SHIELDS UP

A BRIEF OVERVIEW OF RECOMMENDED ACTIONS AND RESOURCES FOR IMPROVING NEAR-TERM CYBER RESILIENCE

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

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

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

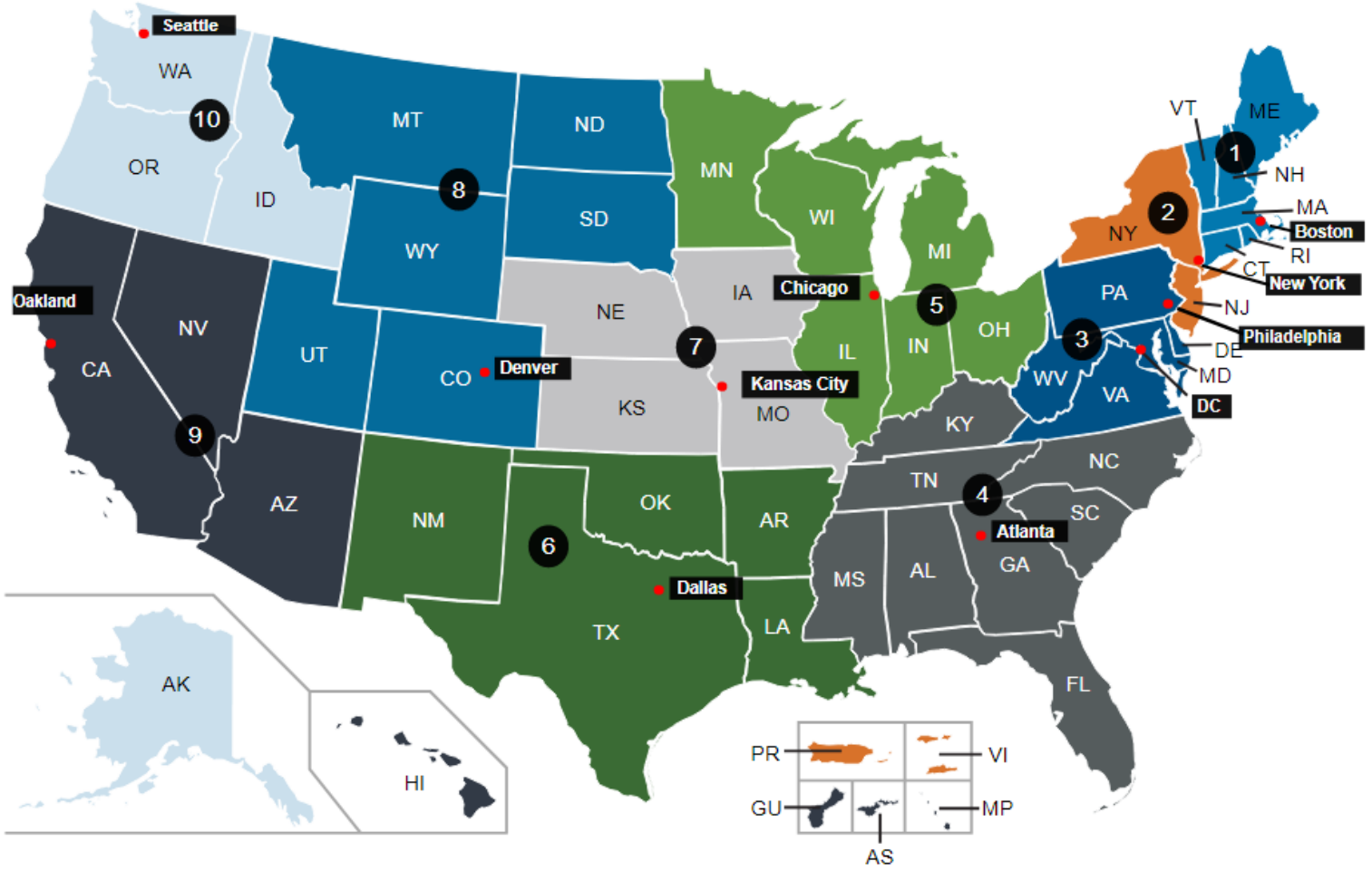
EMERGENCY COMMUNICATIONS

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.

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 (CSC)

The role of the Cybersecurity State Coordinator (CSC) is to build strategic public and private sector relationships in Texas to facilitate the development and maintenance of secure and resilient infrastructure, pursuant to 6 United States Code, Section 665(c) (2021).

- 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 principle 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 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.

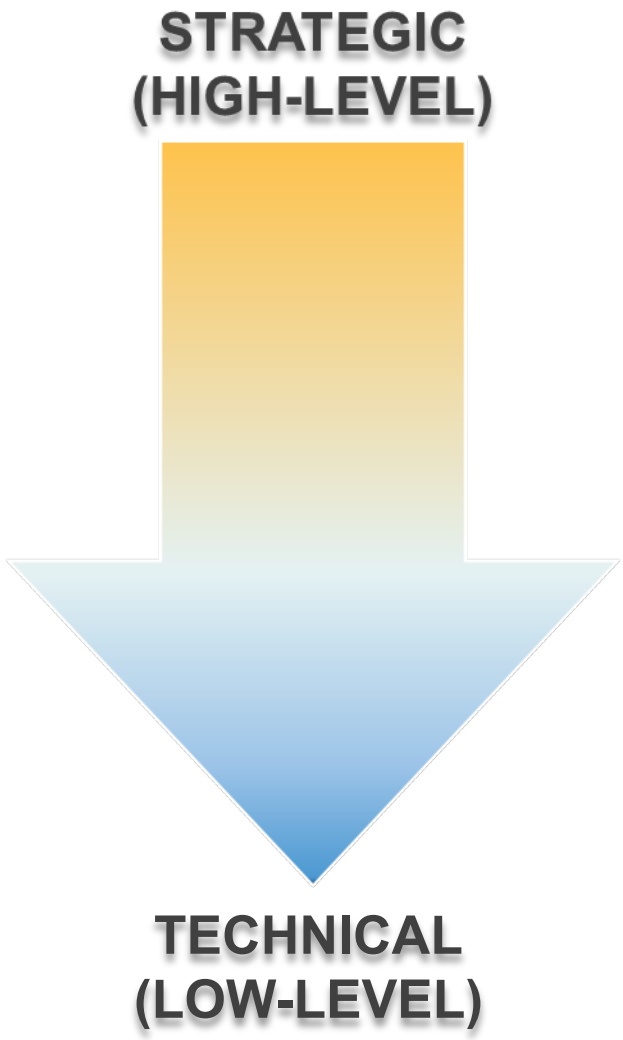
No-Cost Cyber Resources and Assessments

No-Cost Regional Cybersecurity Resources:

- Cyber Resilience Review (CRR) Assessment
- External Dependencies Management (EDM) Assessment
- Cyber Infrastructure Survey (CIS) Assessment
- Ransomware Readiness Assessment (REA)
- Workshops (Incident Management, Cyber Resilience, Vulnerability Management)

No-Cost National Cybersecurity Resources:

- Phishing Campaign Assessment (PCA)
- Cyber Tabletop Exercises (CTTX)
- Vulnerability Scanning Service (CyHy)
  - Web Application Scanning (WAS)
- Validated Architecture Design Review (VADR)
- Remote Penetration Test (RPT)
- Risk & Vulnerability Assessment (RVA)



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

SHIELDS UP

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

What is Information Security?

Definition: Information Security

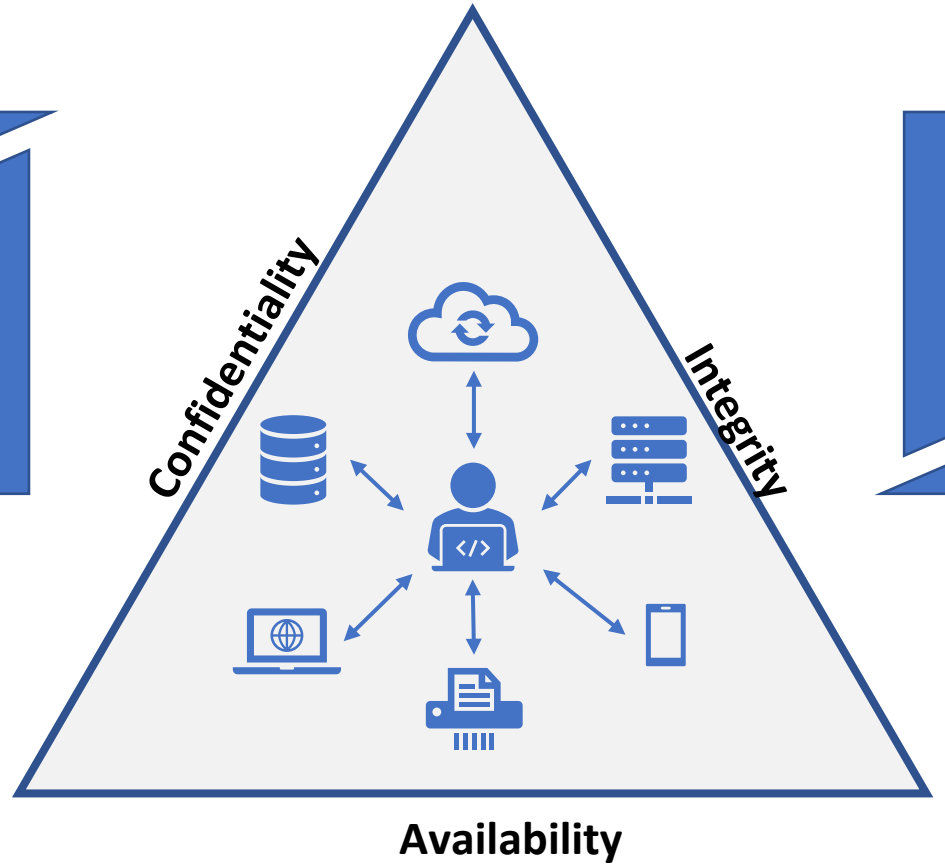
According to NIST, **Information Security** is *"[t]he protection of information and information systems against unauthorized access, use, disclosure, modification, or destruction in order to provide confidentiality, integrity, and availability."*

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



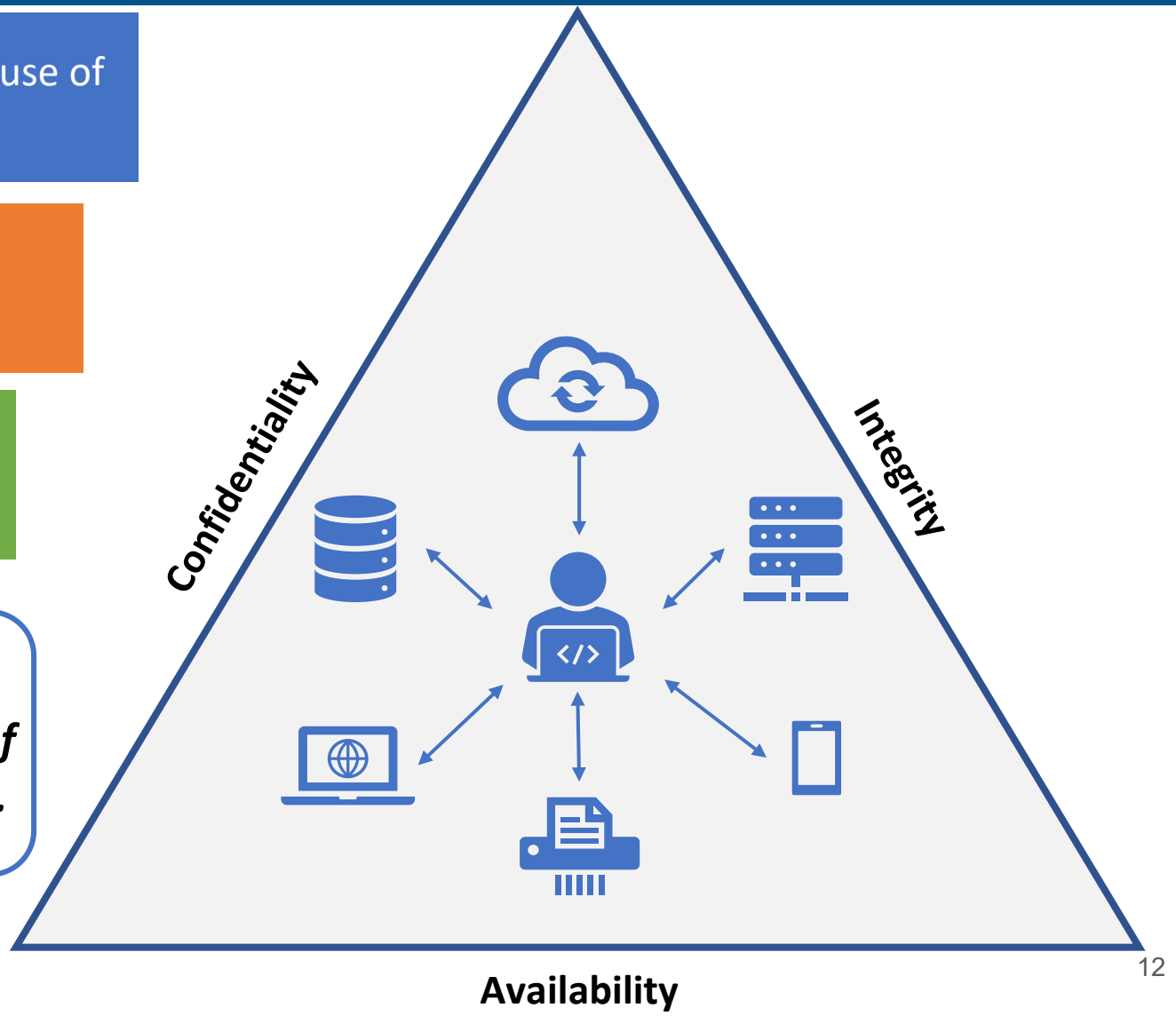
Information System refers to *"[a] discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information."*

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

Core Principles of Information Security

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

Users must exercise due care to ensure the confidentiality, integrity, and availability of the information resources under their care.



Threats

THREATS

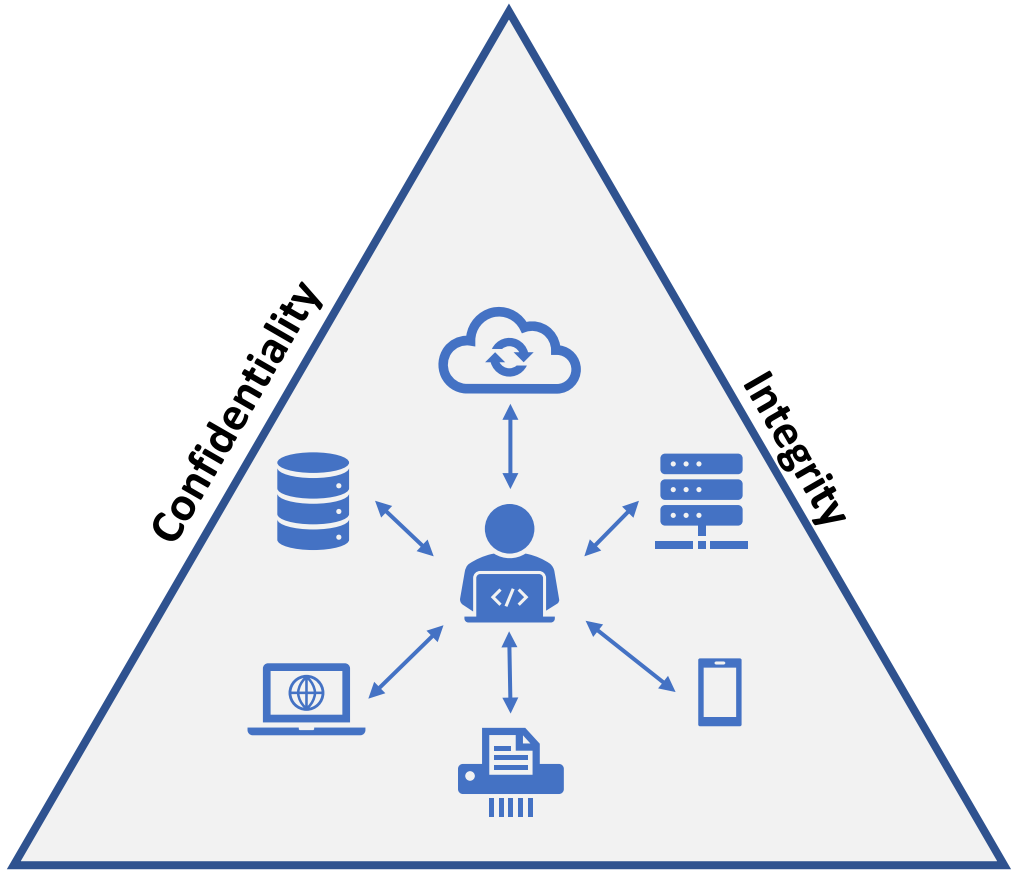
Nature-Based

Threats that naturally occur, such as fires, floods, or hurricanes.

Human-Based

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

Impact: Confidentiality, Integrity, and 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.

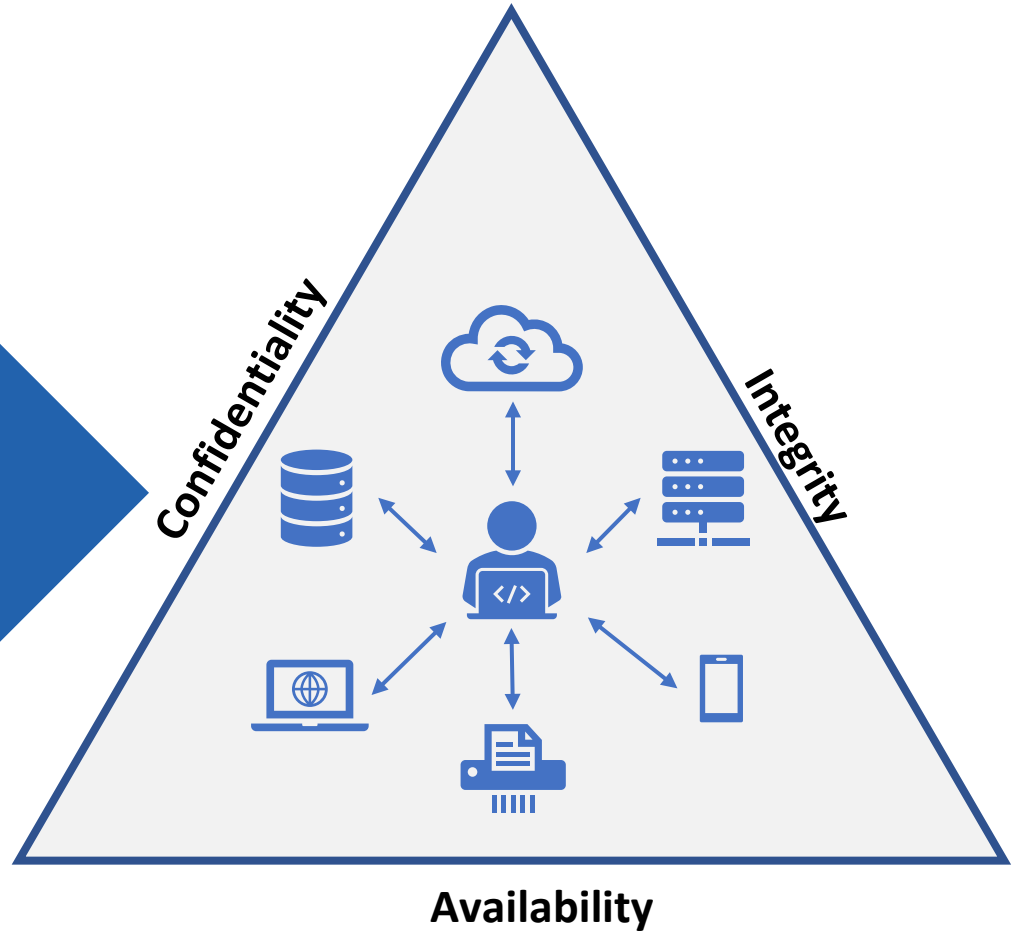
INSIDERS

Conduct attacks in furtherance of personal interests.

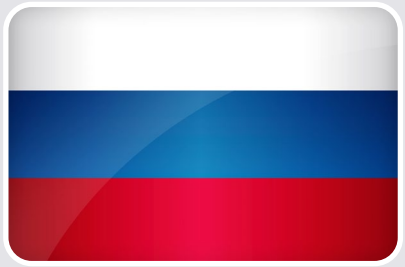
STATE ACTORS

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

Impact: Confidentiality, Integrity, and Availability



ODNI 2021 Annual Threat Assessment



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

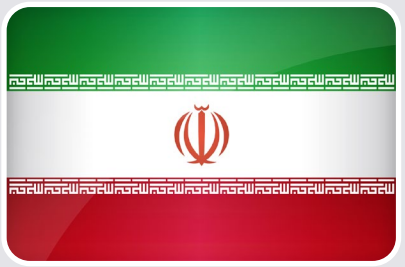
- Continues to target critical infrastructure, including underwater cables and industrial control systems.

- 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.

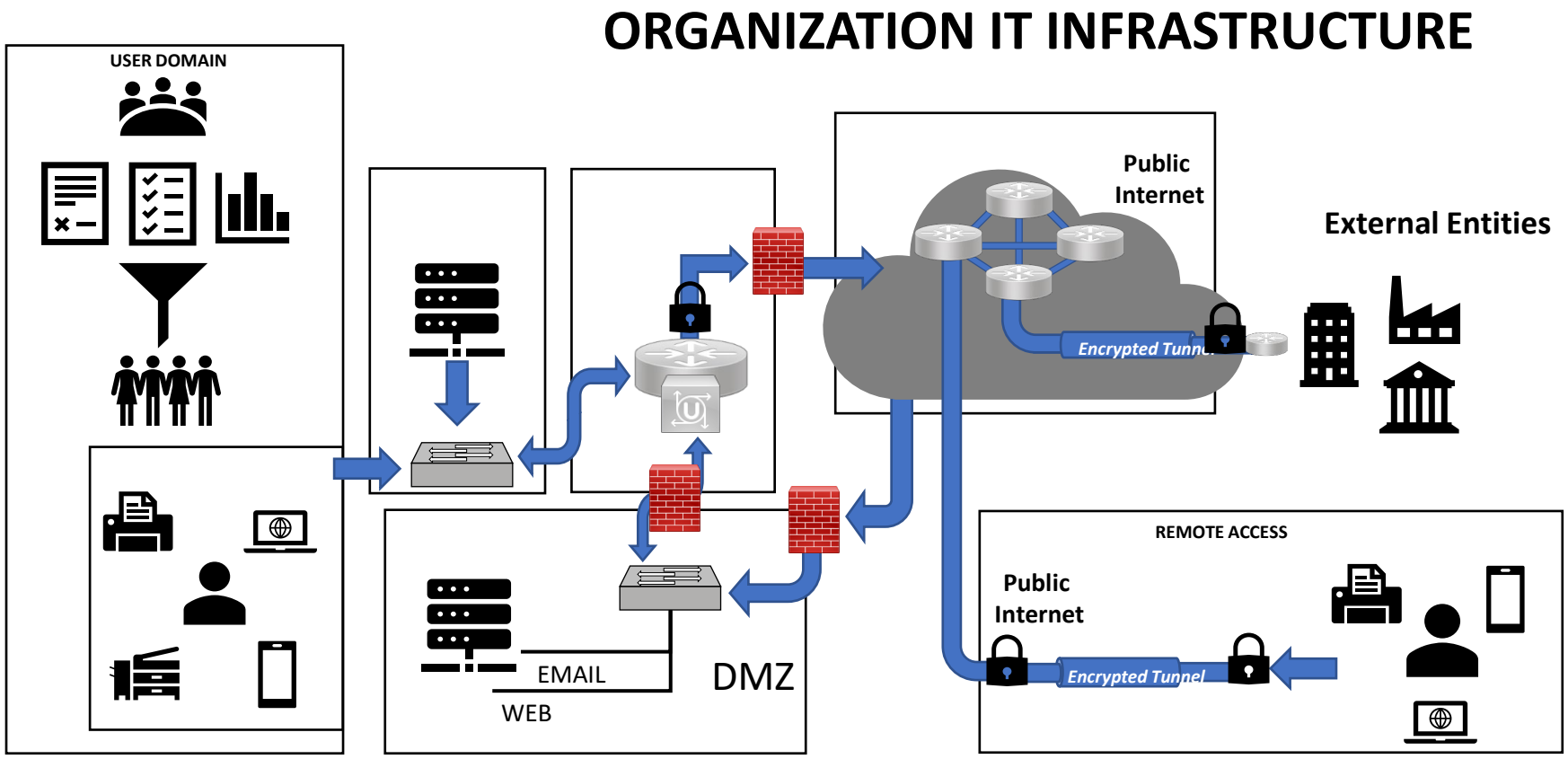
- Responsible for multiple cyber attacks against Israeli water facilities.

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: Assets as Targets



THREAT ACTOR

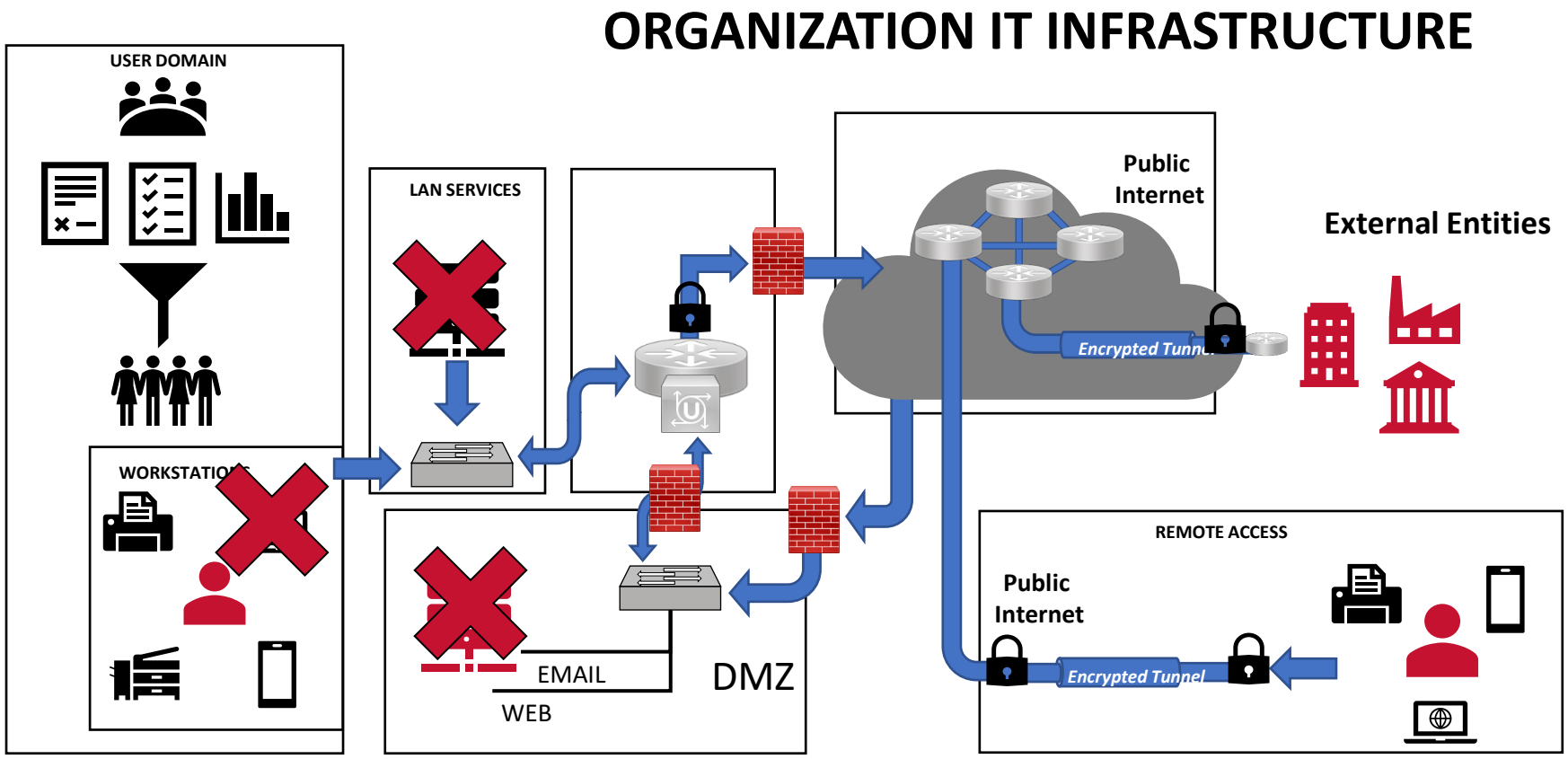
Planning
- Identify target(s)

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

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

Prime Targets: Vulnerable Devices, Users, and Vendors

Cyber Attacks: Service Disruption



THREAT ACTOR

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

Cyber Attacks: Attacks on Users

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 Actor Objective**:
  - Manipulate a target (i.e., a user) into providing unauthorized access to information or information systems.
- **Common Threat Actor Techniques**:

  Phishing (Email-Based)

  SMISHING (SMS-Based)

  VISHING (Voice-Based)

  Masquerading (In-Person/Physical)

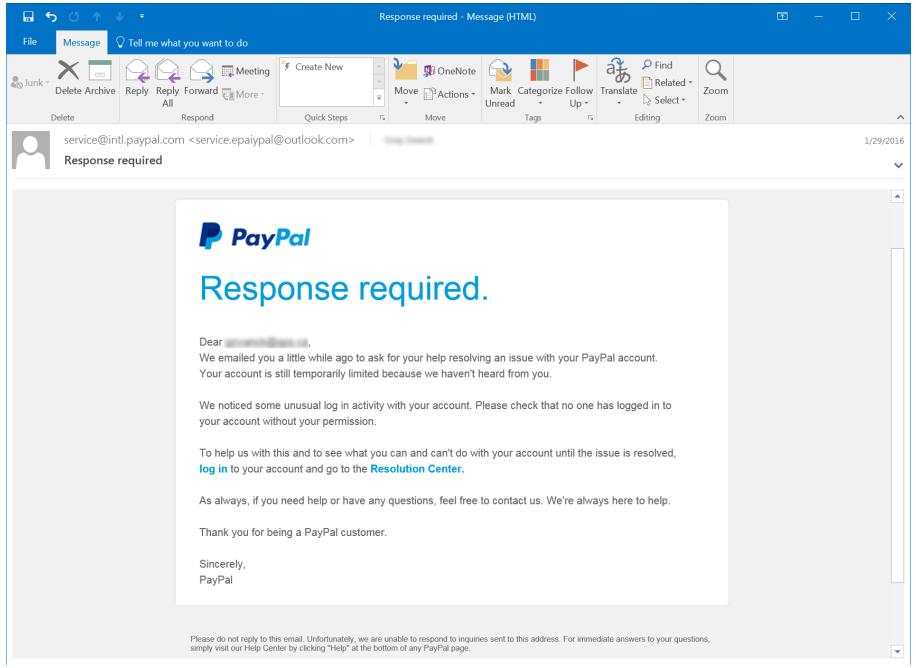
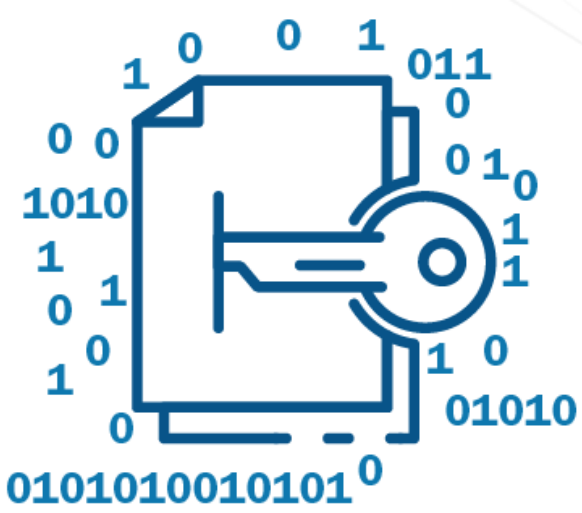


Image Source: knowbe4.com

Cyber Attacks: Ransomware

Ransomware Attack

- **Ransomware:** 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



Shields Up: Objective

https://www.cisa.gov/shields-up

Heightened Cybersecurity Posture

- Objective: Adopt a Heightened Cybersecurity Posture
- Near-Term Actions:
  1. Minimize Attack Surface
     i. Reducing the likelihood of a damaging cyber intrusion
  2. Monitor and Protect Network
     i. Detecting a potential cyber intrusion
  3. Incident Response: Exercise Your Plan
     i. Prepare to respond to cyber intrusions
  4. Operational Resilience: Backups & Redundancy
     i. Maximize operational resilience to a cyber incident
  5. See Something, Report Something

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

https://www.cisa.gov/shields-up

Step 1: Minimize Attack Surface

Reduce the Likelihood of Damaging Cyber Intrusions

Minimize Attack Surface: Near-Term Steps

- Minimize Attack Surface and Harden Assets (Lock Doors & Windows)
  - Implement Multi-Factor Authentication for all accounts according to best practices
  - Enforce a strong password policy across the organization
  - Stop Bad Practices
    - End-of-Life Software, Default Accounts, Single-Factor Authentication
  - Update Software
    - Prioritize known exploitable vulnerabilities identified by CISA
  - System Hardening
    - Remove unnecessary accounts, ports, services, software on machines
  - Adopt CISA's Cloud Services Security Best Practices
    - CISA's Cloud Service Guidance
  - Signup for CISA's Cyber Hygiene Services (External/Internet-Facing Scans)
    - Vulnerability Scanning
    - Web Application Scanning
  - Perform regular internal vulnerability scans
  - Run antivirus software throughout your network
  - Enable strong spam filters to prevent phishing emails from reaching end user
    - Train end users to identify, respond to, and report on phishing attacks

https://www.cisa.gov/uscert/shields-technical-guidance

Vulnerability Scanning Service (CyHy)

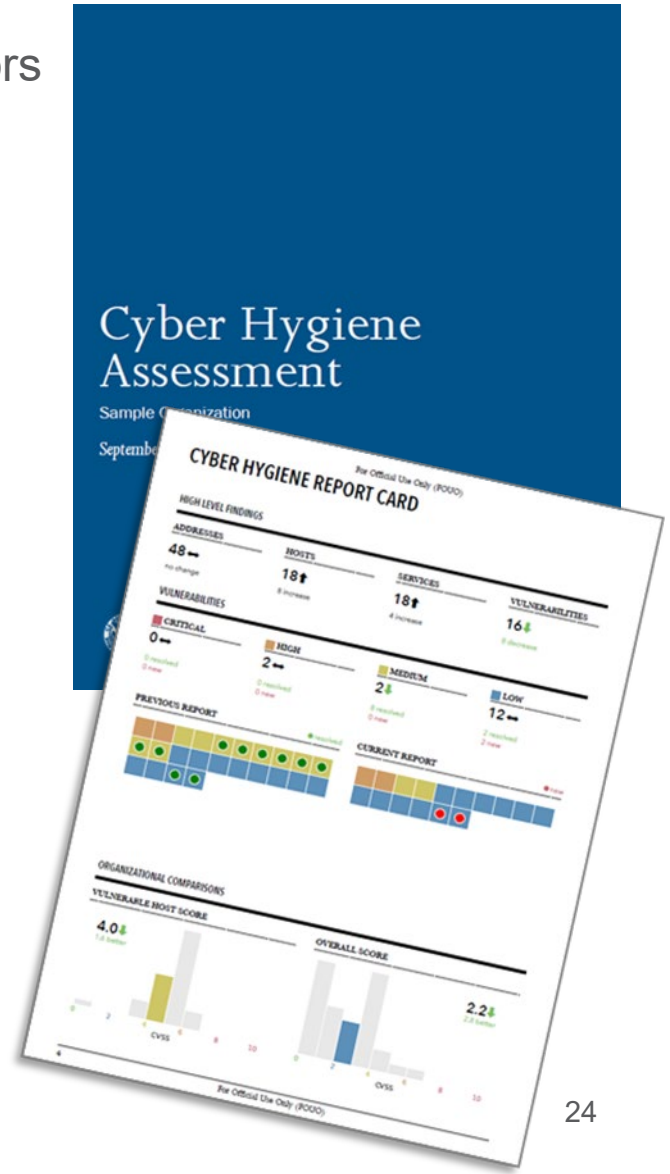
Assess Internet accessible systems for known vulnerabilities and configuration errors

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



https://www.cisa.gov/cyber-hygiene-services

Web Application Scanning Service (CyHy)

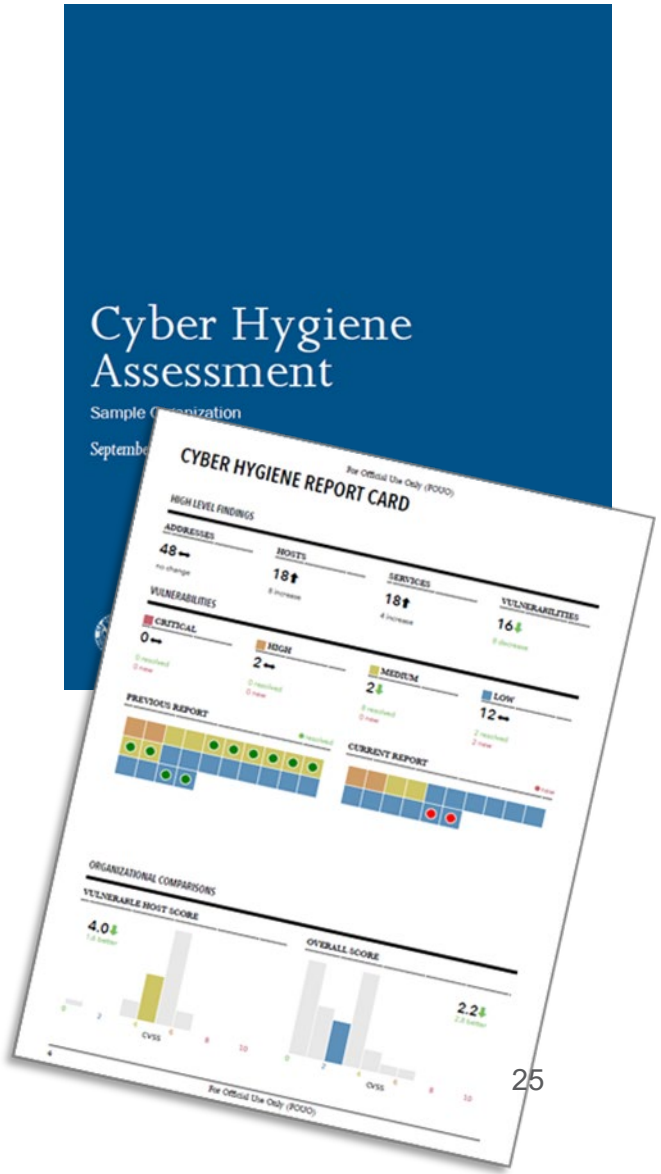
An Internet-based scanning service that assesses the “health” of your publicly accessible web applications, checking for known vulnerabilities and weak configurations.

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: Identifying active, internet-facing web applications
- Vulnerability Scanning: initiate non-intrusive checks to identify vulnerabilities and configuration weaknesses



https://www.cisa.gov/cyber-hygiene-services

Step 2: Monitor and Protect

Take Steps to Quickly Detect a Potential Intrusion

Monitor and Protect

- Monitor and Protect the Network: Near-Term Steps for "Heightened Security Posture"
  - Monitor your network for unusual behavior
    - Enable logging
    - Monitor hosts
    - Monitor network traffic
    - Monitor external vendors and/or contractors
  - Deploy host- and network-based anti-virus/anti-malware controls
    - Keep the signatures updated

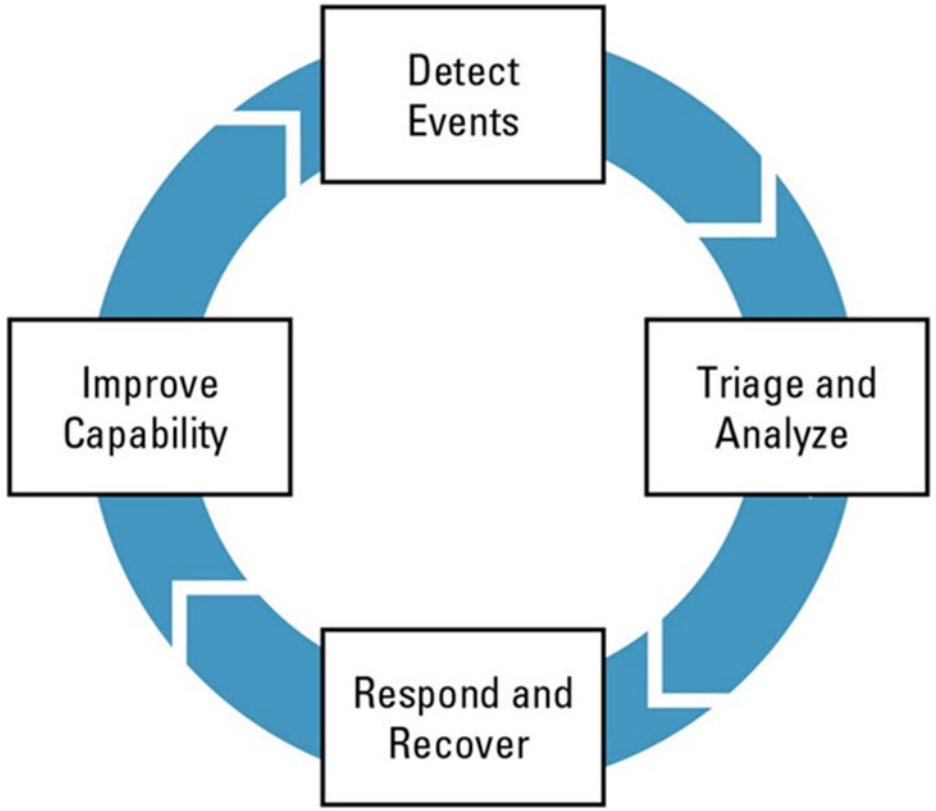
Step 3: Incident Management

Be Prepared to Respond to Cyber Incidents

What is Incident Management?

The process of detecting, analyzing, responding to, and improving from disruptive events is known as incident management.

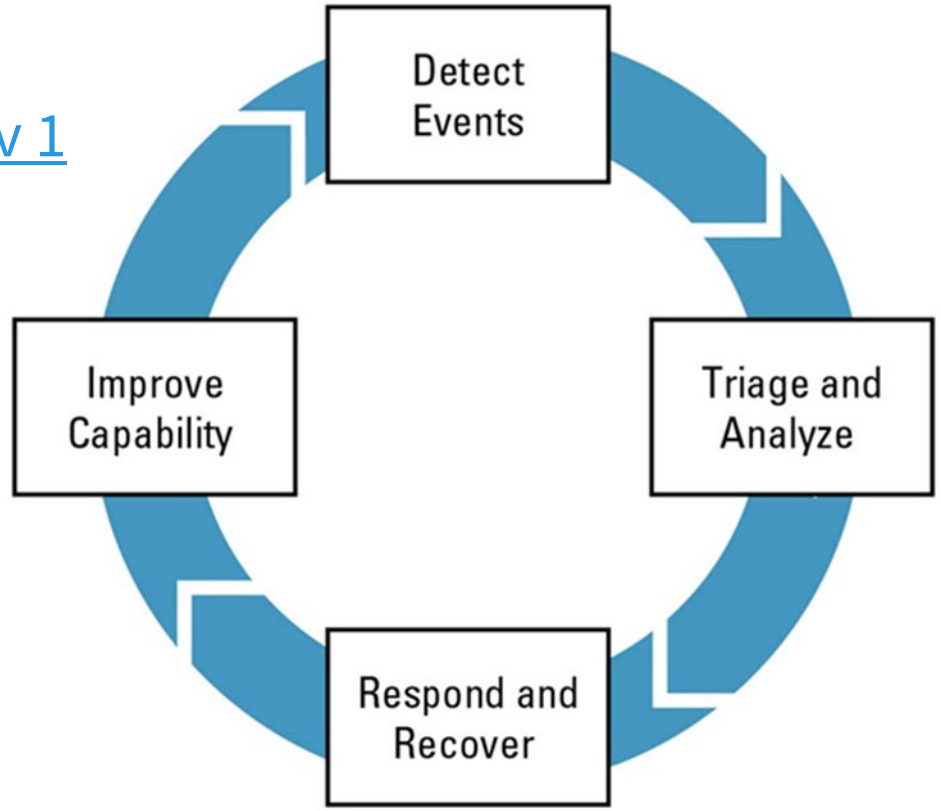
The goal of incident management is to mitigate the impact of a disruptive event.



What is an Incident Response Plan?

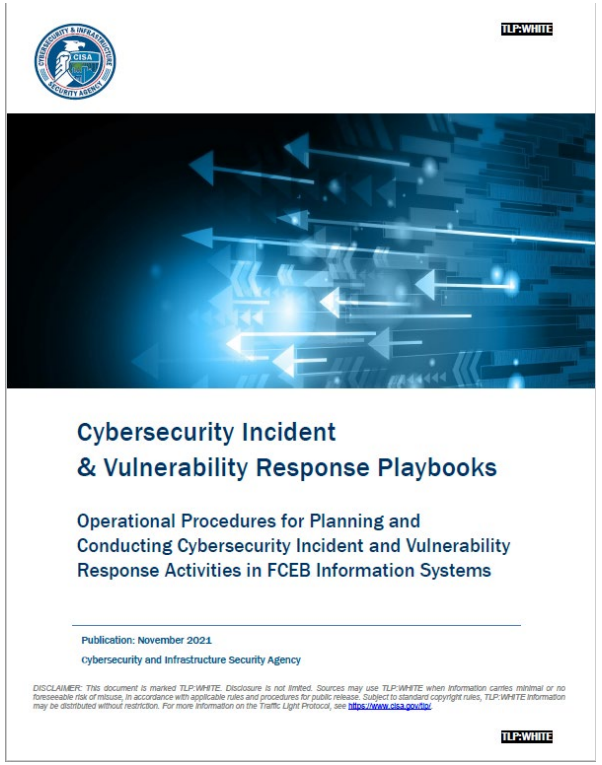
According to NIST, an **Incident Response Plan** is *"[t]he documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization's information system(s)."*

Source: NIST SP 800-34 Rev 1



Incident Management: Near-Term Steps

- Incident Management/Response: Near-Term Steps for “Heightened Security Posture”
  - Designate an incident response team
  - Assure availability of key personnel
  - If you have an incident response plan – assess it with a tabletop exercise
  - If you **DO NOT** have an incident response plan – create one now
    - CISA Ransomware Guide
    - Federal Government Cybersecurity Incident and vulnerability response playbooks
    - CISA Incident Management Workshop
- CISA Ransomware Guide
  - Part 1: Ransomware Prevention Best Practices
  - Part 2: Ransomware Response Checklist



https://www.cisa.gov/uscert/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability

https://www.cisa.gov/cisa-tabletop-exercises-packages

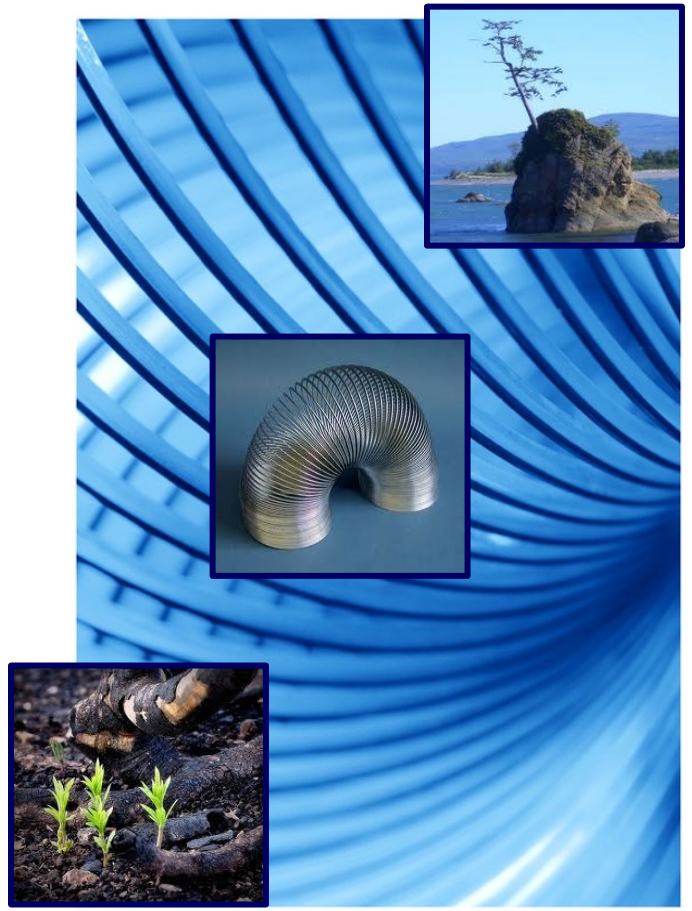
Step 4: Operational Resilience

Maximize Organization Resilience to Destructive Cyber Incidents

What is Operational Resilience?

The emergent property of an organization that allows it to:

- Prevent disruptions from occurring
- Quickly respond to and recover from a disruption affecting its most critical business processes and services



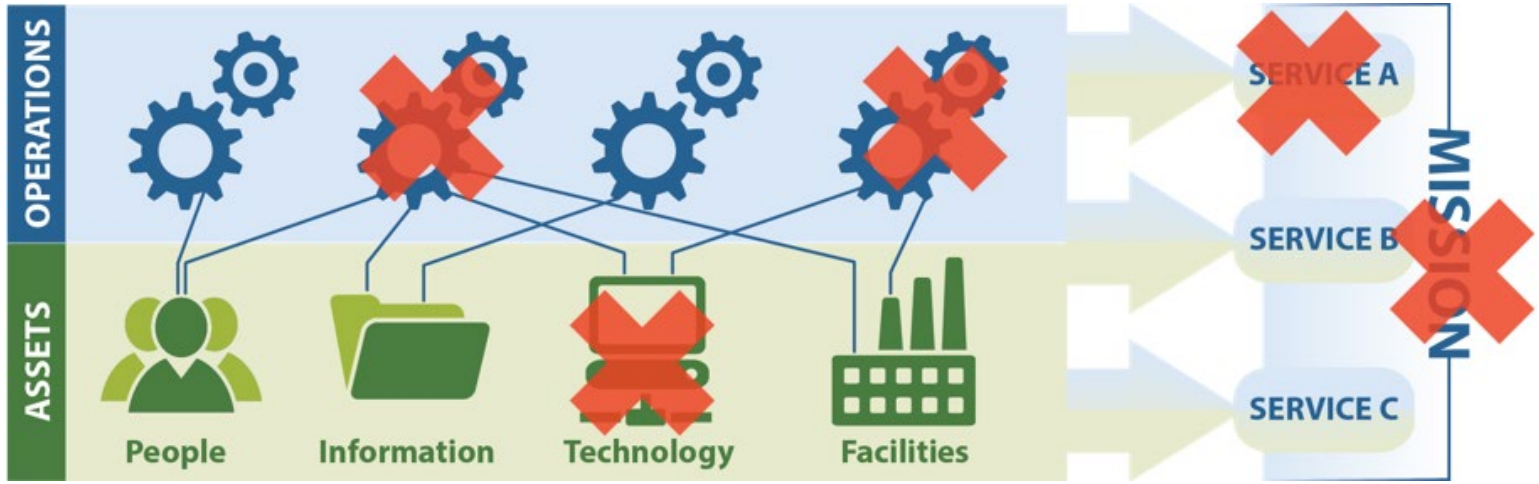
Making Operational Resilience Real

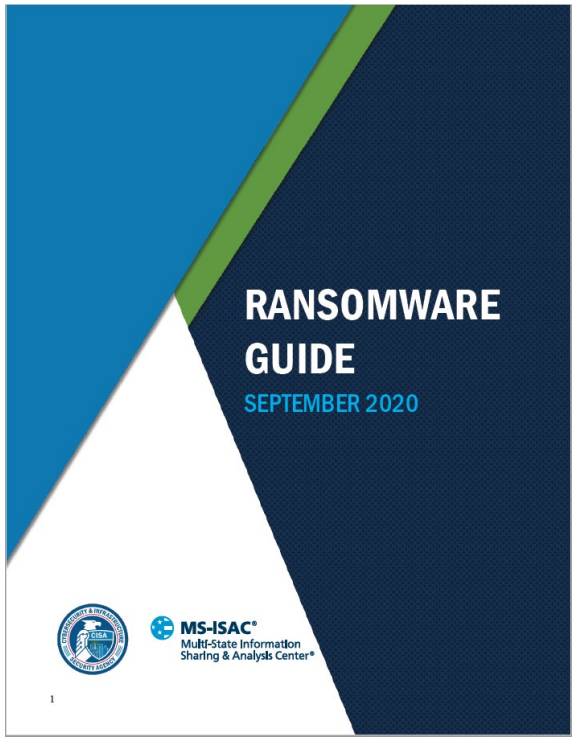
Operational resilience emerges from what we do, such as:

- Identifying critical services and assets
- Identifying and mitigating risks
- Planning for and managing vulnerabilities and incidents
- Performing service-continuity processes and planning
- Managing IT operations
- Managing, training, and deploying people
- Working with external partners

Operational Resilience: Near-Term Steps

- Operational Resilience: Near-Term Steps for “Heightened Security Posture”
  - Backup mission-critical data, software, and “gold images”
  - Store backups off-line (preferably encrypted)
  - Test these backups
  - Acquire backup/redundant mission-critical hardware
  - Assess the readiness of your alternative/recovery site



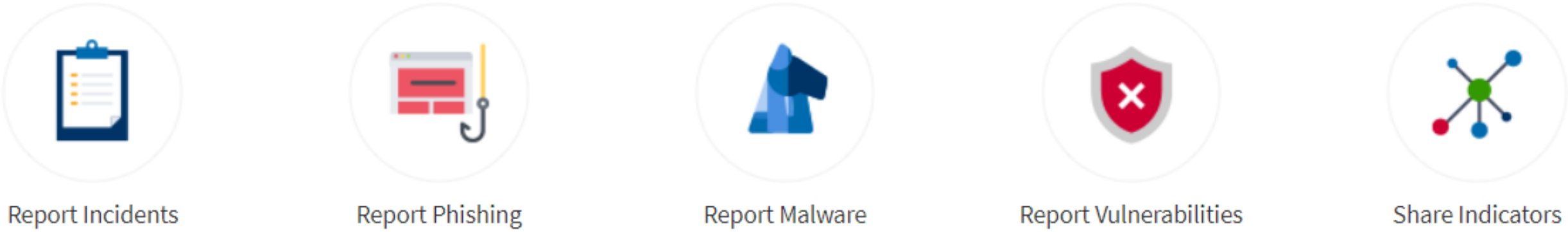


https://www.cisa.gov/stopransomware/ransomware-guide

Step 5: See Something -- Report Something

Lower Reporting Thresholds

See Something – Report Something



Organizations should report anomalous cyber activity and/or cyber incidents 24/7 to report@cisa.gov or (888) 282-0870.

https://www.cisa.gov/uscert/report

Incident Reporting

CISA Incident Reporting System

Report incidents that include:

1. Attempts to gain unauthorized access to a system or its data;
2. Unwanted disruption or denial of service; or
3. Abuse or misuse of a system or data in violation of policy.

Report Incidents

CISA's 24x7 contact number: 888-282-0870 | report@cisa.gov

FBI's 24x7 CyWatch: 855-292-3937 | CyWatch@fbi.gov

https://us-cert.cisa.gov/forms/report

Report Phishing

CISA Phishing Reporting

Report phishing:

1. We partner with the Anti-Phishing Working Group (APWG);
2. Report a phishing email message; or
3. Report a phishing website.

https://www.cisa.gov/uscert/report-phishing

Report Malware

CISA Advanced Malware Analysis Center

Report malware artifacts for analysis:

1. 24x7 dynamic analysis of malicious code;
2. Submissions made online;
3. Receive technical documentation outlining results of the analysis; and
4. Detailed recommendations for removal and recovery activities.

https://www.malware.us-cert.gov/

Report Vulnerabilities

CISA Coordinated Vulnerability Disclosure (CVD) Process

Report newly identified cybersecurity vulnerabilities in products and services with the affected vendor(s):

1. Collection;
2. Analysis;
3. Mitigation coordination;
4. Application of Mitigation; and
5. Disclosure.

https://www.cisa.gov/coordinated-vulnerability-disclosure-process

Share Indicators and Defensive Measures

CISA Automated Indicator Sharing Program

Automated Indicator Sharing (AIS):

1. Real-time exchange of machine-readable cyber threat indicators and defensive measures;
2. AIS information sharing ecosystem of state, local, tribal, territorial, and private sector entities; and
3. Facilitates anonymized sharing with CISA and AIS community.

https://www.cisa.gov/ais

Shields Up: Remain Vigilant

https://www.cisa.gov/shields-up

Next Steps

Forming a Partnership with CISA Pre-Incident

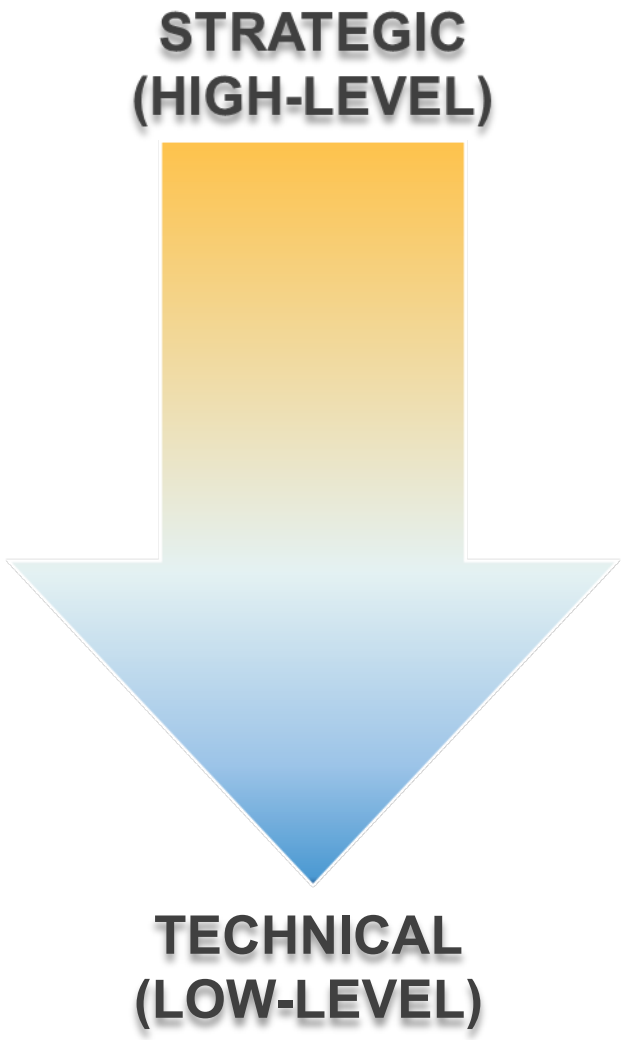
No-Cost Cyber Resources and Assessments

No-Cost Regional Cybersecurity Resources:

- Cyber Resilience Review (CRR) Assessment
- External Dependencies Management (EDM) Assessment
- Cyber Infrastructure Survey (CIS) Assessment
- Ransomware Readiness Assessment (REA)
- Workshops (Incident Management, Cyber Resilience, Vulnerability Management)

No-Cost National Cybersecurity Resources:

- Phishing Campaign Assessment (PCA)
- Cyber Tabletop Exercises (CTTX)
- Vulnerability Scanning Service (CyHy)
  - Web Application Scanning (WAS)
- Validated Architecture Design Review (VADR)
- Remote Penetration Test (RPT)
- Risk & Vulnerability Assessment (RVA)



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

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 CISA Cyber Mission & Resource Briefing from your Cybersecurity Advisor (CSA) or State Cybersecurity Coordinator;
3. Explore partnership opportunities with CISA; and
4. Identify applicable no-cost regional and national cyber resources for your organization.

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

Additional Resources

- CISA Shields Up Webpage
- Alert (AA22-047A): Russian State-Sponsored Cyber Actors Target Cleared Defense Contractor Networks to Obtain Sensitive U.S. Defense Information and Technology (February 2022)
- CISA Insights: Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats (January 2022)
- Alert (AA22-011A): Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure (January 2022)
- CISA Insights: Preparing for and Mitigating Potential Cyber Threats (December 2021)
- Reminder for Critical Infrastructure to Stay Vigilant Against Threats During Holidays and Weekends (November 2021)
- Russian Cyber Threat Overview and Advisories
- CISA Catalog of Free Cybersecurity Services
- CISA Cyber Resource Hub
- CISA's Free Cybersecurity Services and Tools Webpage

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

CISA REGION 6

Ernesto Ballesteros, JD, MS, CISSP, CISA, Security+

State Cybersecurity Coordinator, Region 6 (Texas)
Cybersecurity and Infrastructure Security Agency

EMAIL: ernesto.ballesteros@cisa.dhs.gov
CELL: (210) 202-6646

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