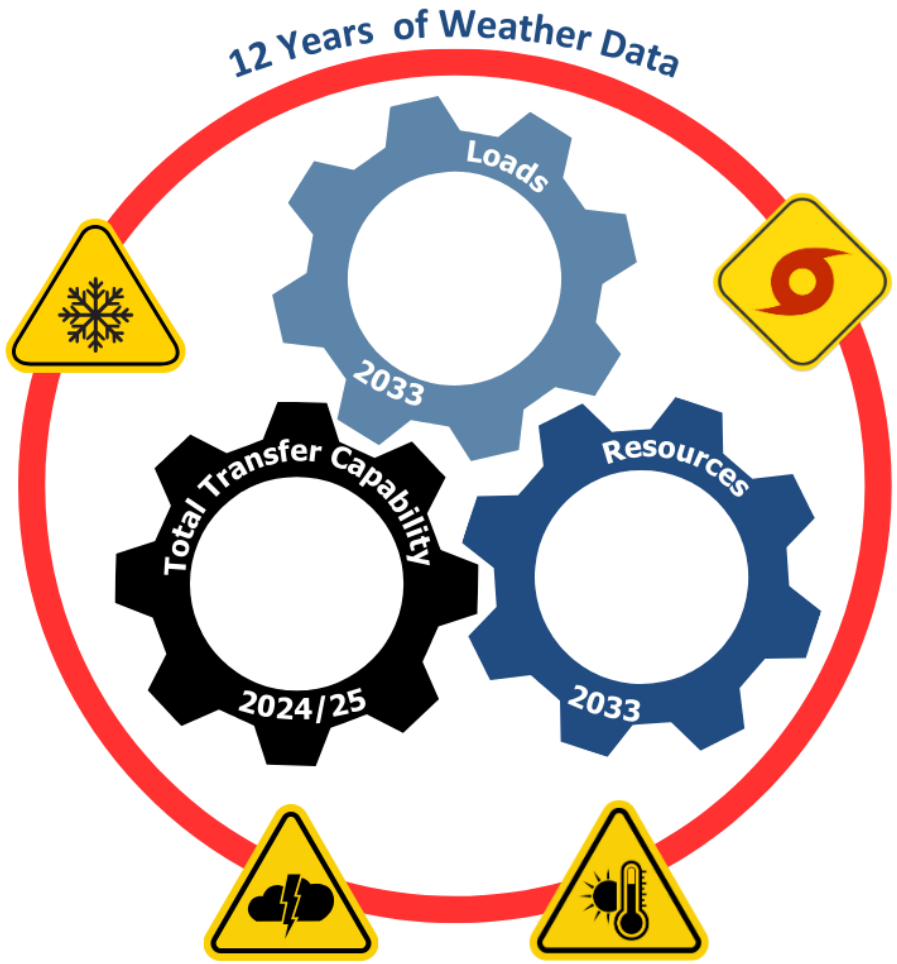
Part I Total Import Capabilities as Percentage of Peak Load (Winter)



To be evaluated in Canadian analysis

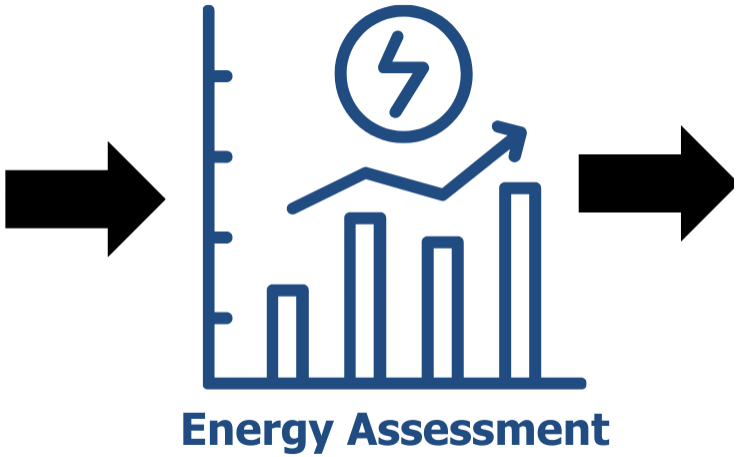
SUMMER ALSO CALCULATED – ALL NEIGHBORS LOWER

Part II Prudent Additions Study Approach



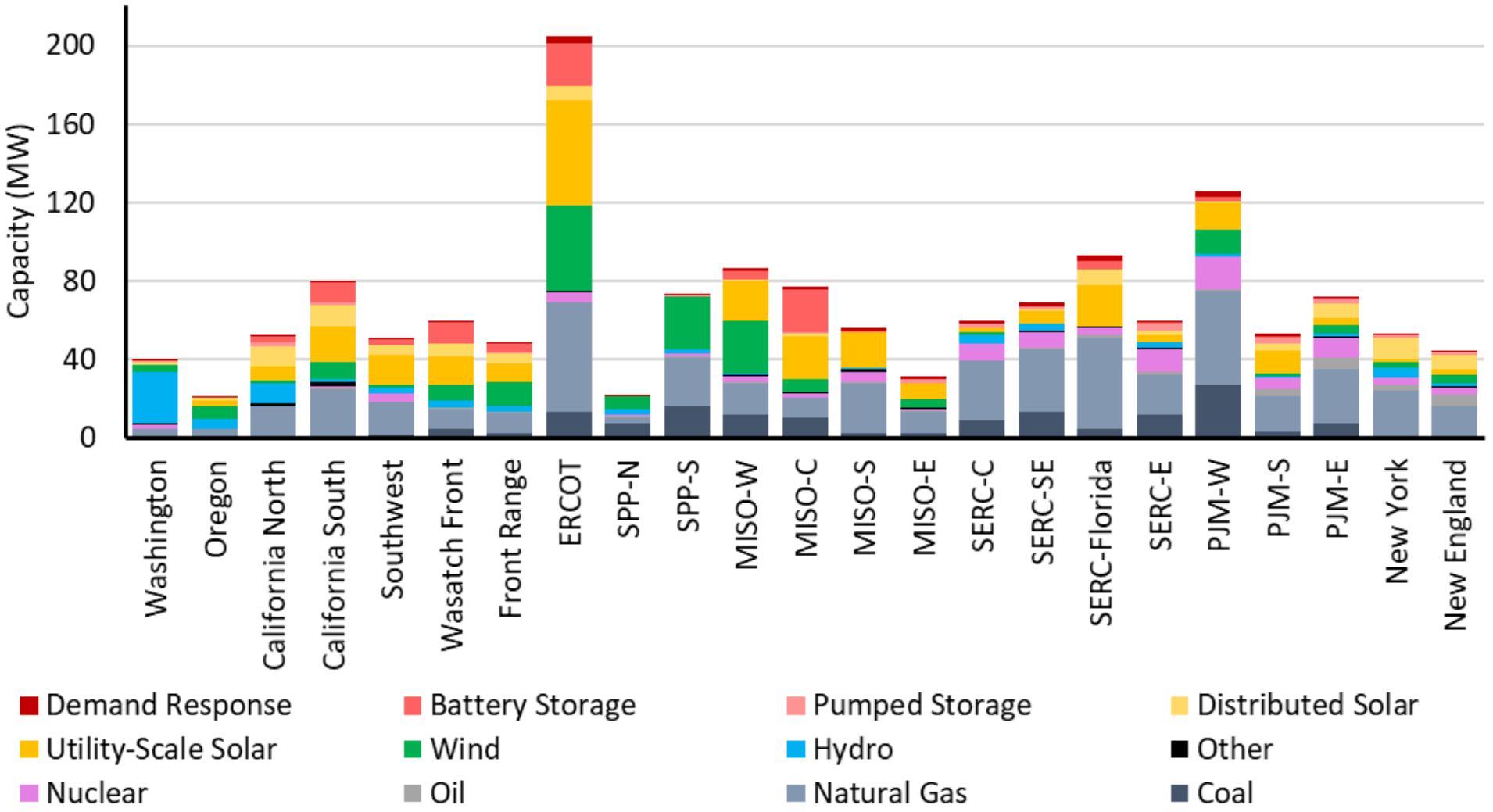
What are technically prudent additions to interregional transfer capability?

- *Strengthen reliability*
- *Serve load under extreme conditions*
- *Do not create other reliability problems*



Prudent Interregional Transfer Capability Additions

2033 Projected Resource Mix Used in ITCS



Energy Margin Methodology for Part II: Scope and Limitations

What this method DOES	What this method DOES NOT DO
✓ Prioritize regions for interregional transfer capability	× Represent actual physical power flows across the network … not a planning study
✓ Tracks daily and hourly availability of all resource types	× Track individual resource performance or replace a full energy assessment/LOLE study
✓ Calculates relative surplus and deficit in each region, at the same time	× Calculate relative costs or prices between regions
✓ Performs a reliability-only dispatch of resources	× Perform an economic, least-cost (production cost) dispatch
✓ Allows regions to import from one region while exporting to another	× Only evaluate “neighbor” flows
✓ Assumes full import capability from neighbors	× Evaluate potential import from non-adjacent planning areas (neighbor’s neighbor)
✓ Obtain results driven by extreme weather	× Consider probability of extreme conditions

Six-Step Prudent Addition Process

Identify

1. **Identify regions that are import constrained during Resource Deficiency hours (region is unable to keep its energy margin above 3%)**

Quantify

2. **Calculate maximum shortage (MW) during Resource Deficiency hours**

Prioritize

3. **Identify constrained interfaces during Tight Margin hours**
   Scarcity Factor Difference = measures relative resource surplus on the sending end (source) relative to the importing region (sink)

Allocate

4. **Increase all constrained interfaces at ~33% of max shortage (MW)**
   - Only increase by a portion of the max shortage to capture interactive effects between regions (increase in one interface affects flows across others)
   - Increase for each interface proportional to the scarcity factor difference
   - Interfaces with relatively high surplus on sending end available during tight margin hours get proportionally larger increase

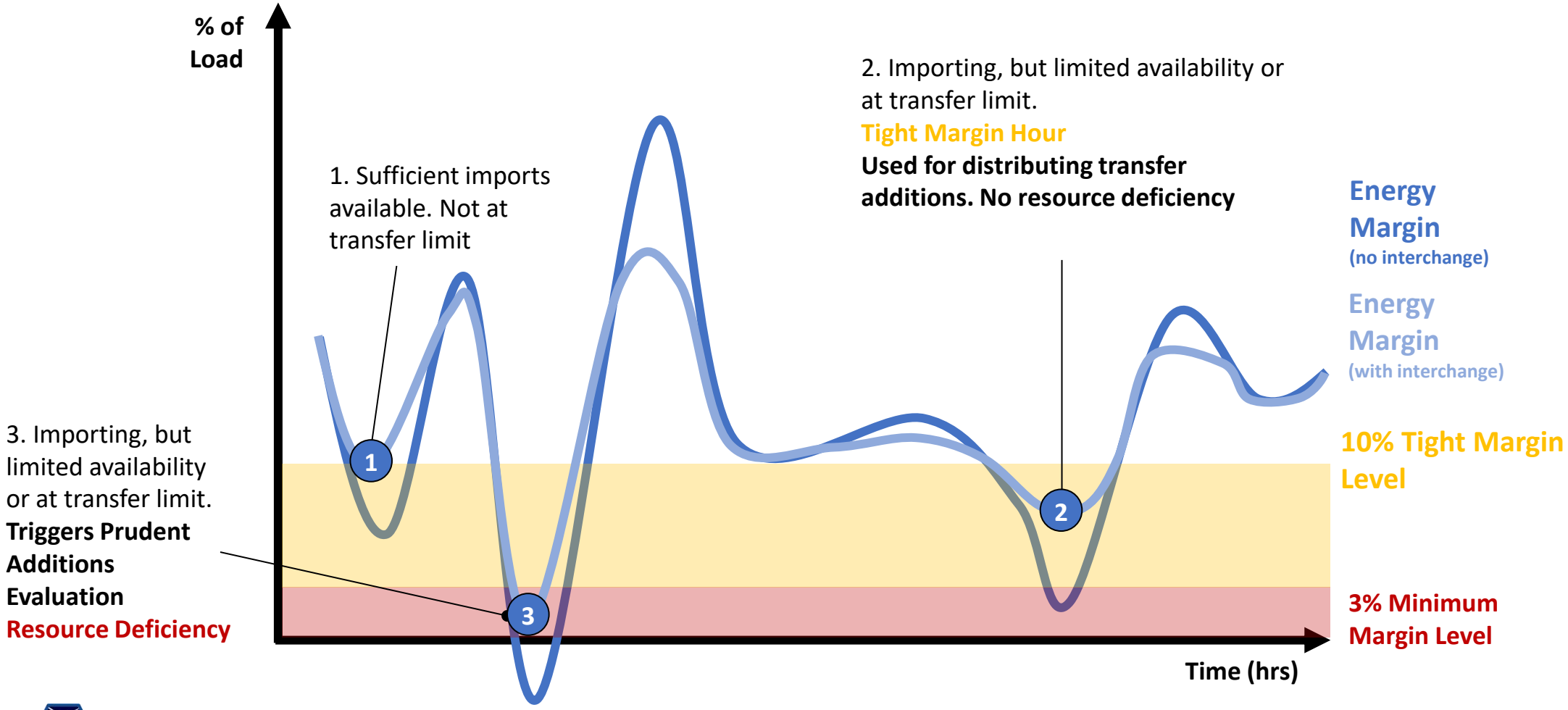
Iterate

5. **Iterate until all resource deficiencies are mitigated, or until improvement stops because there are no available resources on sending end**

Finalize

6. **Determine "prudent" level after all runs are complete based on resolving shortfalls**

Step 1: Identify Hours and Regions with Resource Deficiencies



Step 2: Quantify Maximum Deficiency

Max resource deficiencies by weather year, by region (2033)

Transmission Planning Region	WY2007	WY2008	WY2009	WY2010	WY2011	WY2012	WY2013	WY2019	WY2020	WY2021	WY2022	WY2023	Max Resource Deficiency
Washington	0	0	0	0	0	0	0	0	0	0	0	0	0
Oregon	0	0	0	0	0	0	0	0	0	0	0	0	0
California North	0	0	0	0	0	0	0	0	0	0	3,211	0	3,211
California South	0	0	0	0	0	0	0	0	0	0	0	0	0
Southwest	0	0	0	0	0	0	0	0	0	0	0	0	0
Wasatch Front	0	0	0	0	0	0	0	0	0	0	0	0	0
Front Range	0	0	0	0	0	0	0	0	0	0	0	0	0
ERCOT	1,361	0	0	9,400	0	0	0	8,977	14,853	18,926	14,321	12,108	18,926
SPP-N	0	0	0	0	0	0	0	0	0	155	0	0	155
SPP-S	0	0	0	0	0	0	0	0	0	4,137	0	0	4,137
MISO-W	0	0	0	0	0	0	0	0	0	0	0	0	0
MISO-C	0	0	0	0	0	0	0	0	0	0	0	0	0
MISO-S	0	0	560	0	629	0	0	0	0	0	0	0	629
MISO-E	0	0	0	0	1,676	0	0	0	5,715	979	0	0	5,715
SERC-C	0	0	0	0	0	0	0	0	0	0	0	0	0
SERC-SE	0	0	0	0	0	0	0	0	0	0	0	0	0
SERC-Florida	0	0	1,030	1,152	0	0	0	0	0	0	0	0	1,152
SERC-E	0	0	0	0	0	0	0	0	0	0	5,849	0	5,849
PJM-W	0	0	0	0	0	0	0	0	0	0	0	0	0
PJM-S	0	0	0	0	0	0	0	0	0	0	4,147	0	4,147
PJM-E	0	0	0	0	0	0	0	0	0	0	0	0	0
New York	0	81	0	3,244	1,748	2,631	1,229	0	0	0	0	3,729	3,729
New England	0	0	0	85	0	984	68	0	0	0	0	0	984

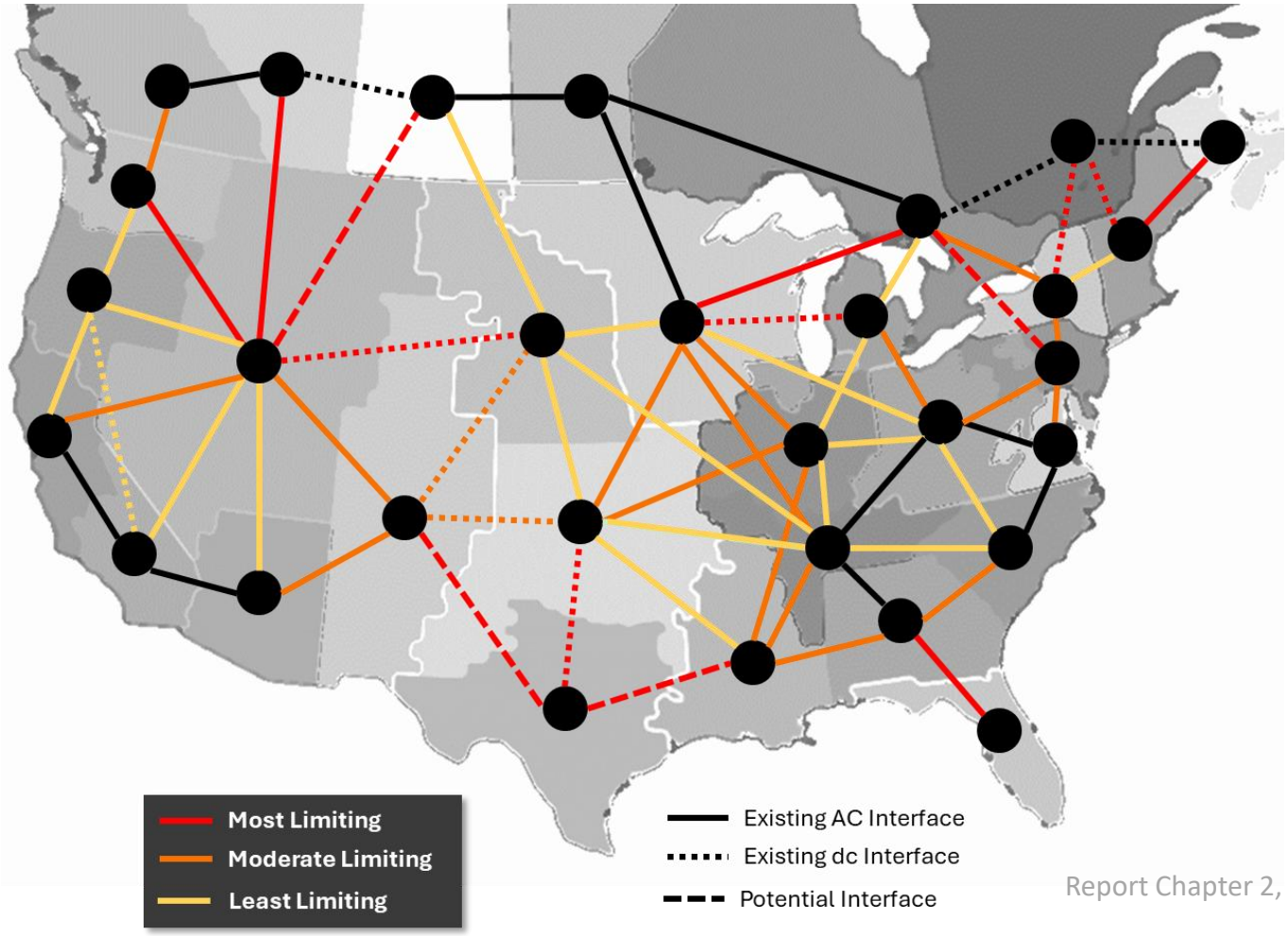
Report Chapter 3, Table 3.4

Summer Winter Dual Season

Step 3: Prioritize Constrained Interfaces for Additions

1. Identify lines importing into deficient regions
2. Consider interfaces that hit their limit during tight margin hours
3. Prioritize interfaces that have relatively more surplus on the sending end.

*Add to both the ac total import interface and dc-only interfaces



Report Chapter 2, Figure 2.6

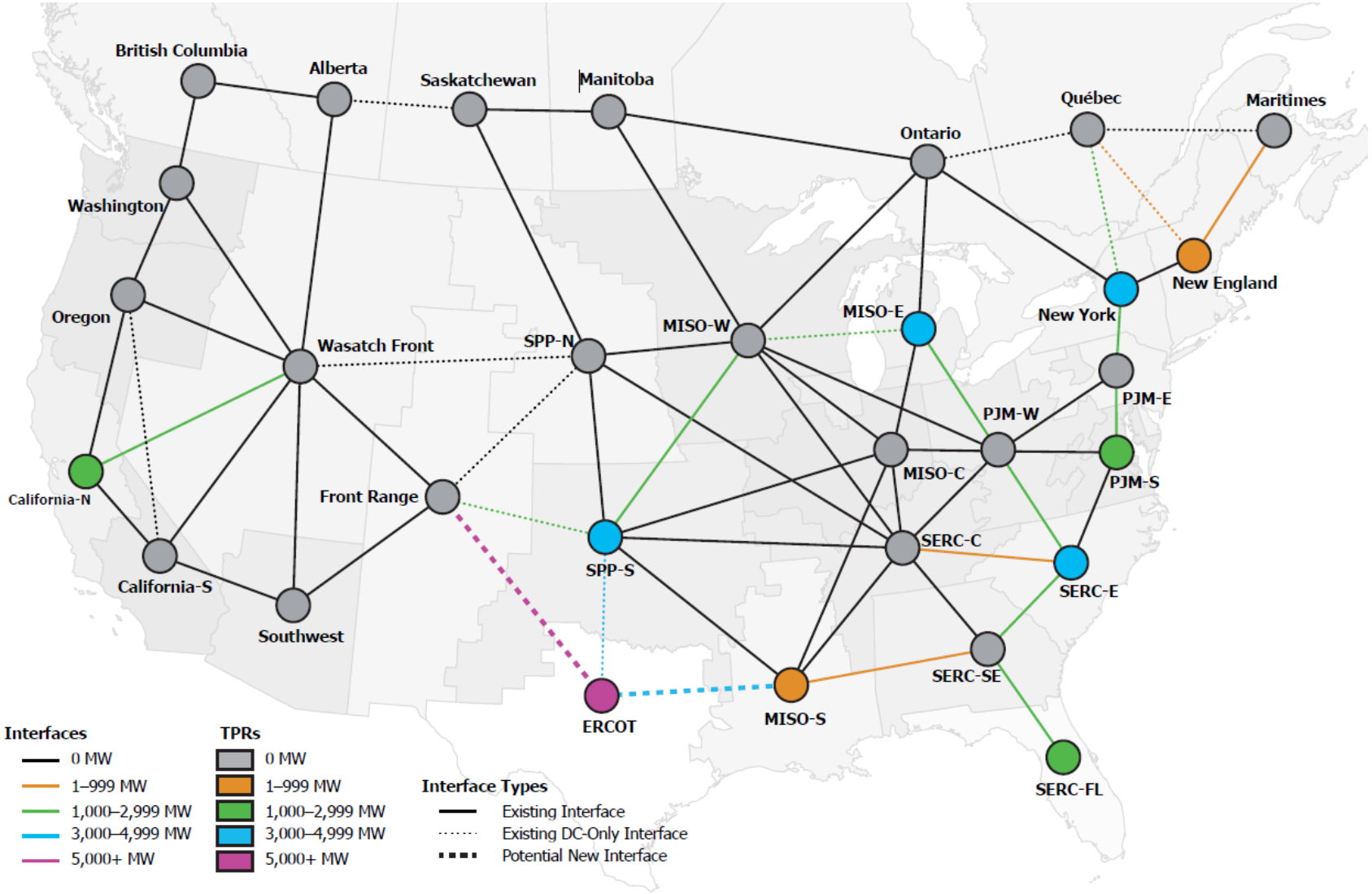
Steps 4 & 5: Allocate and Iterate Until Resource Deficiencies are Resolved

1. **Initial addition to transfer capability set to 33% of maximum resource deficiency**
2. **Allocate across priority interfaces and rerun the energy margin analysis**
3. **Recalculate remaining resource deficiency**
4. **Calculate the reduction in deficiency relative to the addition in transfer capability as a measure of efficacy**
5. **Iterate until all deficiencies are resolved or transfer capability stops helping**
   - Reduce maximum resource deficiency by at least 75% of additional transfer capability, or
   - Reduce resource deficiency by at least 100% of additional transfer capability in at least 4 hours

Why did we iterate?

- **Saturation effects.** As regions start to export more, their energy margins will go down and there will be less to export in the following iteration.
- **Multiplier effects.** Transmission and energy limited resources (Storage and DR) work together.
- **Interactive effects.** Flows between regions will change relative surplus and scarcity

Step 6: Finalize Prudent Addition Recommendations



Part 2 Deficiencies and Recommended Prudent Additions (Final)

Transmission Planning Region	Weather Years (WY) / Events	Resource Deficiency Hours	Maximum Deficiency (MW)	Additional Transfer Capability (MW)	Interface Additions (MW)
California North*	WY2022 Heat Wave	17	3,211	1,100	Wasatch Front (1,100)
ERCOT*	Winter Storm Uri (WY2021) and nine other events	135	18,926	14,100	Front Range (5,700) MISO-S (4,300) SPP-S (4,100)
SPP-S	Winter Storm Uri (WY2021)	34	4,137	3,700	Front Range (1,200) ERCOT (800) MISO-W (1,700)
MISO-E	WY2020 Heat Wave and two other events	58	5,715	3,000	MISO-W (2,000) PJM-W (1,000)
MISO-S	WY2009 and WY2011 summer events	4	629	600	ERCOT (300) SERC-SE (300)
SERC-E	Winter Storm Elliott (WY2022)	9	5,849	4,100	SERC-C (300) SERC-SE (2,200) PJM-W (1,600)
SERC-Florida	Summer WY2009 and Winter WY2010	6	1,152	1,200	SERC-SE (1,200)
PJM-S	Winter Storm Elliott (WY2022)	20	4,147	2,800	PJM-E (2,800)
New York	WY2023 Heat Wave and seven other events	52	3,729	3,700	PJM-E (1,800) Québec (1,900)
New England	WY2012 Heat Wave and two other events	5	984	700	Québec (400) Maritimes (300)
TOTAL				35,000	

*Not all deficiency hours were resolved in these events

Part III Scope: Meet and Maintain

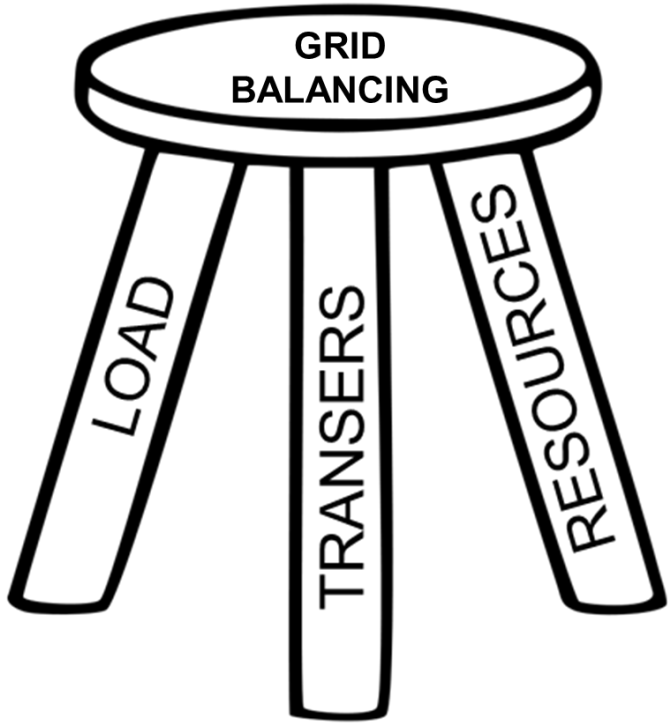
Mandate calls for “recommendations to meet and maintain total transfer capability together with such recommended prudent additions to total transfer capability...”

Report will describe *general* measures and actions needed to achieve and sustain the identified transfer capability and any recommended enhancements

- Additional Analysis
- Capital & Infrastructure
- Grid Enhancing Technologies
- Markets & Regulatory
- Resource Additions

Considerations When Reviewing the Report

- Wide-area energy margin assessment and scenario development called for consistency in assumptions and approach, rather than individual entity practices
- Extreme weather (especially Uri-like scenario) drives results; results do not consider probability of occurrence
- Transfers resolve all deficiencies below a 3% margin, rather than additional internal demand response or generation (beyond 2033 projections)
- Study does not consider costs or economic factors
- No specific transmission projects are identified, nor are implementation barriers addressed, technical, financial or regulatory. Full import capability is assumed



Interregional Transfer Capability Study (ITCS)

TEXAS RE
Ensuring electric reliability for Texans

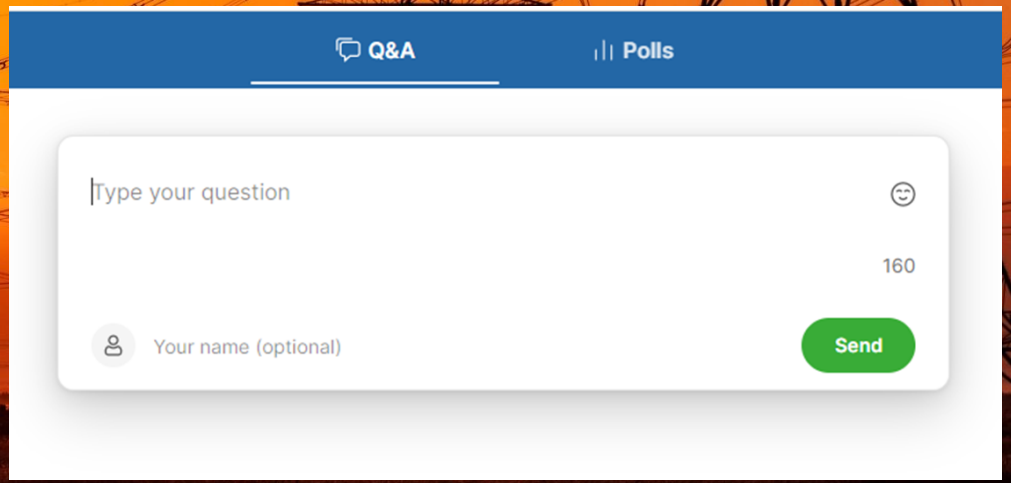
Texas RE Fall Standards, Security, & Reliability Workshop

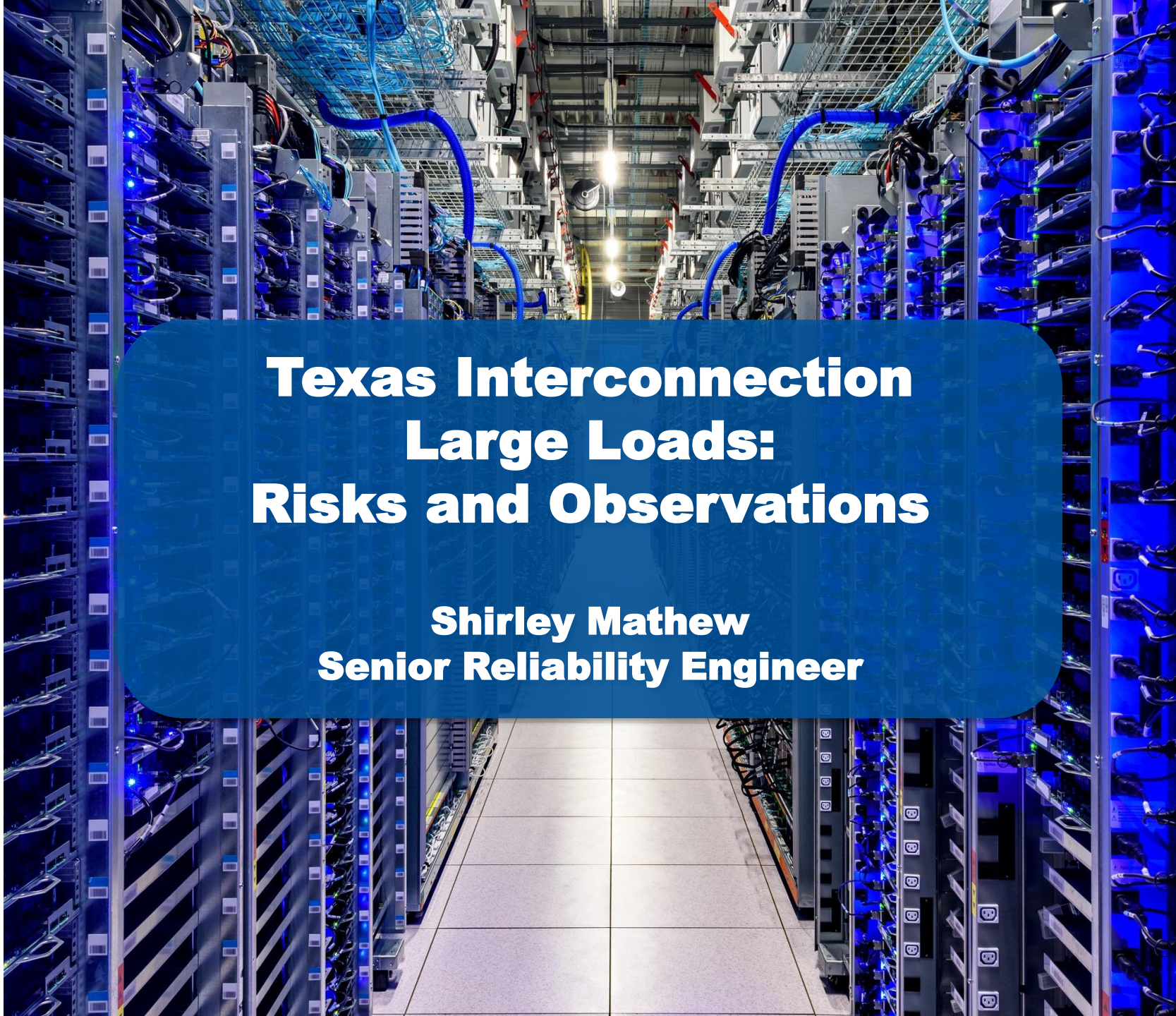
Return at 12:55 p.m.

AGENDA

- Kick-off and Instructions
- Executive Welcome
- CISA Update
- NIST Cybersecurity Framework
- Threat Briefing
- Lonestar Infrastructure Protection Act
- Physical Security
- ITCS
- Large Loads in the Texas Interconnection
- Root Cause Analysis and Cause Codes
- 2025 CMEP IP
- Common and High Risk Violations

To submit questions during the workshop, please visit **slido.com** and enter today's participant code: **TXRE**





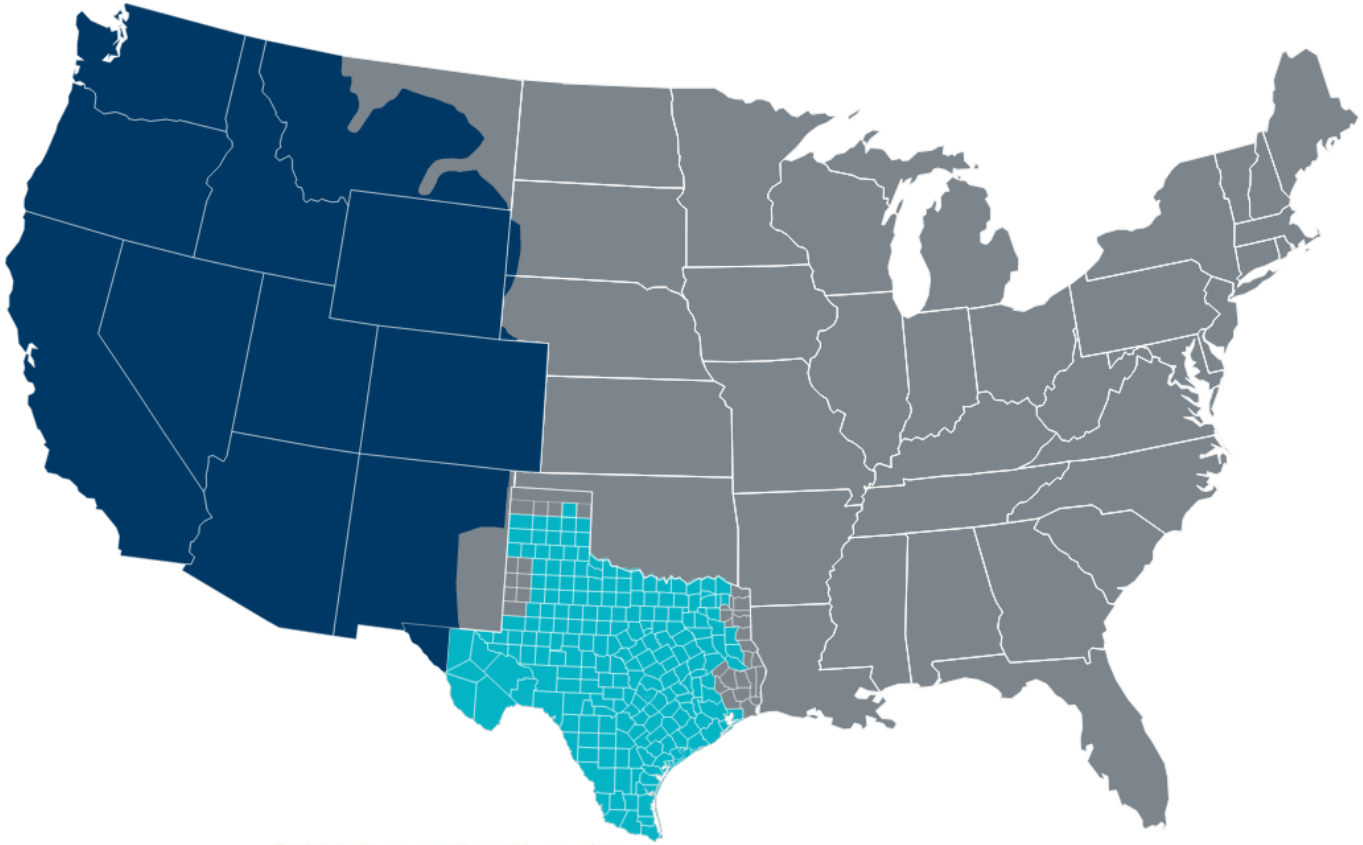
Texas Interconnection Large Loads: Risks and Observations

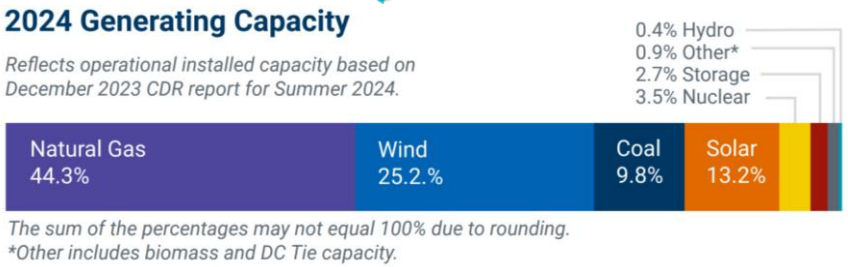
Shirley Mathew
Senior Reliability Engineer

Discussion Topics

- Large Load & Flexible Load Definitions
- Reliability Risks Associated with Large Loads
- Flexible Load Performance During 2023 EEA2 Event
- Discussion Summary
- NERC and ERCOT Initiatives

ERCOT, Texas RE, and the Texas Interconnection





Texas interconnected electrical system serving most of Texas, with limited external connections

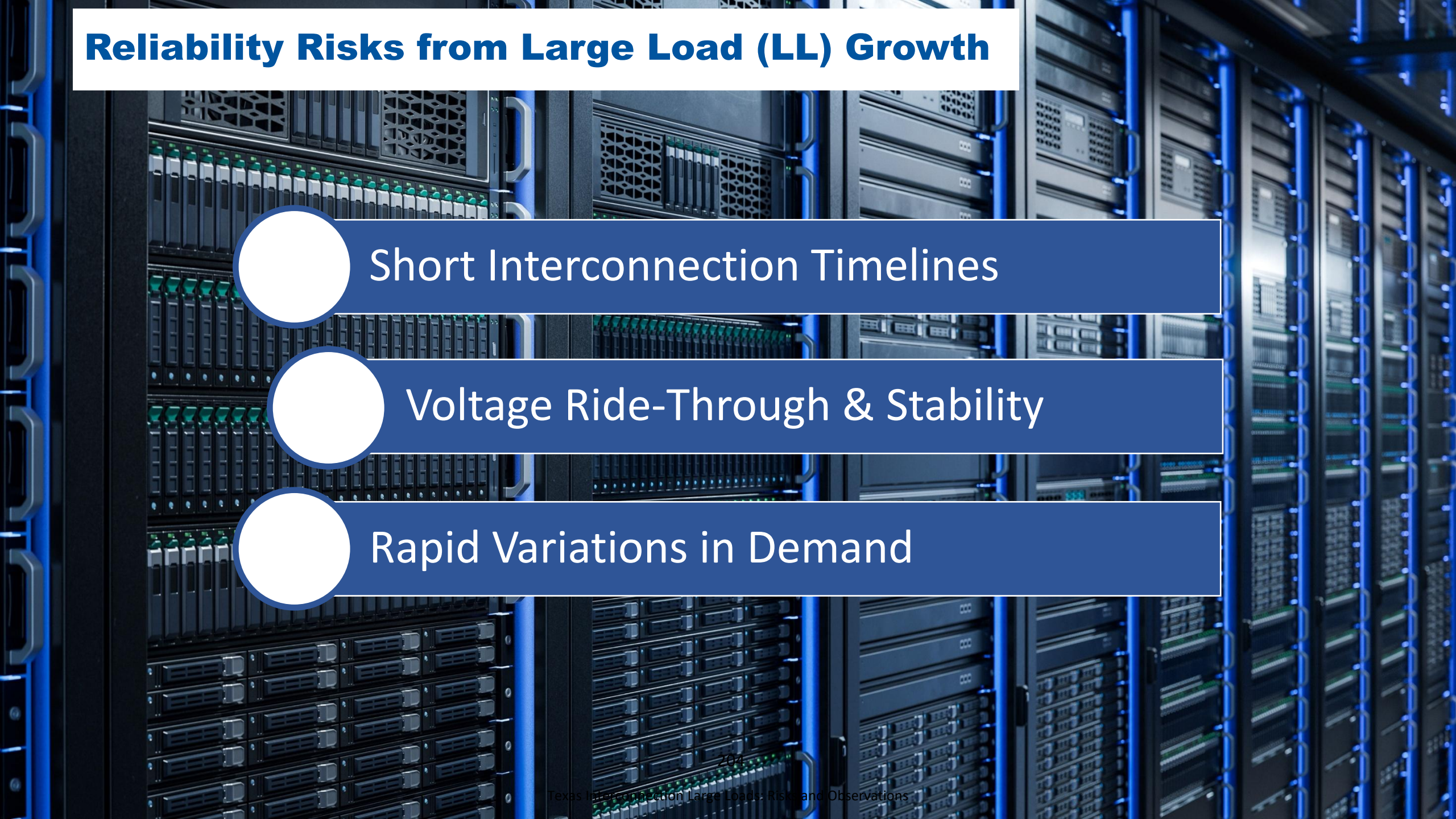
- 90% of Texas electric Load; 75% of Texas land
- 85,508 MW peak, August 10, 2023
- More than 54,100 miles of transmission lines
- 1,250+ generation units, peak capacity for summer peak almost 104 GW

Texas connections to other grids are limited to ~1,220 MW of direct current (DC) ties, which allow control overflow of electricity

Definitions

- **Large Loads have an aggregate Load of 75 MW or greater behind one or more point of interconnection**
  - New loads with total demand of 75 MW or greater
  - New loads co-located with a resource with total demand of 75 MW or greater
- **Flexible Loads can change their consumption in response to power price or other system conditions**

Reliability Risks from Large Load (LL) Growth



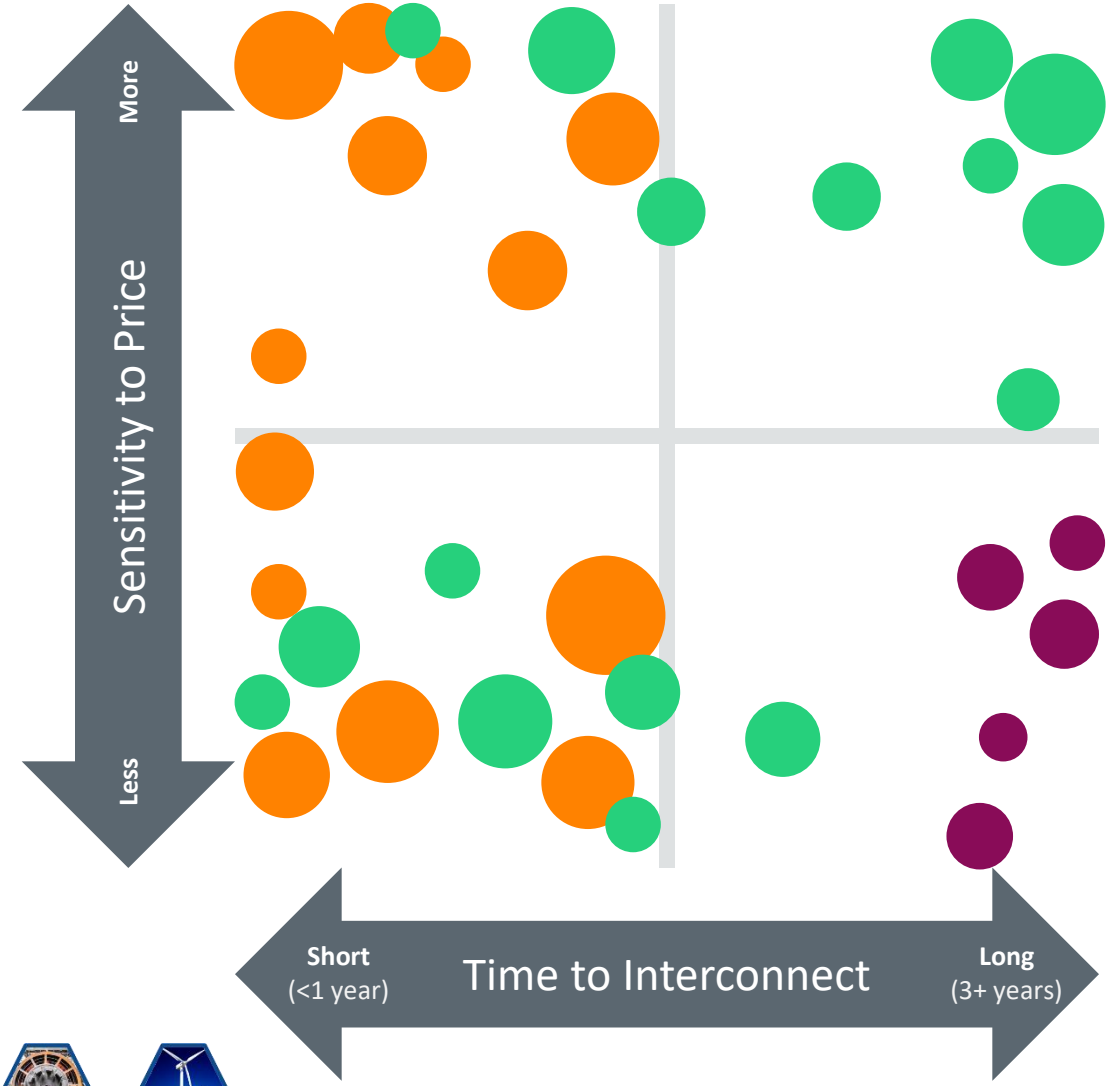
- Short Interconnection Timelines
- Voltage Ride-Through & Stability
- Rapid Variations in Demand

Reliability Risk—Short Interconnection Timelines

New types of Large Loads want to interconnect in less than two years. Traditional planning processes cannot prepare the grid to serve this new Load reliably

- **Traditional planning processes do not review in this timeframe**
- **Transmission upgrades needed to serve the full requested Load amount often cannot be built in less than two years**
- **All Load must be studied as firm – no concept of "Flexible Load"**
- **In March 2022, ERCOT implemented an interim interconnection process for Large Loads wishing to connect within two years or less. A formal process is moving through stakeholder rulemakings**
  - Ensures new interconnection requests are studied for reliability as required by NERC FAC standards
  - Identifies new transmission upgrades that are needed to serve the Load
  - Determines the amount of Loads that can be served **reliably** until transmission upgrades are in service and limits the demand to that amount

Changing Characteristics of Large Loads (>75 MW)



Historical Large Loads

- ❑ Typically industrial facilities
- ❑ Long interconnect timelines studied by traditional planning
- ❑ Little price-sensitive behavior in real-time

Current Wave of Large Loads

- ❑ Mostly cryptomining, data centers, some oil field Load
- ❑ Much shorter timeline to interconnect (months, not years)
- ❑ Some Loads are extremely sensitive to price
- ❑ Some Loads are also flexible and can adjust consumption, either independently or through market bids for energy or ancillary service offers (so-called Large Flexible Loads, LFLs)

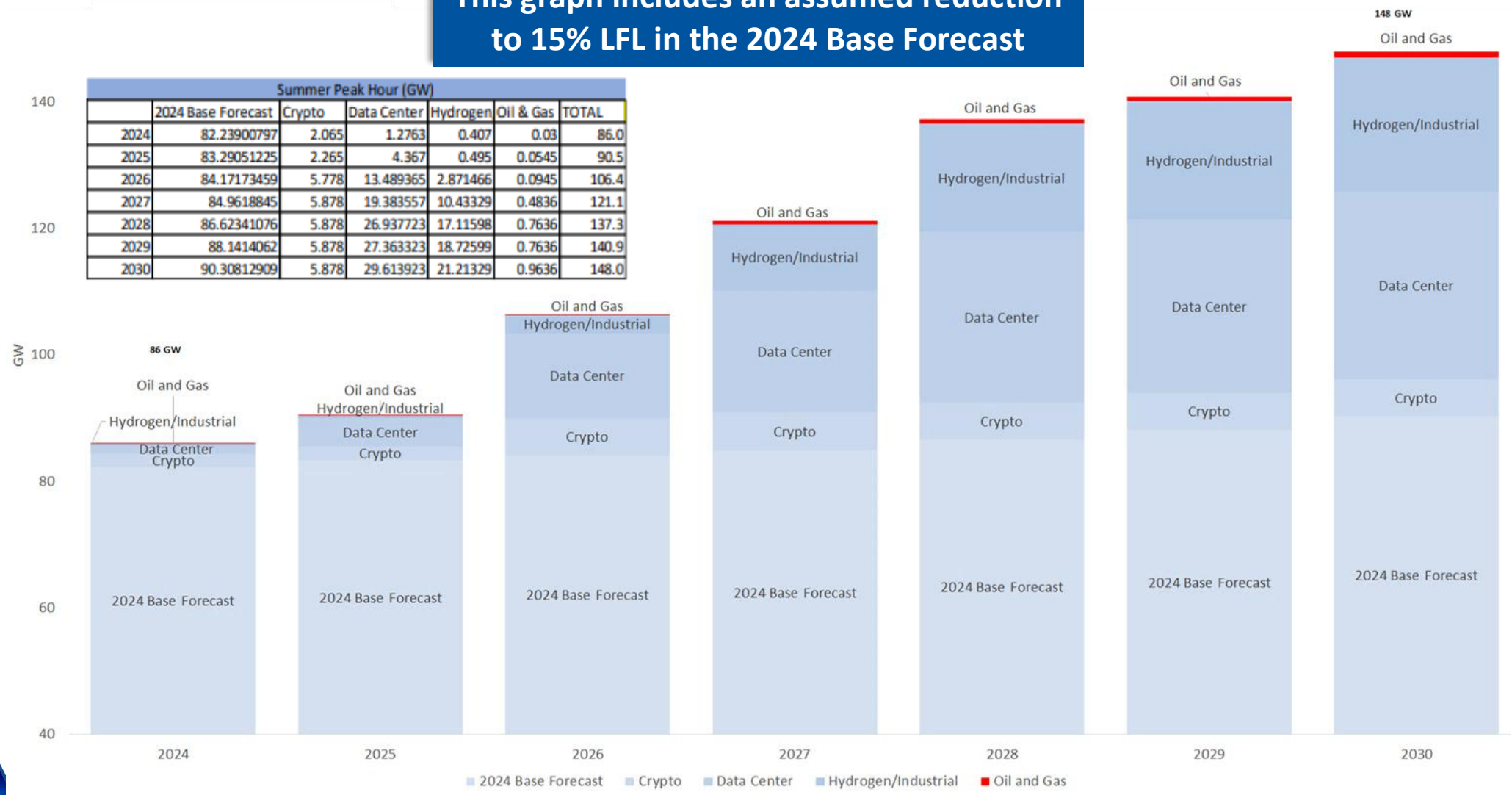
Projected Future Large Loads

- ❑ Hydrogen/electrofuel production, data centers, some crypto
- ❑ Range of interconnection timelines and price sensitivity

ERCOT Load Forecast

This graph includes an assumed reduction to 15% LFL in the 2024 Base Forecast

Summer Peak Hour (GW)						
	2024 Base Forecast	Crypto	Data Center	Hydrogen	Oil & Gas	TOTAL
2024	82.23900797	2.065	1.2763	0.407	0.03	86.0
2025	83.29051225	2.265	4.367	0.495	0.0545	90.5
2026	84.17173459	5.778	13.489365	2.871466	0.0945	106.4
2027	84.9618845	5.878	19.383557	10.43329	0.4836	121.1
2028	86.62341076	5.878	26.937723	17.11598	0.7636	137.3
2029	88.1414062	5.878	27.363323	18.72599	0.7636	140.9
2030	90.30812909	5.878	29.613923	21.21329	0.9636	148.0



Growth of Large Load in ERCOT

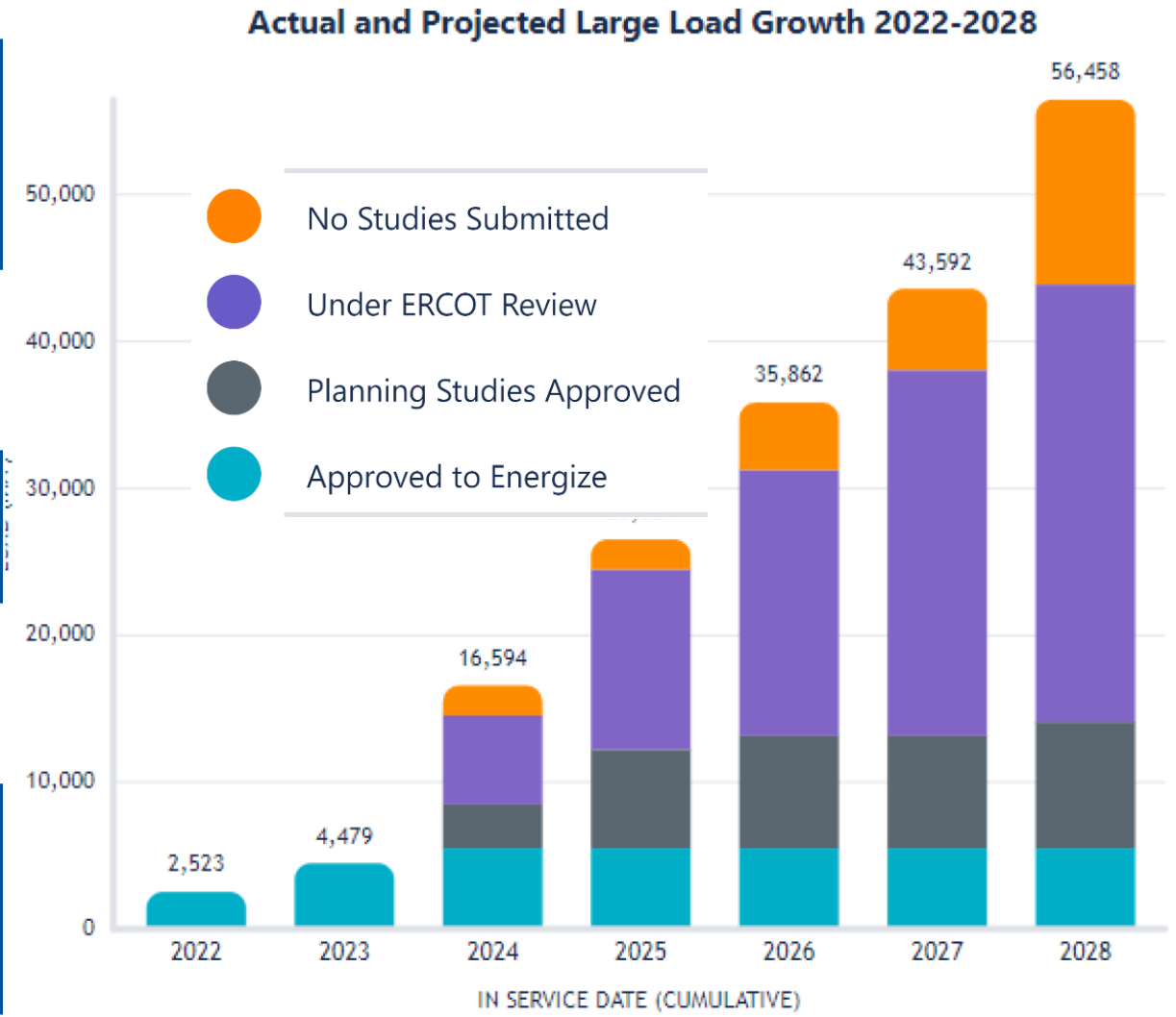
As of September 2024, ERCOT is tracking 56,458 MW of Large Load wanting to energize by end of 2028

- 5,496 MW has already been given approval to energize, 1,570 MW in the past year
- Another 8,598 MW has completed planning review

5,496 MW with approval to energize

- Non-simultaneous peak consumption 3,282 MW; 1,066 MW is co-located with generation
- Simultaneous peak consumption 2,815 MW

Additional Large Load with interconnection dates further in the future under study by TSPs

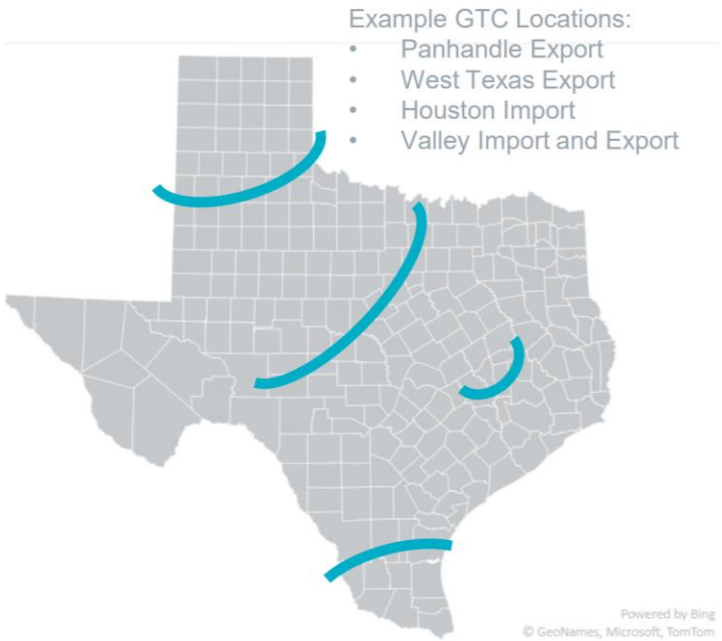


Reliability Risk—Voltage Ride-Through and Stability

Some Load types are reducing consumption during voltage disturbance events (lightning strikes or equipment failure). When these Loads are large, this behavior can cause a significant and unexpected frequency disturbance.

- **ERCOT has observed several new types of Loads (variable frequency drives, datacenters/cryptomining) are particularly sensitive to voltage disturbances. Similar to issues with inverter-based resources**
- **Historically some Load reduction/tripping during a fault/low voltage has been good for the system, particularly for Loads that increase real or reactive power consumption at lower voltages**
- **As the amount of voltage-sensitive Loads increases and system strength decreases, the risk of large amounts (GWs) of Load loss during a voltage disturbance increases**
- **Generators are required to remain connected to the grid (ride-through) during low-voltage events. The amount of time depends on the severity of the voltage drop. *No such requirement currently exists for Loads***

Impacts on Transmission Security

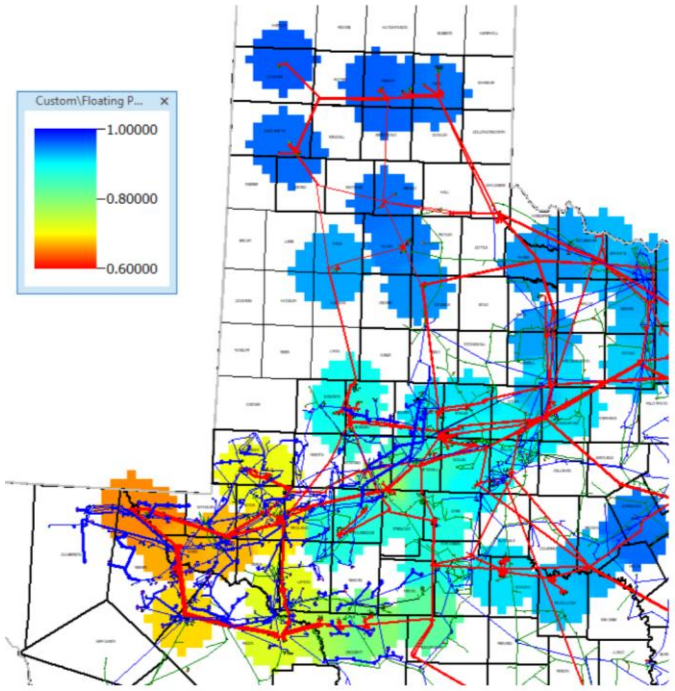


Power flows between two places on the grid may need to be limited due to potential line overloads or voltage/stability issues

Identifying the need for voltage and stability limits, and quantifying those limits, requires special and complex modeling and simulation. ERCOT uses composite Load models that reflect observed dynamic performance of electronics

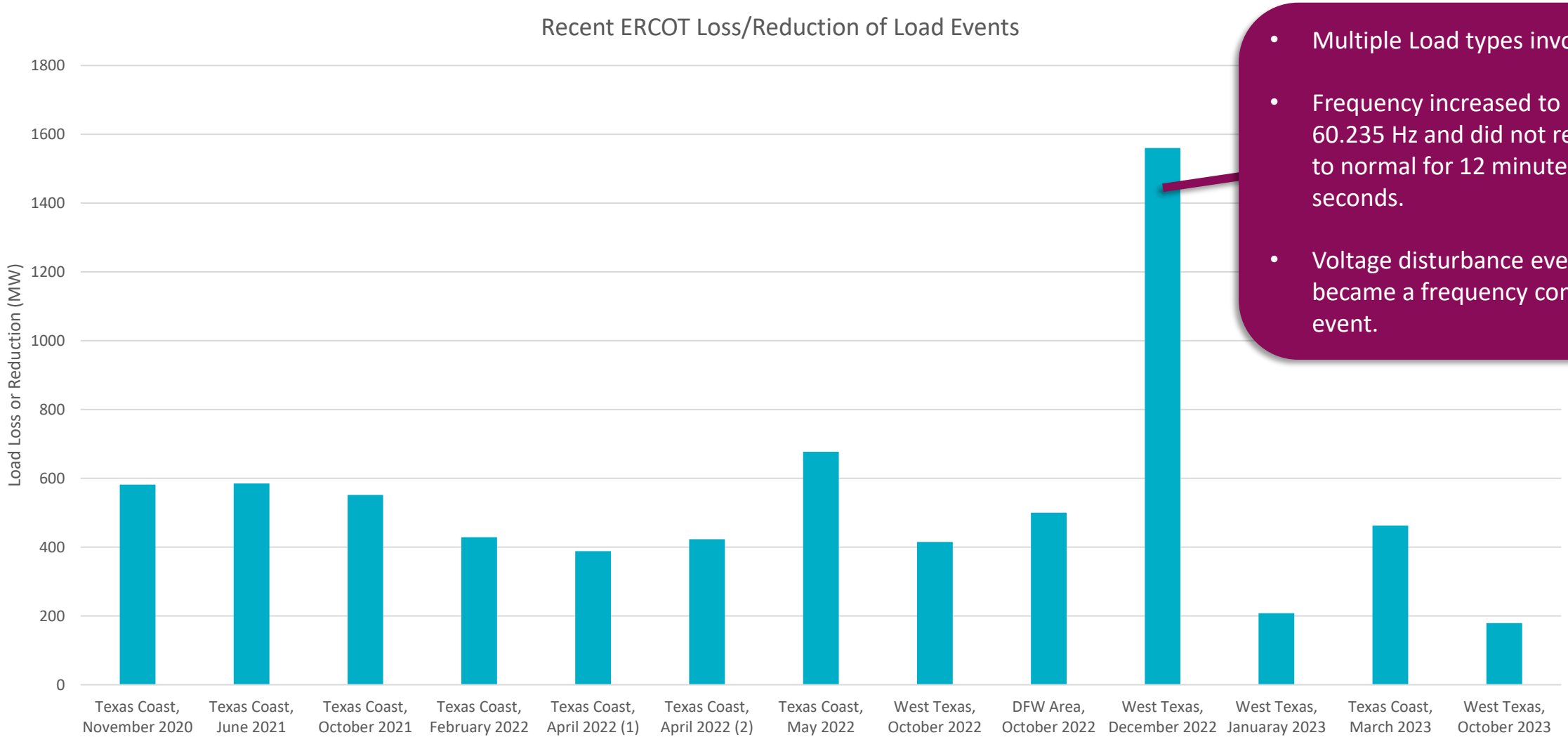
Once calculated, these limits are included as Generic Transmission Constraints (GTCs) in the dispatch algorithm to optimize efficient use of generation while avoiding voltage and stability issues

LLs recently started to have material impact on the GTC limits. For example, ERCOT reported ~200 MW (~6%) reduction for the McCamey GTC in West Texas, under no prior outage conditions



Example ERCOT Voltage Simulation of West Texas Fault

List of Recent Voltage Ride-Through Events



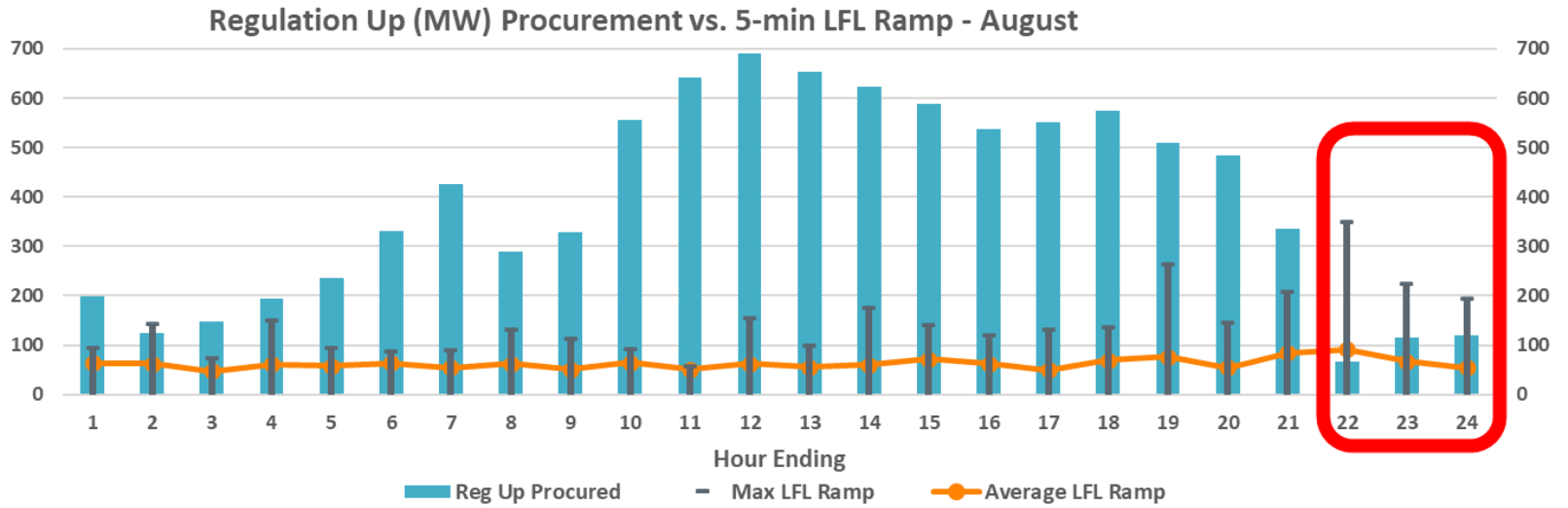
- Multiple Load types involved
- Frequency increased to 60.235 Hz and did not return to normal for 12 minutes 30 seconds.
- Voltage disturbance event became a frequency control event.

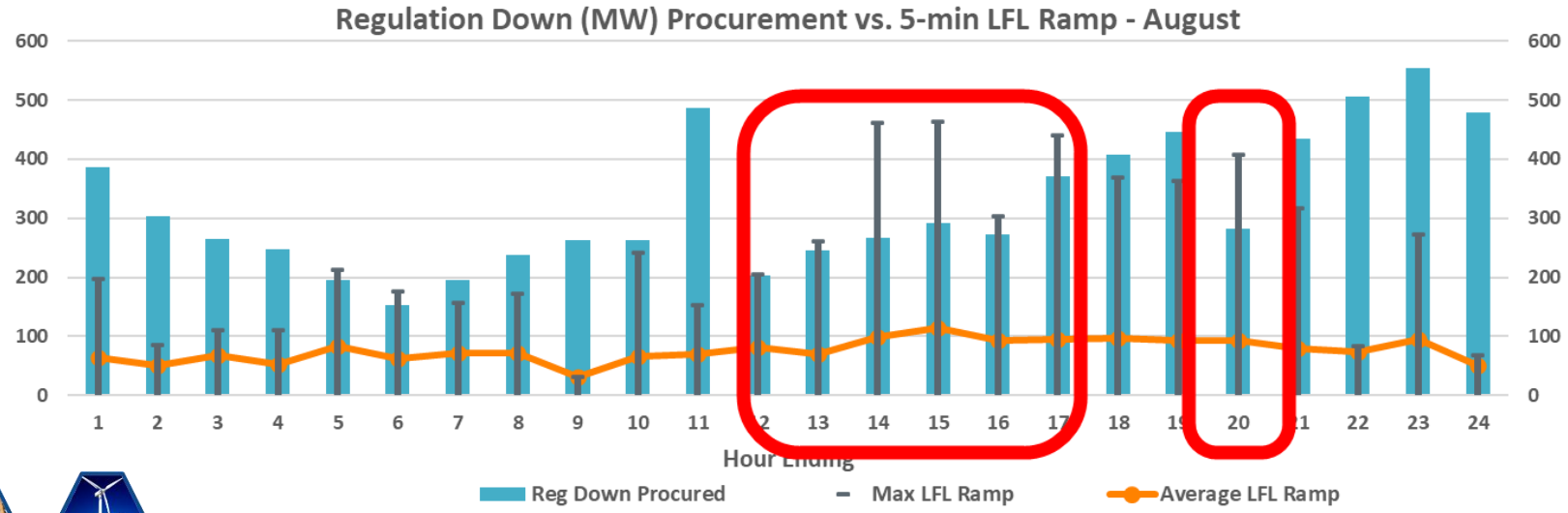
Reliability Risk—Rapid Variations in Demand

A growing number of Large Loads can change their MW consumption rapidly enough to exhaust available Regulation Service and cause other problems.

- **Large majority of Large Loads today do not participate in ERCOT's Security Constrained Economic Dispatch (SCED)**
  - Price responsive Loads may vary consumption at any time without notice or coordination with ERCOT
  - Changes in consumption that occur outside of SCED are also not accounted for when SCED instructs generators how much power to produce
  - The optimal solution for grid reliability is for more Loads to participate in economic dispatch as a Controllable Load Resource (CLR)

LFL Ramping Analysis—August 2023 (Historical Data)





LFL up-ramp in the late evening already exceeds current regulation-up procurement

Hour Ending 2200 has seen up-ramps 4x greater than currently procured regulation-up

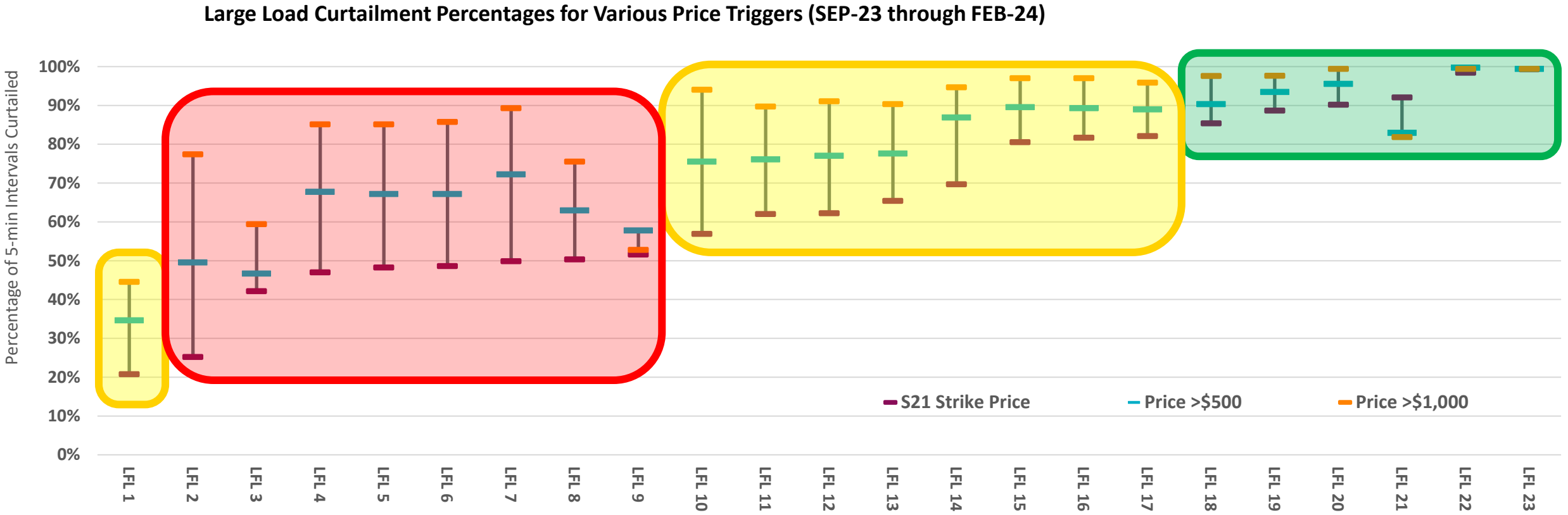
Early afternoon (HE 12 – 17) has seen down-ramps in excess of available reg-down

Similar occurrences happen in other months and has not improved in 2024

Extension: If all LFLs with approved planning studies connect and exhibit similar ramping behavior, it would present a significant reliability risk

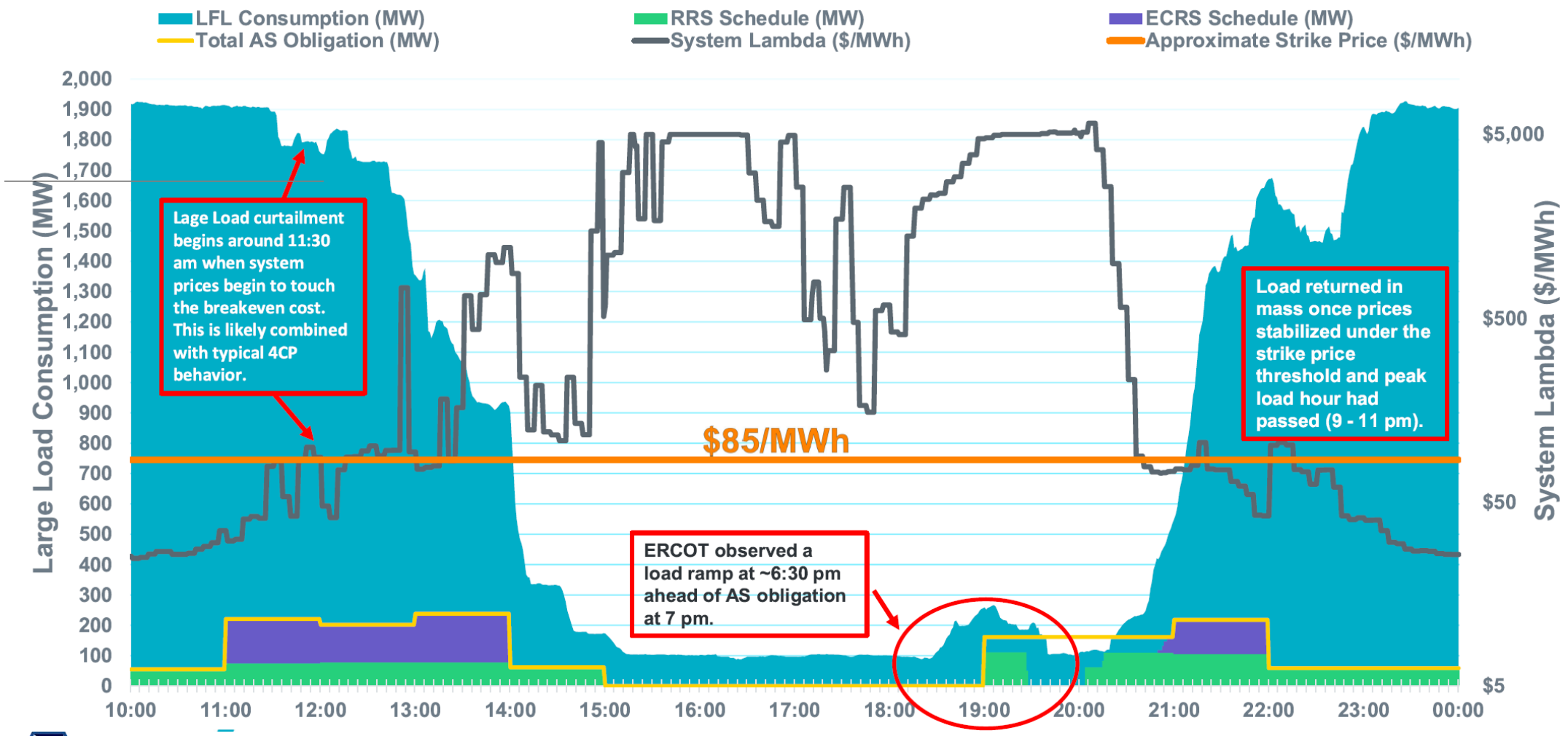
Considerable increases in regulation procurement could potentially be needed for many hours

Analysis of Price Responsive Behavior—ERCOT Observations



- This **chart shows why forecasting flexible behavior is difficult:**
  - Highly price sensitive Loads can be forecasted since their behavior is generally consistent (Green)
  - Other Loads can be forecasted somewhat as not responsive or only responsive to high prices (Yellow)
  - Other Loads are not easily forecasted without additional information (Red)

LFL Performance During September 6, 2023, EEA2 Event



Summary

- Load growth for large industrial and data facilities is unprecedented in volume. Much is forecasted within time periods quicker than transmission can be planned or built. Interconnection processes and terms must adapt.
- Resources needed to serve this Load appear staggering if they must be served around the clock and their ramping managed; but many exhibit demand flexibility, albeit not as predictably as System Operators desire. Their participation in markets as controllable Loads can be beneficial but must consider many factors.
- Modelling and simulations for the electronics-based Load in these facilities is as critical a need as for inverter-based resources to enable system studies and operational adjustments. Concern for expected ride-through performance is evident also, based on analysis of disturbance events.

Additional Information

❑ NERC Large Loads Task Force (LLTF) Work Plan

- White Paper: Characteristics and Risks of Emerging Large Loads by Q2 2025
- White Paper: Assessment of gaps in existing practices, requirements, and Reliability Standards for Emerging Large Loads by Q4 2025
- Reliability Guideline: Risk Mitigation for Emerging Large Loads by Q2 2026

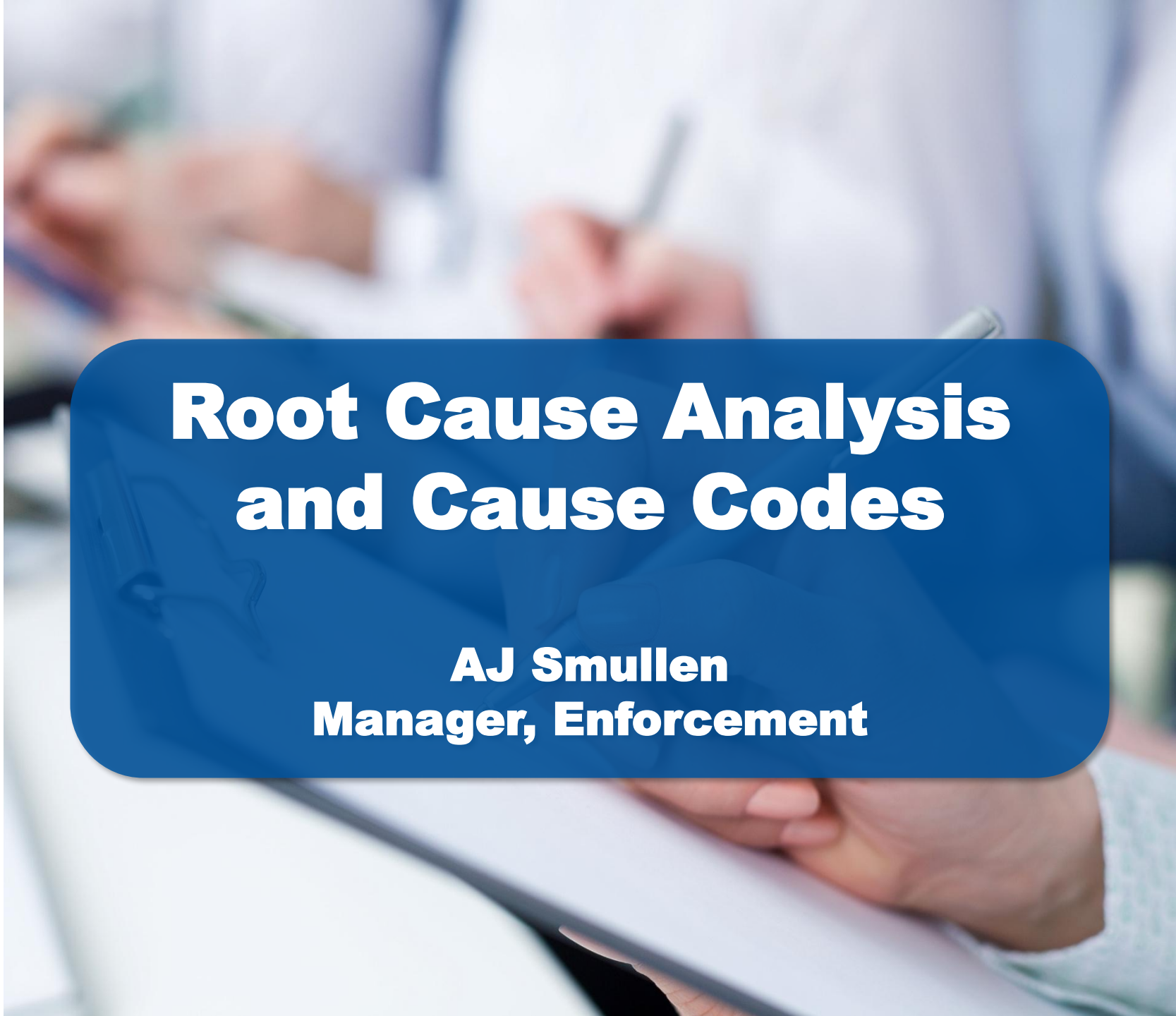
❑ NERC Website: LLTF

❑ ERCOT Website: LFLTF

Questions?

ACKNOWLEDGEMENT: Material in this presentation borrows liberally from analysis in public presentations by Agee Springer, Dan Woodfin, and Yunzi Chen of ERCOT ISO to their system operators, technical committees, and Board

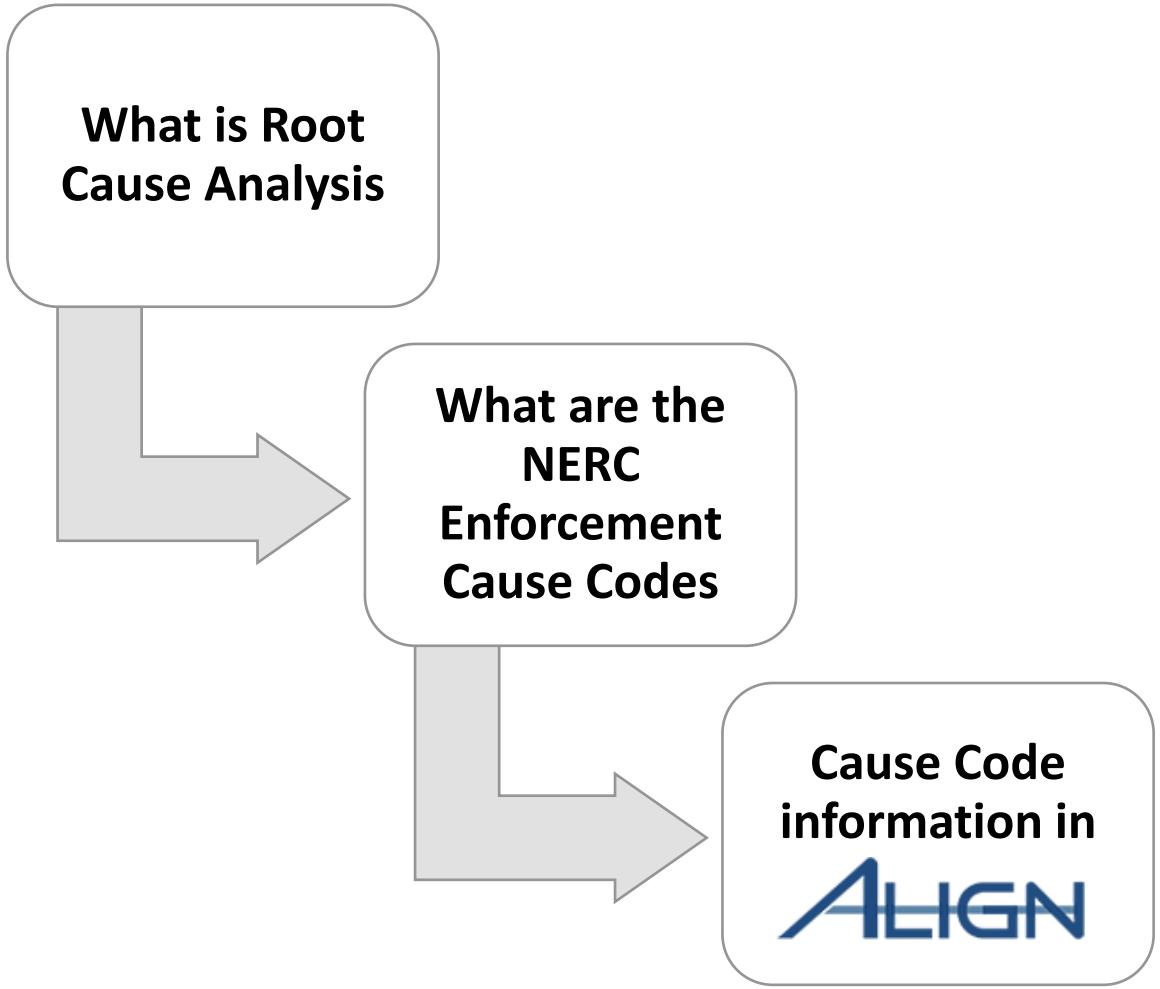
TEXAS RE
Ensuring electric reliability for Texans



Root Cause Analysis and Cause Codes

AJ Smullen
Manager, Enforcement

Roadmap


What is Root Cause Analysis
What are the NERC Enforcement Cause Codes
Cause Code information in
ALIGN

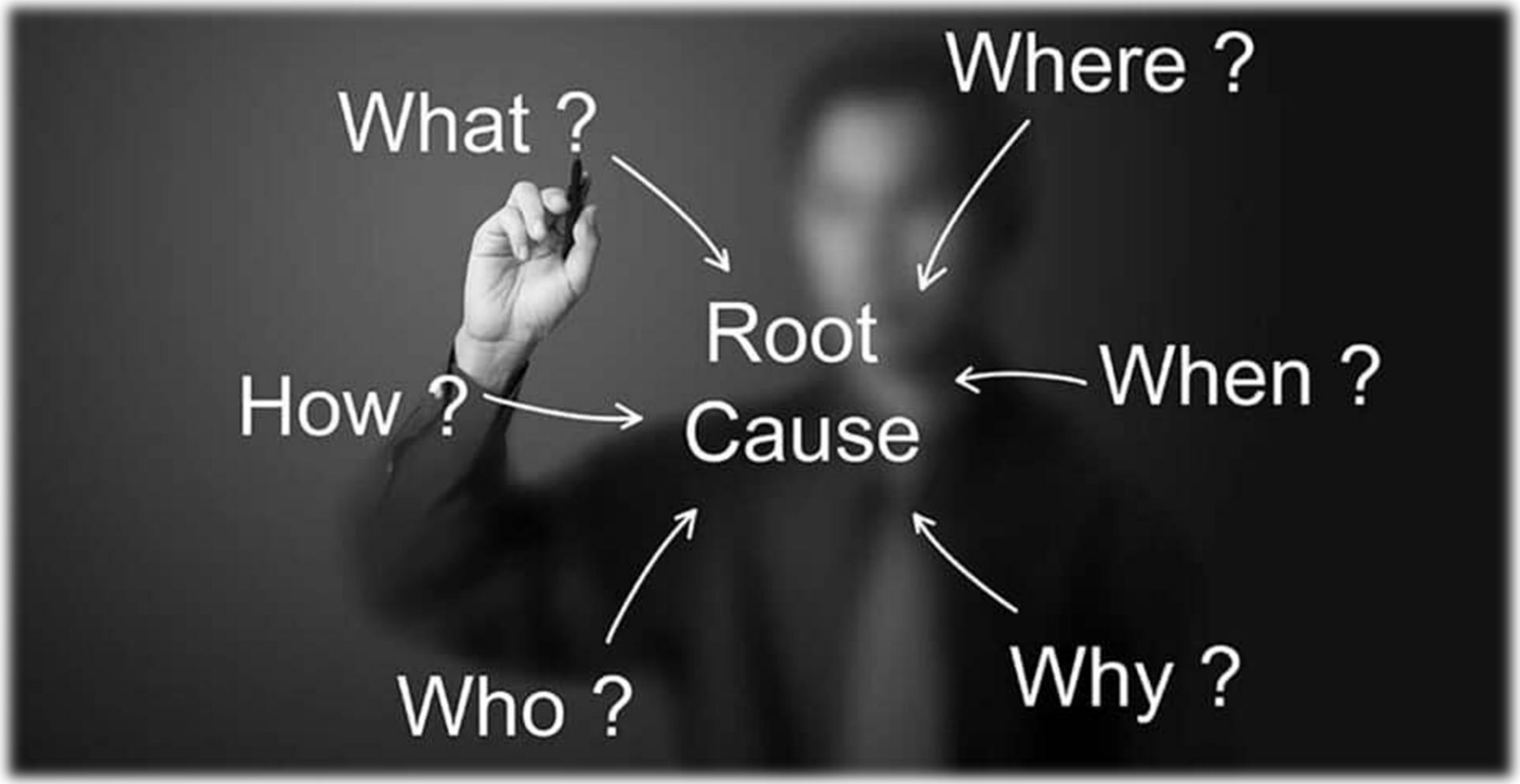
Root Cause Analysis

Discovering the fundamental reason for occurrences

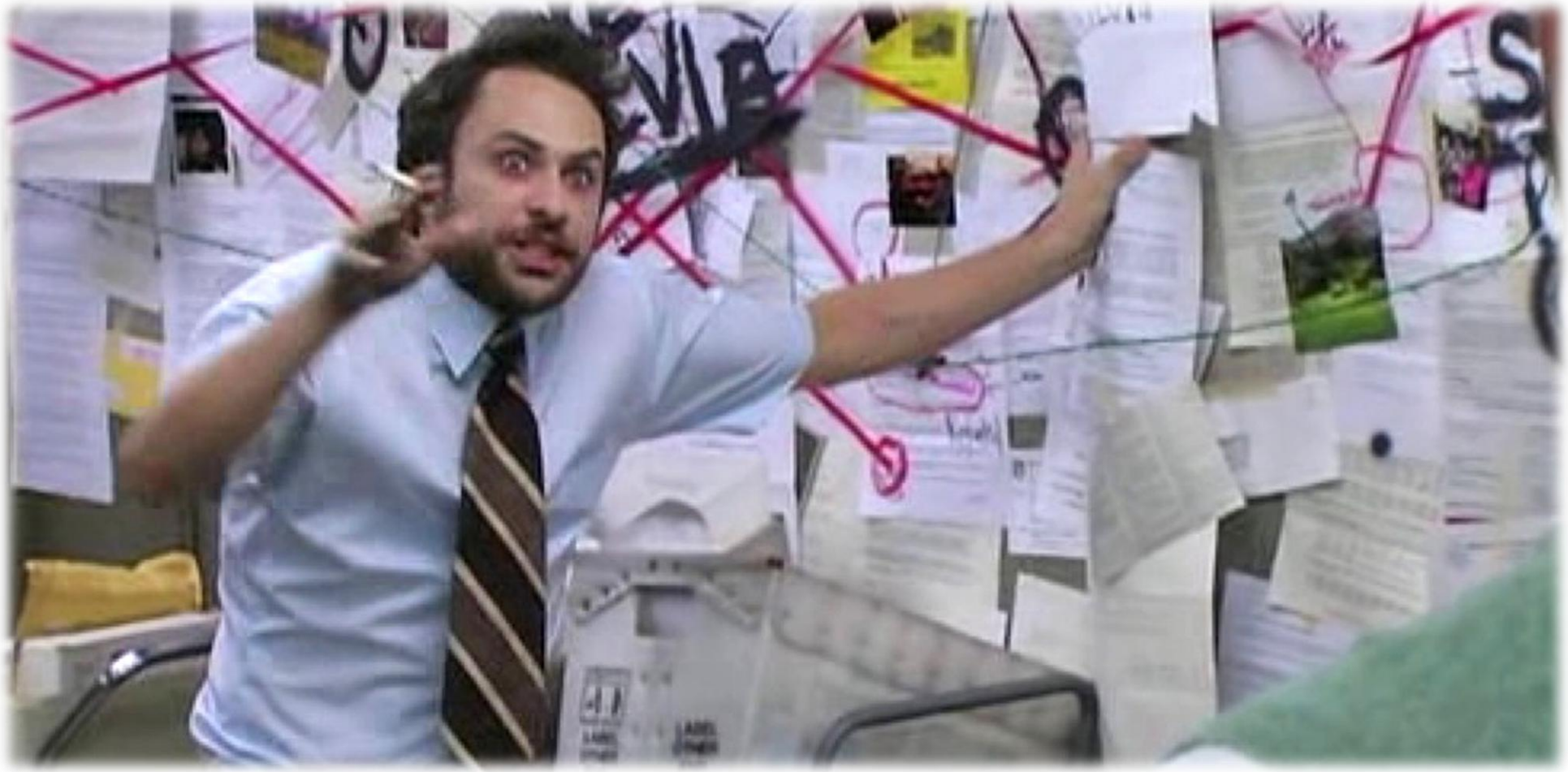
Focus on the cause rather than just the symptoms

Many causes but only one root cause

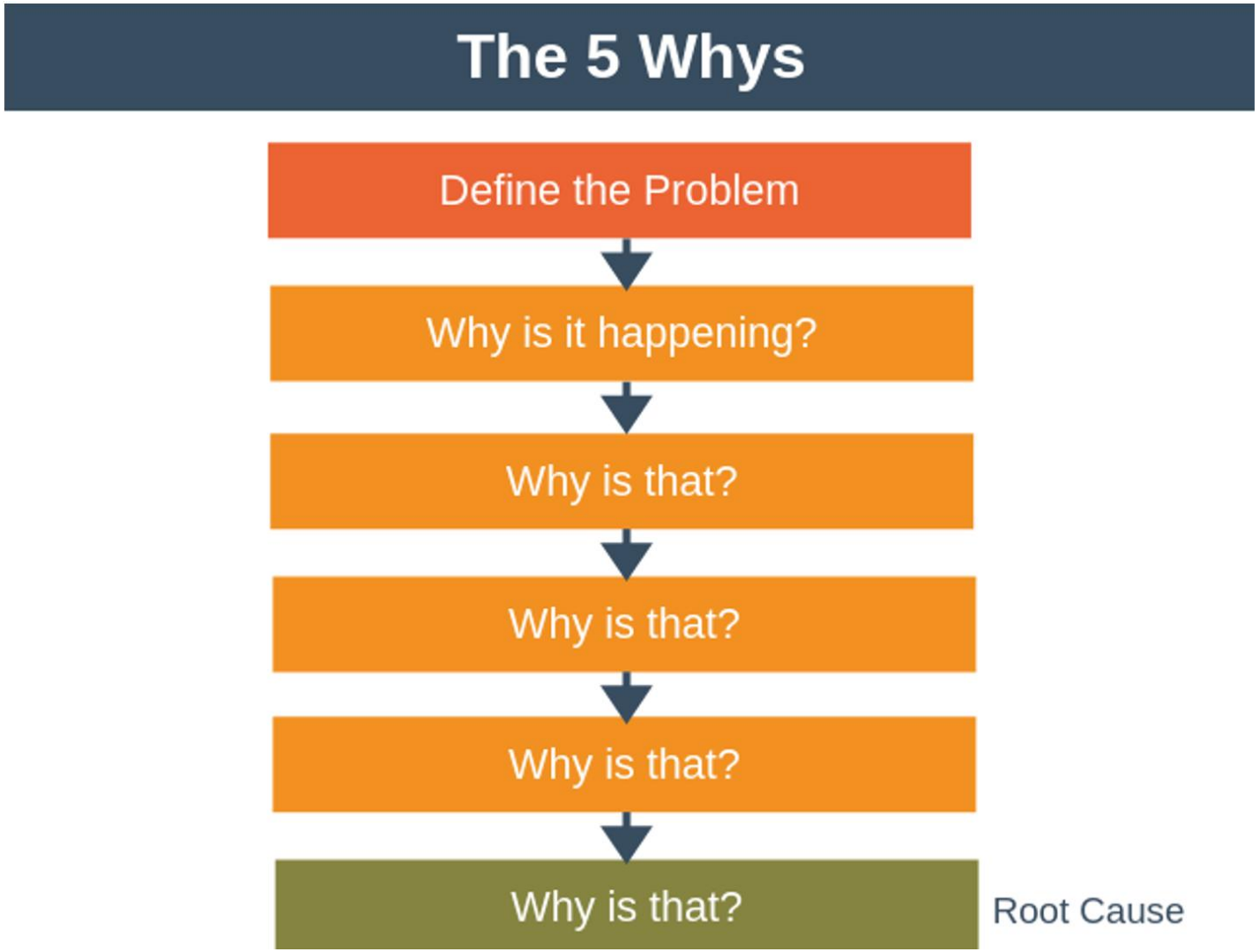
Root Cause Analysis



Root Cause Analysis



Five Whys


The 5 Whys
Define the Problem
Why is it happening?
Why is that?
Why is that?
Why is that?
Why is that?
Root Cause

Human Performance Error

Often the First Why

Rarely the Last Why

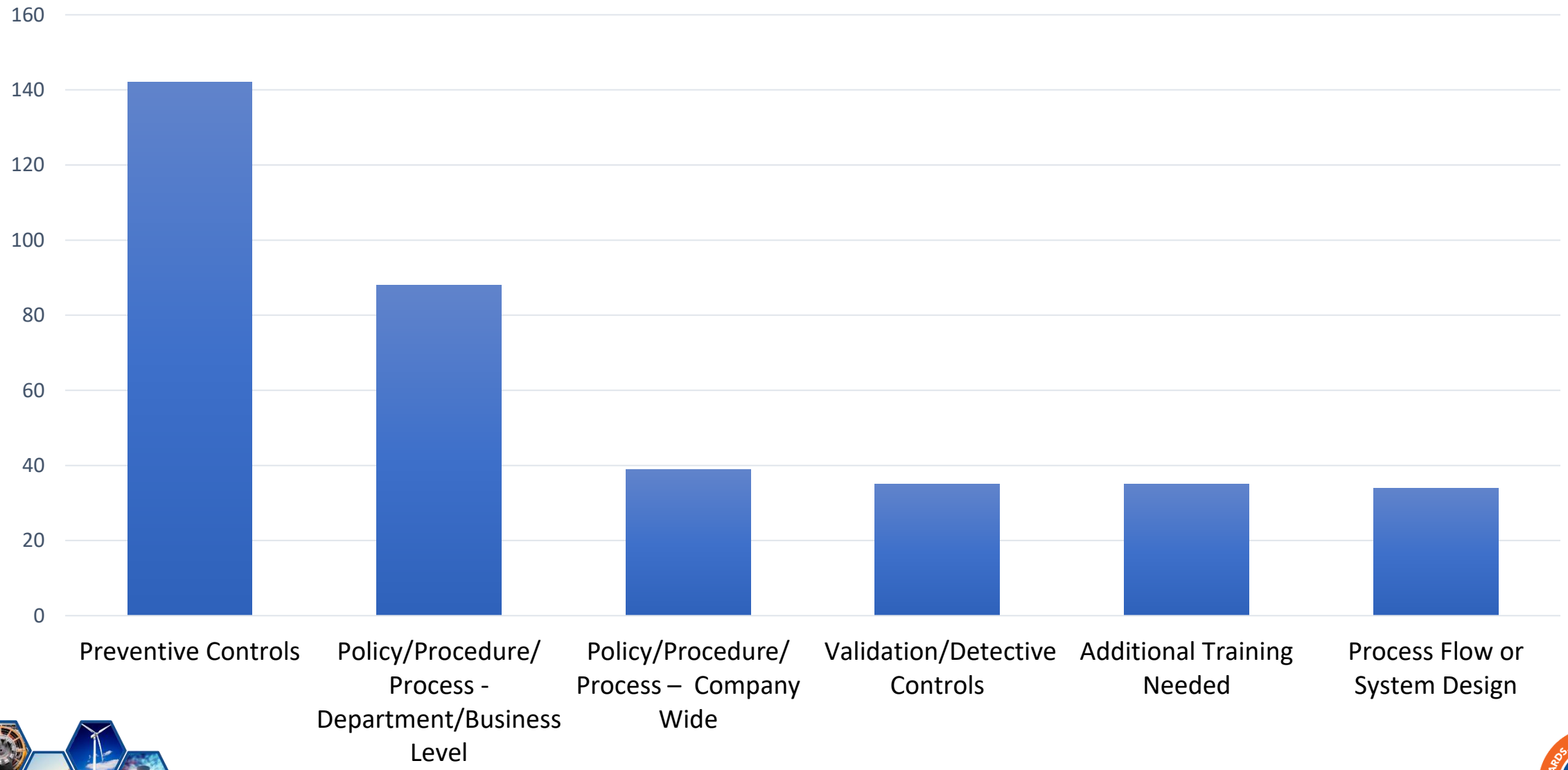
Often Results in an RFI

Essential to Prevention of Recurrence

Mitigating activities should rhyme with the root cause

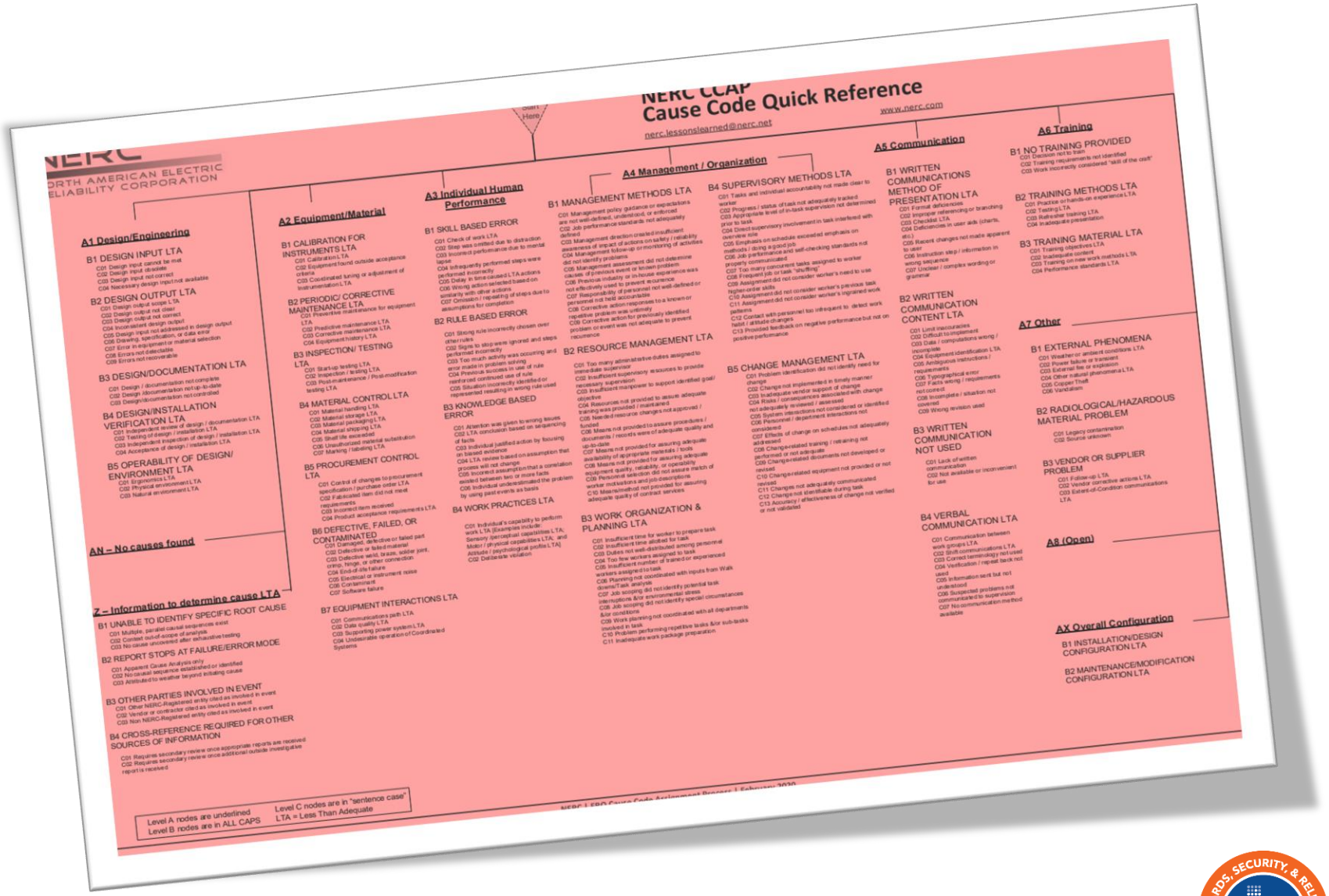
Root Cause	Prevention of Recurrence
Insufficient validation control	Updated validation control
Unclear process document	Revised process document
Ineffective system design	Updated system design

Common Root Causes



Cause Codes

Not using the event analysis codes



New Enforcement-Specific Cause Codes

Enforcement Cause Codes

Table 1 lists the final Enforcement Cause Codes by code name and description of the code, as well as examples of root causes and their appropriate Enforcement Cause Codes. These are meant to serve as a guide and do not represent the entire range of possible root causes of noncompliance.

It may be beneficial to the Subject Matter Experts to keep in mind the Enforcement Cause Codes as they review and evaluate the root cause of the noncompliance. The concurrent consideration should help with proper identification of the root cause and contributing cause of the noncompliance.

Table 1: Cause Code and Descriptions

Code	Name and Description
1	Change Management *Made changes without understanding the downstream impact of the change on other components of the system and its related processes.*
2	Communication/Coordination – Internal *Ineffective coordination or communication between personnel/departments within the same company. Lack of or poor coordination/communication within the same business unit and/or across business units sharing compliance obligations (organizational silos), which resulted in confusion regarding expectations and ownership of tasks.*
3	Communication/Coordination – External *Ineffective coordination/communication between responsible parties, vendors, external entities. Lack of or poor coordination/communication with external individuals the entity relies upon for compliance obligations, which resulted in confusion by either internal or external individuals regarding expectations and ownership of tasks.*
4	Design – Ineffective Process Flow or System Design or failure of system/technology *Items were missing from design, design-related documentation, or system or technology failure.*
5	Lack of/deficient documented evidence.

Cause Codes

NERC training and cause codes guide to be published Q4 2024

Cause codes added to Align registered entity interface 2025

Buckets

I divided the codes into buckets

Not official, just me popping off

How to Use the Buckets

- Useful for narrowing the potential selection
- Where there's overlap, use the code that is more specific

Processes and Procedures Bucket

Codes	Name	Descriptions
1	Change Management	Made changes without understanding the downstream impact of the change on other components of the system and its related processes.
7	Lack of/Deficient Policy/Procedure - Company Wide	Ineffective management policy – high level, company-wide issue. Needs new policy/procedure/process (did not exist) or was deficient.
8	Lack of/deficient policy/procedure - Department/Business Level	Ineffective business-level procedure/process – Standard Operating Procedure, Instructions, department-based. Needs new policy/procedure/process (did not exist) or was deficient.
13	Lack of understanding or lack of compliance awareness	The entity is aware of the obligations of the Reliability Standard but lacks the understanding of how to fully implement the obligations. Or the entity failed to implement certain obligations of the Standard because it was unaware of them; there was an erroneous interpretation of what is required in the Standard, especially a new standard in effect, including the implementation date and which devices and/or activities are covered coordination with another entity.
14	Ineffective Organizational Methods	An event or condition that can be directly traced to organizational actions or methods. An organizational problem may be attributed to methods such as directions, monitoring, assessment, accountability, oversight, corrective actions, and supervisory methods.

Coordination, Planning, and Documenting Bucket

Codes	Name	Descriptions
2	Communication/Coordination – Internal	Ineffective coordination or communication between personnel/departments within the same company. Lack of or poor coordination/communication within the same business unit and/or across business units sharing compliance obligations (organizational silos), which resulted in confusion regarding expectations and ownership of tasks.
3	Communication/Coordination – External	Ineffective coordination/communication between responsible parties, vendors, external entities. Lack of or poor coordination/communication with external individuals the entity relies upon for compliance obligations, which resulted in confusion by either internal or external individuals regarding expectations and ownership of tasks.
5	Lack of/deficient documented evidence	The required activities in the process or procedure were completed but evidence was either not, or partially, documented.
6	Lack of/deficient documented evidence - Third Party/Vendor	Lack of documented evidence by a third-party (e.g., vendor or through a sale or organizational transition). The required activities in the process or procedure were completed but evidence was either not, or partially, documented.
15	Ineffective Resource or Project Planning	There was improper allocation of resources and/or improper scoping of project, including (i) insufficient supervisory resources to provide necessary supervision; (ii) insufficient workforce or and equipment/tools to support identified compliance-related goals/objectives/tasks, including allotting sufficient time to complete tasks, train, or to implement quality procedures or controls; (iii) work planning did not account for potential interruptions and/or special circumstances; and/or (iv) work planning did not include coordination with all departments or business units involved in completing the tasks. This cause often occurs when upgrading equipment or systems, transitioning to NERC Reliability Standards for the first time (e.g., merger/acquisition or transitioning to a new version of the standard).

Training Bucket

Codes	Name	Descriptions
11	Additional Training Needed	Training program is adequate but additional training needed. The overall training program was adequate but training on a required task was not part of the employee's training requirements or frequency of the training was insufficient to maintain the required knowledge and skill to perform the job (e.g., did not consider the complexity of certain tasks or individual's skillset or experience). If the training design/content is adequate, but the entity failed to effectively deliver it to their employees or track the required training.
12	Lack of/deficient training materials and content	The quality of the training objective, or training content and/or material was incomplete or unclear such that it did not contain all the information necessary for staff to fully perform all the task requirements in the procedure.

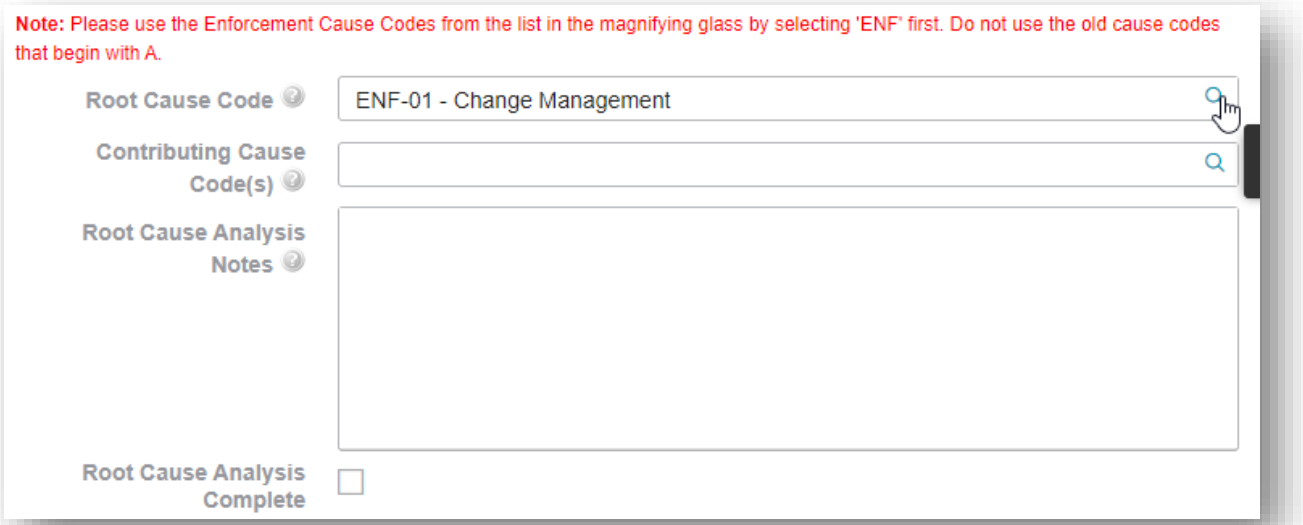
Controls Bucket

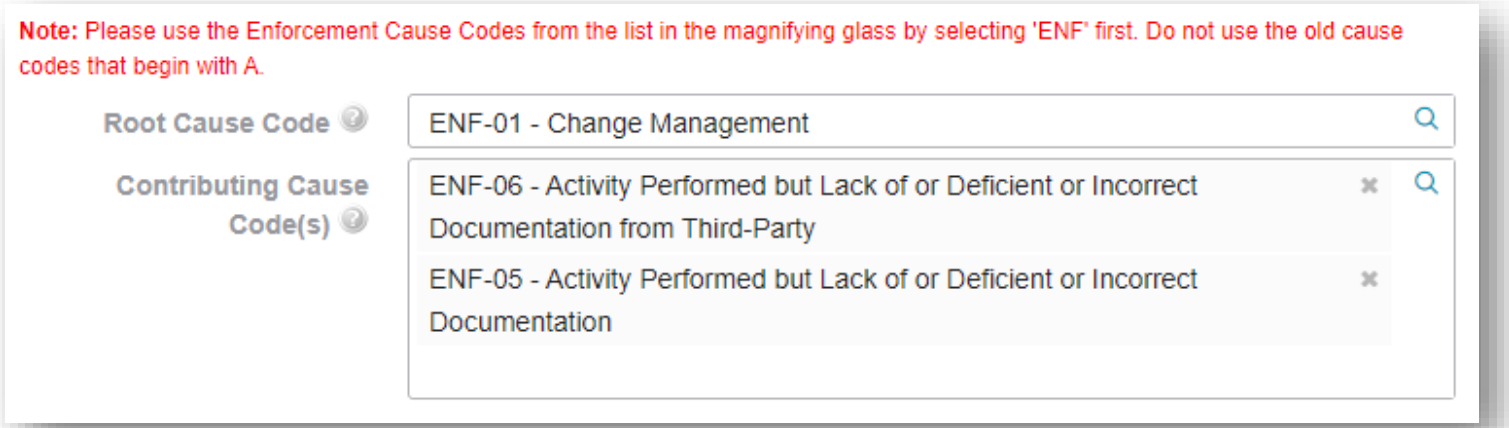
Codes	Name	Descriptions
4	Design – Ineffective Process Flow or System Design or failure of system/technology	Items were missing from design, design-related documentation, or system or technology failure.
9	Ineffective Preventive Controls	Lack of or ineffective internal controls designed to prevent noncompliance. Detective controls were implemented but there was an ineffective or lack of preventative control (e.g., checklist, secondary reviewer, workflow, or a backup or a redundant control).
10	Ineffective Validation/Detective Controls	Lack of or an ineffective validation/detective control. Preventative controls were implemented but there was an ineffective or lack of a validation/detective control after completion of the task.

Other Bucket

Codes	Name	Descriptions
16	Exceptional Circumstances	Noncompliance occurred from unpreventable factors beyond the control of the entity. Factors beyond the control of the entity including weather, natural disaster, fire (lightning/sabotage), or other phenomena, such as power loss attributed to outside supplied power and infectious disease outbreak or pandemic.
17	Human Performance Failure	Sufficient controls, procedures, and training implemented but not followed due to human error.
18	Other	Other should only be used if there were no other Cause Code in the list that would apply to the noncompliance.

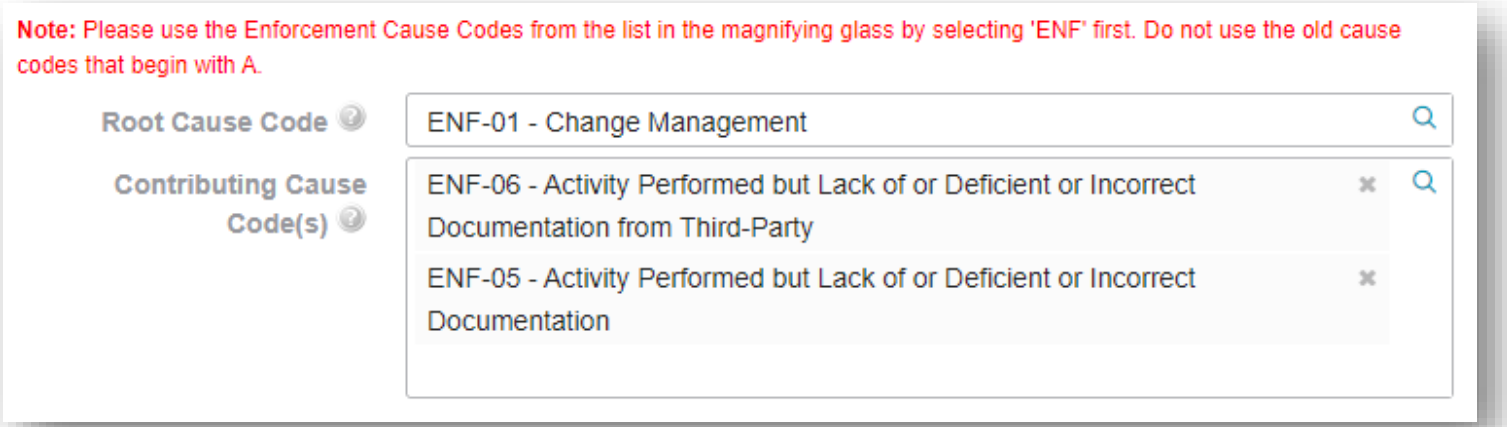
Align


Note: Please use the Enforcement Cause Codes from the list in the magnifying glass by selecting 'ENF' first. Do not use the old cause codes that begin with A.
Root Cause Code
ENF-01 - Change Management
Contributing Cause Code(s)
Root Cause Analysis Notes
Root Cause Analysis Complete


Note: Please use the Enforcement Cause Codes from the list in the magnifying glass by selecting 'ENF' first. Do not use the old cause codes that begin with A.
Root Cause Code
ENF-01 - Change Management
Contributing Cause Code(s)
ENF-06 - Activity Performed but Lack of or Deficient or Incorrect Documentation from Third-Party
ENF-05 - Activity Performed but Lack of or Deficient or Incorrect Documentation

Contributing Cause

- The penultimate “why”s
- Optional input in Self-Report
- Highlights additional mitigation
- Events can have multiple contributing causes
- Still only one root cause



TEXAS RE
Ensuring electric reliability for Texans

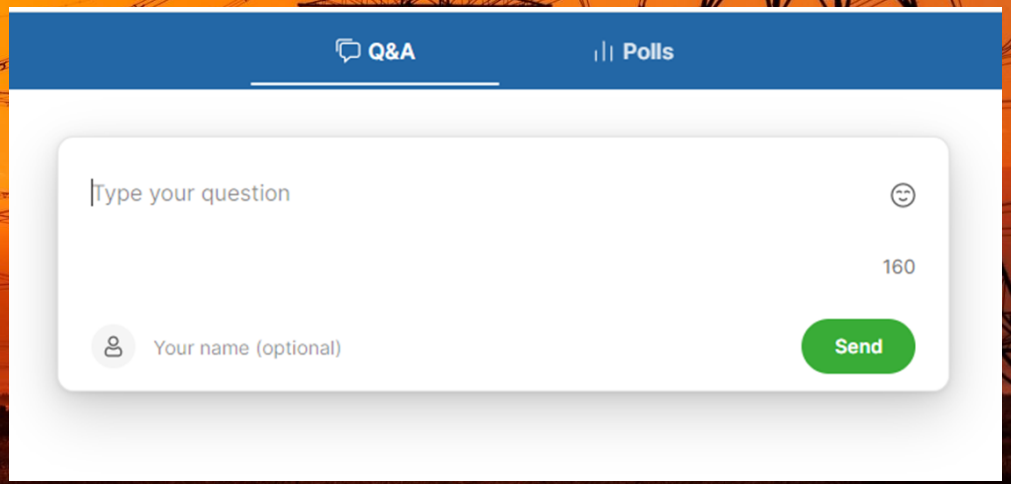
Texas RE Fall Standards, Security, & Reliability Workshop

Return at 1:55 p.m.

AGENDA

- Kick-off and Instructions
- Executive Welcome
- CISA Update
- NIST Cybersecurity Framework
- Threat Briefing
- Lonestar Infrastructure Protection Act
- Physical Security
- ITCS
- Large Loads in the Texas Interconnection
- Root Cause Analysis and Cause Codes
- 2025 CMEP IP
- Common and High Risk Violations

To submit questions during the workshop, please visit **slido.com** and enter today's participant code: **TXRE**



2025 ERO CMEP Implementation Plan

Rashida Caraway
Manager, Risk Assessment

Agenda

- CMEP IP Purpose
- Risk Element Changes
- Risk Elements Review
- Summary

CMEP Implementation Plan (CMEP IP) Purpose

Reflects ERO and Regional Entity-specific risk elements that Regions prioritize for oversight of registered entities

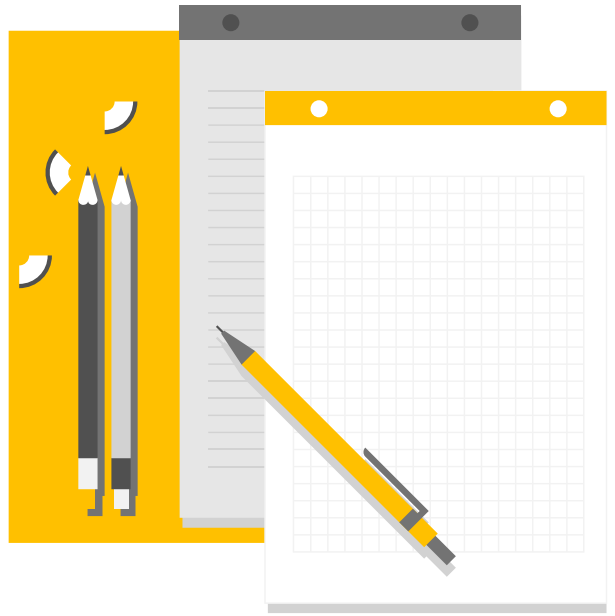
Developed by NERC and the Regional Entities

Serve as an input in determining the appropriate monitoring of risks

Risk Elements

Risk elements developed using:

- Compliance findings
- Recent event analysis
- Data analysis
- Committees
- Publications



Risk elements are considered when Regions:

- Complete an Inherent Risk Assessment (IRA)
- Complete a Compliance Oversight Plan (COP)
- Scope an engagement
  - engagement team may use to focus on sampling and internal controls

What's New with Risk Elements?

2024	2025
Remote Connectivity	Remote Connectivity
Supply Chain	Supply Chain
Physical Security	Physical Security
Incident Response	Incident Response
Stability Studies	**Transmission Planning and Modeling**
Inverter-Based Resources	Inverter-Based Resources
Facility Ratings	Facility Ratings
Extreme Weather Response	Extreme Weather Response

Remote Connectivity

2024 CIP Themes and Lessons Learned

- Use of remote workers continuing
- How do entities protect their technology with the changes taking place?
- Risk identified with low impact BCS

Standard	Requirement
CIP-003-8	R2
CIP-005-7	R2, R3
CIP-007-6	R3
CIP-012-1	R1

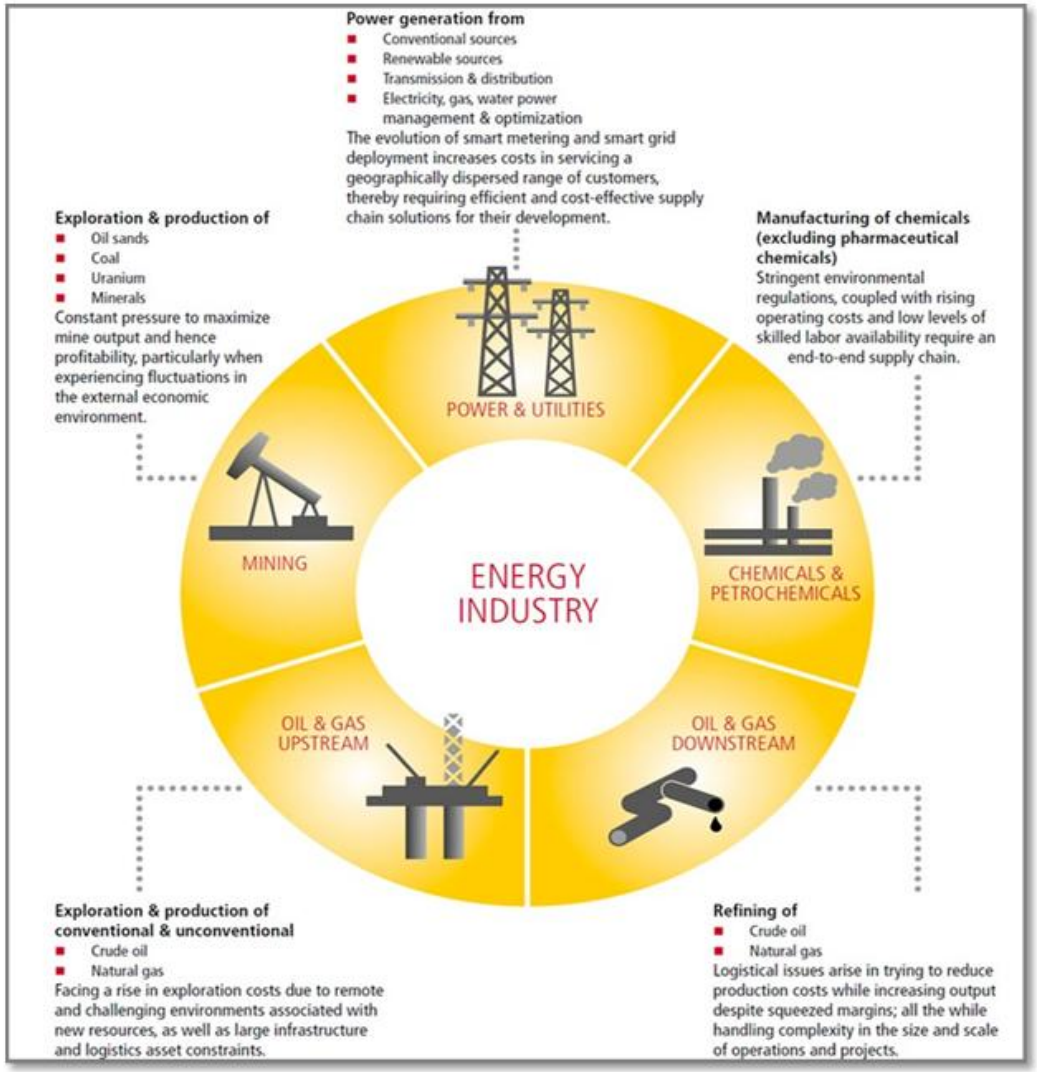
Supply Chain

Standard	Requirement
CIP-010-4	R1
CIP-013-2	R1, R2

Lead times for facility equipment have increased significantly since 2020

Renewable energy supply chain is heavily concentrated; makes renewables more vulnerable to sourcing risks

Supply Chain Example



Source: 2025 ERO Enterprise CMEP Implementation Plan

Slido.com (#TXRE)

Slido Question

The Remote Connectivity Risk Element is a risk for:

A. Facilities with low-impact BCS
B. Facilities with medium-impact BCS
C. Facilities with high-impact BCS
D. All of the above

Physical Security

Continues to be a top concern

Added focus on assets that contain low impact BCS

Standard	Requirement
CIP-003-8	R2
CIP-014-3	R4, R5

Incident Response

Ransomware attacks increase

Added focus on assets that contain low impact BCS

Standard	Requirement
CIP-003-8	R2
CIP-008-6	R1, R2, R3

Transmission Planning and Modeling

Replaces Stability Studies Risk Element

Flexible resources, large loads, and data centers are being incorporated into the planning processes

Standard	Requirement
CIP-014-3	R1
MOD-025-2	R1, R2, R3
MOD-026-1	R6
MOD-027-1	R5
MOD-031-3	R1, R2
MOD-032-1	R1, R2, R3, R4
TPL-001-5.1	R1, R2, R3, R4, R5, R6, R7

Inverter-Based Resources (IBRs)

Standards	Requirements
FAC-001-4	R1, R2
FAC-002-4	R1, R2
MOD-026-1	R2
PRC-005-6	R3, R5
PRC-024-3	R1, R2
PRC-027-1	R1, R2, R3

IBRs account for over 70% of new generation connected to the BPS

Additional areas of focus added in 2025

Facility Ratings

Facility Ratings

- Inaccurate Facility Ratings undermine the usefulness of transmission planning and modeling
- Risk with entities having inaccurate Facility Ratings
- ERO CMEP Practice Guide Facility Ratings
- ERO Themes and Best Practices Facility Ratings

Standard	Requirement
FAC-008-6	R6

Extreme Weather Response

Several notable extreme events in 2024

Small Group Advisory Sessions (SGAS) offered in last few years

Standard	Requirement
EOP-011-2	R1, R2, R3, R6, R7, R8
EOP-011-4	R1, R2, R3
EOP-012-2	R1, R2, R3, R4, R5, R6, R7
TPL-007-4	R1, R2, R4, R5, R7

Slido.com (#TXRE)

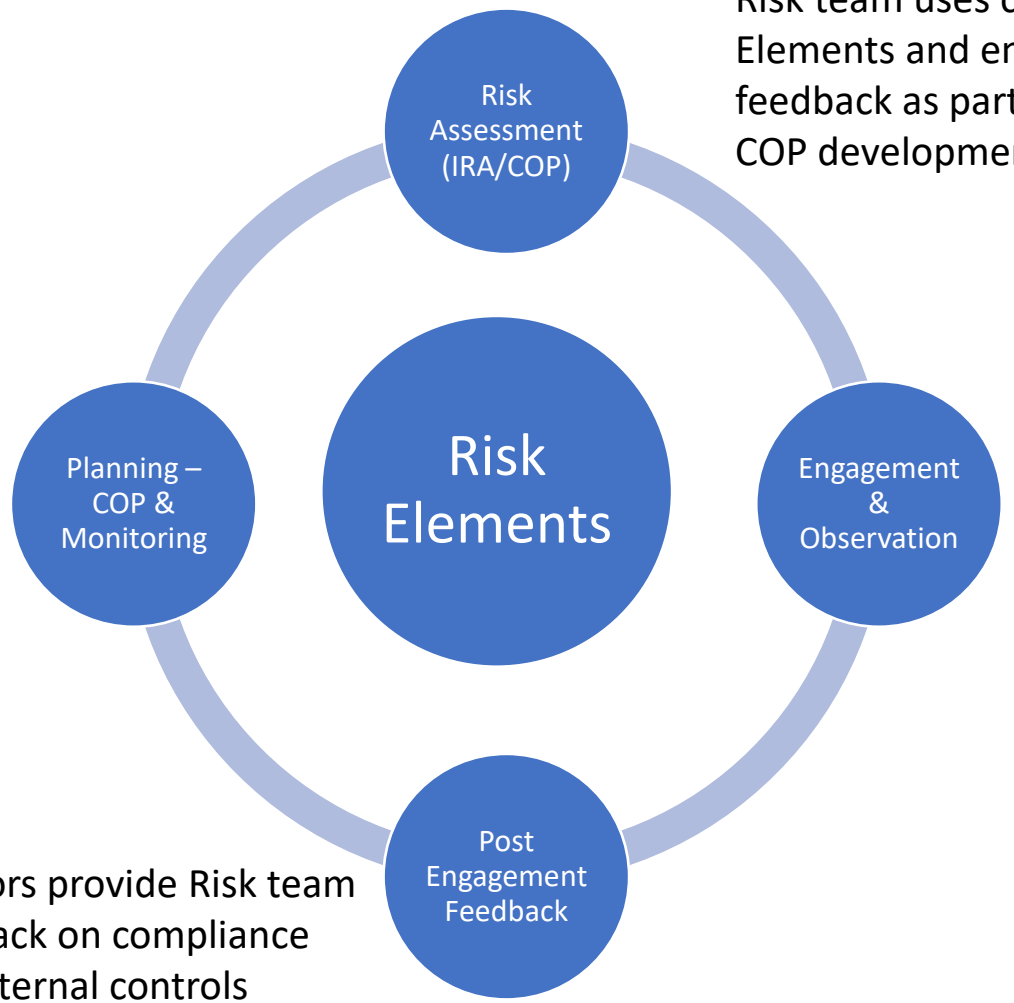
Slido Question

In your opinion, which area of focus do you believe poses the highest risk to the BPS?

- ❑ *Remote Connectivity*
- ❑ *Supply Chain*
- ❑ *Physical Security*
- ❑ *Incident Response*
- ❑ *Transmission Planning and Modeling*
- ❑ *Inverter-Based Resources*
- ❑ *Facility Ratings*
- ❑ *Extreme Weather Response*

Tying it All Together

Risk team uses current Risk Elements and engagement feedback as part of IRA and COP development process



Auditors will sample and look at internal controls during engagements

Post Engagement Feedback: Auditors provide Risk team feedback on compliance and internal controls

Planning – COP & Monitoring: Engagement feedback may impact monitoring interval, scope, method, or sampling

TEXAS RE
Ensuring electric reliability for Texans

Common and High-Risk Violations: A View from Texas RE Enforcement

William Sanders, Cybersecurity Principal
Alexander Petak, Enforcement Attorney

Why We Are Here

Data trends in Enforcement

Explanation of most violated standards

Why are we telling you this information?

- Awareness in preventing, catching, and reporting

Most Reported Standards

2022			
ERO		Texas RE	
Standard	**Count**	**Standard**	**Count**
CIP-010	240	CIP-003	15
CIP-004	238	PRC-005	13
CIP-007	173	MOD-025	12
CIP-003	125	PRC-024	11
CIP-006	107	PRC-019	9
PRC-005	99	BAL-001	8
PRC-024	75	FAC-008	8
MOD-025	73	MOD-026	8
FAC-008	67	MOD-027	8
CIP-011	58	CIP-010	7

2023			
ERO		Texas RE	
Standard	**Count**	**Standard**	**Count**
CIP-007	226	CIP-003	25
CIP-010	210	MOD-025	20
CIP-004	171	FAC-008	20
CIP-003	121	CIP-010	17
FAC-008	98	CIP-007	17
MOD-025	77	MOD-026	12
PRC-005	75	CIP-004	12
CIP-006	73	MOD-027	11
PRC-024	53	VAR-002	11
CIP-002	44	CIP-005	11

2024			
ERO		Texas RE	
Standard	**Count**	**Standard**	**Count**
CIP-010	146	FAC-008	16
CIP-007	143	CIP-003	12
CIP-004	124	VAR-002	11
CIP-003	109	MOD-025	10
CIP-006	82	CIP-004	10
PRC-005	68	MOD-026	8
FAC-008	63	CIP-010	7
MOD-025	61	MOD-027	7
CIP-002	56	PRC-005	6
VAR-002	44	CIP-007	5

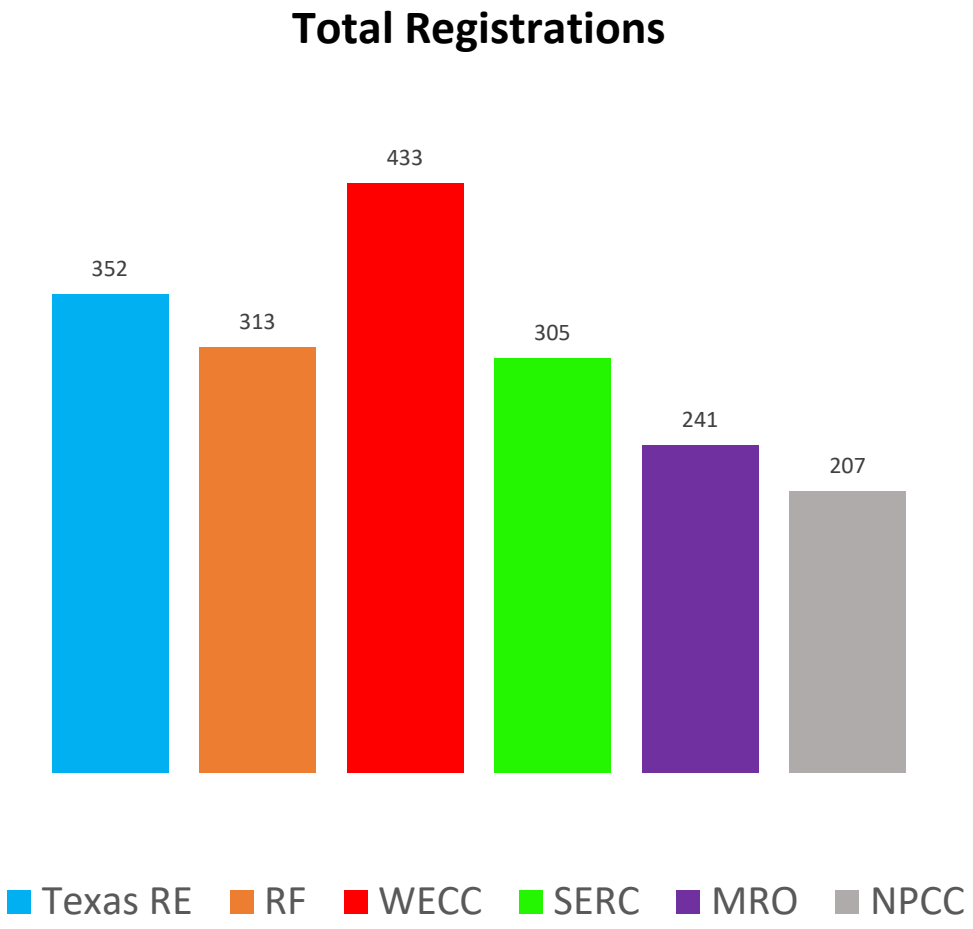
Most Reported Standards—CIP and O&P

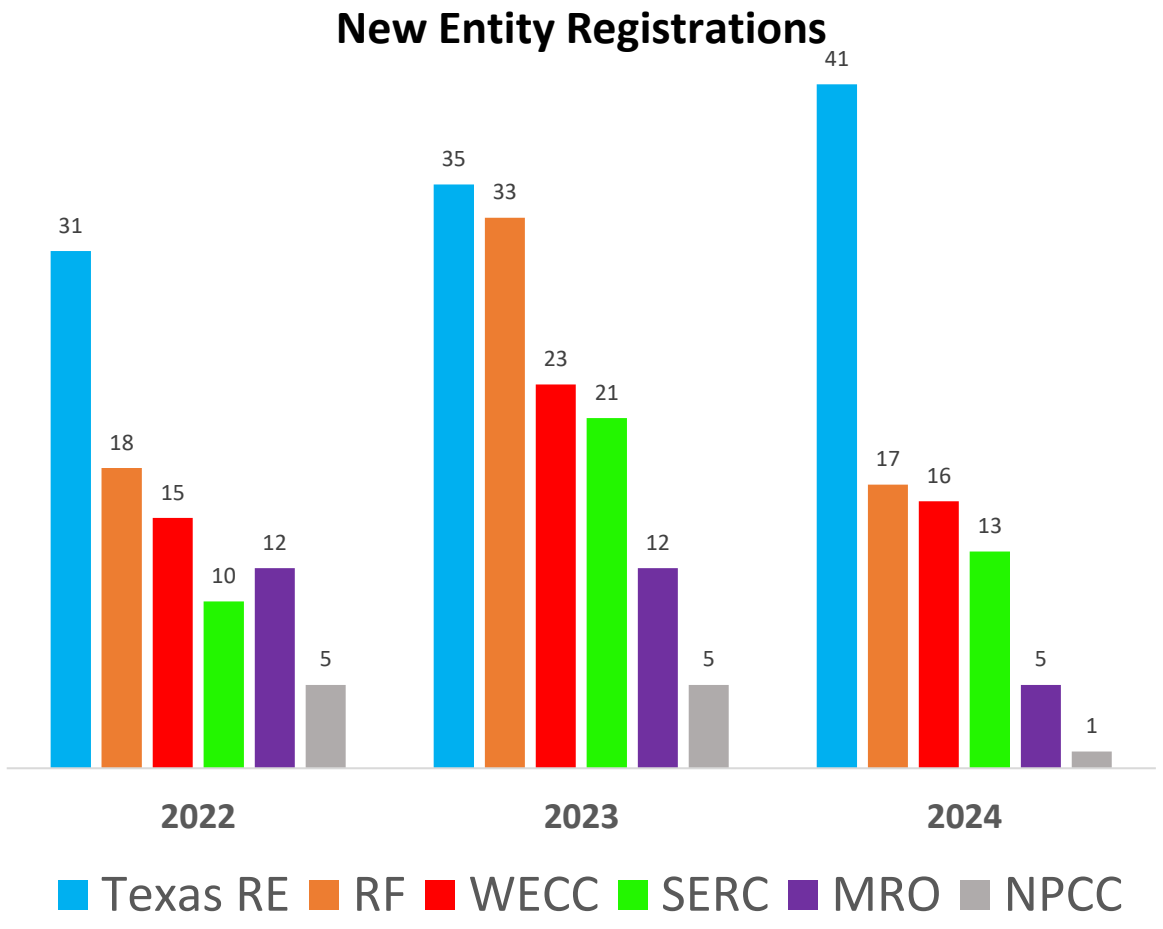
2022			
ERO		Texas RE	
Standard	Count	Standard	Count
CIP-010	240	CIP-003	15
CIP-004	238	PRC-005	13
CIP-007	173	MOD-025	12
CIP-003	125	PRC-024	11
CIP-006	107	PRC-019	9
PRC-005	99	BAL-001	8
PRC-024	75	FAC-008	8
MOD-025	73	MOD-026	8
FAC-008	67	MOD-027	8
CIP-011	58	CIP-010	7

2023			
ERO		Texas RE	
Standard	Count	Standard	Count
CIP-007	226	CIP-003	25
CIP-010	210	MOD-025	20
CIP-004	171	FAC-008	20
CIP-003	121	CIP-010	17
FAC-008	98	CIP-007	17
MOD-025	77	MOD-026	12
PRC-005	75	CIP-004	12
CIP-006	73	MOD-027	11
PRC-024	53	VAR-002	11
CIP-002	44	CIP-005	11

2024			
ERO		Texas RE	
Standard	Count	Standard	Count
CIP-010	146	FAC-008	16
CIP-007	143	CIP-003	12
CIP-004	124	VAR-002	11
CIP-003	109	MOD-025	10
CIP-006	82	CIP-004	10
PRC-005	68	MOD-026	8
FAC-008	63	CIP-010	7
MOD-025	61	MOD-027	7
CIP-002	56	PRC-005	6
VAR-002	44	CIP-007	5

New Entity Registrations





Most Reported Standards

2022

ERO		Texas RE	
Standard	**Count**	**Standard**	**Count**
CIP-010	240	CIP-003	15
CIP-004	238	PRC-005	13
CIP-007	173	MOD-025	12
CIP-003	125	PRC-024	11
CIP-006	107	PRC-019	9
PRC-005	99	BAL-001	8
PRC-024	75	FAC-008	8
MOD-025	73	MOD-026	8
FAC-008	67	MOD-027	8
CIP-011	58	CIP-010	7

2023

ERO		Texas RE	
Standard	**Count**	**Standard**	**Count**
CIP-007	226	CIP-003	25
CIP-010	210	MOD-025	20
CIP-004	171	FAC-008	20
CIP-003	121	CIP-010	17
FAC-008	98	CIP-007	17
MOD-025	77	MOD-026	12
PRC-005	75	CIP-004	12
CIP-006	73	MOD-027	11
PRC-024	53	VAR-002	11
CIP-002	44	CIP-005	11

2024

ERO		Texas RE	
Standard	**Count**	**Standard**	**Count**
CIP-010	146	FAC-008	16
CIP-007	143	CIP-003	12
CIP-004	124	VAR-002	11
CIP-003	109	MOD-025	10
CIP-006	82	CIP-004	10
PRC-005	68	MOD-026	8
FAC-008	63	CIP-010	7
MOD-025	61	MOD-027	7
CIP-002	56	PRC-005	6
VAR-002	44	CIP-007	5

Risks Associated with Most Violated Standards

Standard	Description
CIP-007	Covers patching, antivirus, and passwords.
CIP-010	Vulnerability management, transient devices
CIP-003	Firewall rules, transient devices

Texas RE	
2022	
Standard	**Count**
CIP-003	15
PRC-005	13
MOD-025	12
PRC-024	11
PRC-019	9
BAL-001	8
FAC-008	8
MOD-026	8
MOD-027	8
CIP-010	7

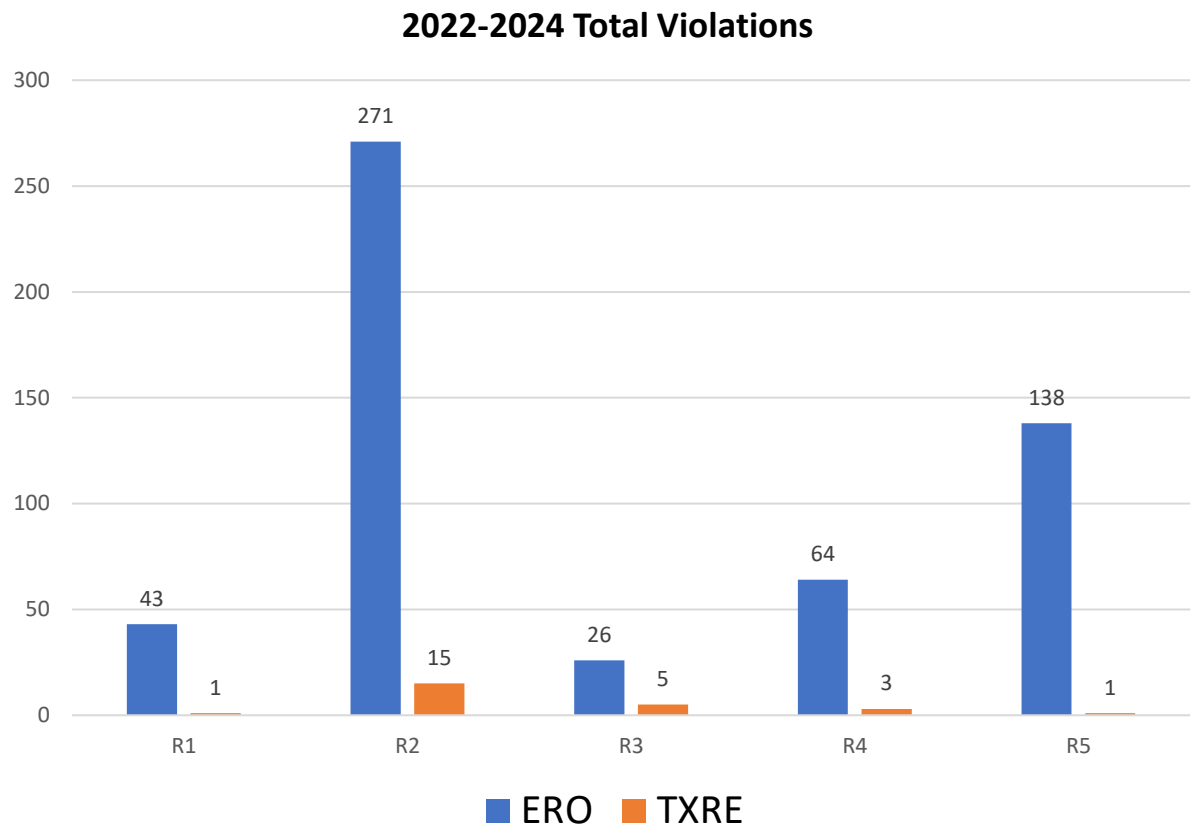
Texas RE	
2023	
Standard	**Count**
CIP-003	25
MOD-025	20
FAC-008	20
CIP-010	17
CIP-007	17
MOD-026	12
CIP-004	12
MOD-027	11
VAR-002	11
CIP-005	11

Texas RE	
2024	
Standard	**Count**
FAC-008	16
CIP-003	12
VAR-002	11
MOD-025	10
CIP-004	10
MOD-026	8
CIP-010	7
MOD-027	7
PRC-005	6
CIP-007	5

CIP-007 | Systems Security Management

CIP-007

- R1: Ports and Services
- R2: Patching
- R3: Antivirus
- R4: Logging
- R5: Password management



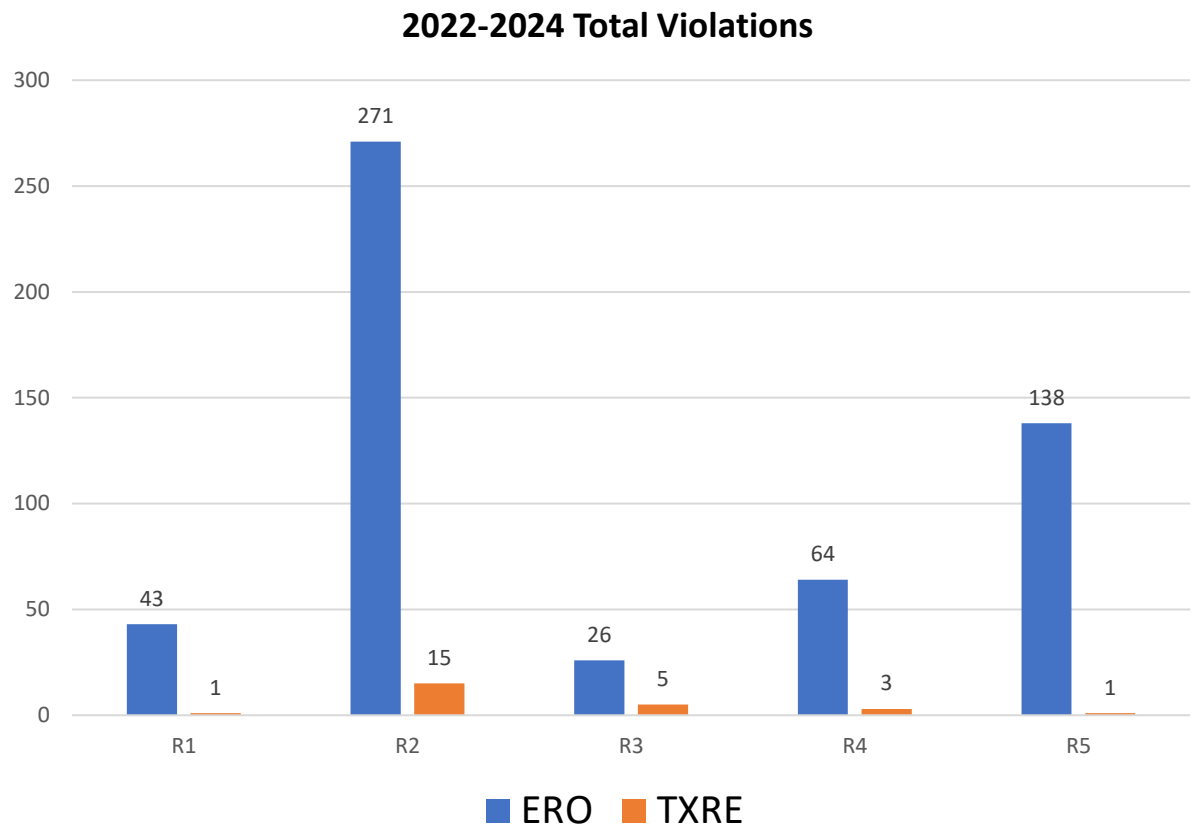
CIP-007 | Systems Security Management

Patching

- Patching is a high frequency activity
- Create recurring tasks
- Train users on how to evaluate patches

Password management

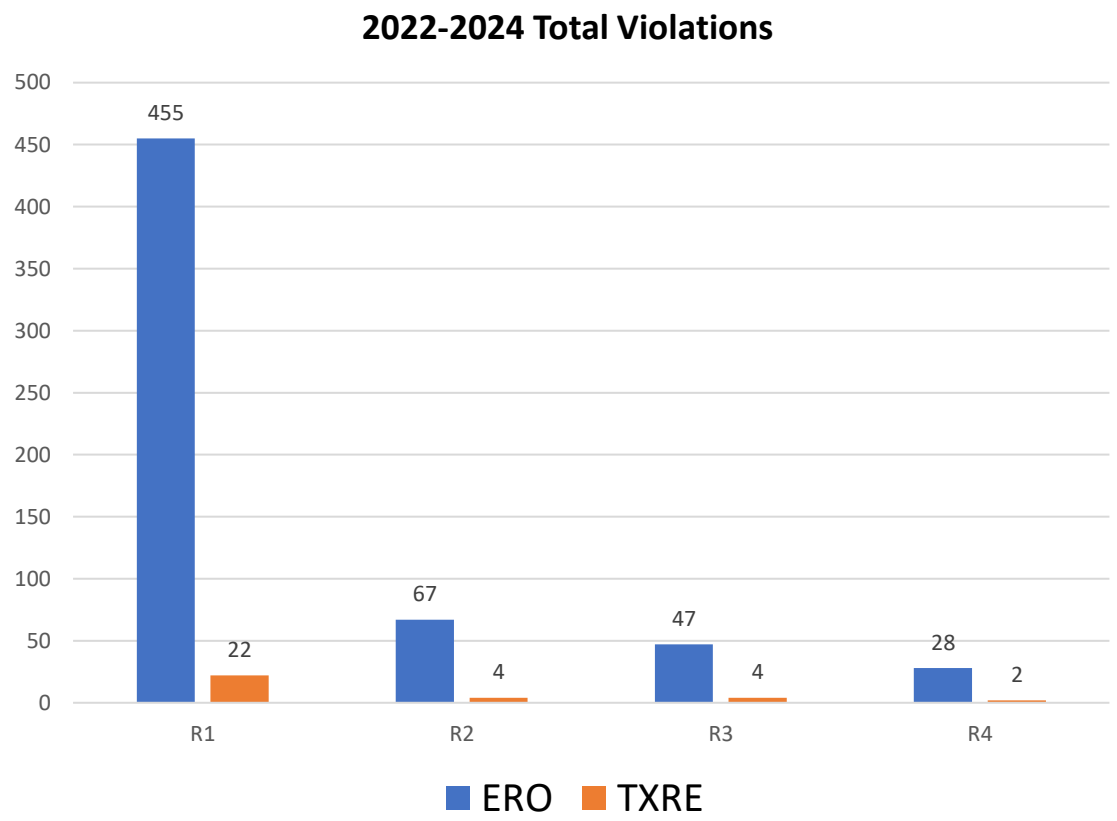
- Low frequency, high volume activity
- Create recurring tasks
- Use technical controls where safe and feasible



CIP-010 | Configuration Change Management and Vulnerability Assessments

CIP-010

- R1: Baseline management
- R2: Baseline monitoring
- R3: Vulnerability assessments
- R4: Transient Cyber Asset and Removable Media management



CIP-010 | Configuration Change Management and Vulnerability Assessments

Baseline management

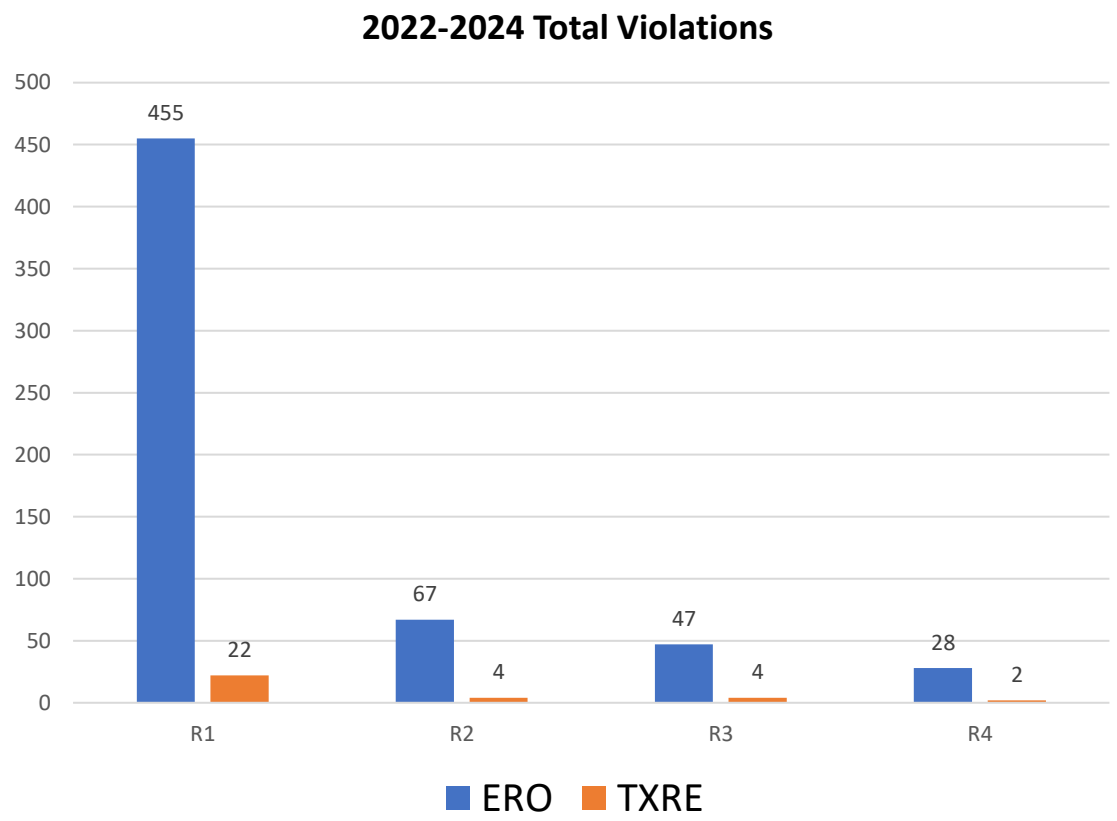
- High frequency activity
- Create recurring tasks and reminders
- Reinforce diligence among users

Vulnerability assessments

- Periodic activity
- Standard does not allow for vulnerability acceptance
- For vulnerabilities that will be mitigated create thorough documentation and review as necessary

Transient Cyber Asset and Removable Media management

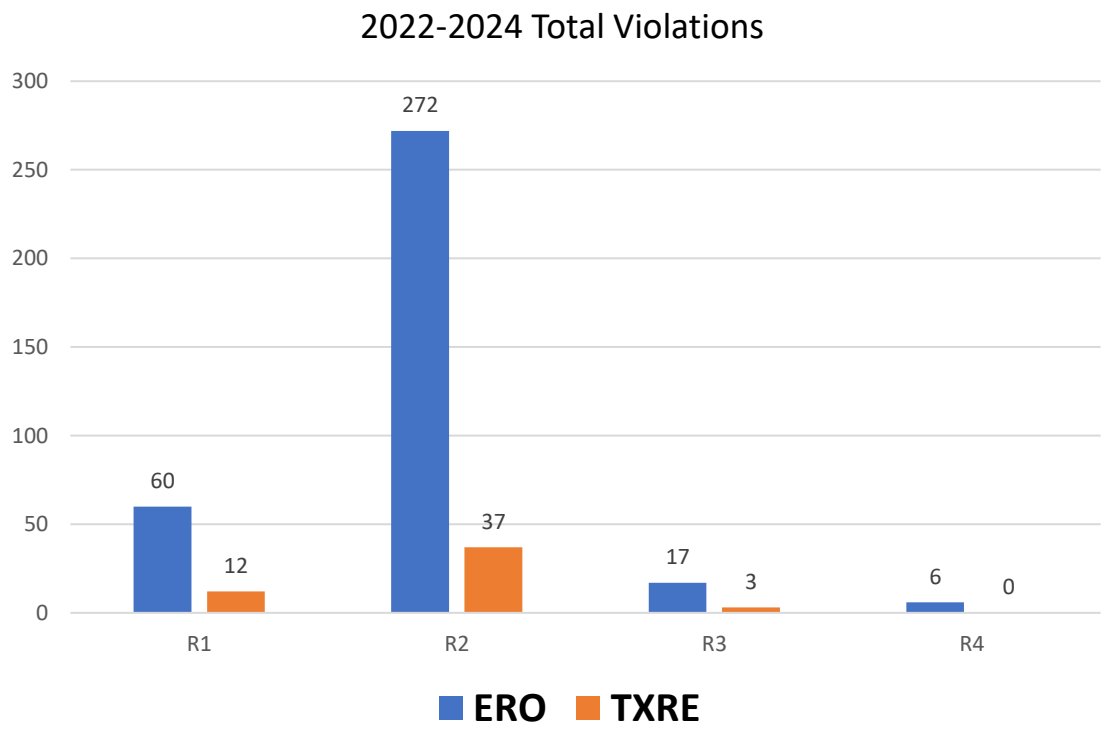
- Ongoing or on-demand activity
- Potentially high risk, depending on program implementation
- Review program and make modifications as necessary



CIP-003 | Security Management Controls

CIP-003

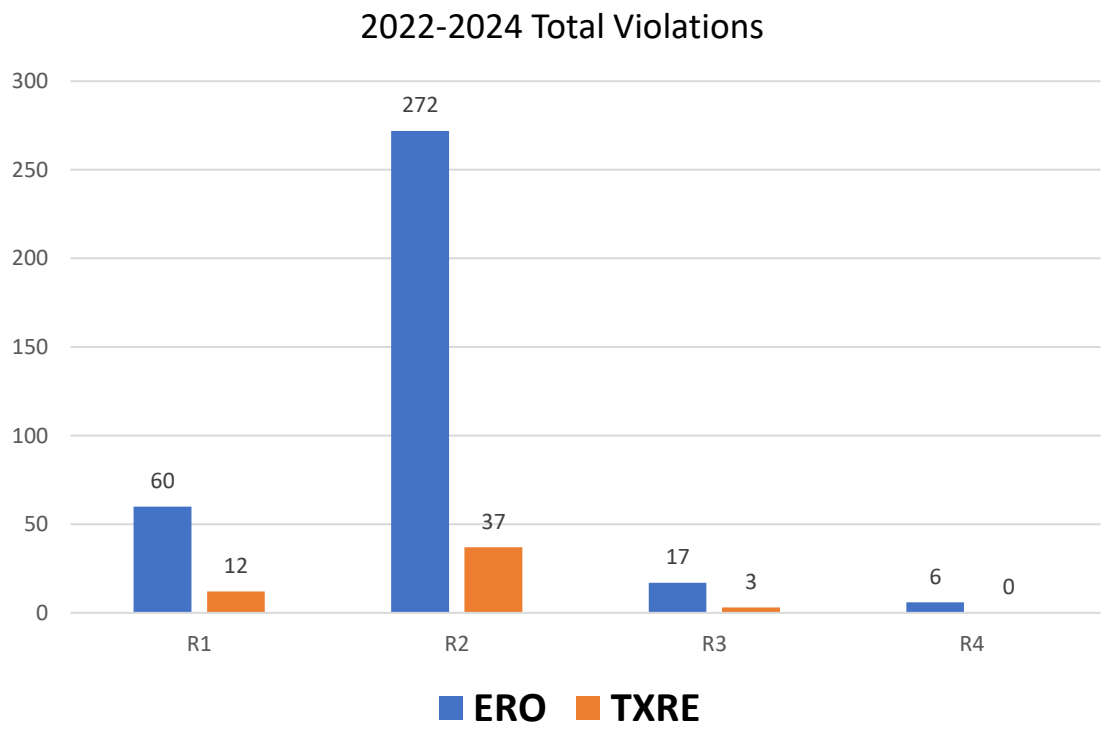
- R1: Policy documents
- R2: Cybersecurity Plan
- R3: CIP Senior Manager identification
- R4: CIP Senior Manager authority delegation



CIP-003 | Security Management Controls

CIP-003 Cybersecurity Plan

- Cybersecurity Awareness
- Physical Security Controls
- Electronic Access Controls
- Cybersecurity Incident Response
- Transient Cyber Asset and Removable Media management



Reporting Information

What we want to see when reporting issues

- General information
  - Relevant start and end dates
  - Full description of what happened
  - What was the cause
  - Mitigation, both to end the issue and to prevent recurrence
- Extent of Condition Review
- Risk
  - Other safety measures in place
  - Whether trips or Misoperations actually occurred
  - Generation involved

Comprehensive Internal Compliance Program

Internal Detection and Prevention Controls

- Training, supervision, incentives for catching issues, quick response time
- Compliance tracking software - track deadlines and review compliance

Catch potential issues before they turn into violations

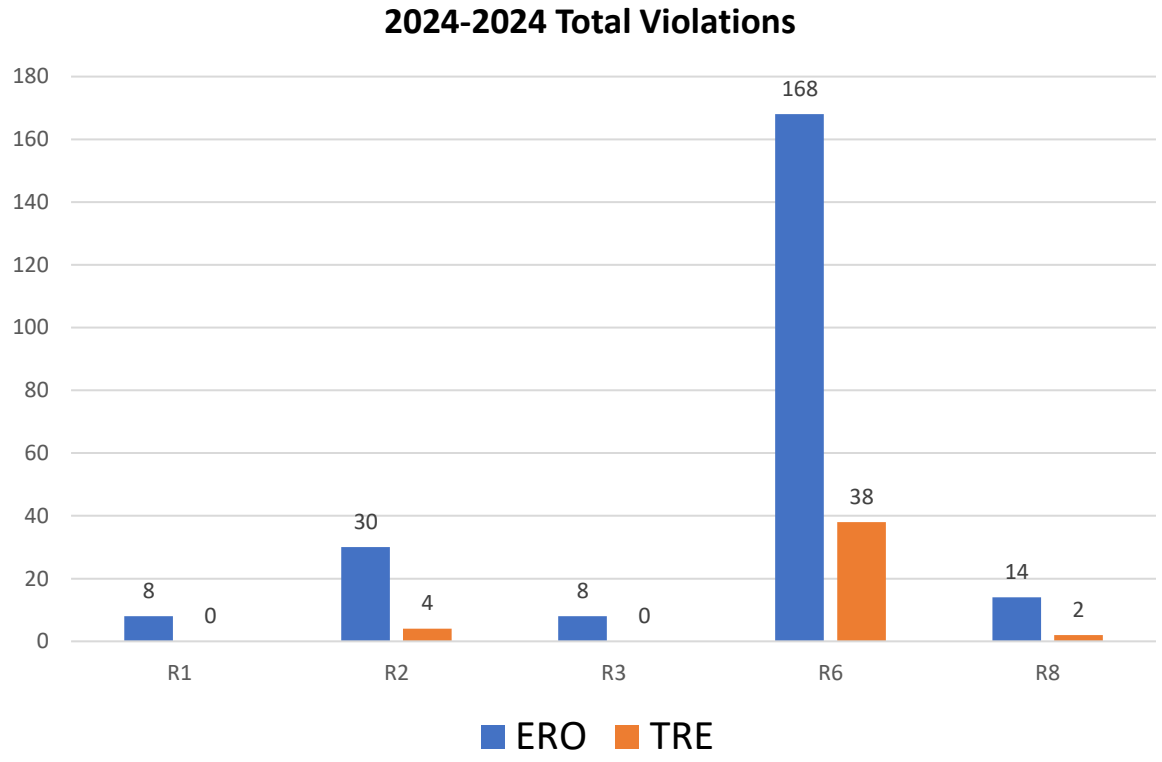
- Can prevent issues from happening
- Can detect issues early, so that durations don’t become extended

Looked upon favorably when penalties are being considered

FAC-008 | Facility Ratings

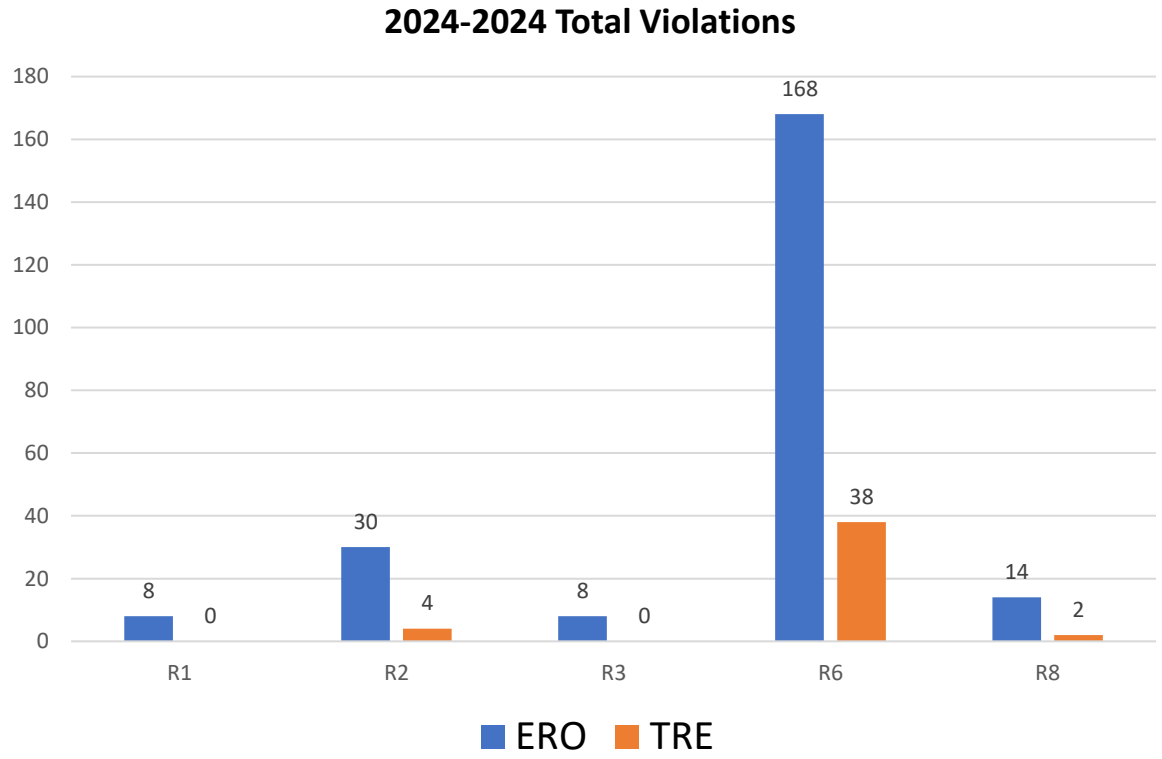
FAC-008

- R2: GOs having methodology between R1 and POI
- R6: Facility Ratings matching methodology



FAC-008 | Facility Ratings

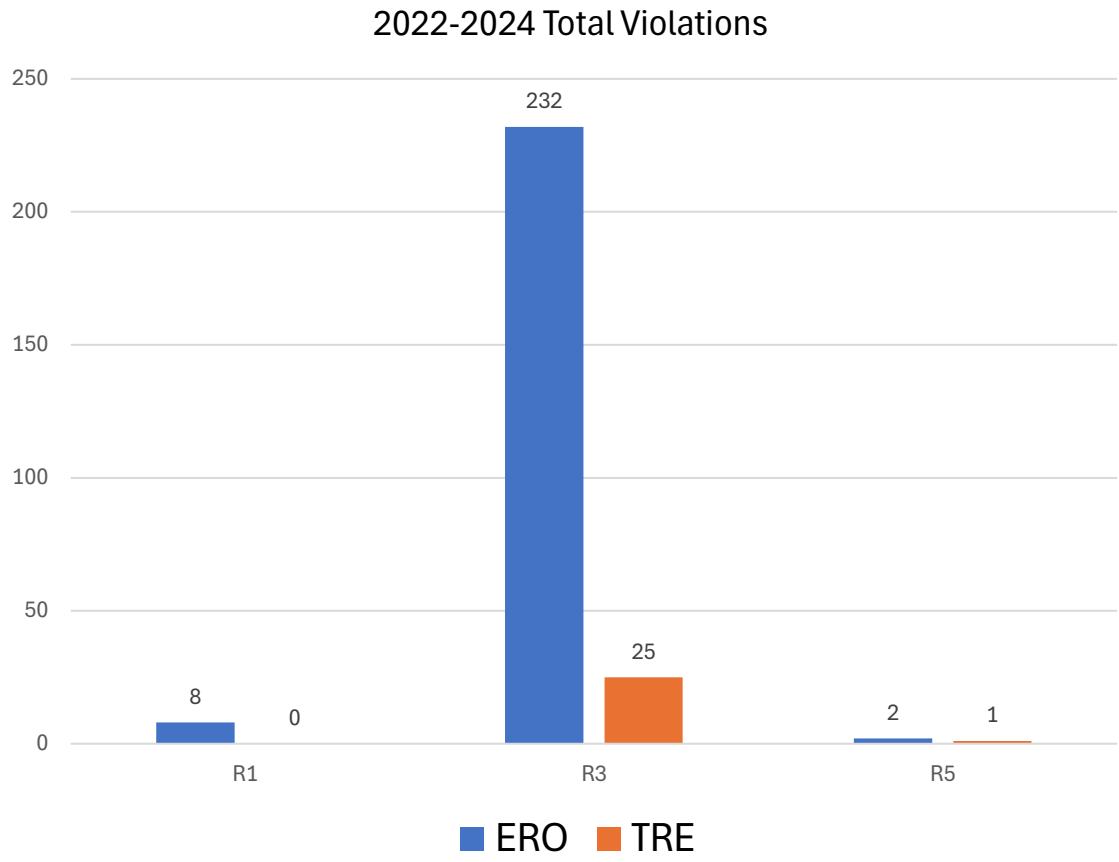
- Input errors on spreadsheets
- Equipment that is missed
- Incomplete one-line diagrams
- High and Low issues



PRC-005 | Protection System Maintenance Program | PSMP

R1 – Have a PSMP for Protection Systems, Automatic Reclosing, and Sudden Pressure Relaying

R3 - Perform maintenance at appropriate intervals

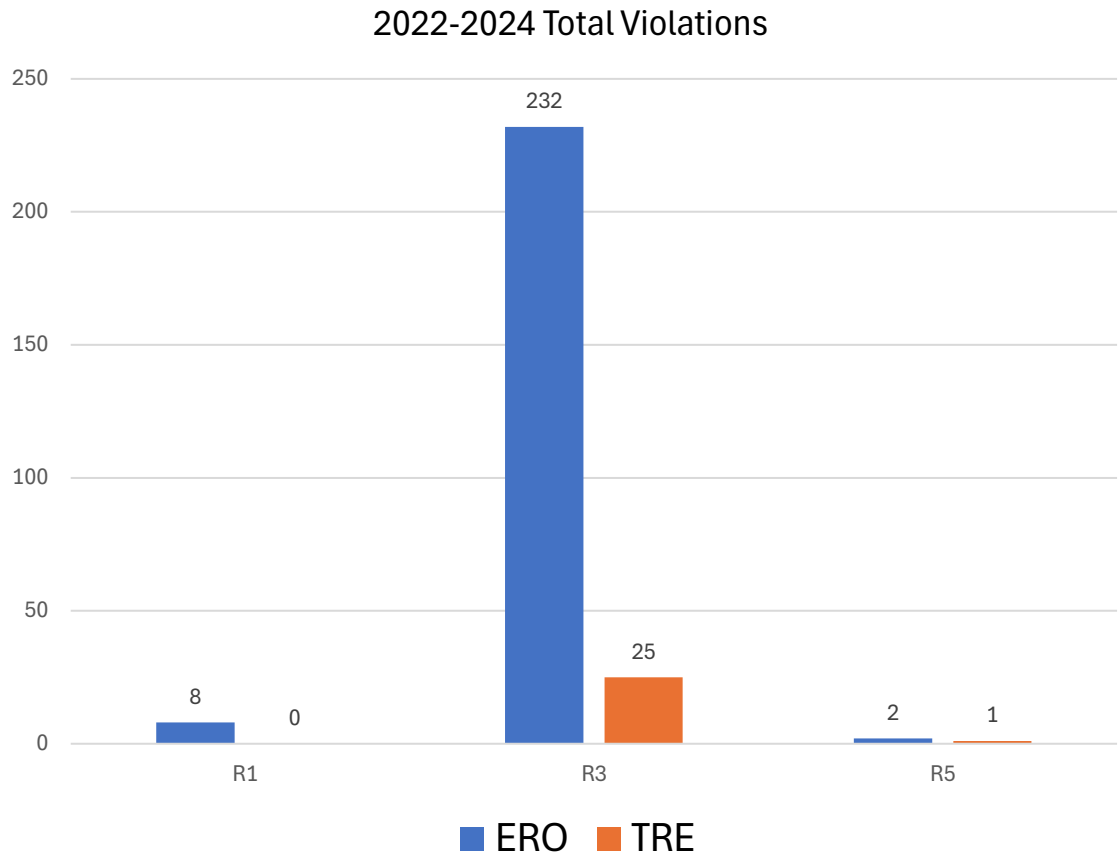


PRC-005 | Protection System Maintenance Program | PSMP

Lots of different types of equipment to maintain, all operating on different maintenance schedules

Insufficient checklists, records

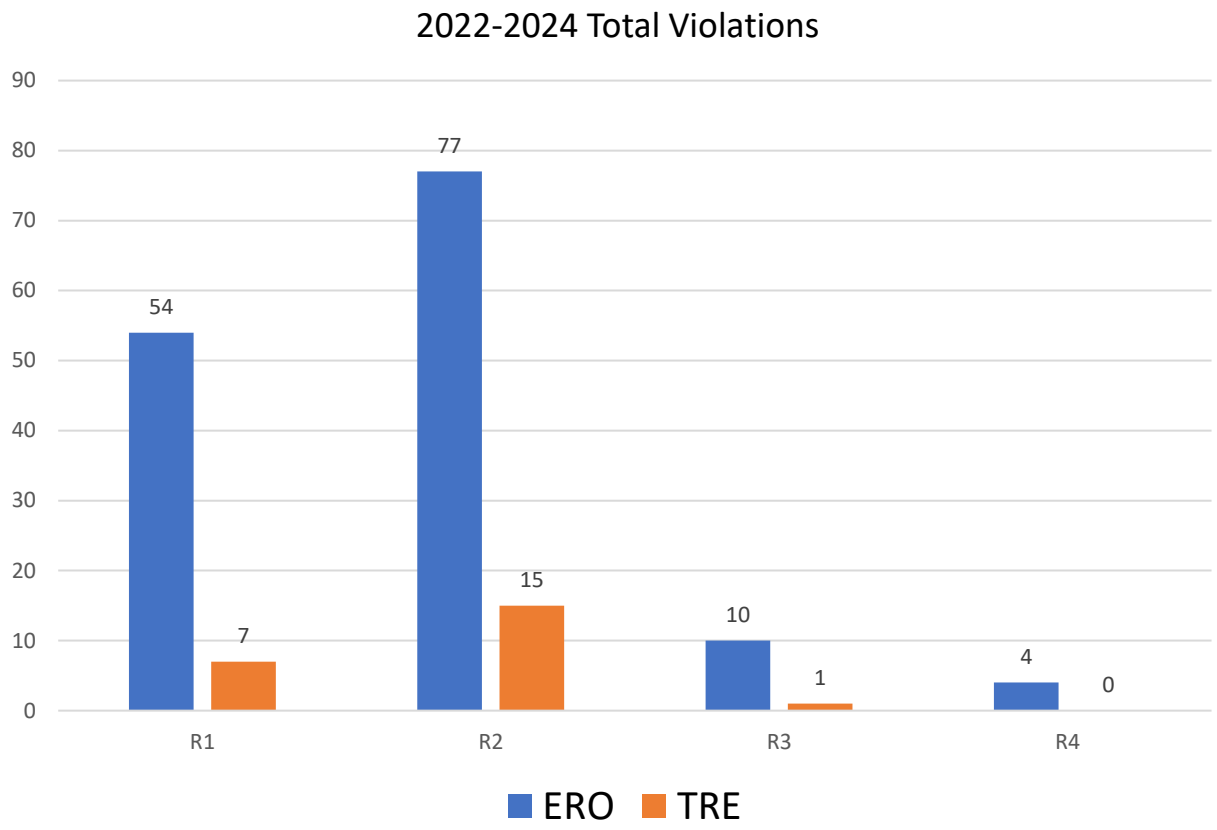
Inadequate discovery devices to catch missed intervals leads to long durations



PRC-024 | Settings Within “No Trip Zone"

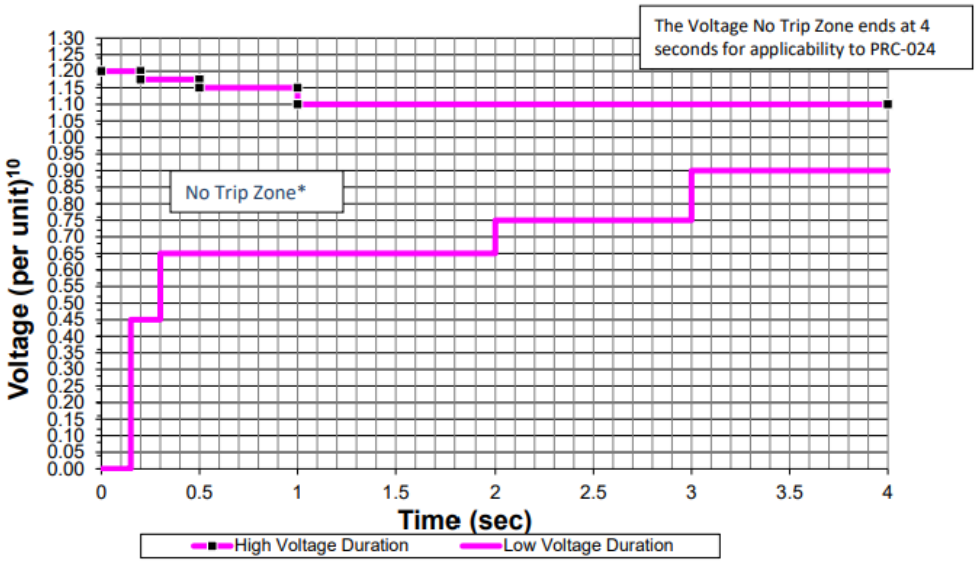
PRC-024

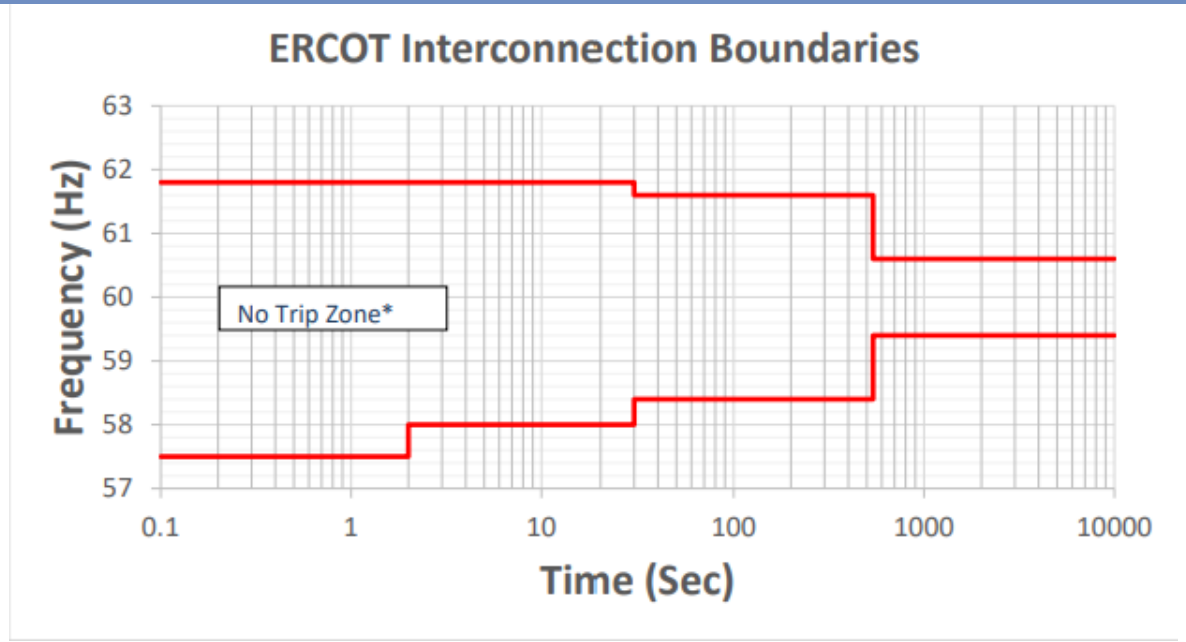
- R1: Frequency
- R2: Voltage
- R3: Recorded Limitations



PRC-024 | Settings Within “No Trip Zone"

- Confirming settings when changed
- Not understanding rule when settings put in place



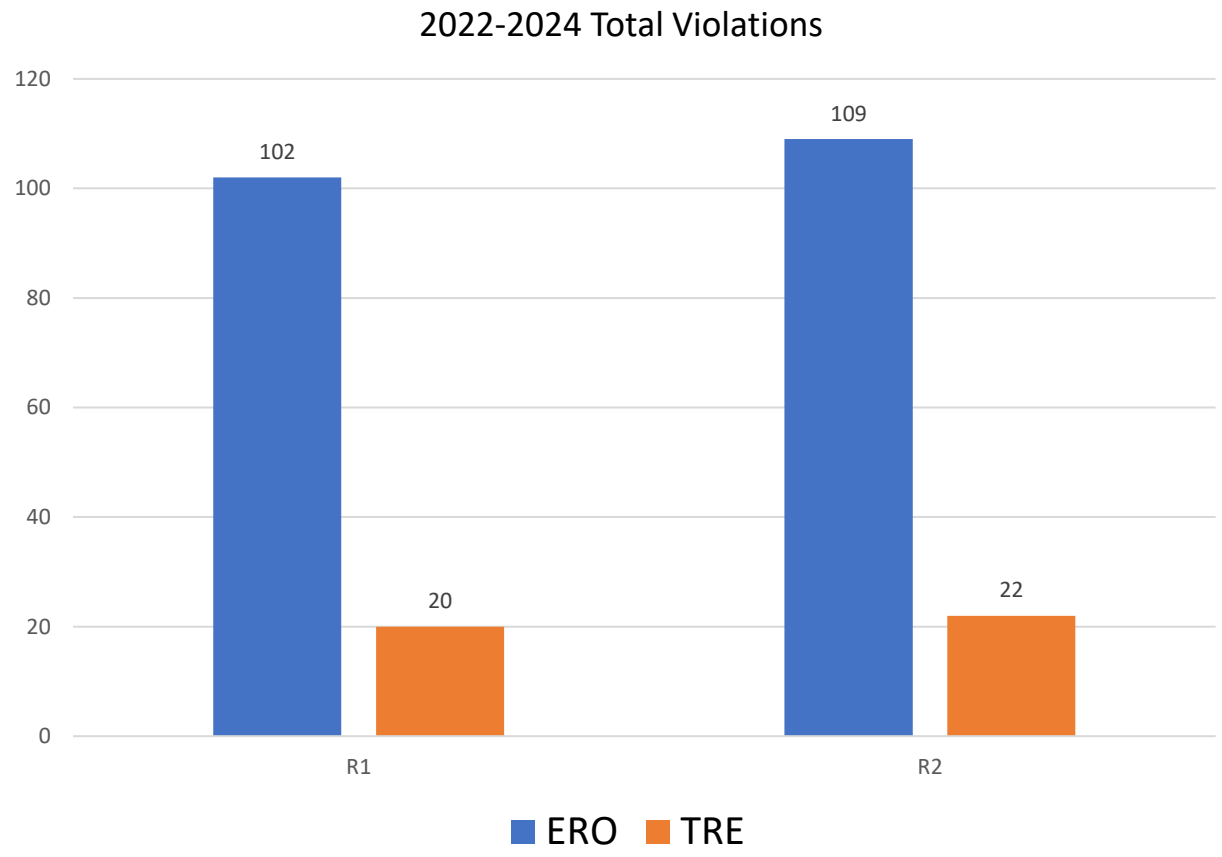


Low side voltage can’t be on the line, others can be

MOD-025 | Verify Real/Reactive Power

MOD-025

- R1: Verify Real Power
- R2: Verify Reactive Power
- Submit verification to Transmission Planner within 90 days

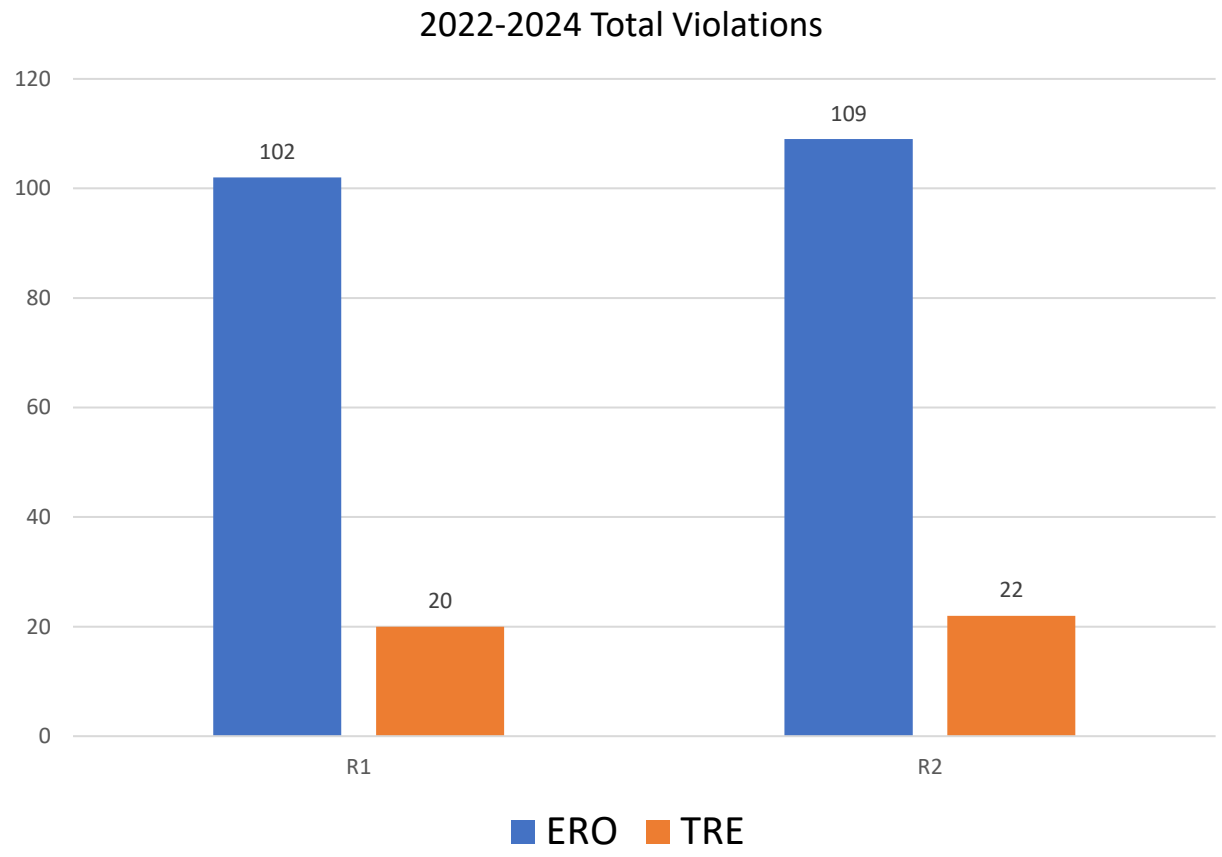


MOD-025 | Verify Real/Reactive Power

Unaware of deadlines

Don’t give enough lead time to contractor

Unexpected delays in modeling, waiting for right conditions



Settlements Filed Since 2020

With monetary penalties: CIP-007, CIP-010, FAC-008

Without monetary penalties: CIP-005, CIP-007 and CIP-010, IRO-010 and TOP-001

For FAC cases, long durations, multiple Facilities and incorrect overall Facility Ratings

For CIP cases – long durations, many machines, large size of Facilities, multiple violations across Standards found at same time

TEXAS RE
Ensuring electric reliability for Texans

Wrap-Up

Thank you for coming!

You will receive a short survey via e-mail. Please complete it to help Texas RE develop future outreach.