OT/IT SECURITY: A BRIEF OVERVIEW OF CONCEPTS AND RESOURCES

Ernesto Ballesteros, JD, MS, CISSP, CISA
Cybersecurity State Coordinator of Texas
Region VI | Cybersecurity and Infrastructure Security Agency

About CISA

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

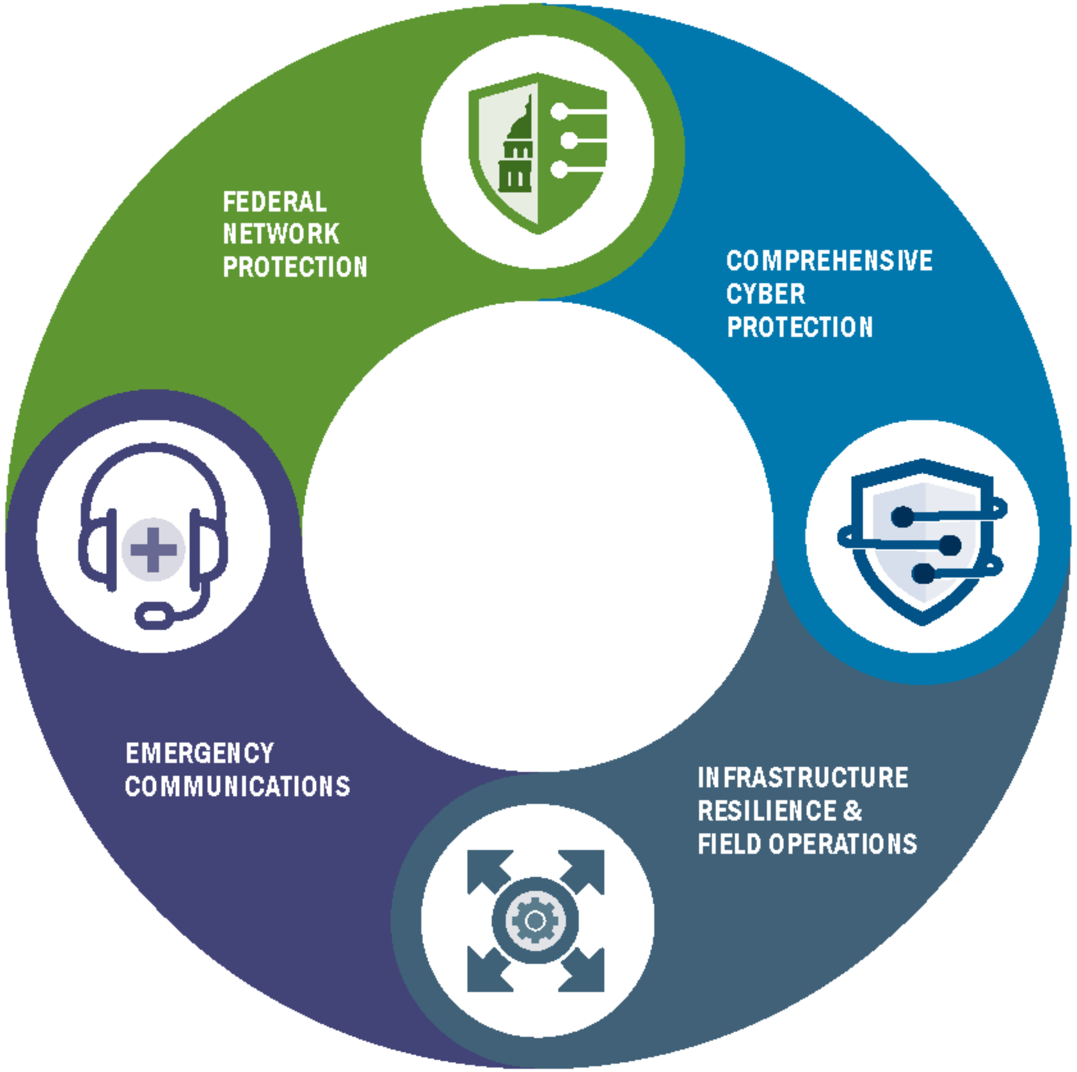
Strengthen critical infrastructure and address long-term risks

months | years | decades

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

We are the Nation's Risk Advisor

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure


FEDERAL NETWORK PROTECTION
COMPREHENSIVE CYBER PROTECTION
INFRASTRUCTURE RESILIENCE & FIELD OPERATIONS
EMERGENCY COMMUNICATIONS

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

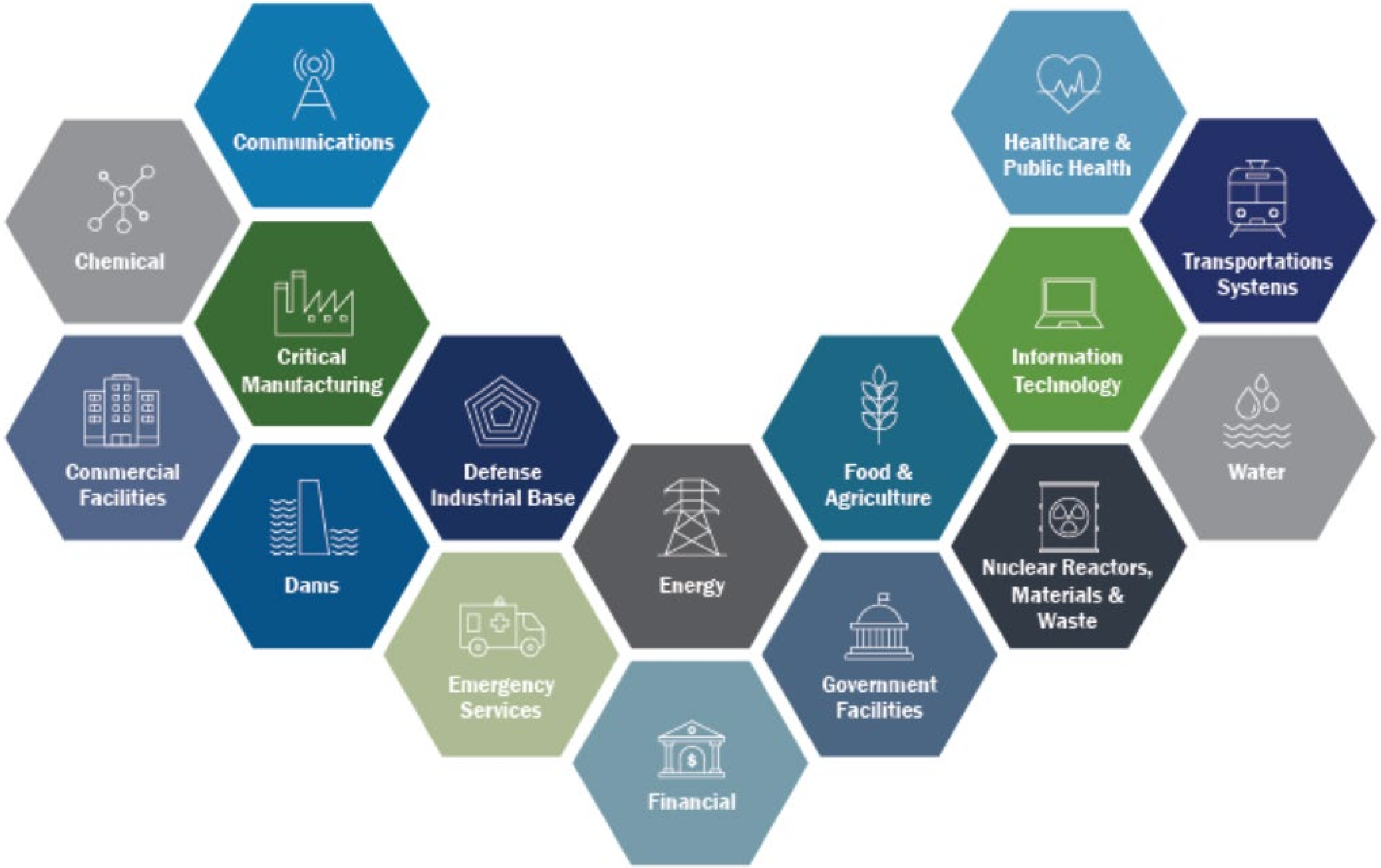
Our Work

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future

- PARTNERSHIP DEVELOPMENT
- INFORMATION AND DATA SHARING
- CAPACITY BUILDING
- INCIDENT MANAGEMENT & RESPONSE
- RISK ASSESSMENT AND ANALYSIS
- NETWORK DEFENSE
- EMERGENCY COMMUNICATIONS

Critical Infrastructure Sectors

CISA assists the public and private sectors to secure their networks and focuses on organizations in the following 16 critical infrastructure sectors.



Communications

Chemical

Critical Manufacturing

Commercial Facilities

Dams

Defense Industrial Base

Emergency Services

Energy

Financial

Food & Agriculture

Government Facilities

Healthcare & Public Health

Information Technology

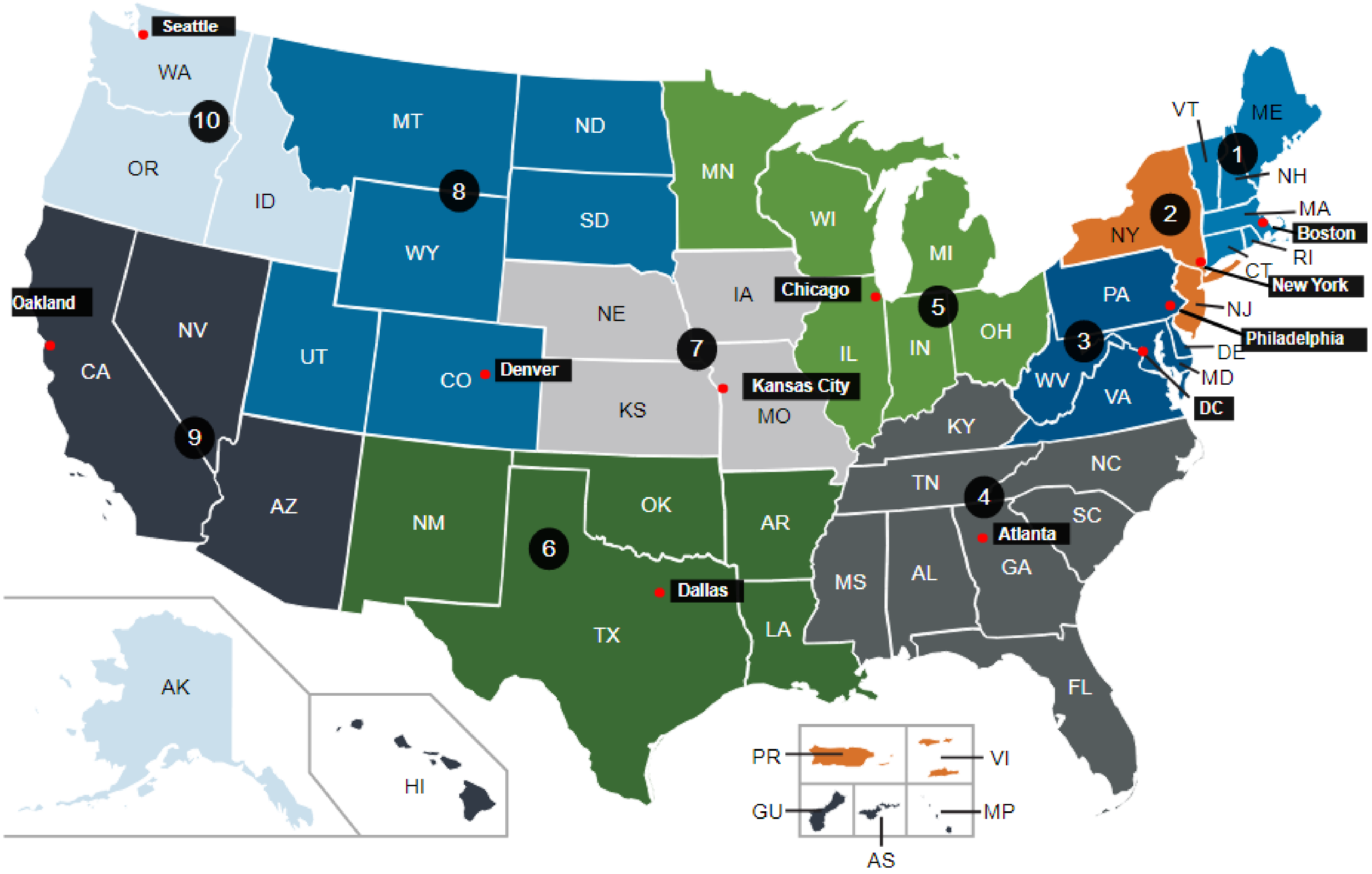
Nuclear Reactors, Materials & Waste

Transportations Systems

Water

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



CISA Region 6: CISARegion6@hq.dhs.gov

Cybersecurity State Coordinator Authorities

The role of the Cybersecurity State Coordinator is to serve as the principal point of contact for non-Federal entities to engage the Federal Government on preparing, managing, and responding to cyber incidents, as well as to build strategic public and private sector relationships, pursuant to 6 United States Code, Section 665(c) (2021) (Cybersecurity State Coordinator Act of 2020).

- Build strategic public and private sector relationships;
- Serve as the Federal cybersecurity risk advisor;
- Facilitate the sharing of cyber threat information;
- Raise awareness of cyber resources from the Federal Government to non-Federal entities;
- Support training, exercises, and planning for continuity of operations from cyber incidents;
- Serve as a principal point of contact for non-Federal entities to engage the Federal Government on preparing, managing, and responding to cyber incidents;
- Assist State, local, Tribal, and territorial governments in development of State cyber plans;
- Coordinate with appropriate officials within the Agency (CISA).

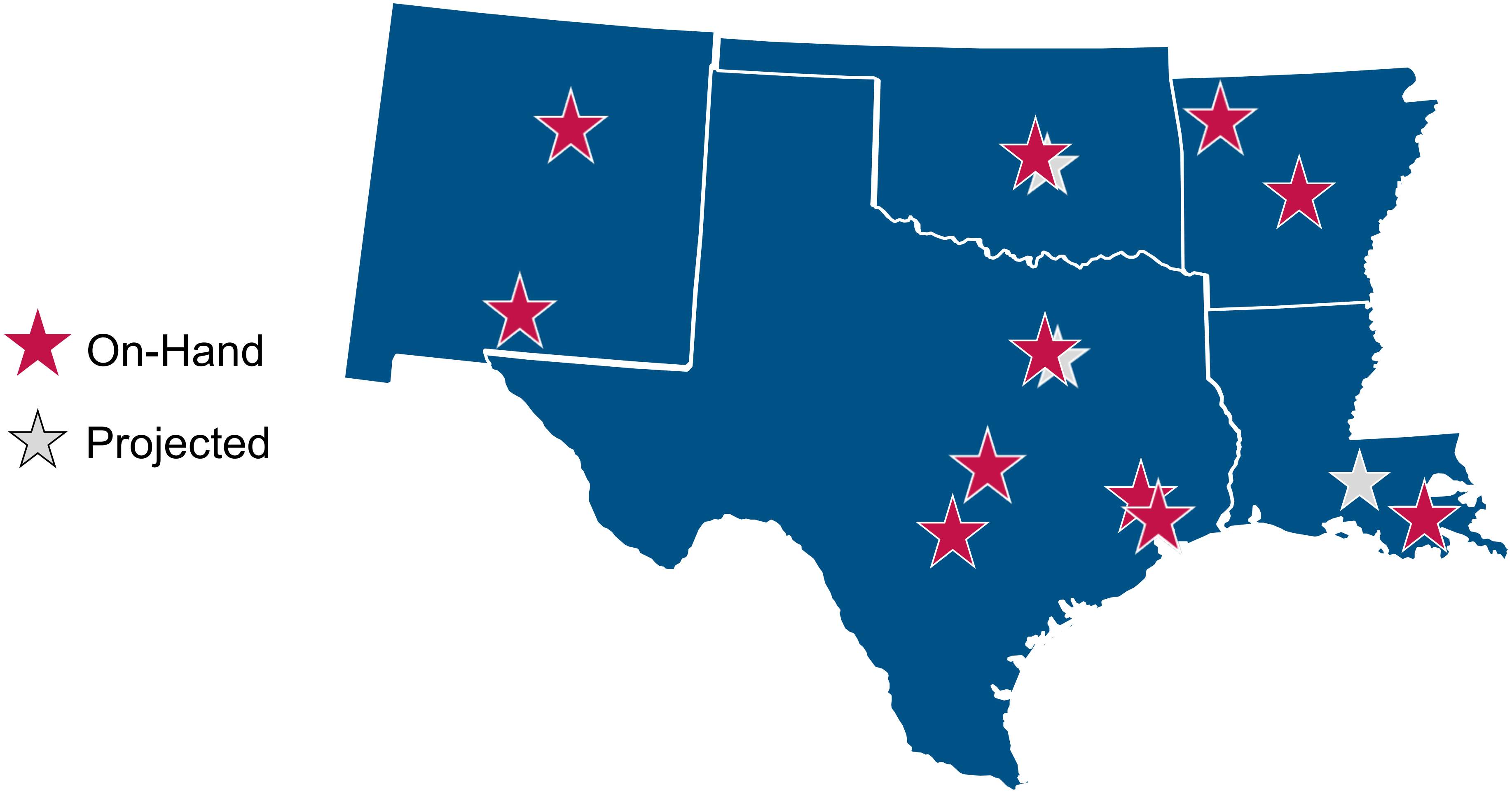
Cybersecurity State Coordinator of Texas: Ernesto Ballesteros
Email: ernesto.ballesteros@cisa.dhs.gov

Cybersecurity Advisors (CSAs)

To 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.

Reg 6 | On-Hand / Projected Cyber Personnel



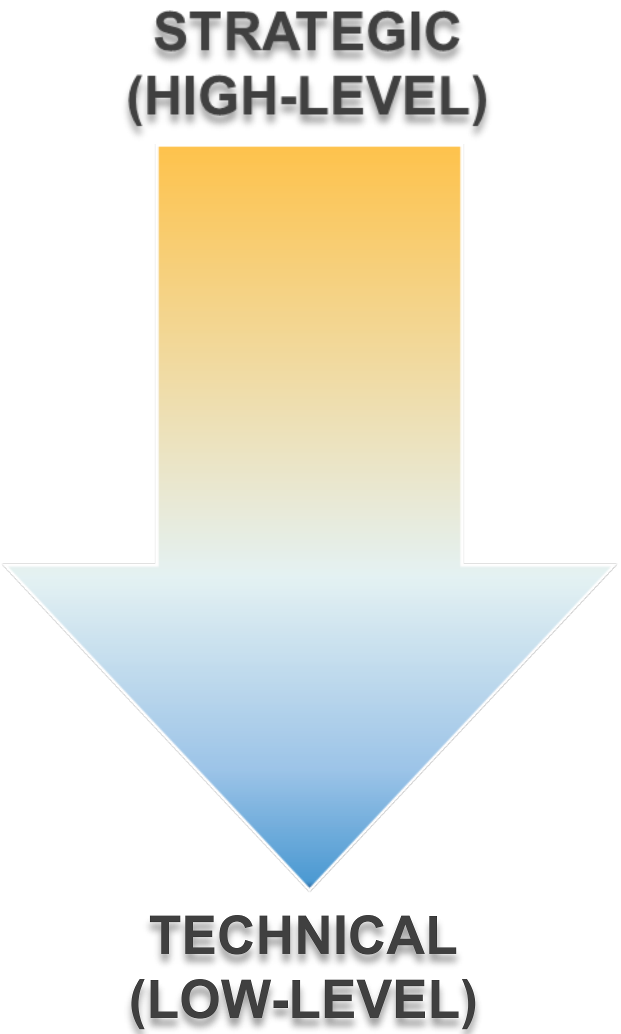
CISA Cybersecurity Resources

Regional Resources:

- Cybersecurity Assessments
  - ➢ Ransomware Readiness Assessment (RRA)
  - ➢ Cybersecurity Performance Goals (CPG)
  - ➢ Cyber Infrastructure Survey (CIS)
  - ➢ Cyber Resilience Essentials (CRE)
  - ➢ Incident Management Review (IMR)
  - ➢ Cyber Resilience Review (CRR)
  - ➢ External Dependencies Management (EDM)
- Workshops
  - ➢ Cyber Resilience Workshop (CRW)
  - ➢ Incident Management Workshop (IMW)
  - ➢ Vulnerability Management Workshop (VMW)
  - ➢ Digital Forensics Workshop I & II (DFW)
  - ➢ Cybersecurity Tabletop Exercise (CTTX)

National Resources:

- Vulnerability Scanning Service (CyHy)



Cybersecurity State Coordinator of Texas: Ernesto Ballesteros
Email: ernesto.ballesteros@cisa.dhs.gov

Core Concepts

What is cybersecurity?

Definition: cybersecurity

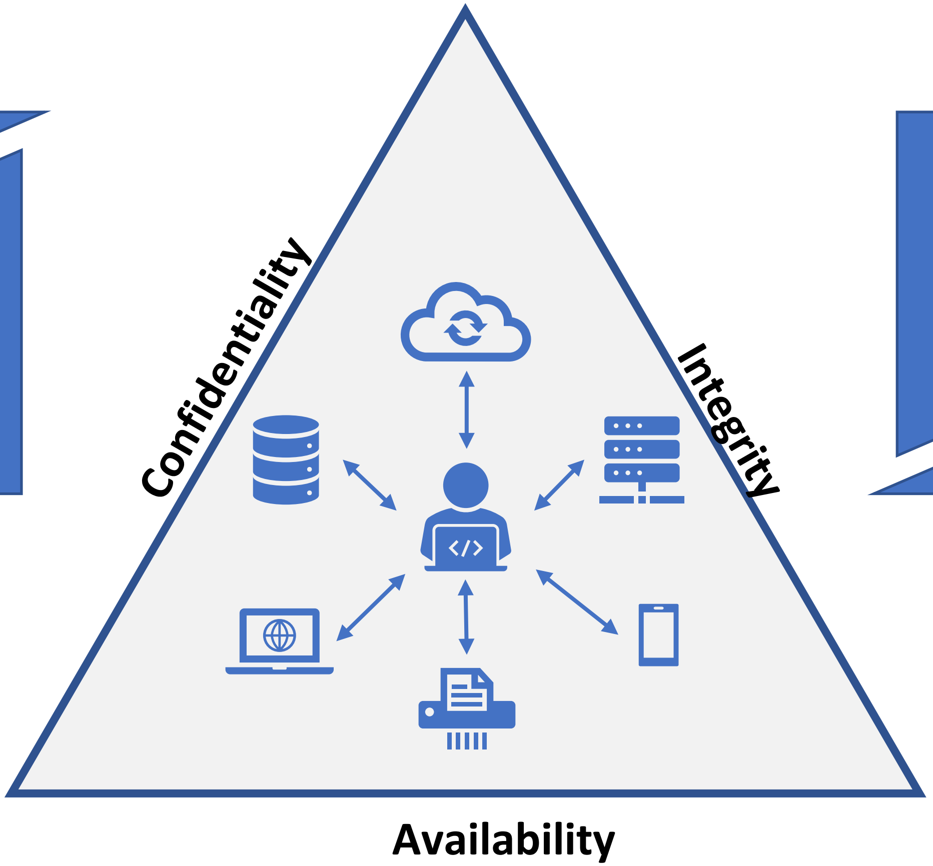
According to NIST, **cybersecurity** is *"[t]he protection of information and information systems against unauthorized access, use, disclosure, modification, or destruction in order to provide confidentiality, integrity, and availability."*

National Institute of Standards and Technology

Source: [NIST SP 800-171 Rev. 1]()

Information refers to *"[a]ny communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual."*

Source: [NIST SP 800-171 Rev. 1 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations]()



Information System refers to *"[a] discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."*

Source: [NIST SP 800-53 Rev. 4 Security and Privacy Controls for Federal Information Systems and Organization]()

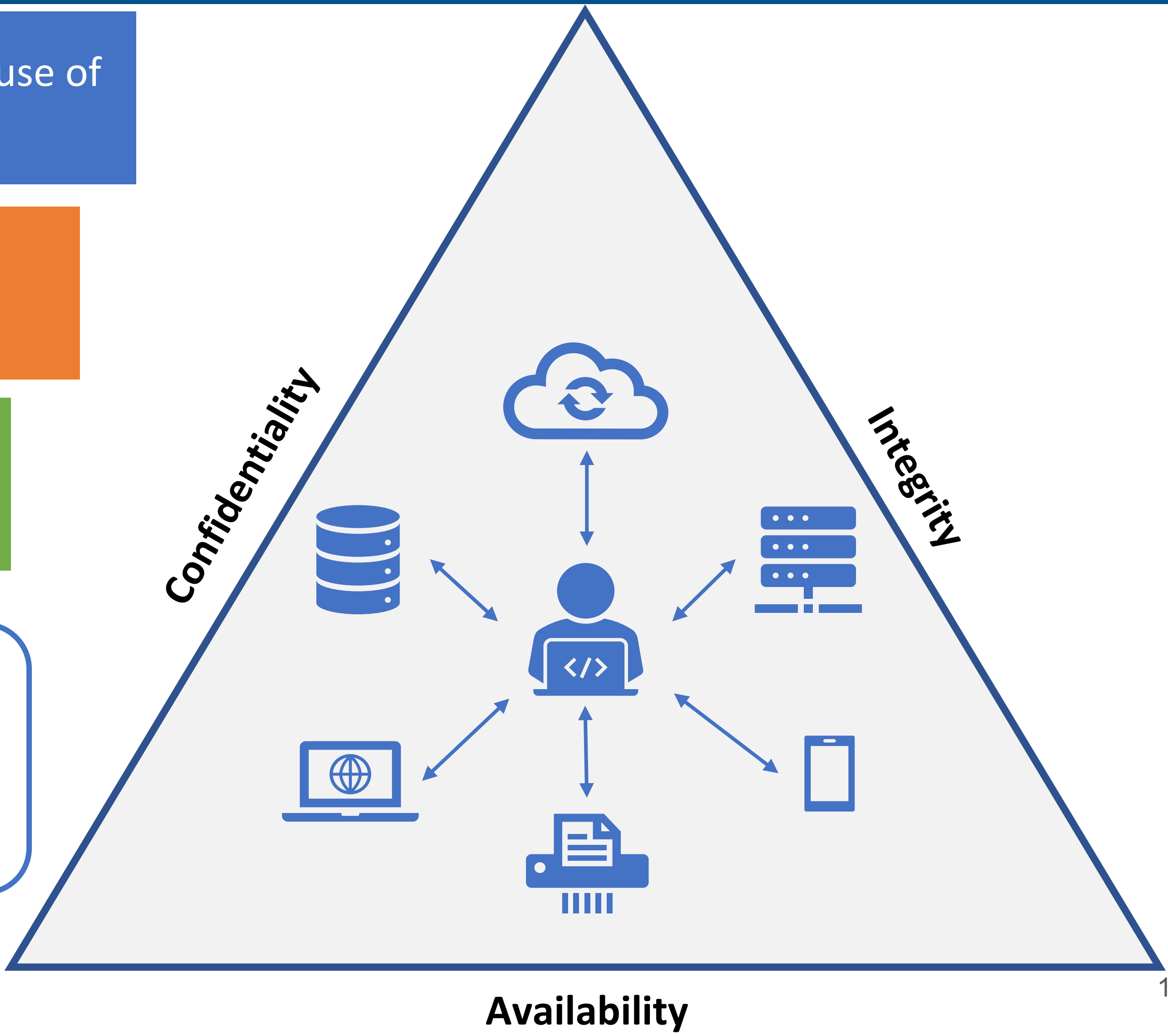
Core Objectives of Cybersecurity

C Prevent unauthorized access and use of information resources

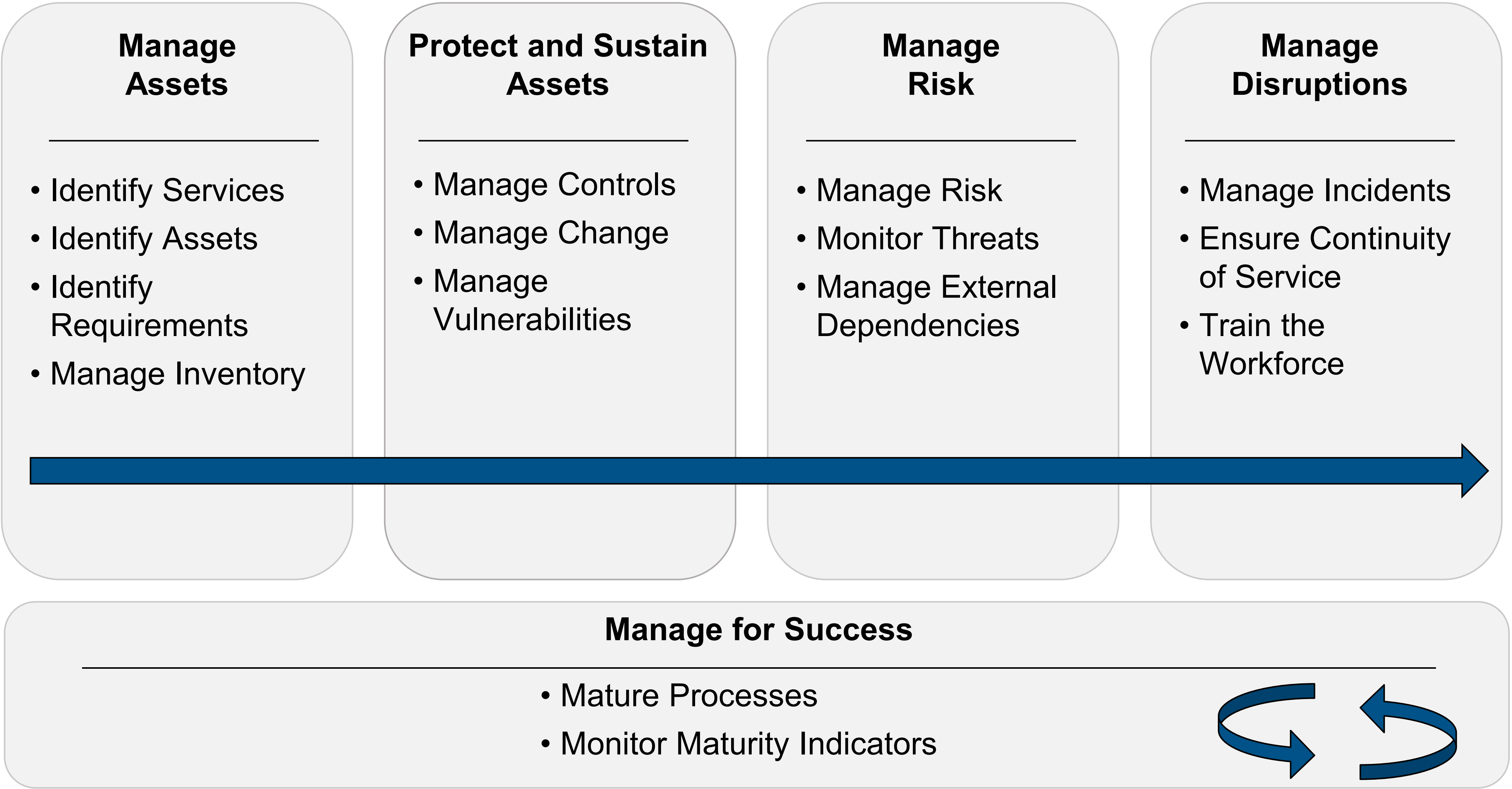
I Prevent unauthorized change and ensure reliability of information resources

A Ensure timely availability of information resources

Organizations engage in practices and deploy administrative, technical, and physical controls to achieve these objectives.



Framework for Achieving Operational Resilience IT/OT



Manage Assets

- Identify Services
- Identify Assets
- Identify Requirements
- Manage Inventory

Protect and Sustain Assets

- Manage Controls
- Manage Change
- Manage Vulnerabilities

Manage Risk

- Manage Risk
- Monitor Threats
- Manage External Dependencies

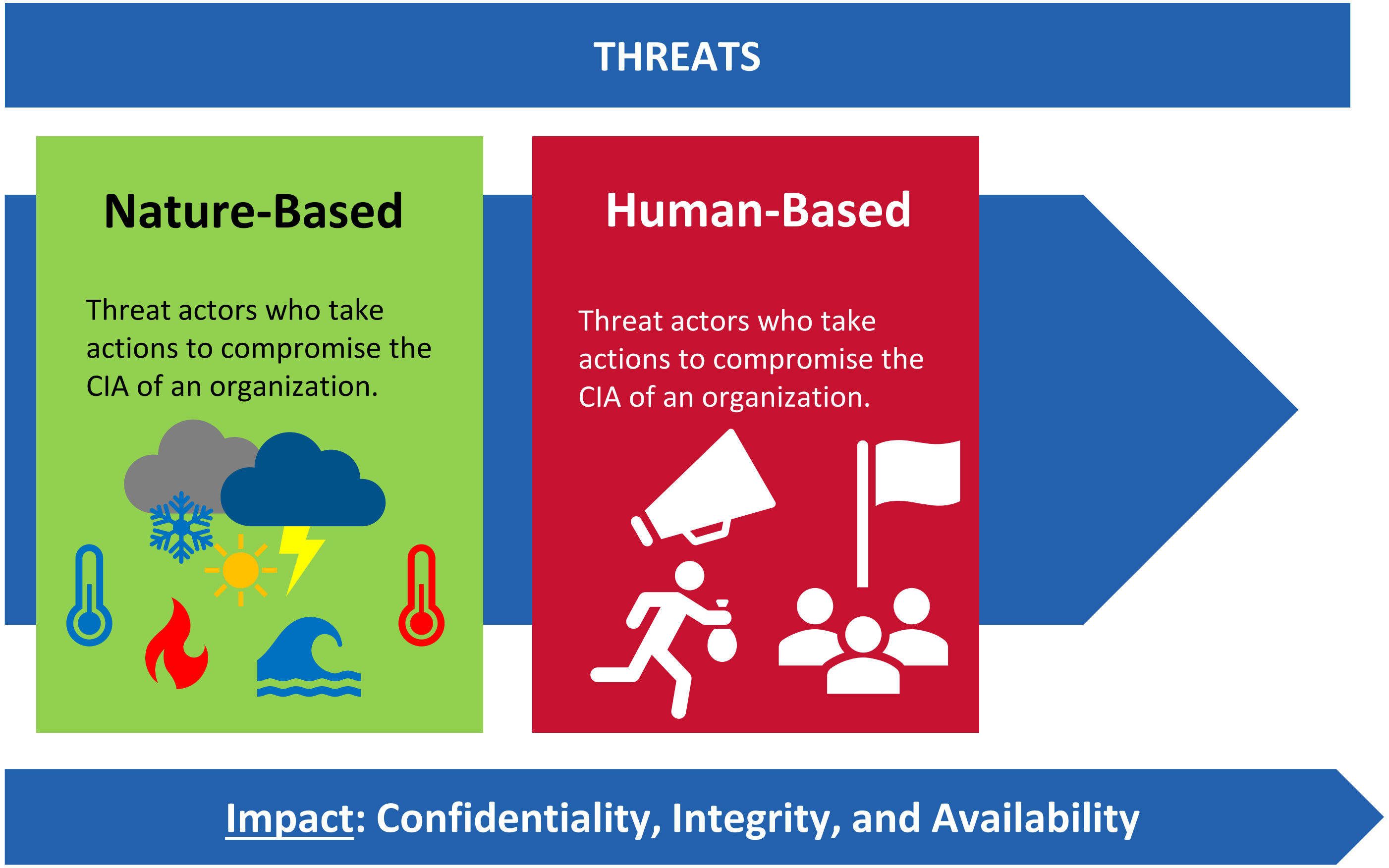
Manage Disruptions

- Manage Incidents
- Ensure Continuity of Service
- Train the Workforce

Manage for Success

- Mature Processes
- Monitor Maturity Indicators

Threats



THREATS

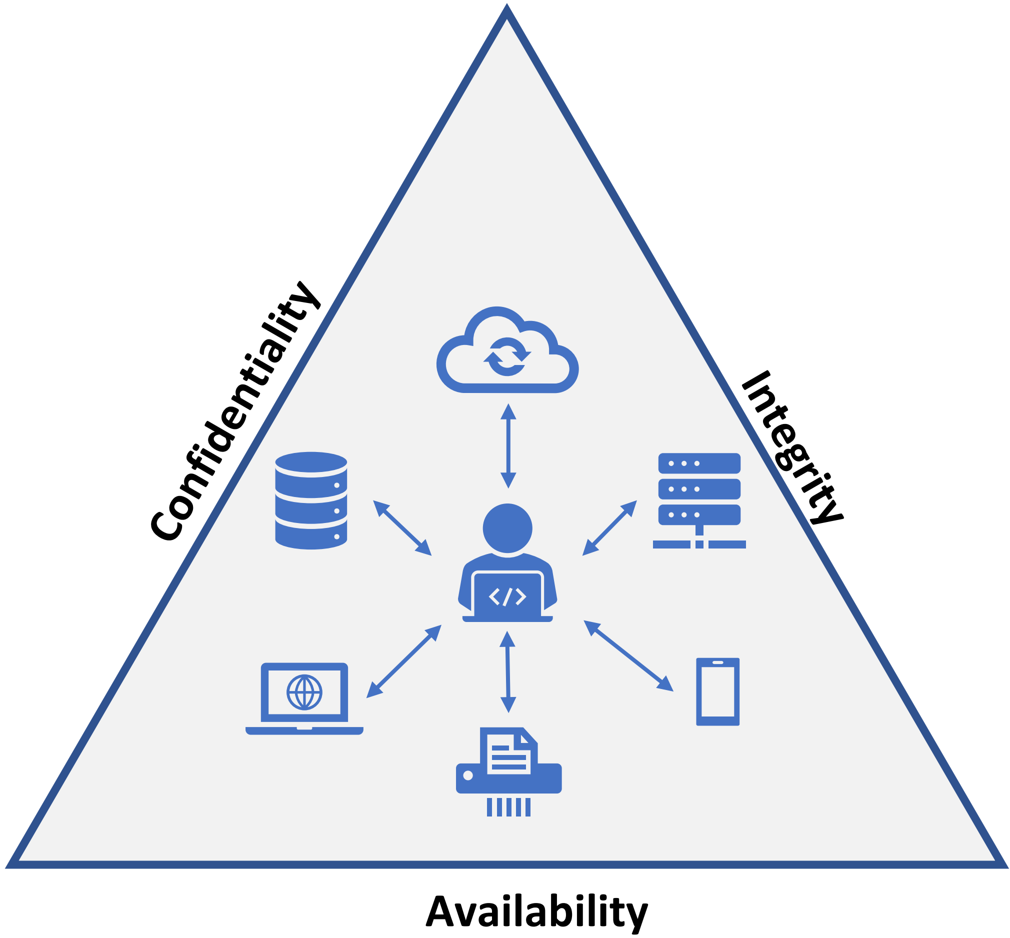
Nature-Based

Threat actors who take actions to compromise the CIA of an organization.

Human-Based

Threat actors who take actions to compromise the CIA of an organization.

Impact: Confidentiality, Integrity, and Availability



Confidentiality

Integrity

Availability

Definition: Threat

According to NIST, the term “**threat**” refers to *“[a]ny circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.”*

Source: NIST SP 800-171 Rev. 1

Threat Actors

THREAT ACTORS

HACKTIVISTS

Conduct attacks in furtherance of political interests.

CRIMINALS

Conduct attacks in furtherance of financial interests.

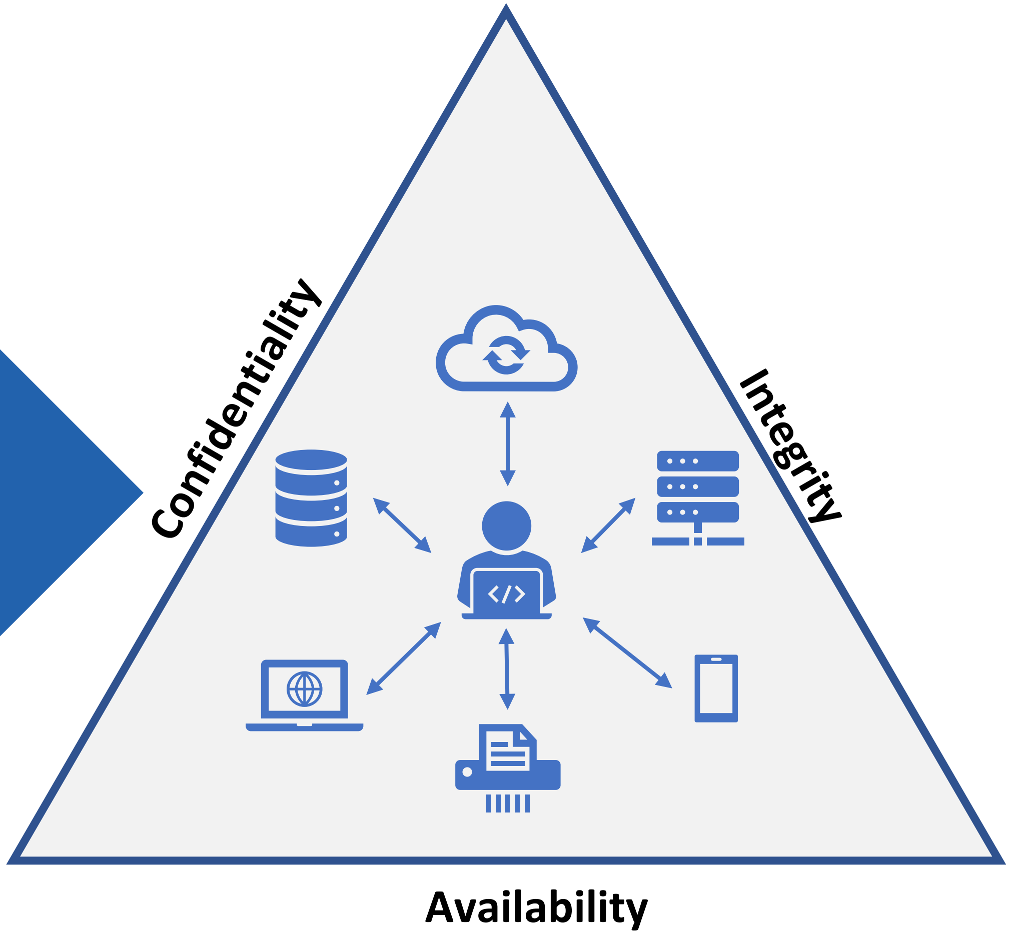
INSIDERS

Conduct attacks in furtherance of personal interests.

STATE ACTORS

Destruction, disruption, and espionage in furtherance of national interests.

Impact: Confidentiality, Integrity, and Availability

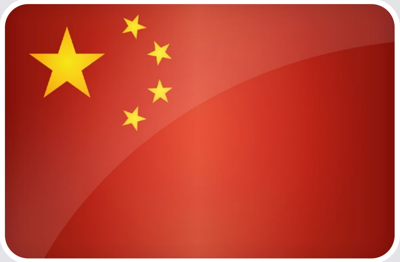


ODNI 2022 Annual Threat Assessment

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.

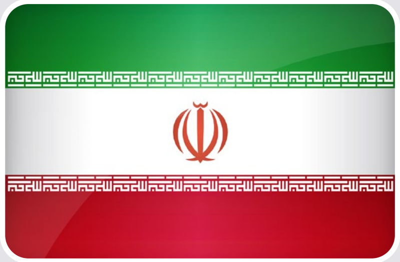
- Considers cyber attacks an acceptable option to deter adversaries, control escalation, and prosecute conflicts.



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.

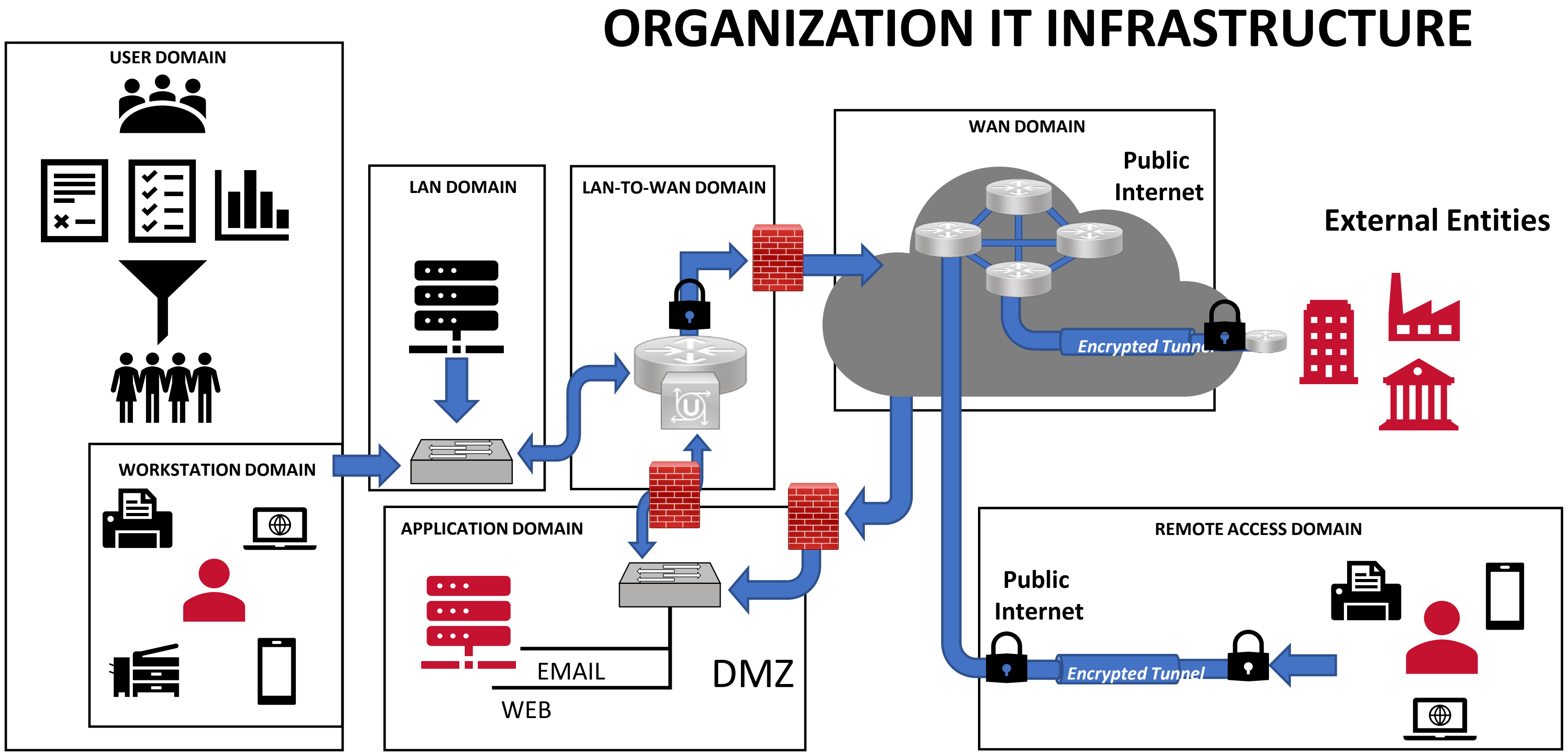
- Responsible for multiple cyber attacks against Israeli water facilities.

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.

Cyber Attacks: Organization Assets Targeted



THREAT ACTORS

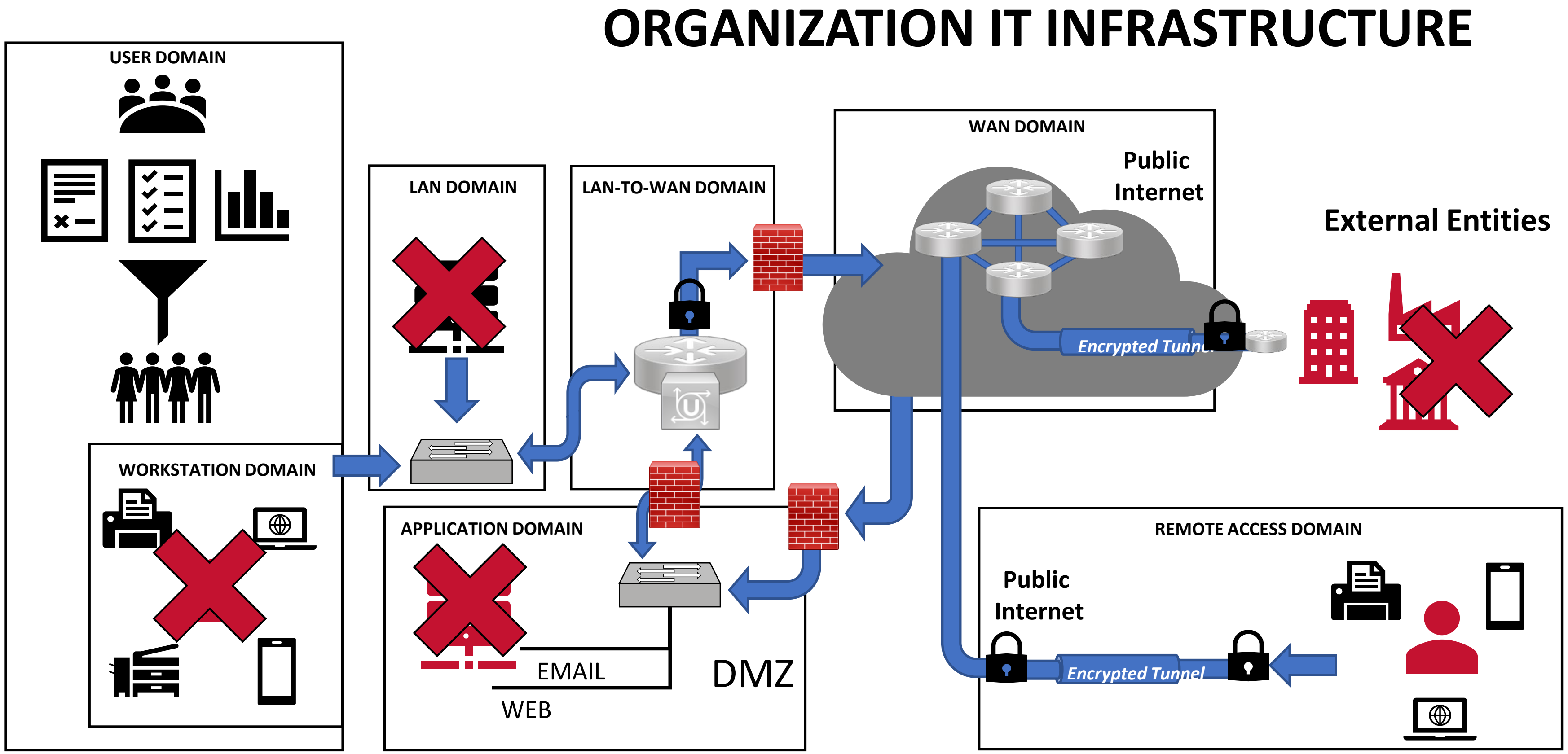
Planning
- Identify target(s)

Discovery
- Identify target systems/users
- Identify vulnerabilities
- Identify exploits

Attack
- Gain access
- Maintain access
- Hide tracks
- Accomplish attack goal

Prime Targets: Vulnerable Users, Technology, and External Partners/Vendors

Cyber Attacks: Service Disruption



THREAT ACTORS

Planning

- Identify target(s)

Discovery

- Identify target systems/users
- Identify vulnerabilities
- Identify exploits

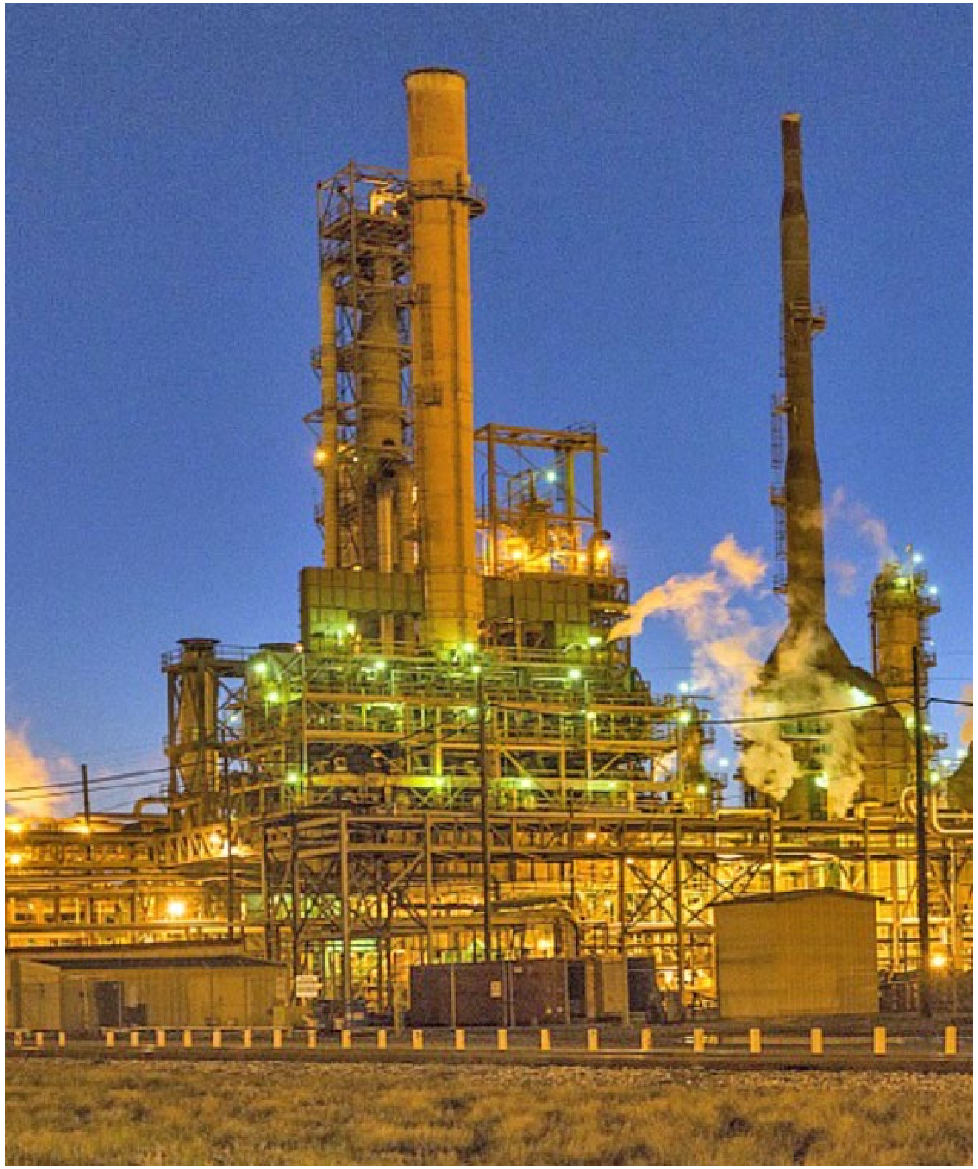
Attack

- Gain access
- Maintain access
- Hide tracks
- Accomplish attack goal

Attacks on Assets>Service Disruption>Mission Failure

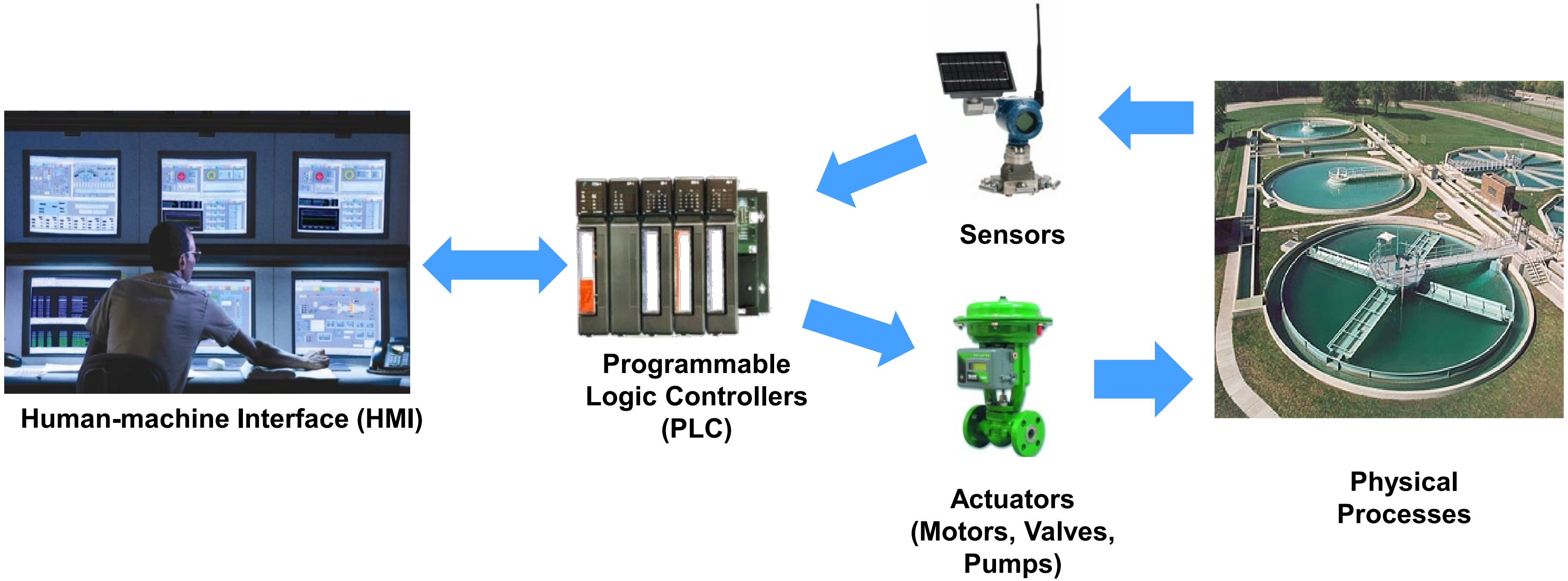
Industrial Control Systems Overview

- Industrial control systems and their graphical user interface systems, SCADA (which stands for supervisory control and data acquisition) have increasingly become a cause of concern ever since they started connecting to the internet
- Considered secure in the past because they were isolated from the outside world, ICS/SCADA are now exposed
- Like any other computer systems, they're vulnerable to exploits by attackers



What are Industrial Control Systems?

- ICS are the components that govern and execute complex processes within chemical, critical manufacturing, energy, nuclear, transportation, and water and wastewater sectors.
- We rely on control systems and their processes to sustain our way of modern life.



Human-machine Interface (HMI)

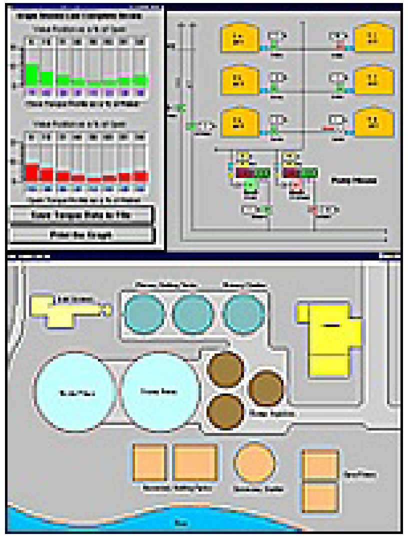
Programmable Logic Controllers (PLC)

Sensors

Actuators (Motors, Valves, Pumps)

Physical Processes

Human-Machine Interface



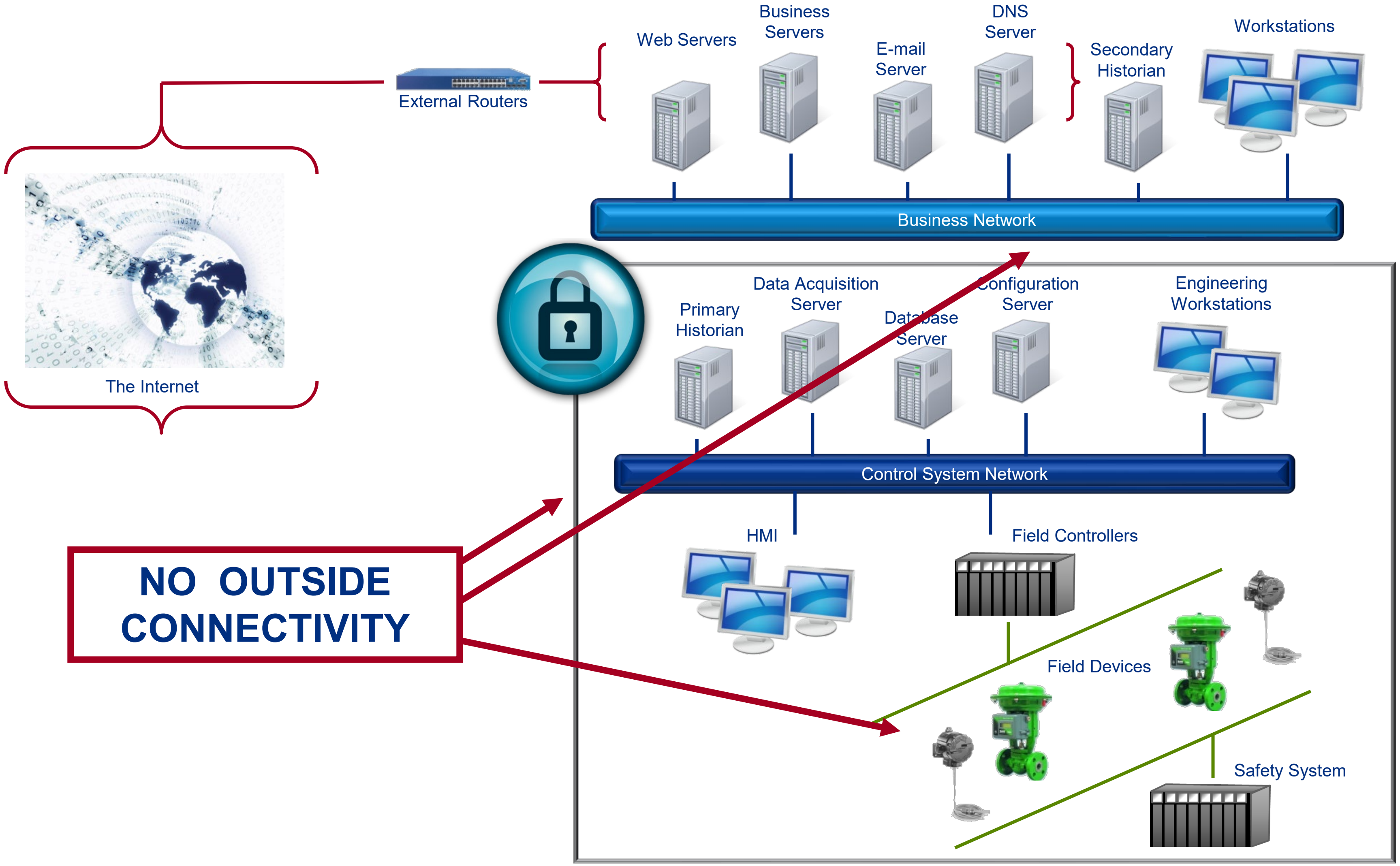
Human-Machine Interface (HMI)

- A graphical representation of the process for the operator
- Used for control, monitoring, alarming, and trending
- Can be software systems on a PC or standalone systems like touch panels, handheld devices, or panel-mounted displays
- Used to collect data from devices and display or send the data to a database for historical trending

Significance of Industrial Control Systems

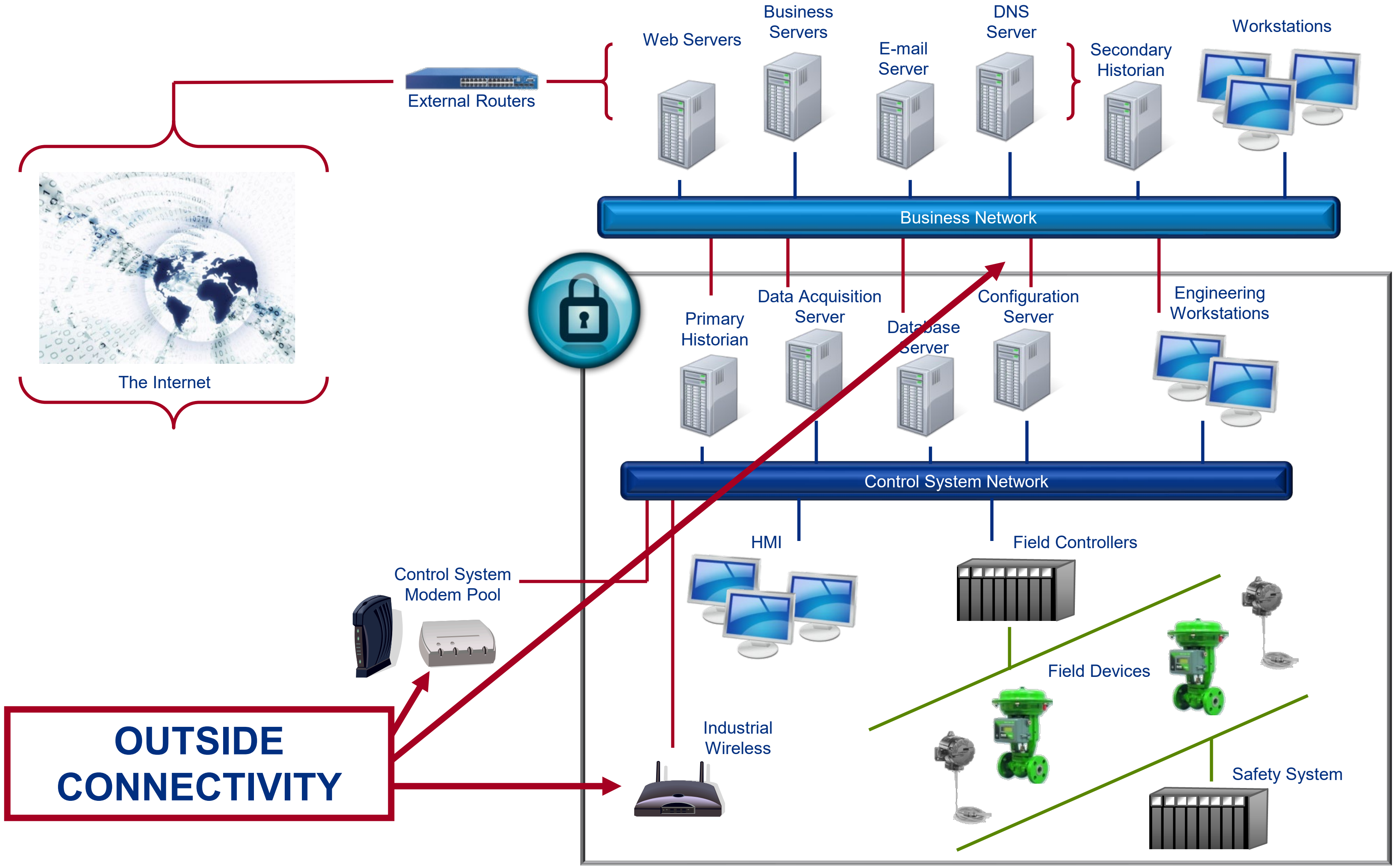
- Automated ICS are present in almost every aspect of our modern society
  - ICS provide safe and reliable operations for critical infrastructure
  - Increase productivity
  - Lower costs
- Today, most control systems are interconnected with business networks, introducing IT vulnerabilities and attack/exploitation paths into the ICS network
- A successful cyber attack on a control system could result in physical consequences and cascading effects that could disrupt services.

ICS – Traditional Isolation



NO OUTSIDE CONNECTIVITY

ICS – Modern Connectivity



Key Risk Factors

Increasing ICS Vulnerability Landscape

- Product Risks (zero-days & other unpatched vulnerabilities)
- Available Exploit Tools
- Lower skill level required to attack

Control System Connectivity

- Project SHINE, Shodan, Internet-facing devices
- Interconnectivity: ICS exposed thru business network
- Weak Credentials
- Inadequate policies and procedures

The Human Factor

- Jumping the airgap, USB Drives/Laptops
- Lack of Policies and Procedures
- Lack of training or adherence to procedures

Intrusions into the Supply Chain

- Targeting control system vendors
- Connectivity to third-party services and vendors

Unprotected Sensitive Information

- Limit public information about your ICS
- Protect sensitive information and files

Inadequate Detection Capability

- Ability to know when you've been compromised
- Lack of logging & detection within the ICS network

Threat Landscape

Cyber Threat Actors Target ICSs

- Concerns with the recent rise in targeted and successful malware campaigns against industrial control systems (ICSs).
- These campaigns were associated with sophisticated threat actors with demonstrated capabilities to compromise control system networks.
- The depth of intrusion into the control system network provided the threat actors with the ability to potentially:
  - Manipulate control system settings
  - Control the process
  - Destroy data and/or equipment

Well-Known ICS-Tailored Attacks

- **Stuxnet (2010):** Stuxnet was the first ICS malware found in the wild, when it was targeting the centrifuges in Iranian nuclear facilities, with the goal of inflicting physical damage by altering their rotation speed. It was considered novel at the time, and introduced some malicious techniques that are still used by adversaries today, regardless of ICS environments, such as process hollowing and persistence using WMI consumers.

Well-Known ICS-Tailored Attacks

- **Pipedream (2022)**: Pipedream was the most sophisticated ICS-specific malware to date, able to natively interact with a long list of ICS devices from various vendors. According to a CISA advisory, the malware is able to "***scan for, compromise, and control certain ICS/SCADA devices***." Those capabilities, according to Dragos, present "*a clear and present threat to the availability, control, and safety of industrial control systems and processes*" and "*can be used to endanger operations and lives*."

Drawing on this brief history of ICS-specific malware, it appears that the threat groups are getting bolder by trying to inflict physical damage and strike safety systems, thereby indicating a growing general intent to cause harm.

ICS Mitigation Recommendations

- Limit exposure of system information
- Identify and secure remote access points to ICS
- Restrict tools and scripts
- Conduct regular security audits
- Implement a dynamic network environment

Limit Exposure of System Information

- To the extent possible, **avoid disclosing information about system hardware, firmware, and software in any public forum**
- Incorporate **information protection education into training for personnel**
- Limit information that is sent out from the system
- Share only the data necessary to comply with applicable legal requirements, such as those contractually required by vendors—nothing more
- Do not allow other uses of the data and other accesses to the system without strict administrative policies designed specifically to protect the data
- Prevent new connections to the control system using strict administrative accountability

Identify and Secure Remote Access Points

Once owner/operators have identified all remote access points on their systems, they can implement the following recommendations to improve their security posture:

- Reduce the attack surface by proactively limiting and hardening Internet-exposed assets
- Establish a firewall and a demilitarized zone (DMZ) between the control system and the vendor’s access points and devices
- Do not allow direct access into the system; use an intermediary service to share only necessary data and only when required
- Consider using virtual private networks (VPNs) at specific points to and from the system rather than allowing separate access points for individual devices or vendors

Restrict Tools and Scripts

- Limit access to network and control system application tools and scripts to legitimate users performing legitimate tasks on the control system
- Carefully apply access and use limitations to particularly vulnerable processes and components to limit the threat
- Identify any engineering, configuration, or diagnostic tools
- Securely store gold copies of these tools external to the system if possible
- Remove all non-critical tools
- Prevent these tools from being reinstalled
- Perform routine audits to check that these tools have not been reinstalled

Conduct Regular Security Audits

- Validate all connections (e.g., network, serial, modem, wireless, etc.)
- Review system software patching procedures.
- Confirm secure storage of gold copies (e.g., OS, firmware, patches, configurations, etc.)
- Verify removal from the system of all non-critical software, services, and tools
- Audit the full asset inventory
- Implement CISA ICS mitigations and best practices
- Monitor system logs and intrusion detection system (IDS) logs
- Monitoring of access logs, system changes, IDS logs, and other tracking data should be performed continuously, with a deeper look at this data during periodic audits

Implement a Dynamic Network Environment

A static network can provide cyber actors the opportunity to collect bits of intelligence about the system over time, **establish long-term accesses into the system, and develop the tools and TTPs to affect the control system as intended**

- Deploy additional firewalls and routers from different vendors
- Modify IP address pools
- Replace outdated hardware (e.g., workstations, servers, printers, etc.)
- Upgrade operating systems
- Install or upgrade commercially available security packages for vendor access points and methodologies

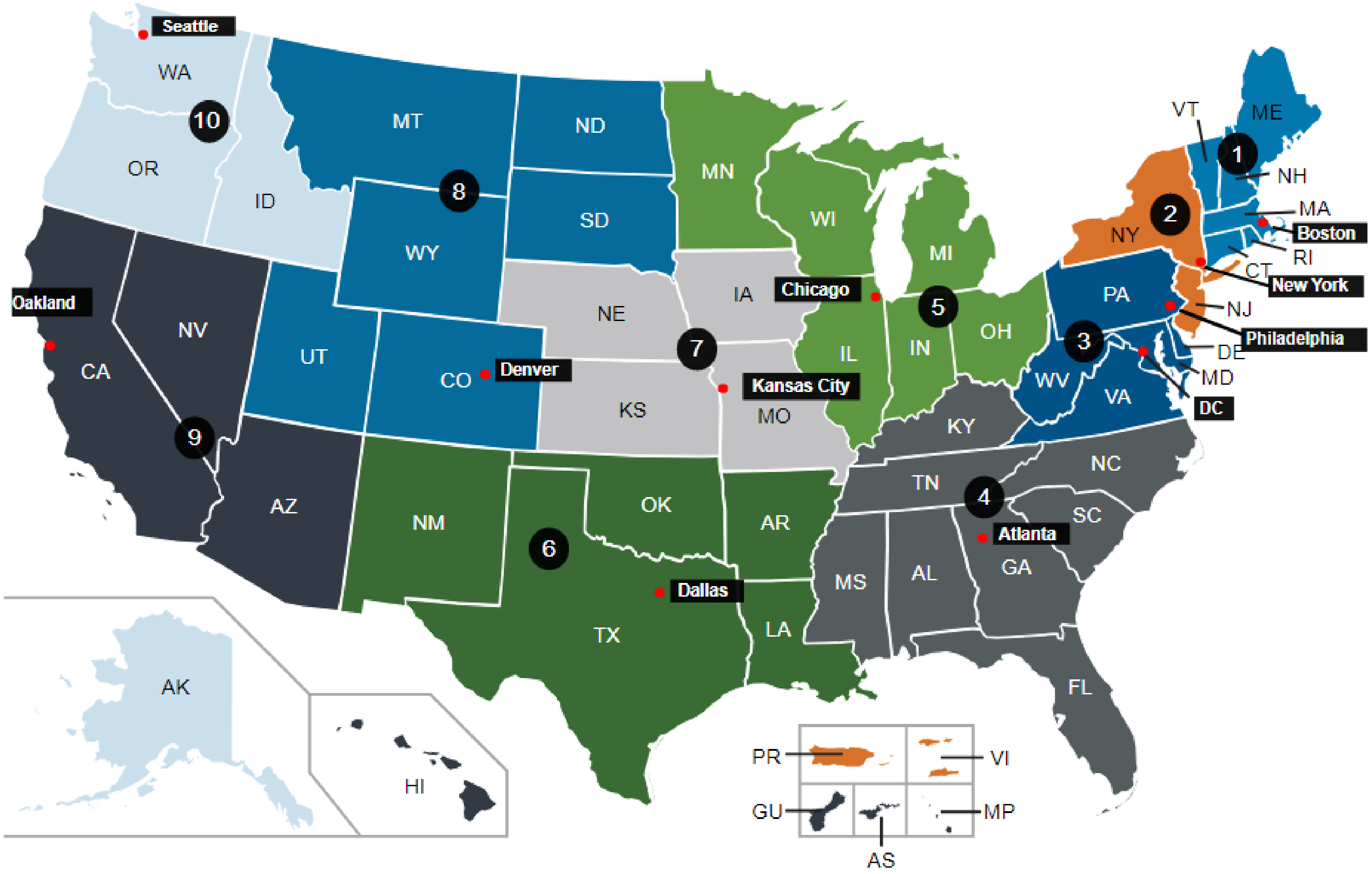
Conclusion

- The combination of integrated, simplified tools and remote accesses creates an environment ripe for malicious actors to target control systems networks
- New IT-enabled accesses provide cyber actors with a larger attack surface into cyber-physical environments
- It is vital for OT/ICS defenders to anticipate the TTPs of cyber actors combining IT expertise with engineering know-how
- Defenders can employ the mitigations listed to limit unauthorized access, lock down tools and data flows, and deny malicious actors from achieving their desired effects

Cybersecurity Resources and Services

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



[CISA Region 6: CISARegion6@hq.dhs.gov](mailto:CISARegion6@hq.dhs.gov)

Cybersecurity State Coordinator Authorities

The role of the Cybersecurity State Coordinator is to serve as the principal point of contact for non-Federal entities to engage the Federal Government on preparing, managing, and responding to cyber incidents, as well as to build strategic public and private sector relationships, pursuant to 6 United States Code, Section 665(c) (2021) (Cybersecurity State Coordinator Act of 2020).

- Build strategic public and private sector relationships;
- Serve as the Federal cybersecurity risk advisor;
- Facilitate the sharing of cyber threat information;
- Raise awareness of cyber resources from the Federal Government to non-Federal entities;
- Support training, exercises, and planning for continuity of operations from cyber incidents;
- Serve as a principal point of contact for non-Federal entities to engage the Federal Government on preparing, managing, and responding to cyber incidents;
- Assist State, local, Tribal, and territorial governments in development of State cyber plans;
- Coordinate with appropriate officials within the Agency (CISA).

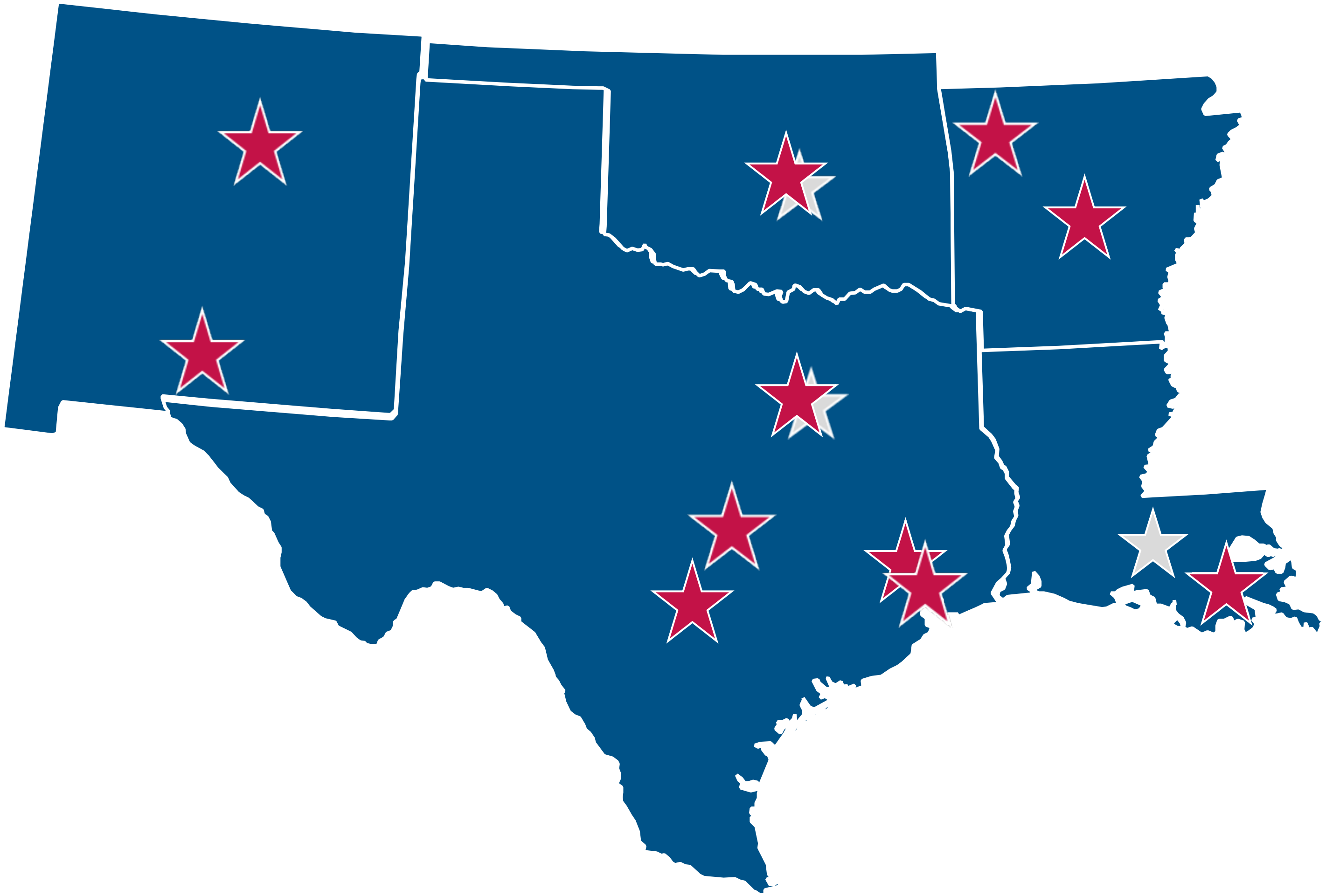
Cybersecurity State Coordinator of Texas: Ernesto Ballesteros
Email: ernesto.ballesteros@cisa.dhs.gov

Cybersecurity Advisors (CSAs)

To 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.

Reg 6 | On-Hand / Projected Cyber Personnel



★ On-Hand

☆ Projected

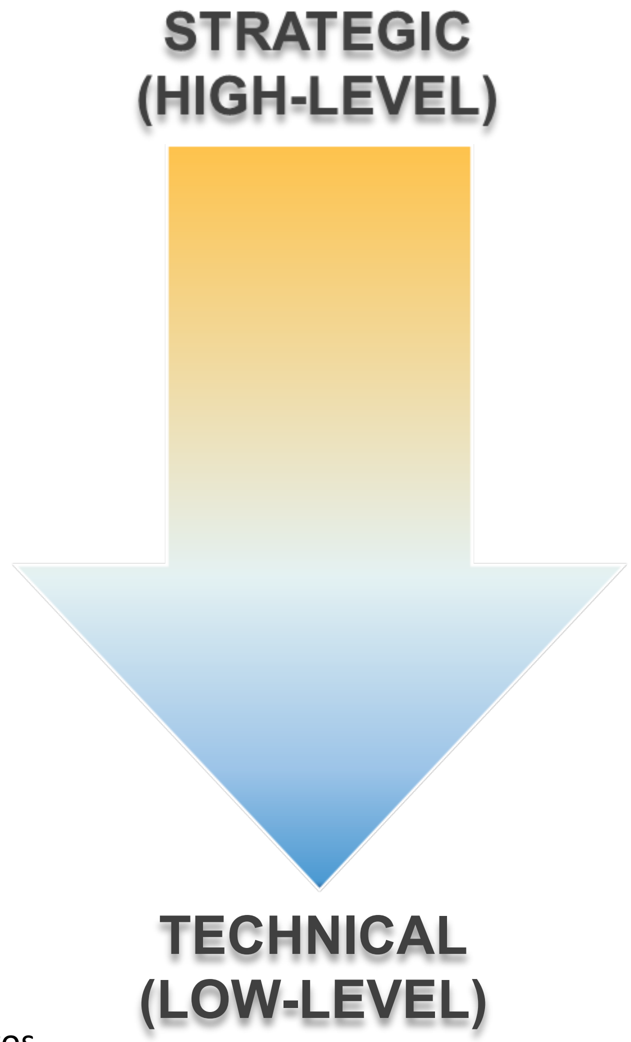
CISA Cybersecurity Resources

Regional Resources:

- Cybersecurity Assessments
  - ➢ Ransomware Readiness Assessment (RRA)
  - ➢ Cybersecurity Performance Goals (CPG)
  - ➢ Cyber Infrastructure Survey (CIS)
  - ➢ Cyber Resilience Essentials (CRE)
  - ➢ Incident Management Review (IMR)
  - ➢ Cyber Resilience Review (CRR)
  - ➢ External Dependencies Management (EDM)
- Workshops
  - ➢ Cyber Resilience Workshop (CRW)
  - ➢ Incident Management Workshop (IMW)
  - ➢ Vulnerability Management Workshop (VMW)
  - ➢ Digital Forensics Workshop I & II (DFW)
  - ➢ Cybersecurity Tabletop Exercise (CTTX)

National Resources:

- Vulnerability Scanning Service (CyHy)



STRATEGIC (HIGH-LEVEL)

TECHNICAL (LOW-LEVEL)

Cybersecurity State Coordinator of Texas: Ernesto Ballesteros
Email: ernesto.ballesteros@cisa.dhs.gov

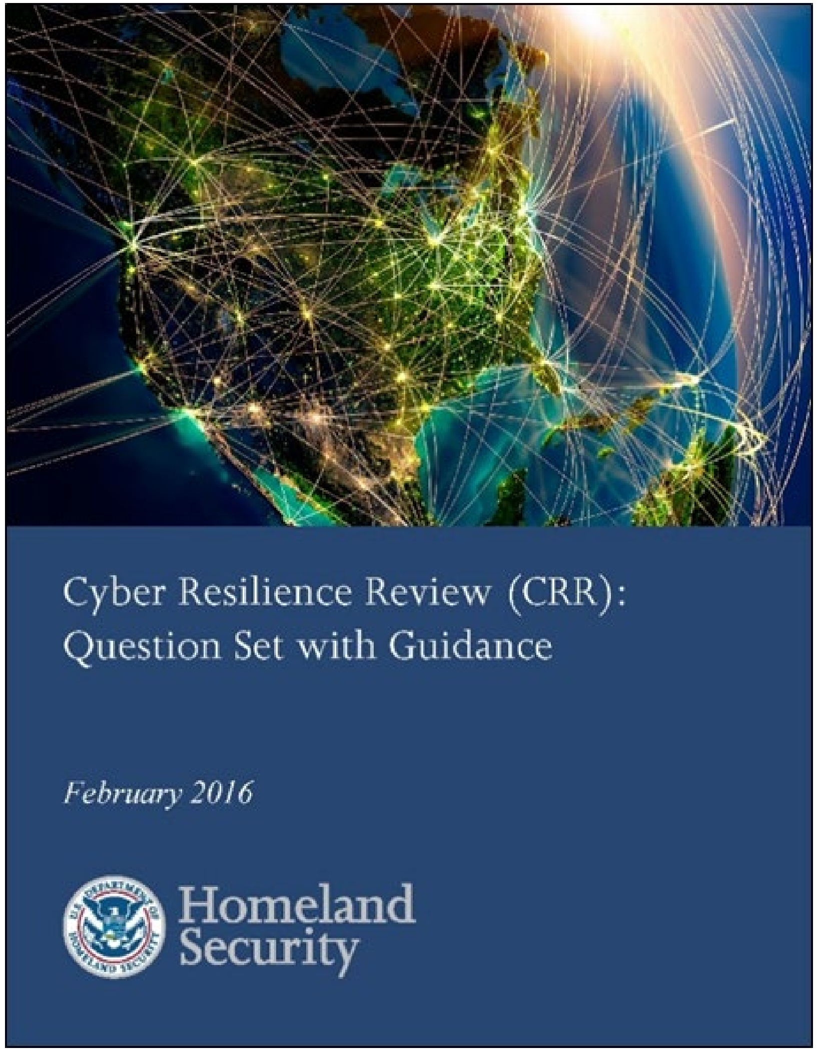
Cybersecurity Assessments

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

Goal: Helps partners understand and measure cyber security capabilities as they relate to operational resilience and cyber risk

- Evaluates the maturity of an organization’s capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity capabilities
- Based on the CERT ® Resilience Management Model (CERT® RMM)



Cyber Resilience Review (CRR):
Question Set with Guidance

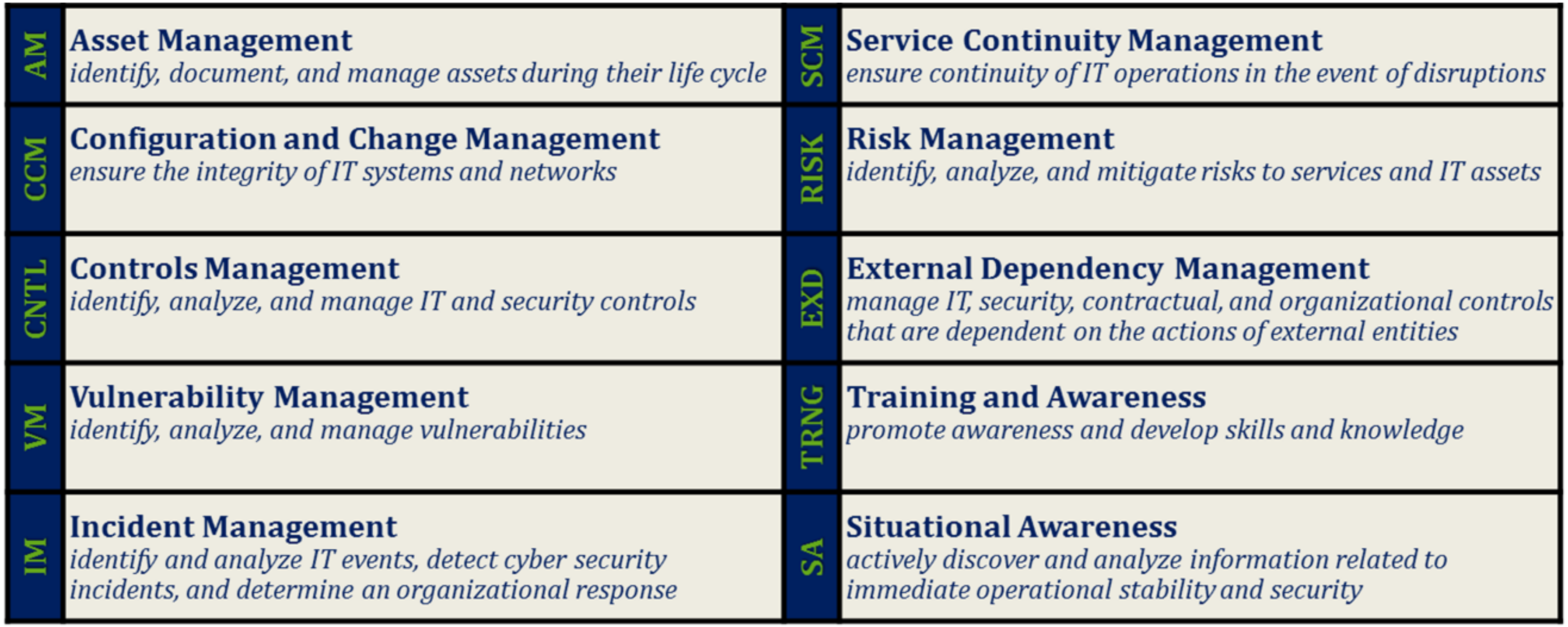
February 2016

Homeland
Security

Cyber Resilience Review (CRR) | Domains

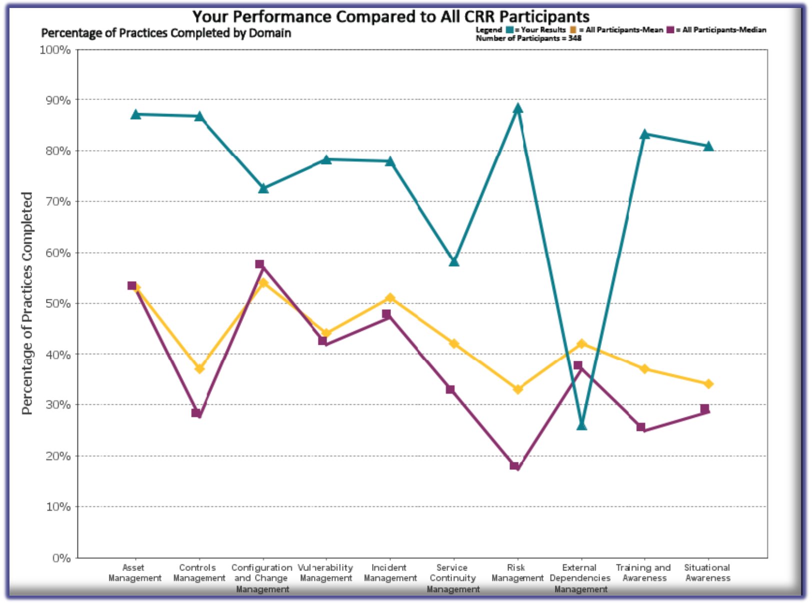
These represent key areas that typically contribute to an organization’s cyber resilience— each domain focuses on:

- 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*

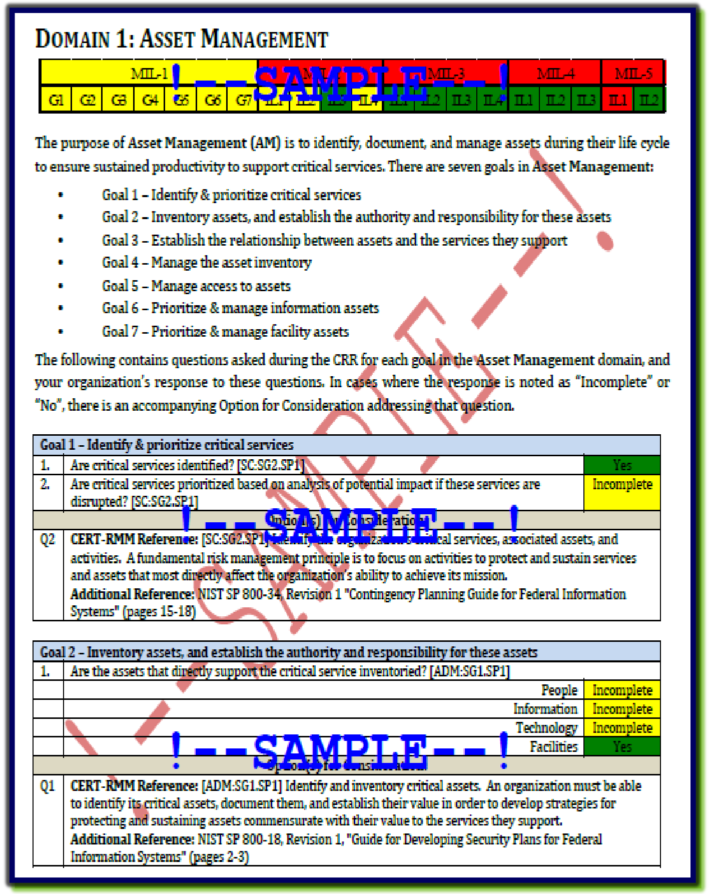
Benefits of CRR



Comparison data with other CRR participants

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	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)	

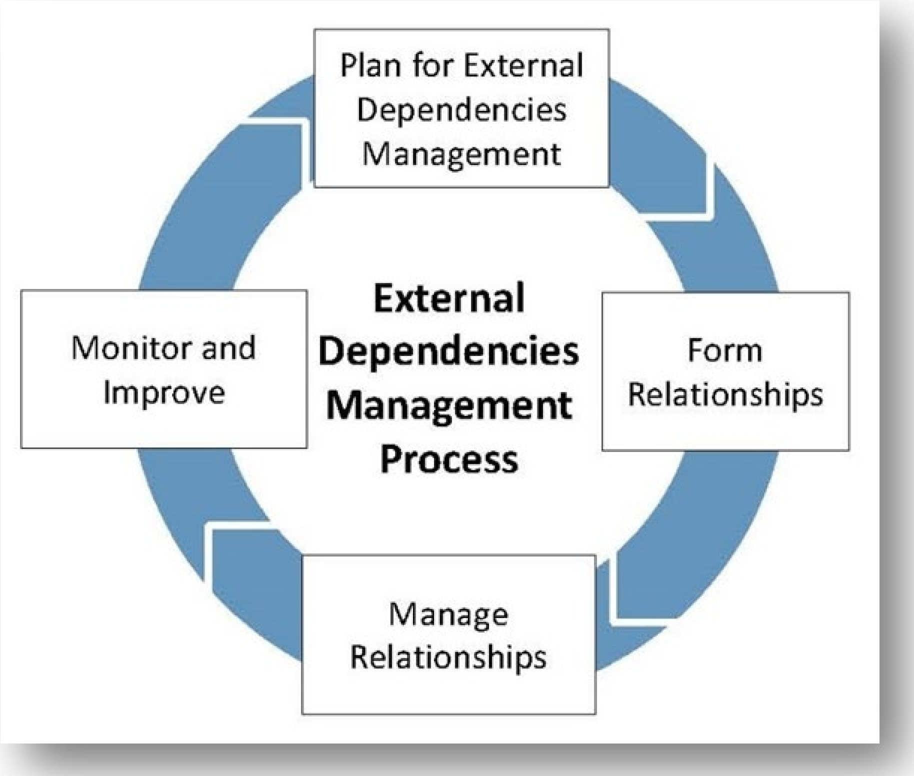
CRR Mappings to Other Frameworks

The Cyber Resilience Review has been mapped to:

- NIST Cybersecurity Framework (CSF)
- Health Insurance Portability and Accountability Act (HIPAA) Security Rule
- Federal Financial Institutions Examination Council’s (FFIEC) Cybersecurity Assessment Tool (CAT)
- NIST Special Pub 800-53 rev 4 (This mapping has not yet been published)

Most Cybersecurity Frameworks are being mapped to the NIST Cybersecurity Framework as a result that mapping can be used to indirectly map them to the CRR

External Dependency Management (EDM)


Plan for External Dependencies Management
Form Relationships
Manage Relationships
Monitor and Improve
External Dependencies Management Process

EDM process outlined in the External Dependencies Management Resource Guide

Overview: In 2016, DHS launched the External Dependencies Management (EDM) Assessment, focusing specifically on ensuring the protection and sustainment of services and assets that are dependent on the actions of third-party entities.

Background: External Dependencies Management is a domain covered by the CRR. However, EDM and associated issues (e.g., supply-chain management, vendor management) are not addressed at a comprehensive level within the CRR, resulting in the creation of a separate assessment.

Linkages to CRR: Despite operating at a more granular level than the CRR, the EDM Assessment borrows heavily from the CRR's methodological architecture and scoring system but remains a CISA facilitated assessment.

External Dependency Management (EDM)

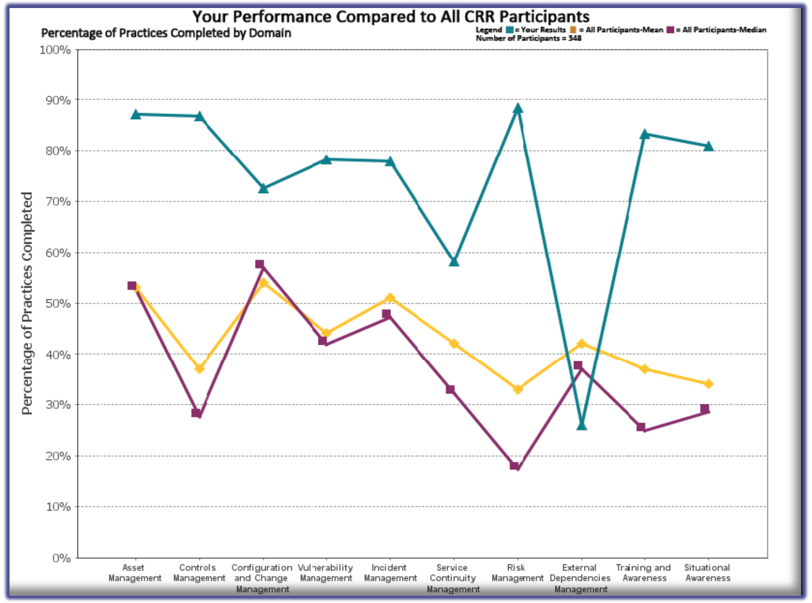
To provide the organization with an understandable and useful structure for the evaluation, the EDM Assessment is divided into three distinct areas (domains):

1. **RELATIONSHIP FORMATION** – how the organization considers third party risks, selects external entities, and forms relationships with them so that risk is managed from the start

2. **RELATIONSHIP MANAGEMENT AND GOVERNANCE** – how the organization manages ongoing relationships with external entities to support and strengthen its critical services at a managed level of risk and cost

3. **SERVICE PROTECTION AND SUSTAINMENT** – how the organization plans for, anticipates, and manages disruption or incidents related to external entities

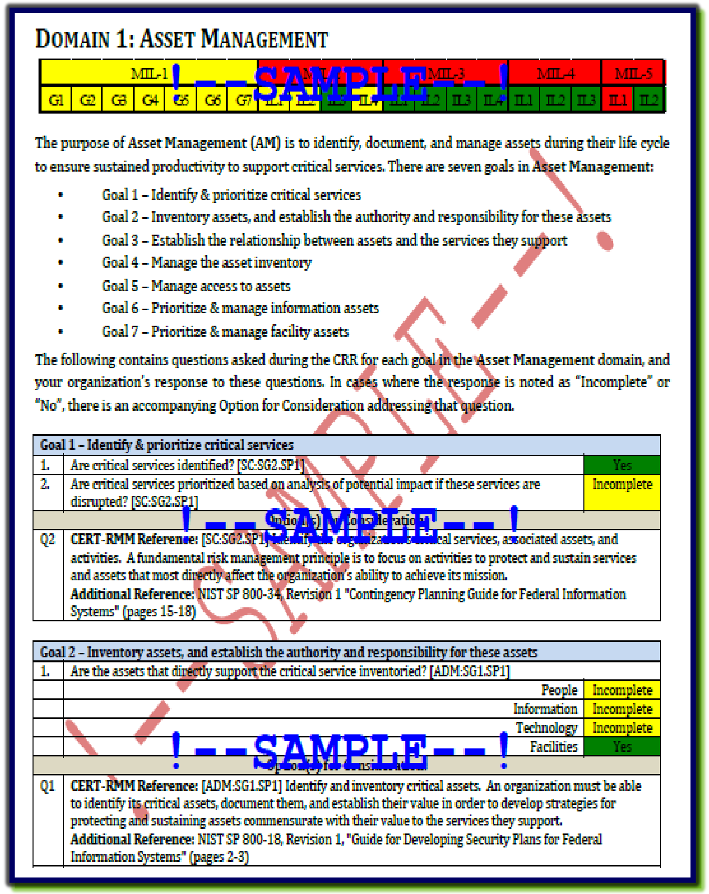
Benefits of EDM



Comparison data with other EDM participants

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	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)	

Cybersecurity Workshops & Exercises

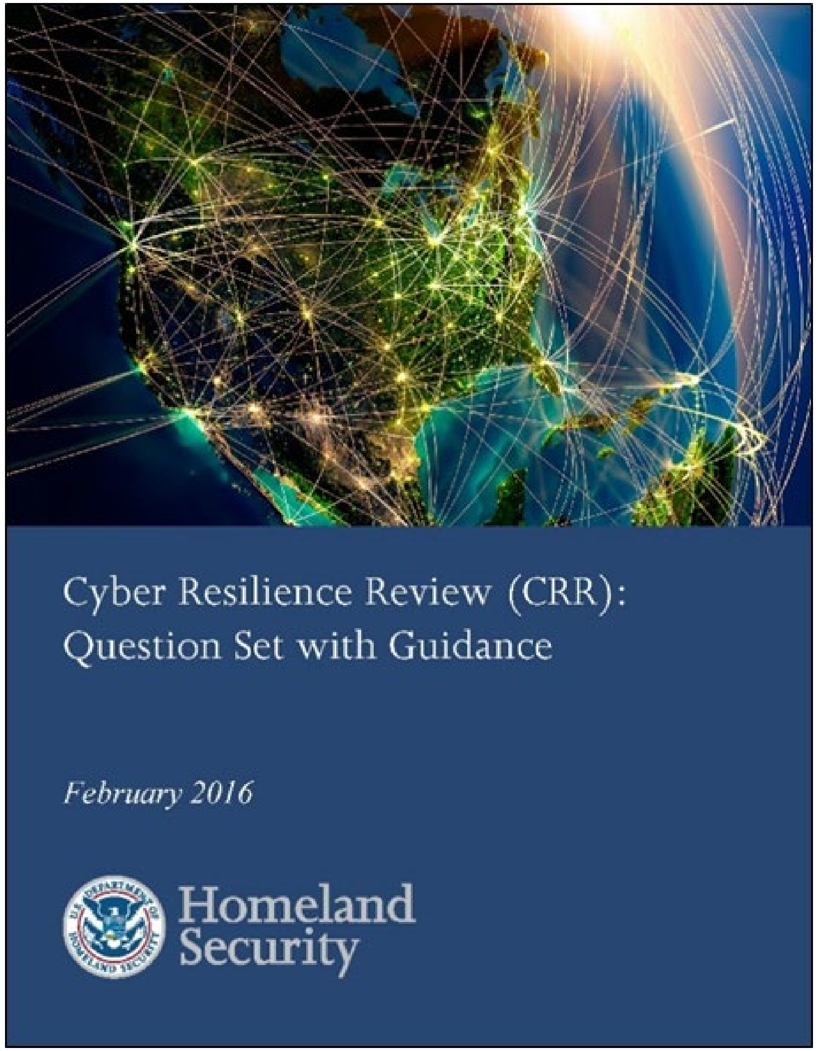
Cyber Resilience Workshop (CRW)

Description: A non-technical and informative session designed to help organizations understand cyber resilience concepts and ways to improve management of cyber resilience.

Goal: The goal of the workshop is to provide your organization with tangible takeaway information related to risk-based decision making and security planning for critical services.

Audience: Organizations that want to learn about an approach to developing repeatable cybersecurity capabilities and practices to protect and sustain their organization’s operating environment.

Format: In-Person or Virtual



Cyber Resilience Review (CRR):
Question Set with Guidance

February 2016

Homeland
Security

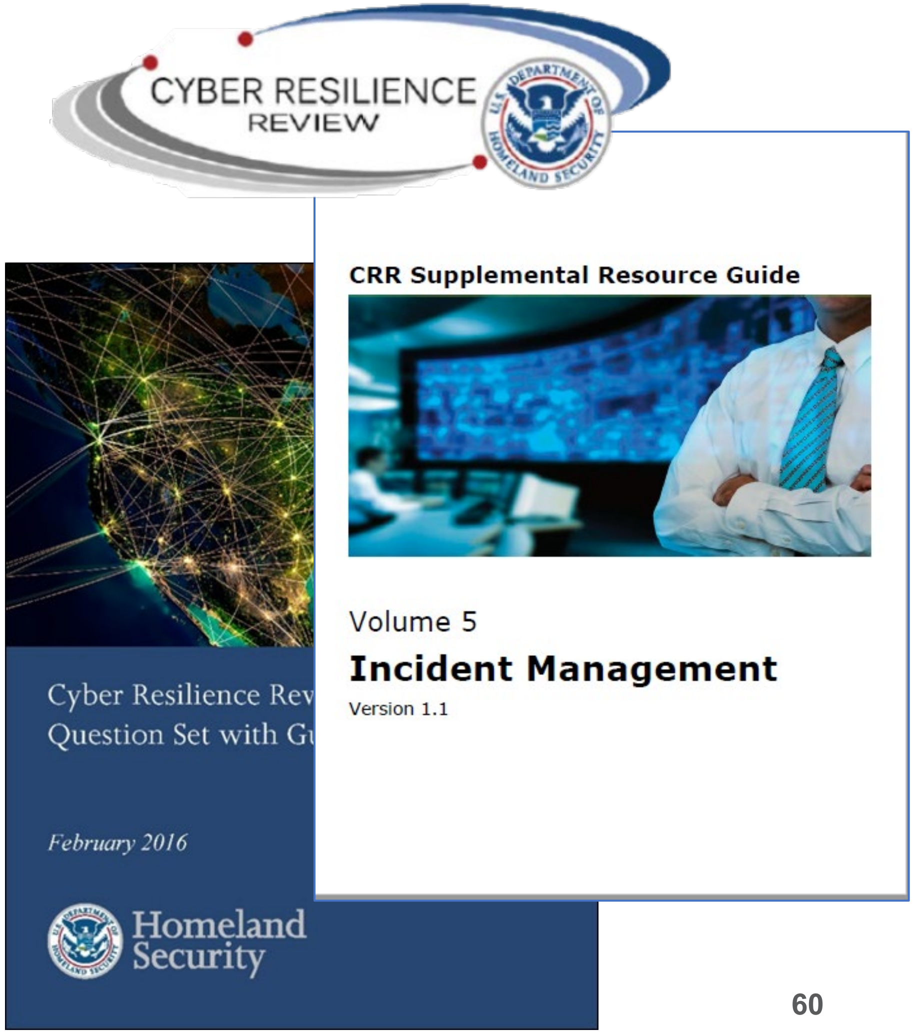
Incident Management Workshop (IMW)

Description: A 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 RESILIENCE REVIEW

CRR Supplemental Resource Guide

Volume 5

Incident Management

Version 1.1

Cyber Resilience Rev
Question Set with Gu

February 2016

Homeland Security

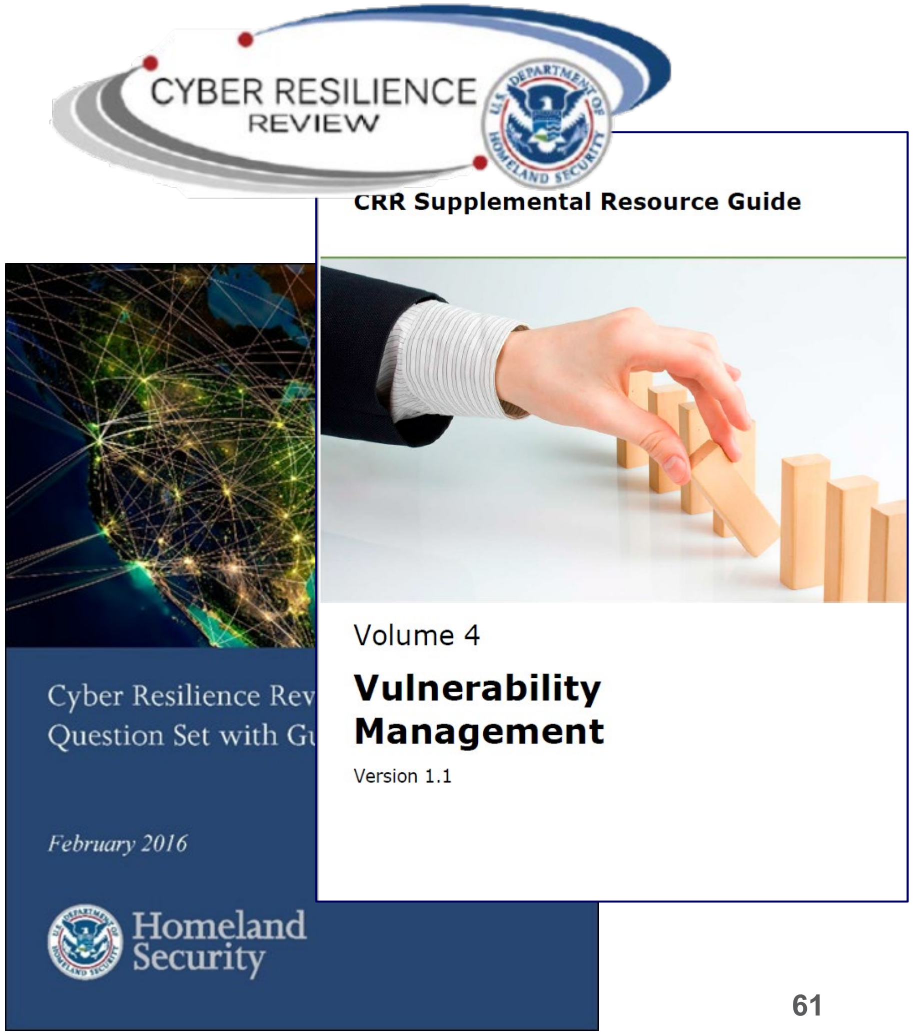
Vulnerability Management Workshop (VMW)

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

Goal: The goal of the workshop is to provide your organization with tangible takeaway information on how to manage cybersecurity vulnerabilities effectively and ultimately achieve operational resilience.

Audience: Organizations that want to learn about an approach to developing a cyber vulnerability management program to identify, analyze, and manage vulnerabilities in their operating environment.

Format: In-Person or Virtual



CYBER RESILIENCE REVIEW

CRR Supplemental Resource Guide

Volume 4

Vulnerability Management

Version 1.1

Cyber Resilience Rev
Question Set with Gu

February 2016

Homeland Security

Cybersecurity State Coordinator of Texas: Ernesto Ballesteros
Email: ernesto.ballesteros@cisa.dhs.gov

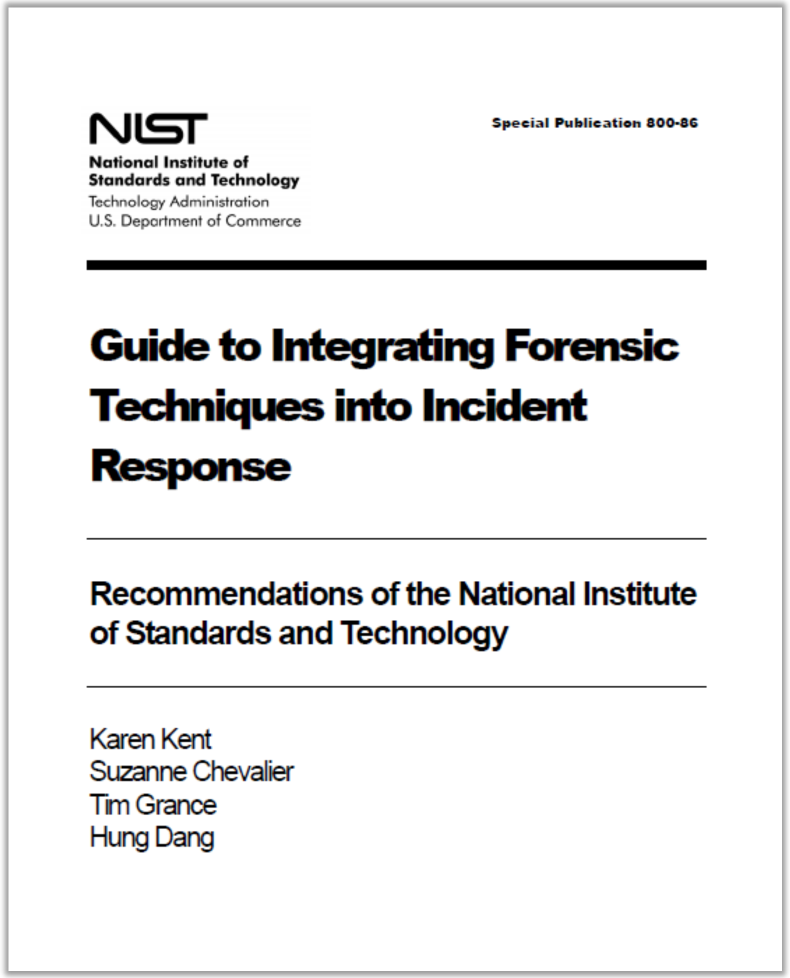
Introduction to Digital Forensics Workshop (DFW)

Description: An informative and hands-on session designed to help organizations understand digital forensics concepts, key elements, planning and implementation.

Goal: The goal of the workshop is to provide your organization with tangible takeaway information on how to manage digital forensics effectively.

Audience: Tailored for incident response teams; forensic analysts; system, network, and security administrators; and computer security program managers who are responsible for performing forensics for investigative, incident response, or troubleshooting purposes.

Required: A laptop is required for the hands-on portion of the workshop.



NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Special Publication 800-86

Guide to Integrating Forensic Techniques into Incident Response

Recommendations of the National Institute of Standards and Technology

Karen Kent
Suzanne Chevalier
Tim Grance
Hung Dang

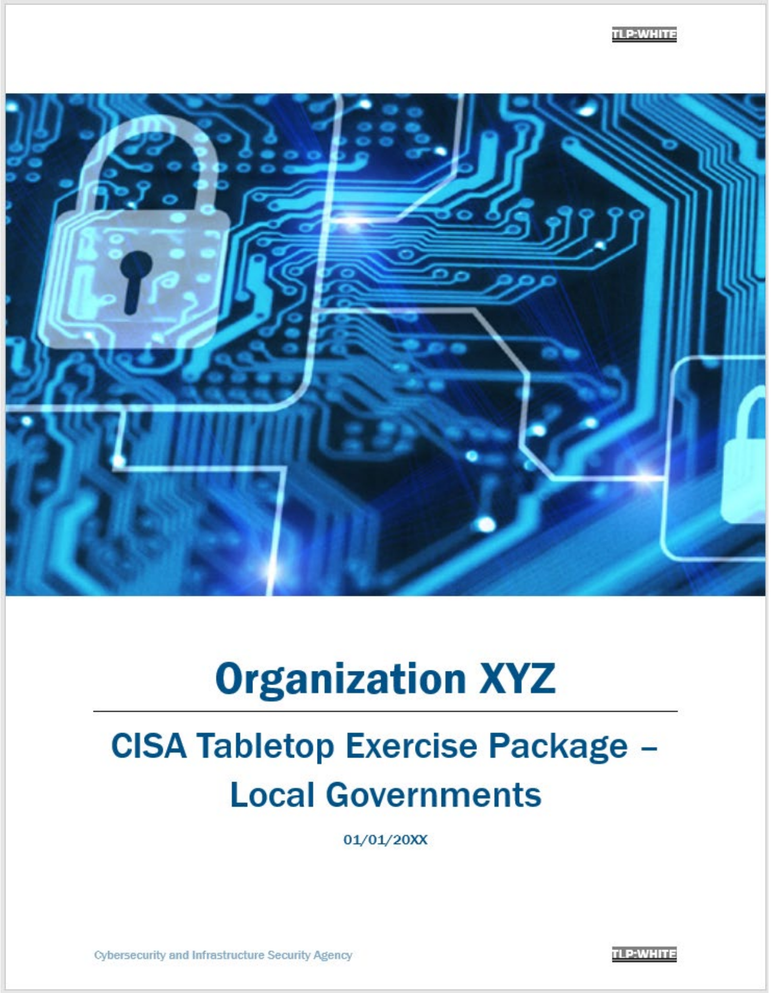
Cybersecurity Tabletop Exercise (CTTX)

Description: A non-technical 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 workshop 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



TLP:WHITE

Organization XYZ

CISA Tabletop Exercise Package – Local Governments

01/01/20XX

Cybersecurity and Infrastructure Security Agency

TLP:WHITE

National Resources

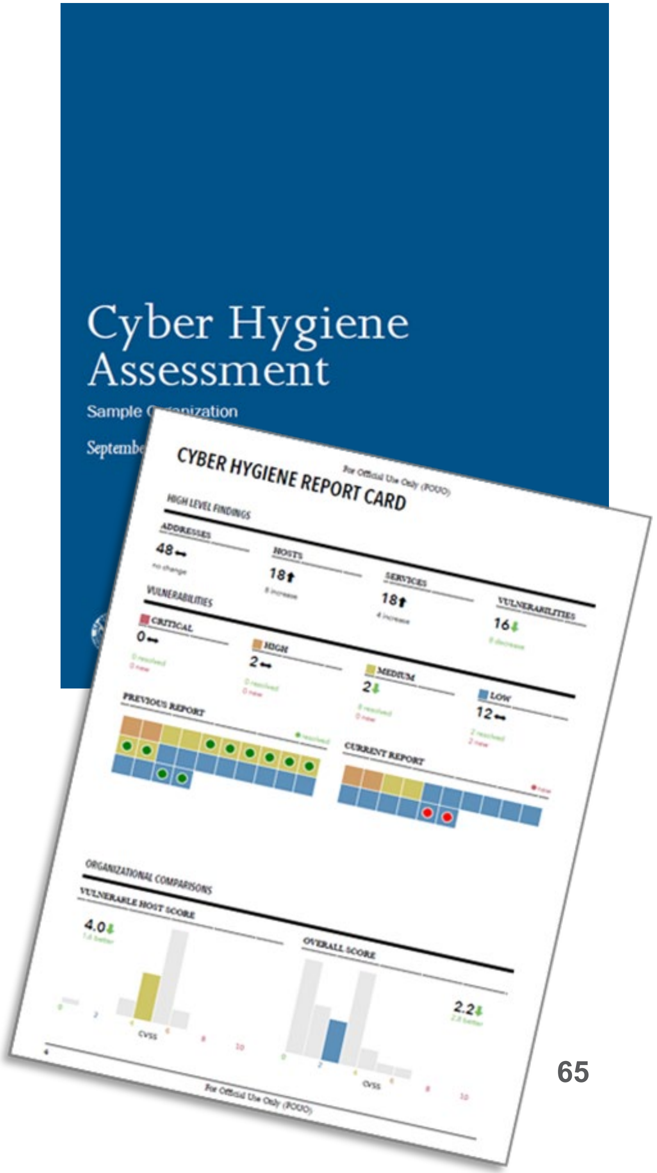
Vulnerability Scanning Service (CyHy)

Assess Internet accessible systems for known vulnerabilities and configuration errors

Work with organization to proactively mitigate threats and risks to systems

Activities include:

- Network Mapping
  - ➢ Identify public IP address space
  - ➢ Identify hosts that are active on IP address space
  - ➢ Determine the O/S and Services running
  - ➢ Re-run scans to determine any changes
  - ➢ Graphically represent address space on a map
- Network Vulnerability & Configuration Scanning
  - ➢ Identify network vulnerabilities and weakness



Cyber Hygiene Assessment

Sample Organization

Septembe

CYBER HYGIENE REPORT CARD

For Official Use Only (FOUO)

HIGH LEVEL FINDINGS

ADDRESSES 48 ⟷ no change

HOSTS 18 ↑ 8 increase

SERVICES 18 ↑ 4 increase

VULNERABILITIES 16 ↓

VULNERABILITIES

CRITICAL 0 ⟷ 0 resolved 0 new

HIGH 2 ⟷ 0 resolved 0 new

MEDIUM 2 ↓ 8 resolved 0 new

LOW 12 ⟷ 2 resolved 2 new

PREVIOUS REPORT

CURRENT REPORT

ORGANIZATIONAL COMPARISONS

VULNERABLE HOST SCORE 4.0 ↓

OVERALL SCORE 2.2 ↓

For Official Use Only (FOUO)

Cybersecurity State Coordinator of Texas: Ernesto Ballesteros
Email: ernesto.ballesteros@cisa.dhs.gov

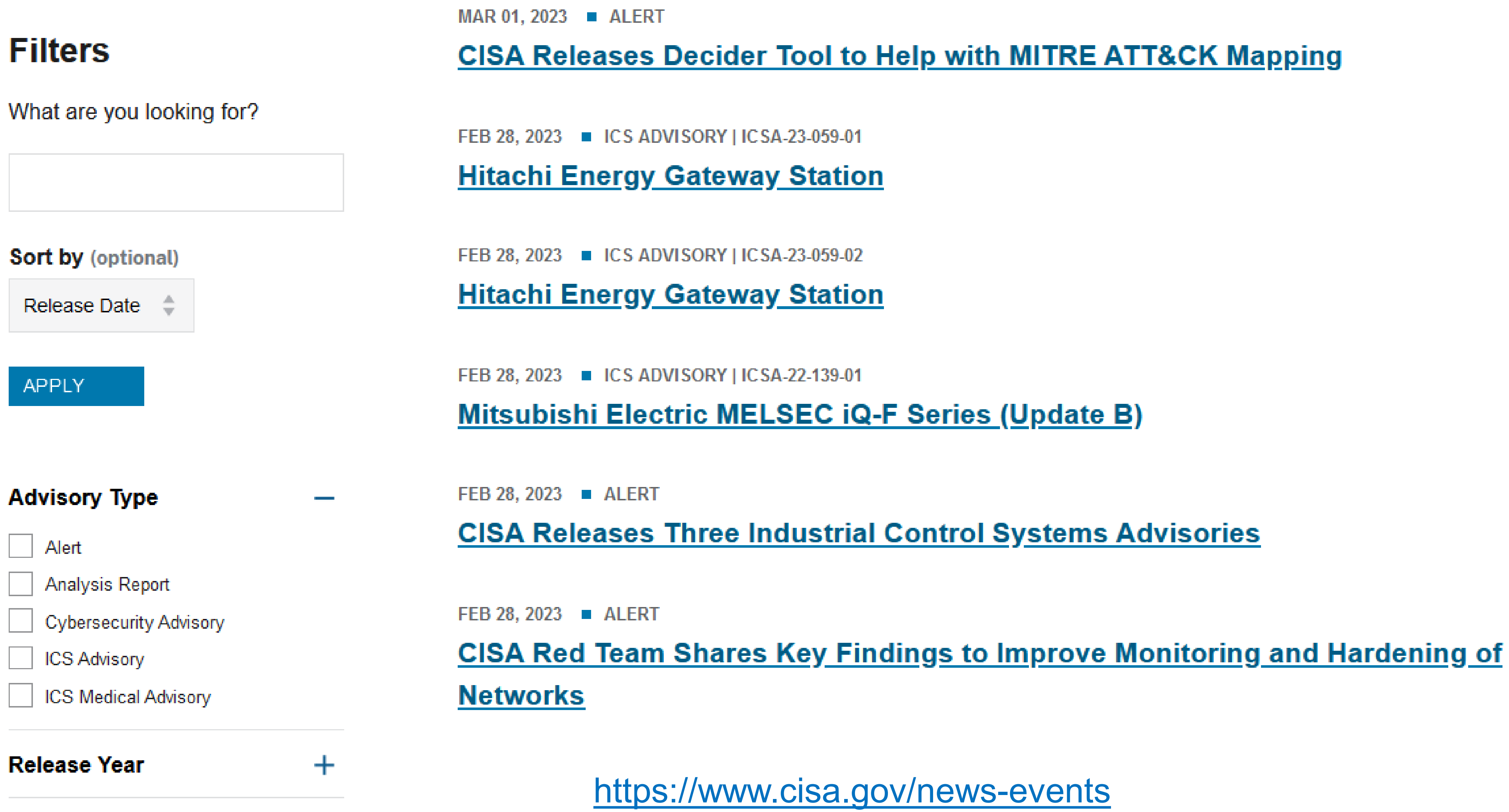
Information Sharing & Situational Awareness Resources

Automated Indicator Sharing (AIS)

- **Automated Indicator Sharing (AIS**): Rapid and wide sharing of machine-readable cyber threat indicators and defensive measures at machine-speed for network defense purposes
- AIS is about volume and velocity of sharing indicators, ***not*** human validation.

Link: [Automated Indicator Sharing (AIS) | CISA]()

Cybersecurity Alerts & Advisories



Filters

What are you looking for?

Sort by (optional)

Release Date

APPLY

Advisory Type

□ Alert
□ Analysis Report
□ Cybersecurity Advisory
□ ICS Advisory
□ ICS Medical Advisory

Release Year

MAR 01, 2023 ■ ALERT
CISA Releases Decider Tool to Help with MITRE ATT&CK Mapping

FEB 28, 2023 ■ ICS ADVISORY | ICSA-23-059-01
Hitachi Energy Gateway Station

FEB 28, 2023 ■ ICS ADVISORY | ICSA-23-059-02
Hitachi Energy Gateway Station

FEB 28, 2023 ■ ICS ADVISORY | ICSA-22-139-01
Mitsubishi Electric MELSEC iQ-F Series (Update B)

FEB 28, 2023 ■ ALERT
CISA Releases Three Industrial Control Systems Advisories

FEB 28, 2023 ■ ALERT
CISA Red Team Shares Key Findings to Improve Monitoring and Hardening of Networks

https://www.cisa.gov/news-events

Cybersecurity Education and Training Resources

Federal Virtual Training Environment (FedVTE)

Cyber professionals can continue to improve their skills through hands-on training opportunities.

FedVTE is an online, on-demand training center that provides free cybersecurity training for federal, state, local, tribal, and territorial government employees and to U.S. veterans.

Example Content:

- Cloud Computing Security
- Cloud Security - What Leaders Need to Know
- Cryptocurrency for Law Enforcement for the Public
- Cyber Supply Chain Risk Management for the Public
- Cyber-essentials
- Understanding DNS Attack
- Understanding Web and Email Server Security
- Don't Wake Up to a Ransomware Attack
- Foundations of Cybersecurity for Managers
- Fundamentals of Cyber Risk Management
- Introduction to Cyber Intelligence
- Securing Internet-Accessible Systems
- 101 Coding for the Public
- 101 Reverse Engineering for the Public

https://fedvte.usalearning.gov

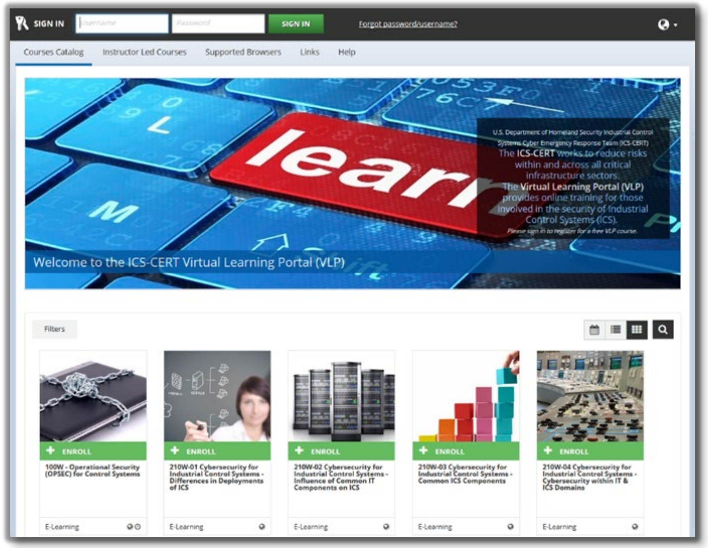
ICS Training Opportunities

ICS-CERT Virtual Learning Portal (VLP)

- Virtual & Instructor Led Training; No Cost

Courses:

- Introduction to Control Systems Cybersecurity (101) - 8 hrs
- Intermediate Cybersecurity for Industrial Control Systems (201) - 8 hrs
- Intermediate Cybersecurity for Industrial Control Systems (202) - 8 hrs
- ICS Cybersecurity (301V) - 12 hrs
- ICS Cybersecurity (301L) - 5 days
- ICS Cybersecurity (401) - 5 days



U.S. Department of Homeland Security Industrial Control Systems Cyber Emergency Response Team (ICS-CERT)
The ICS-CERT works to reduce risks within and across all critical infrastructure sectors.
The Virtual Learning Portal (VLP) provides online training for those involved in the security of Industrial Control Systems (ICS).
Please sign in to register for a free VLP course.

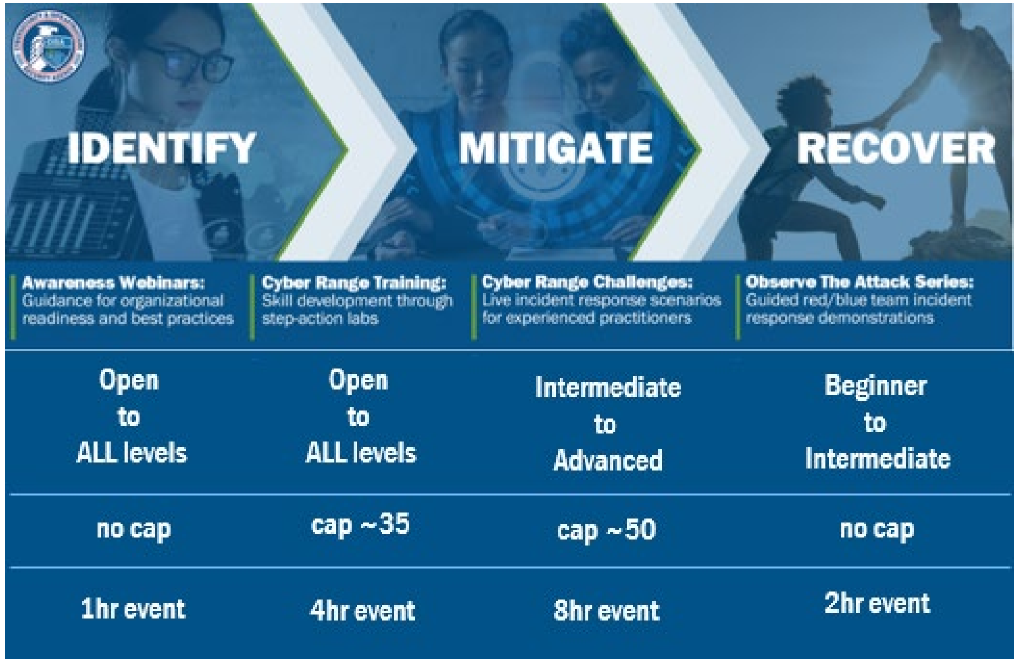
Welcome to the ICS-CERT Virtual Learning Portal (VLP)

100W - Operational Security (OPSEC) for Control Systems	E-Learning
210W-01 Cybersecurity for Industrial Control Systems - Differences in Deployments of ICS	E-Learning
210W-02 Cybersecurity for Industrial Control Systems - Influence of Common IT Components on ICS	E-Learning
210W-03 Cybersecurity for Industrial Control Systems - Common ICS Components	E-Learning
210W-04 Cybersecurity for Industrial Control Systems - Cybersecurity within IT & ICS Domains	E-Learning

https://ics-training.inl.gov/learn/signin

IMR Training Series

The Identify, Mitigate, and Recover (IMR) incident response curriculum provides a range of training offerings encompassing cybersecurity awareness and best practices for organizations, live red/blue team network defense demonstrations emulating real-time incident response scenarios, and hands-on cyber range training courses for incident response practitioners.



Awareness Webinars: Guidance for organizational readiness and best practices	**Cyber Range Training:** Skill development through step-action labs	**Cyber Range Challenges:** Live incident response scenarios for experienced practitioners	**Observe The Attack Series:** Guided red/blue team incident response demonstrations
Open to ALL levels	Open to ALL levels	Intermediate to Advanced	Beginner to Intermediate
no cap	cap ~35	cap ~50	no cap
1hr event	4hr event	8hr event	2hr event

Topics for Awareness Webinars & Cyber Range Training:

- Ransomware
- Cloud Security
- Business Email Compromise
- Vulnerabilities of Internet-Accessible Systems
- Web and Email Server Attacks
- DNS Infrastructure Attacks
- High Value Assets/Critical Assets
- Indicators of Compromise
- Incident Analysis with tool demo
- Investigating logs for incidents

Topics for Cyber Range Challenges & Observe the Attack Series:

- Ransomware
- Cloud Security
- Business Email Compromise

For more info: education@cisa.dhs.gov
Or visit: https://www.cisa.gov/incident-response-training

Cybersecurity Incident Reporting

Phishing and Incident Reporting / Malware Analysis

24x7 contact number: 888-282-0870 | central@cisa.dhs.gov

Where/How/When to Report Incidents: https://www.cisa.gov/forms/report

If there is a suspected or confirmed cyber attack or incident that affects core government or critical infrastructure functions and/or results in the loss of data, system availability or control of systems.

Report Phishing to: phishing-report@us-cert.gov

CISA partners with the Anti-Phishing Working Group (APWG) to collect phishing email messages and website locations to help people avoid becoming victims of phishing scams.

Advanced Malware Analysis Center: https://malware.us-cert.gov

Provides 24x7 dynamic analyses of malicious code. Stakeholders submit samples via an online website and receive a technical document outlining the results of the analysis. Experts will detail recommendations for malware removal and recovery activities.

Next Steps: Partnership Formation

Would you like to know more about CISA’s no-cost cyber resources and partnership opportunities?

Next Steps:

1. Contact your CISA Regional Office (Region Offices);
2. Request an initial Cyber Protective Visit (CPV) from your Cybersecurity Advisor (CSA) or State Cybersecurity Coordinator (CSC); and
3. Explore discuss how CISA can assist you in assessing and managing your organization’s cybersecurity risk.

Email: ernesto.ballesteros@cisa.dhs.gov

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

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@hq.dhs.gov

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