# Leveraging CISA Cybersecurity Services

**Greg Mallette**
Cybersecurity and Infrastructure Security Agency

October 5, 2022

# WHO WE ARE

# CISA Mission and Vision

MISSION:

We lead the National effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

VISION:

Secure and resilient infrastructure for the American people.

CISA
CYBER+INFRASTRUCTURE

# Divisions of CISA

CYBERSECURITY DIVISION

INTEGRATED OPERATIONS DIVISION

INFRASTRUCTURE SECURITY DIVISION

NATIONAL RISK MANAGEMENT CENTER

EMERGENCY COMMUNICATIONS DIVISION

STAKEHOLDER ENGAGEMENT DIVISION



CISA
CYBER+INFRASTRUCTURE

4

# CYBERSECURITY ADVISOR PROGRAM

# Cybersecurity Advisor Program

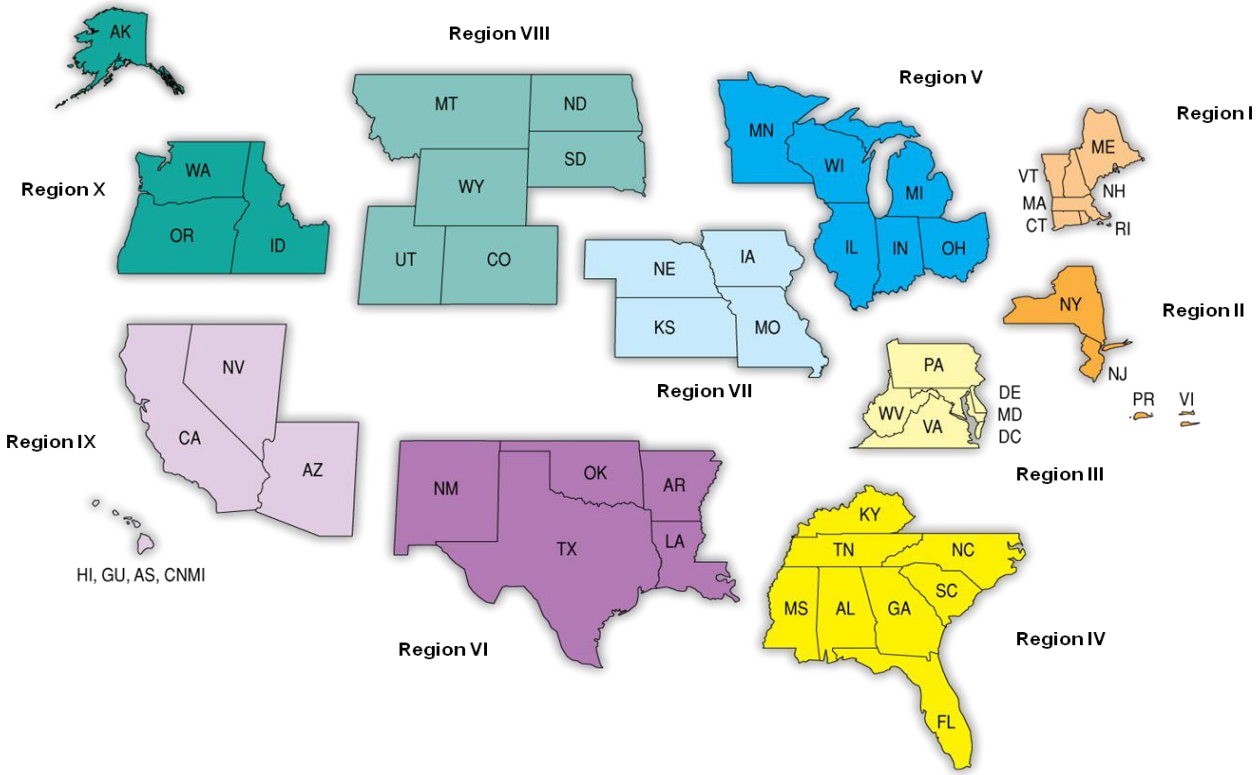
**CISA mission**: Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure

In support of that mission: Cybersecurity Advisors (CSAs):

- **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.

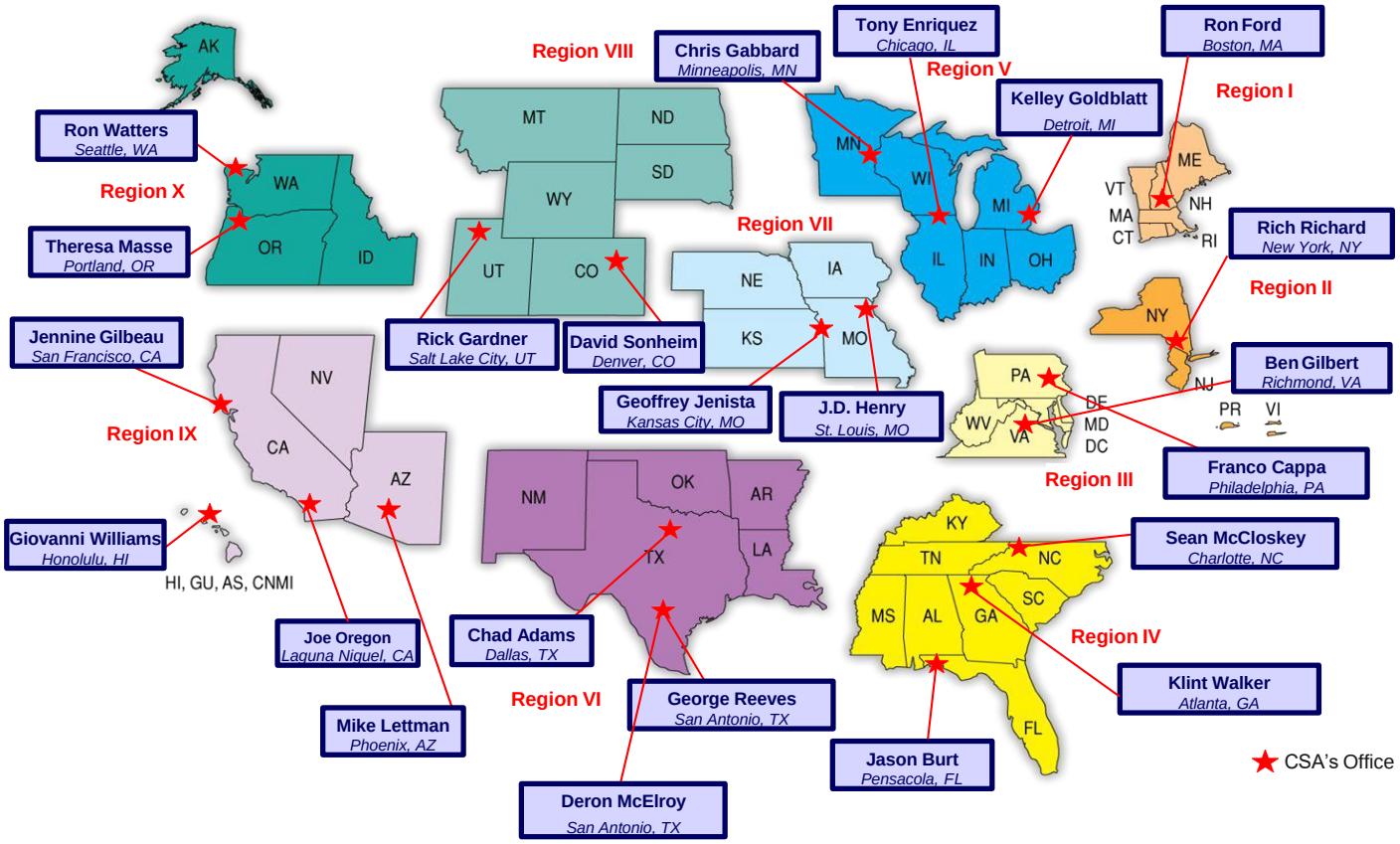
CISA
CYBER+INFRASTRUCTURE

# CSA Regionally Deployed Personnel



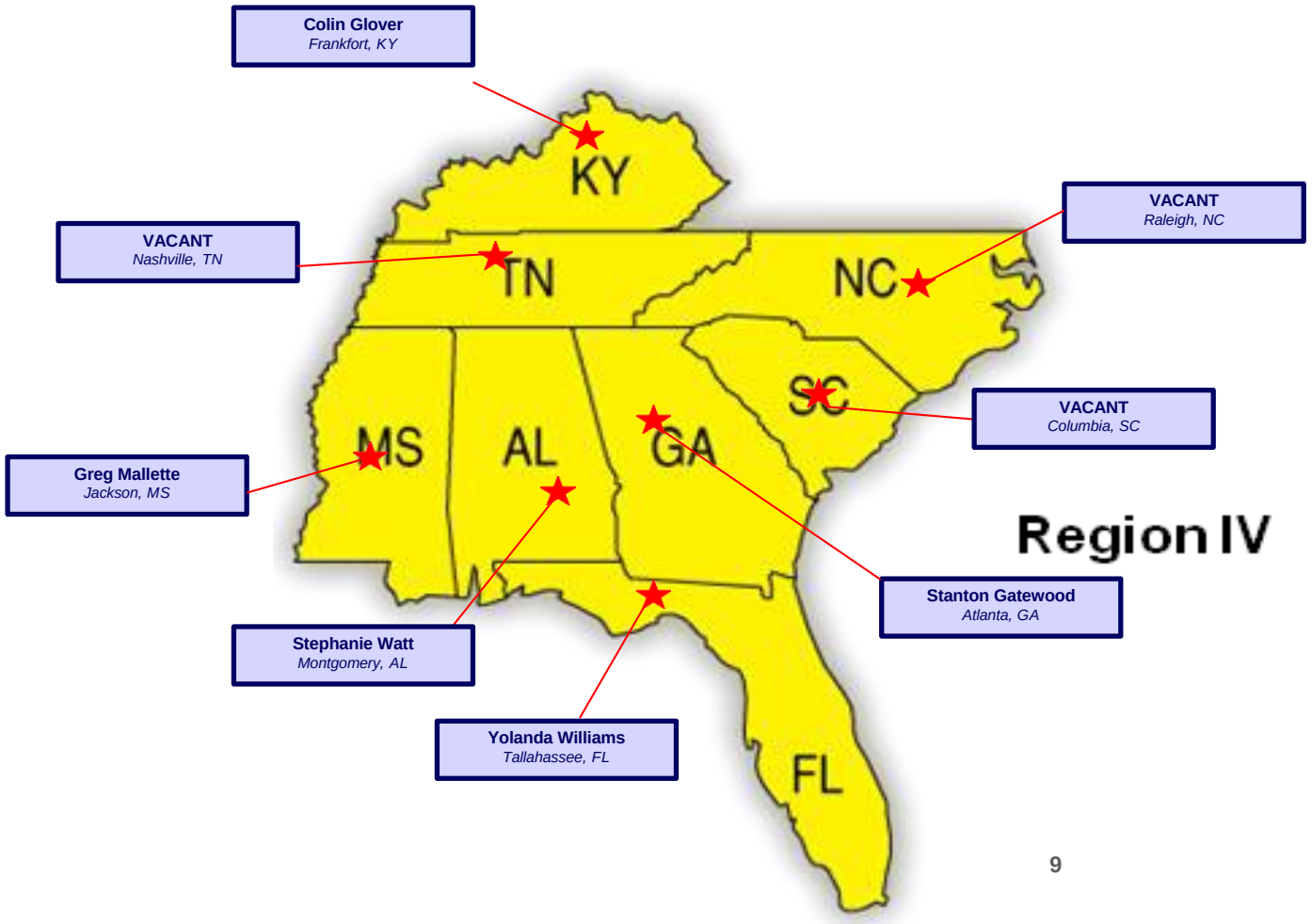

CISA
CYBER+INFRASTRUCTURE

# CSA Regionally Deployed Personnel




CISA
CYBER+INFRASTRUCTURE

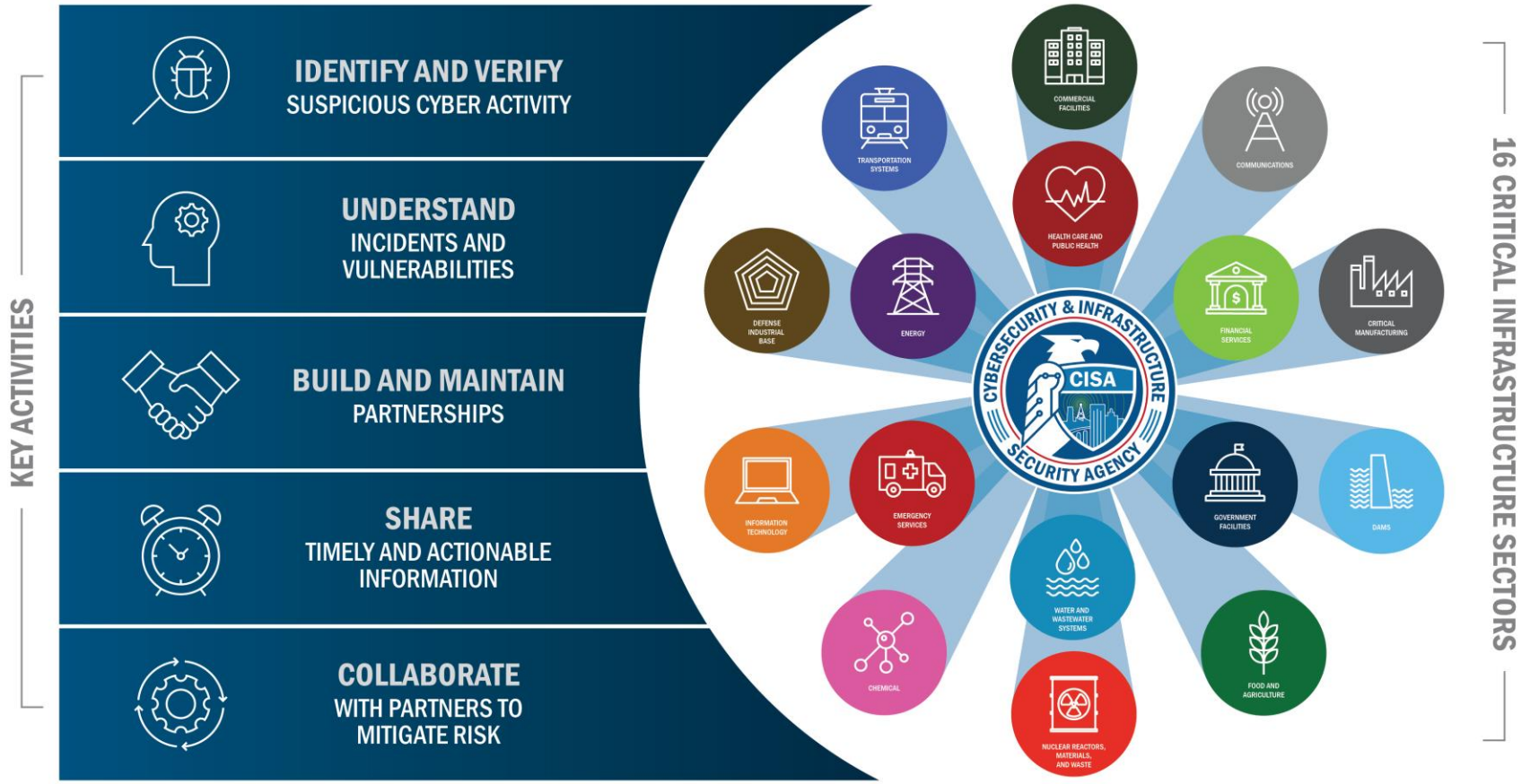
# Region 4 Cybersecurity State Coordinators






CISA
CYBER+INFRASTRUCTURE

# Serving Critical Infrastructure




CISA
CYBER+INFRASTRUCTURE

# CYBER THREATS – AM I A TARGET?

# Today's Risk Landscape

America remains at risk from a variety of threats:

INSIDER THREAT

ACTS OF TERRORISM

CYBER ATTACKS

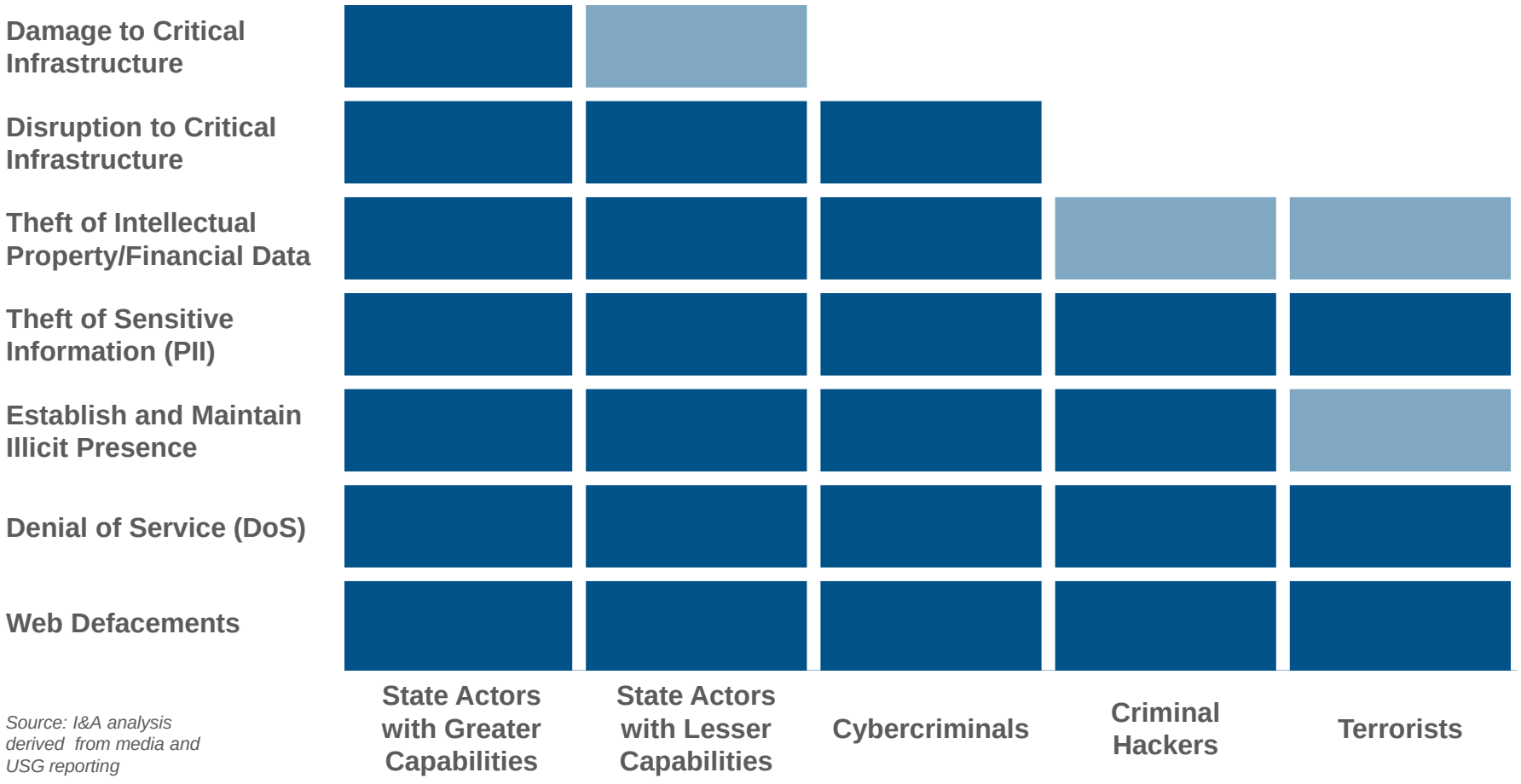
EXTREME WEATHER

PANDEMICS

ACCIDENTS OR TECHNICAL FAILURES

CISA
CYBER+INFRASTRUCTURE

# Cyber Actor Capabilities




*Source: I&A analysis derived from media and USG reporting*

*Note: Darker color indicates greater capability .*

CISA CYBER+INFRASTRUCTURE

# Cyber Criminals

*Source: DHS I&A*

- Cybercriminals
  - Look for targets of opportunity
  - Take the path of least resistance
  - Financially motivated
  - Personal information and proprietary data: high value, high-demand commodities
- Hacking as a service (HaaS) and Ransomware (RaaS)
  - Malicious tools readily available for purchase or download.
  - Enable less skilled actors to effectively operate

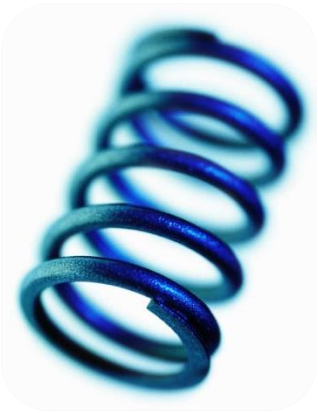
CISA CYBER+INFRASTRUCTURE

# CYBERSECURITY AND RESILIENCE

# Resilience Defined

*"… the ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents…"*

- Presidential Policy Directive 21
February 12, 2013



| | |
|---|---|
| **Protect (Security)** | **Sustain (Continuity)** |
| **Perform (Capability)** | **Repeat (Maturity)** |

CISA
CYBER+INFRASTRUCTURE

# Operational Resilience in Practice

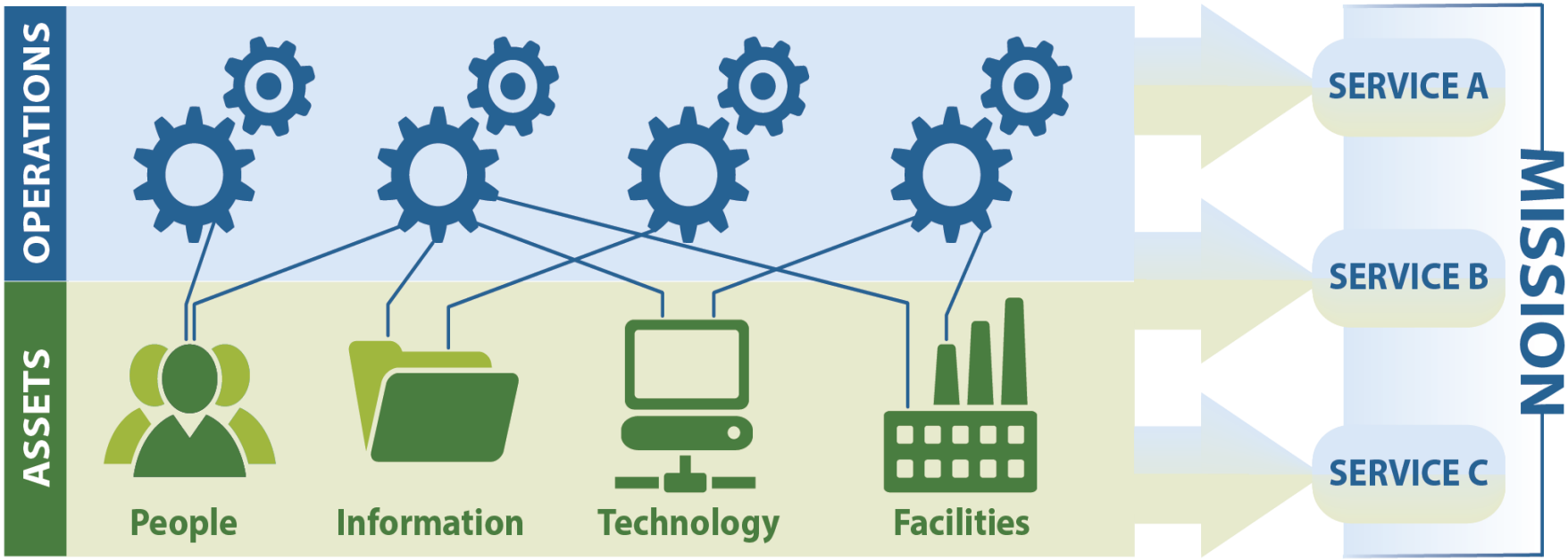
Operational resilience emerges from what we do, such as:

- Identifying and mitigating risks,
- Planning for and managing vulnerabilities and incidents,
- Performing service-continuity processes and planning,
- Managing IT operations,
- Managing, training, & deploying people,
- Protecting and securing important assets, and
- Working with external partners.


CISA
CYBER+INFRASTRUCTURE

# Cybersecurity Assets and Services

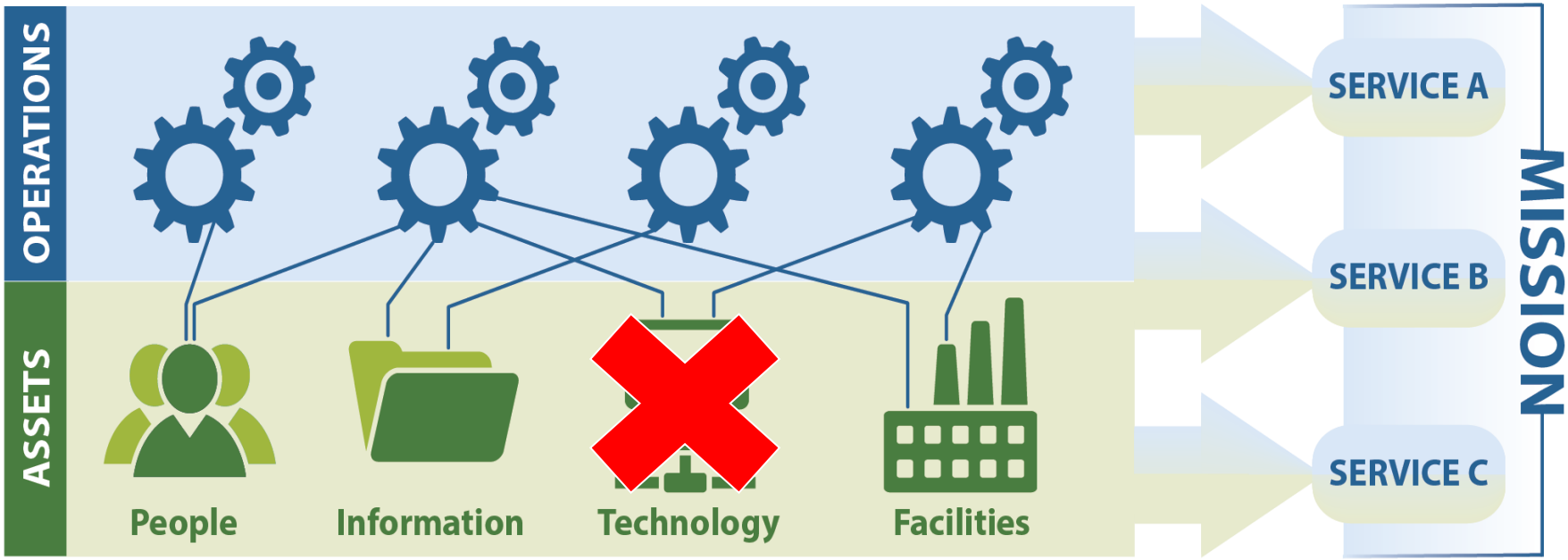
Organizations use **assets (people, information, technology, and facilities)** to provide operational **services** and accomplish **missions.**




CISA
CYBER+INFRASTRUCTURE

# Cybersecurity Assets and Services

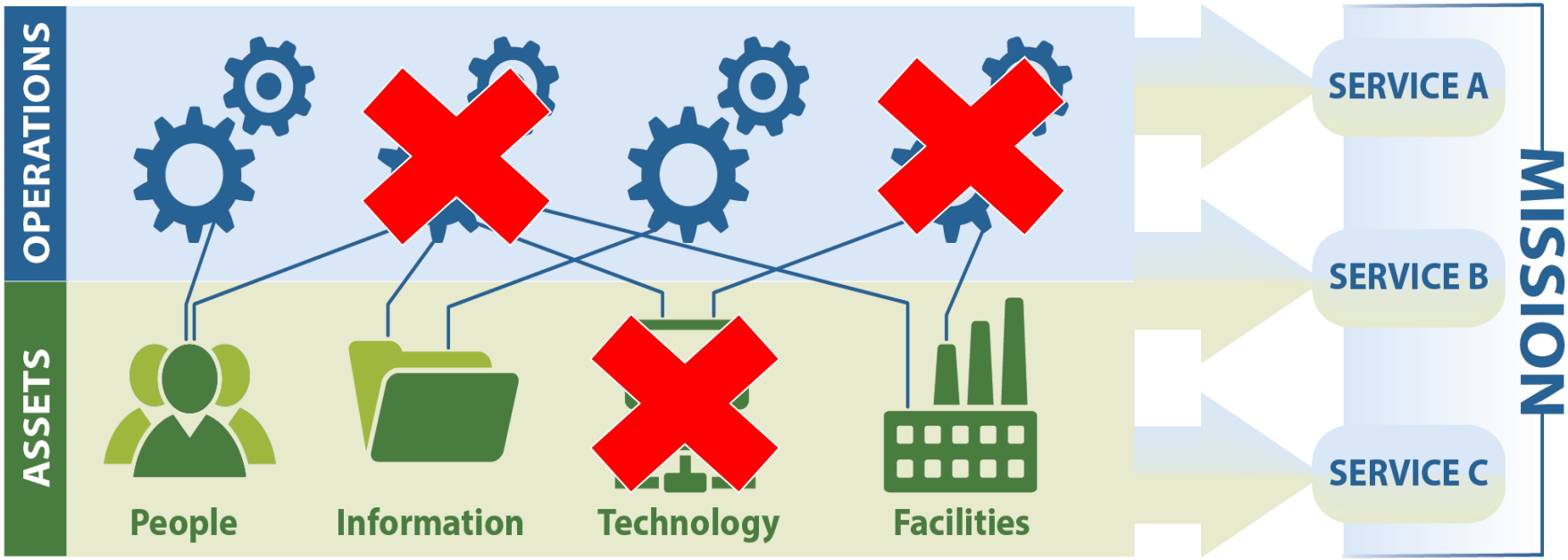
Organizations use **assets (people, information, technology, and facilities)** to provide operational **services** and accomplish **missions**.




CISA
CYBER+INFRASTRUCTURE

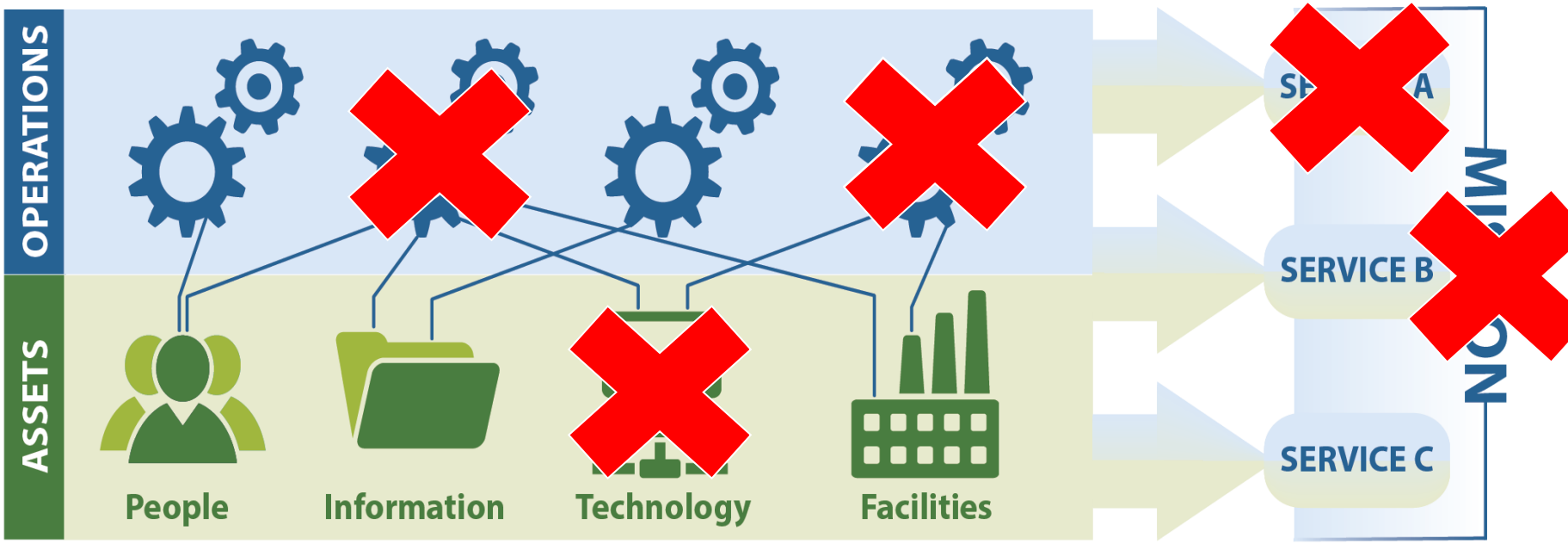
# Cybersecurity Assets and Services

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



# Cybersecurity Assets and Services

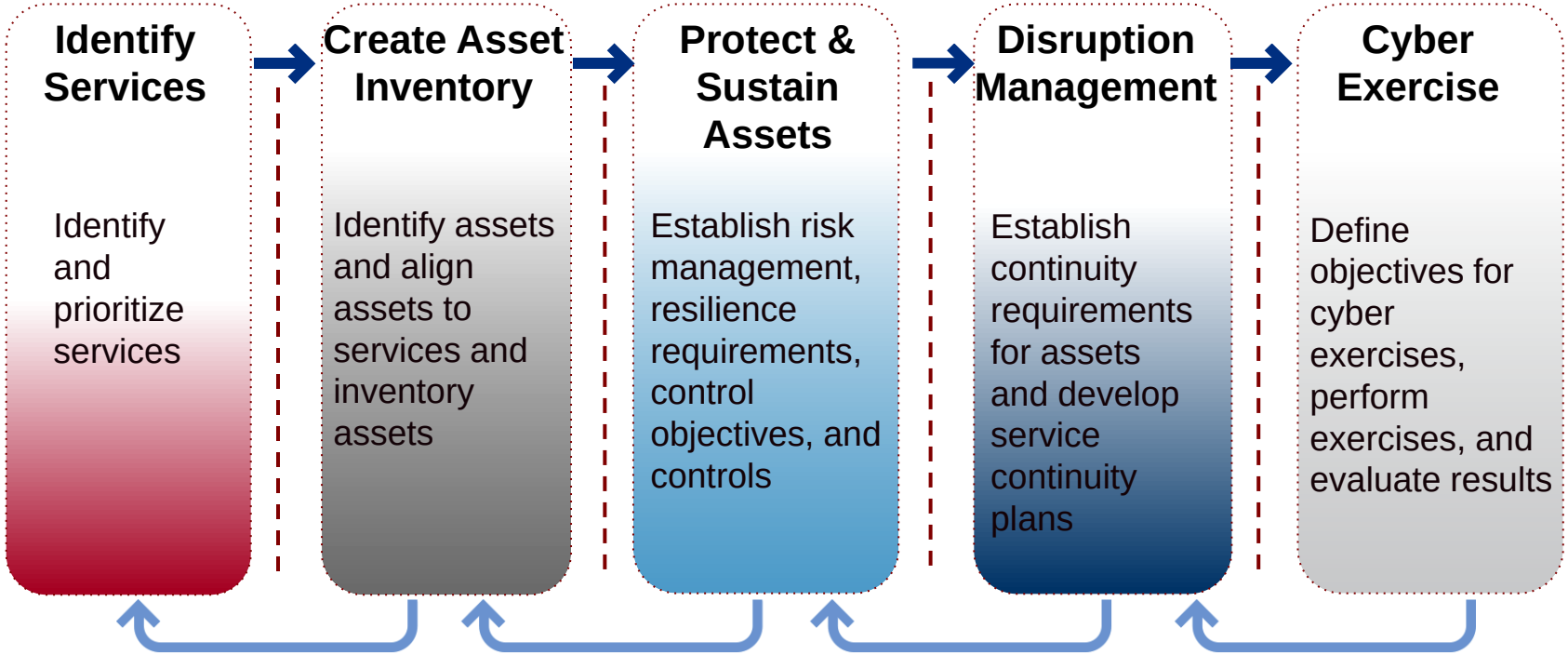
Organizations use **assets (people, information, technology, and facilities)** to provide operational **services** and accomplish **missions.**



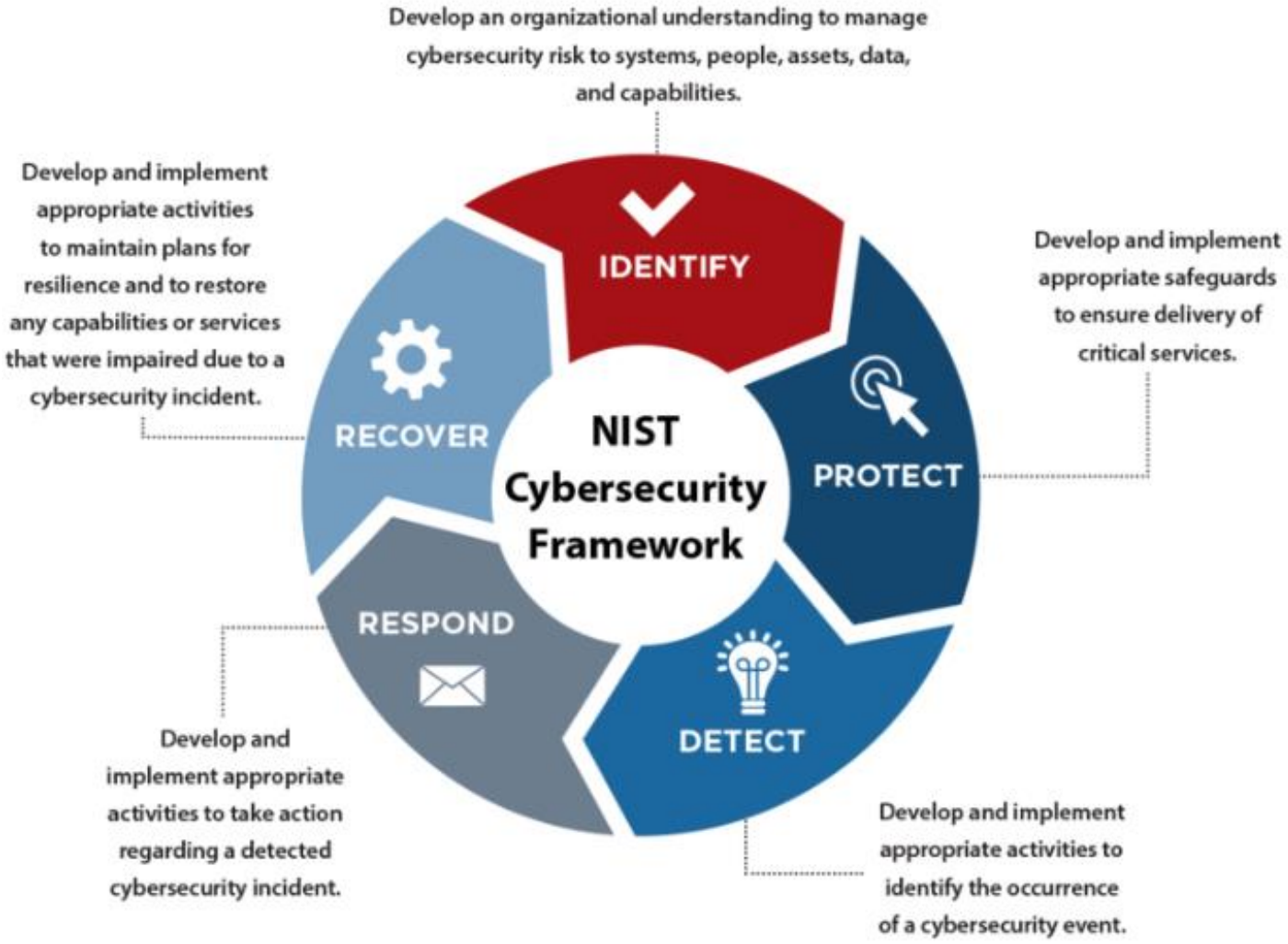

CISA
CYBER+INFRASTRUCTURE

# Working Toward Cyber Resilience

Follow a **framework** or general approach to cyber resilience.
One successful approach includes:



# NIST – Cybersecurity Framework




CISA
CYBER+INFRASTRUCTURE

# CISA CYBER ESSENTIALS

# CYBER GUIDANCE FOR SMALL BUSINESSES


## A DIFFERENT KIND OF CYBERSECURITY ADVICE

Cyber incidents have surged among small businesses that often do not have the resources to defend against devastating attacks like ransomware. As a small business owner, you have likely come across security advice that is out of date or that does not help prevent the most common compromises. For example, odds are that you have heard advice to never shop online using a coffee shop's wi-fi connection. While there was some truth to this fear a decade ago, that's not how people and organizations are compromised today. The security landscape has changed, and our advice needs to evolve with it.

**This advice is different.**

Below, we offer an action plan informed by the way cyber attacks actually happen. We break the tasks down by role, starting with the CEO. We then detail tasks for a Security Program Manager, and the Information Technology (IT) team. While following this advice is not a guarantee you will never have a security incident, it does lay the groundwork for building an effective security program.

## ROLE OF THE CEO

Cybersecurity is about culture as much as it is about technology. Most organizations fall into the trap of thinking the IT team alone is responsible for security. As a result, they make common mistakes that increase the odds of a compromise. Culture cannot be delegated. CEOs play a critical role by performing the following tasks:

1. **Establish a culture of security.** Make it a point to talk about cybersecurity to direct reports and to the entire organization. If you have regular email communications to staff, include updates on security program initiatives. When you set quarterly goals with your leadership team, include meaningful security objectives that are aligned

# SHIELDS UP

Russia's invasion of Ukraine could impact organizations both within and beyond the region, to include **malicious cyber activity** against the U.S. homeland, including as a response to the unprecedented economic costs imposed on Russia by the U.S. and our allies and partners. Evolving intelligence indicates that the Russian Government is exploring options for potential cyberattacks. Every organization—large and small—must be prepared to respond to disruptive cyber incidents. As the nation's cyber defense agency, CISA stands ready to help organizations prepare for, respond to, and mitigate the impact of cyberattacks. When cyber incidents are reported quickly, we can use this information to render assistance and as warning to prevent other organizations and entities from falling victim to a similar attack.

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

## Executive Messages

- Statement by President Biden on our Nation's Cybersecurity
- White House Fact Sheet: Act Now to Protect Against Potential Cyberattacks
- United States and Ukraine Expand Cooperation on Cybersecurity

## SHIELDS UP Guidance for All Organizations

CISA recommends all organizations—regardless of size—adopt a heightened posture when it comes to cybersecurity and protecting their most critical assets. Recognizing that many organizations find it challenging to identify resources for urgent security improvements, we've compiled **free cybersecurity services and tools** from government partners, and industry to assist. Recommended actions include:

**Reduce the likelihood of a damaging cyber intrusion**

# BOOTING UP

Things to Do First

## Backup Data

Employ a backup solution that automatically and continuously backs up critical data and system configurations.

## Multi-Factor Authentication

Require multi-factor authentication (MFA) for accessing your systems whenever possible. MFA should be required of all users, but start with privileged, administrative and remote access users.

## Patch & Update Management

Enable automatic updates whenever possible. Replace unsupported operating systems, applications and hardware. Test and deploy patches quickly.

# ESSENTIALS VOL.1

# THE IT PROFESSIONAL'S GUIDE

✔ *Actions for leaders.*
✔ *Discuss with IT staff or service providers.*

**Essential Actions** for Building a ***Culture of Cyber Readiness:***

## Yourself

Drive cybersecurity strategy, investment and culture

*Organizations living the culture have:*

- Lead investment in basic cybersecurity.
- Determined how much of their operations are dependent on IT.
- Built a network of trusted relationships with sector partners and government agencies for access to timely cyber threat information.
- Approached cyber as a business risk.
- Lead development of cybersecurity policies.

## Your Staff

Develop security awareness and vigilance

*Organizations living the culture have:*

- Leveraged basic cybersecurity training to improve exposure to cybersecurity concepts, terminology and activities associated with implementing cybersecurity best practices.
- Developed a culture of awareness to encourage employees to make good choices online.
- Learned about risks like phishing and business email compromise.
- Identified available training resources through professional associations, academic institutions, private sector and government sources.
- Maintained awareness of current events related to cybersecurity, using lessons-learned and reported events to remain vigilant against the current threat environment and agile to cybersecurity trends.

## Your Systems

Protect critical assets and applications

*Organizations living the culture have:*

- Learned what is on their network. Maintained inventories of hardware and software assets to know what is in-play and at-risk from attack.
- Leveraged automatic updates for all operating systems and third-party software.
- Implemented secure configurations for all hardware and software assets.
- Removed unsupported or unauthorized hardware and software from systems.
- Leveraged email and web browser security settings to protect against spoofed or modified emails and unsecured webpages.
- Created application integrity and whitelisting policies so that only approved software is allowed to load and operate on their systems.

## Your Surroundings

Ensure only those who belong on your digital workplace have access

*Organizations living the culture have:*

- Learned who is on their network. Maintained inventories of network connections (user accounts, vendors, business partners, etc.).
- Leveraged multi-factor authentication for all users, starting with privileged, administrative and remote access users.
- Granted access and admin permissions based on need-to-know and least privilege.
- Leveraged unique passwords for all user accounts.
- Developed IT policies and procedures addressing changes in user status (transfers, termination, etc.).

## Your Data

Make backups and avoid loss of info critical to operations

*Organizations living the culture have:*

- Learned what information resides on their network. Maintained inventories of critical or sensitive information.
- Established regular automated backups and redundancies of key systems.
- Learned how their data is protected.
- Leveraged malware protection capabilities.
- Leveraged protections for backups, including physical security, encryption and offline copies.
- Learned what is happening on their network. Managed network and perimeter components, host and device components, data-at-rest and in-transit, and user behavior activities.

## Your Actions Under Stress

Limit damage and quicken restoration of normal operations

*Organizations living the culture have:*

- Lead development of an incident response and disaster recovery plan outlining roles and responsibilities. Test it often.
- Leveraged business impact assessments to prioritize resources and identify which systems must be recovered first.
- Learned who to call for help (outside partners, vendors, government / industry responders, technical advisors and law enforcement).
- Lead development of an internal reporting structure to detect, communicate and contain attacks.
- Leveraged in-house containment measures to limit the impact of cyber incidents when they occur.



*Consistent with the NIST Cybersecurity Framework and other standards, these actions are the starting point to Cyber Readiness. To learn more, visit* CISA.gov/Cyber-Essentials.

# CISA Cyber Essentials (1 of 6)

**Essential Practice 1: Drive Strategy, Investment, and Culture**

- Cyber should be approached as a business risk. **(NOT AN IT PROBLEM)**
- Look into your organizations' operations to learn how much you are dependent on IT. **(IT is woven throughout organizations)**
- Lead investment into basic cybersecurity.
- Leverage sector partners and government agencies to build a network of trusted relationships to better collaborate and quickly access cyber threat information.

***https://www.cisa.gov/cyber-essentials***

CISA
CYBER+INFRASTRUCTURE

# CISA Cyber Essentials (2 of 6)

## Essential Practice 2: Develop Security Awareness and Vigilance

- Learn what training resources are available through professional associations, academic institutions, private sector and government sources.
- Develop a culture of awareness to encourage employees to make better choices online.
- Always uphold cybersecurity policies and continuously look for ways to reinforce these policies.
- Take advantage of available training resources to educate employees on recognizing and responding to cyber threats.

***https://www.cisa.gov/cyber-essentials***

CISA
CYBER+INFRASTRUCTURE

# CISA Cyber Essentials (3 of 6)

## Essential Practice 3: Protect Critical Assets and Applications

- Understand what is on your network to create an inventory of all your hardware and software assets.
- Safeguard your network by removing unsupported or unauthorized hardware and software from systems.
- Implement secure configurations for all hardware and software assets.
- Leverage automatic updates for all operating systems and third-party software.
- Use email and web browser security settings to protect against spoofed or modified emails, and unsecured webpages.

***https://www.cisa.gov/cyber-essentials***

CISA
CYBER+INFRASTRUCTURE

# CISA Cyber Essentials (4 of 6)

**Essential Practice 4: Ensure Only Those Who Belong on Your Network Have Access**

- Identify who is on your network and create an inventory of all your network connections (user accounts, vendors, business partners, etc.).
- Create a culture focused on access and admin permissions based on need-to-know and least privileged.
- Foster the development of IT policies and procedures addressing changes in user status (transfers, termination, etc.).
- Leverage multiple forms of authentication to gain admin privileges and remote access.
- Enforce the use of unique passwords for all user accounts.

***https://www.cisa.gov/cyber-essentials***

CISA
CYBER+INFRASTRUCTURE

# CISA Cyber Essentials (5 of 6)

**Essential Practice 5: Make Backups and Avoid Loss of Info Critical to Operations**

- Learn what information resides on your network. Inventory critical or sensitive information.
- Establish regular automated backups and redundancies of key systems.
- Be aware of what is happening on your network. Manage network and perimeter components, host and device components, data at rest and in transit, and user behavior and activities.
- Understand how your data is protected.
- Protect your backups with physical security, encryption and offline copies.
- Learn ways in which you can protect yourself from malware.

***https://www.cisa.gov/cyber-essentials***

CISA
CYBER+INFRASTRUCTURE

# CISA Cyber Essentials (6 of 6)

**Essential Practice 6: Limit Damage and Quicken Restoration of Normal Operations**

- Identify who to call for help (e.g., outside partners, vendors, government/industry responders, technical advisors and law enforcement).
- Spearhead the development of incident response and disaster recovery plans outlining roles and responsibilities. Test these plans often.
- Lead the development of internal reporting structures to detect, communicate, and contain attacks.
- Prioritize your resources and identify which systems must be recovered first by conducting business impact assessments.

***https://www.cisa.gov/cyber-essentials***

CISA
CYBER+INFRASTRUCTURE

# CISA
# CYBERSECURITY SERVICES

# Sampling of Cybersecurity Offerings

- **Preparedness Activities**
  - Information / Threat Indicator Sharing
  - Cybersecurity Training and Awareness
  - Cyber Exercises and “Playbooks”
  - National Cyber Awareness System
  - Vulnerability Notes Database
  - Information Products and Recommended Practices
  - Cybersecurity Evaluations
    - Cyber Resilience Reviews (CRR™)
    - Cyber Infrastructure Surveys
    - Phishing Campaign Assessment
    - Vulnerability Scanning
    - Risk and Vulnerability Assessments (aka “Pen” Tests)
    - External Dependency Management Reviews
    - Cyber Security Evaluation Tool (CSET™)
    - Validated Architecture Design Review (VADR)

- **Response Assistance**
  - Remote / On-Site Assistance
  - Malware Analysis
  - Hunt and Incident Response Teams
  - Incident Coordination

- **Cybersecurity Advisors**
  - Assessments
  - Working group collaboration
  - Best Practices private-public
  - Incident assistance coordination

- **Protective Security Advisors**
  - Assessments
  - Incident liaisons between government and private sector
  - Support for National Special Security Events

CISA
CYBER+INFRASTRUCTURE

# ASSESSMENTS

# Criticality of Periodic Assessments

- Periodic assessments are essential for resilience
- Can’t protect if you don’t know what needs protection
- Can’t fix what needs to be fixed if you don’t know what’s wrong

# Cybersecurity Services (Voluntary & No Cost)


CISA
CYBER+INFRASTRUCTURE

# Protected Critical Infrastructure Information Program

**Protected Critical Infrastructure Information** (PCII) Program Guards Your Information

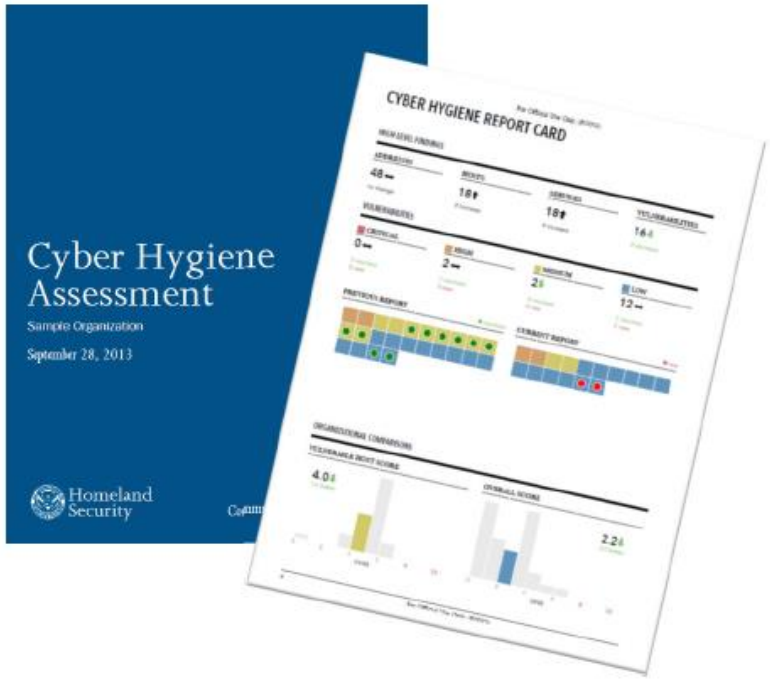
- Sensitive critical infrastructure information voluntarily given to CISA is protected by law from
  - Public release under Freedom of Information Act requests,
  - Public release under State, local, tribal, or territorial disclosure laws,
  - Use in civil litigation and
  - Use in regulatory purposes.

CISA CYBER+INFRASTRUCTURE

# Vulnerability Scanning / Hygiene

**Purpose**: Assess Internet-accessible systems for known vulnerabilities and configuration errors.

**Delivery**: Identify public-facing Internet security risks, through service enumeration and vulnerability scanning online by CISA.




**Benefits**:

- Continual review of system to identify potential problems
- Weekly reports detailing current and previously mitigated vulnerabilities
- Recommended mitigation for identified vulnerabilities

**Network Vulnerability & Configuration Scanning**:

- Identify network vulnerabilities and weakness

CISA
CYBER+INFRASTRUCTURE

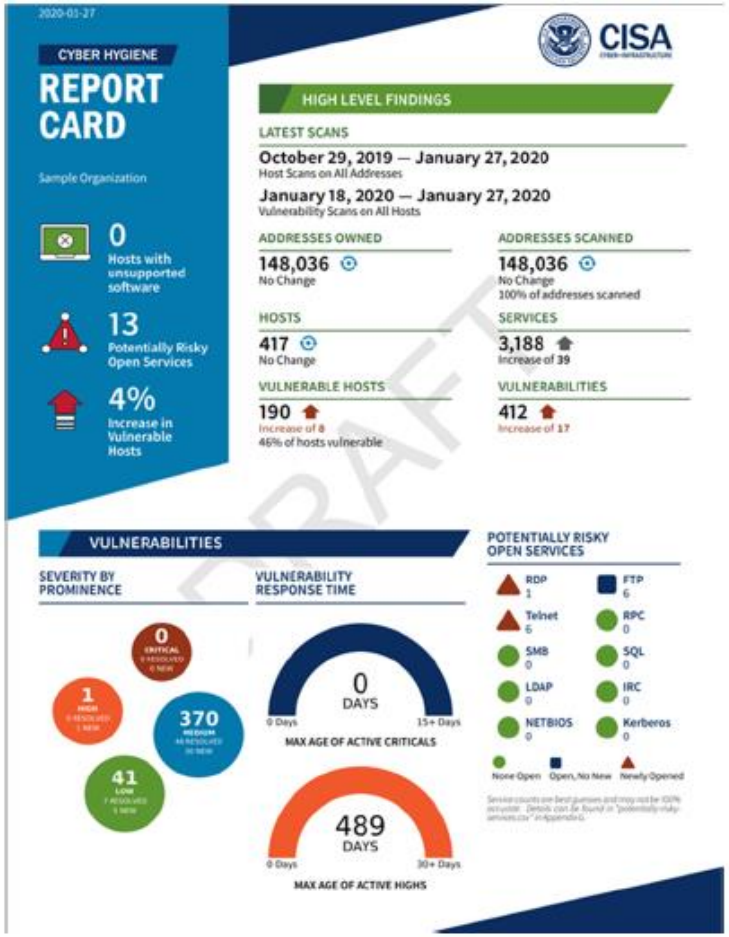
# Cyber Hygiene Report Card

**High Level Findings**

- Latest Scans
- Addresses Owned
- Addresses Scanned
- Hosts
- Services
- Vulnerable Hosts
- Vulnerabilities

**Vulnerabilities**

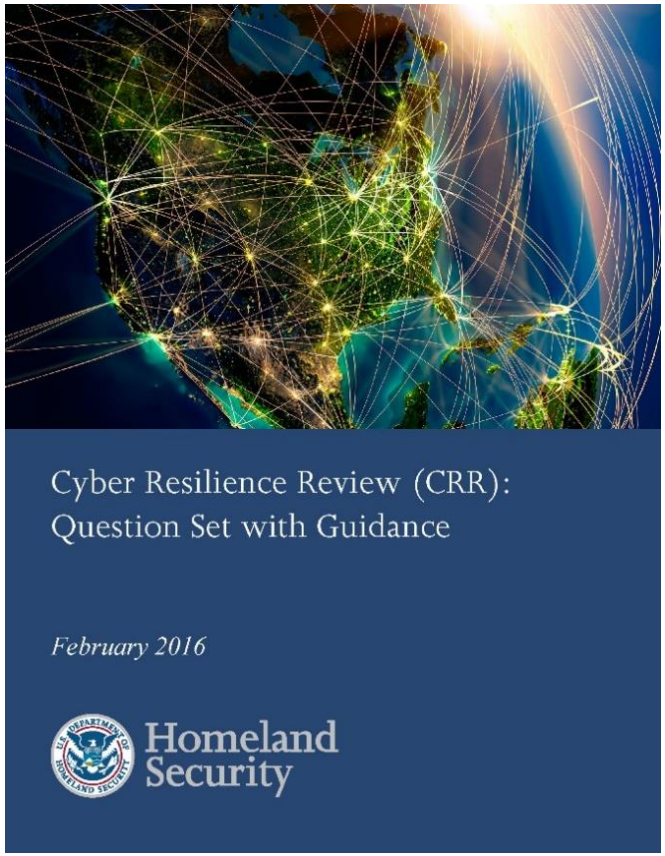
- Severity by Prominence
- Vulnerability Response Time
- Potentially Risky Open Services




CISA CYBER+INFRASTRUCTURE

# Cyber Resilience Review

- **Purpose:** Evaluate operational resilience and cybersecurity practices of **critical services.**
- Delivery: Either
  - CSA-facilitated, or
  - Self-administered
- Benefits include: Helps public and private sector partners understand and measure cybersecurity capabilities as they relate to operational resilience and cyber risk




*CRR Question Set & Guidance*

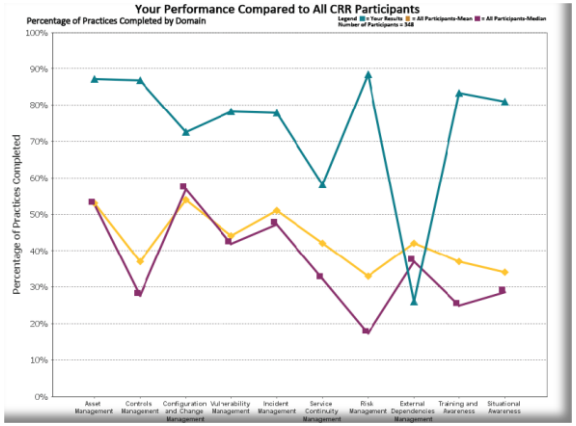
CISA
CYBER+INFRASTRUCTURE

# Cyber Resilience Review Domains

| | |
|---|---|
| **Asset Management**<br>Know your assets being protected & their requirements, e.g., CIA | **Risk Management**<br>Know and address your biggest risks that considers cost and your risk tolerances |
| **Configuration and Change Management**<br>Manage asset configurations and changes | **Service Continuity Management**<br>Ensure workable plans are in place to manage disruptions |
| **Controls Management**<br>Manage and monitor controls to ensure they are meeting your objectives | **Situational Awareness**<br>Discover and analyze information related to immediate operational stability and security |
| **External Dependencies Management**<br>Know your most important external entities and manage the risks posed to essential services | **Training and Awareness**<br>Ensure your people are trained on and aware of cybersecurity risks and practices |
| **Incident Management**<br>Be able to detect and respond to incidents | **Vulnerability Management**<br>Know your vulnerabilities and manage those that pose the most risk |

# CRR Sample Report

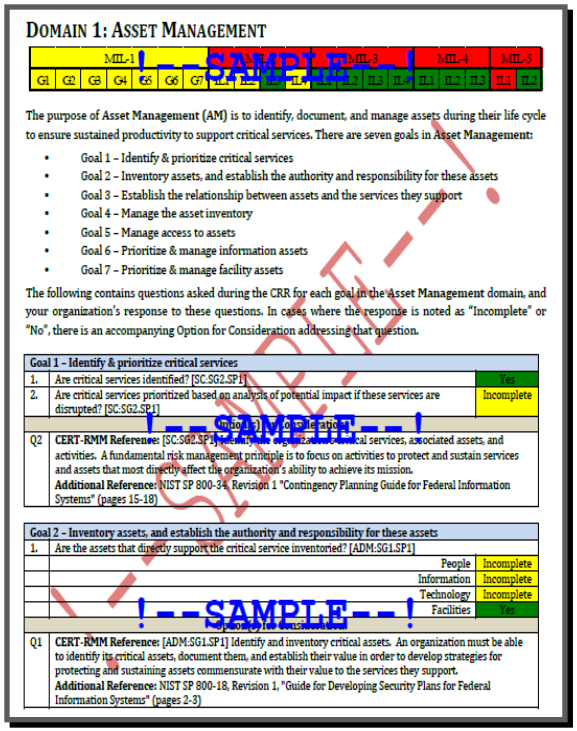
## Each CRR report includes:




Comparison data with other CRR participants **facilitated only*


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 | IL1 IL2 IL3 | IL1 IL2 IL3 | IL1 IL2

!--SAMPLE--!

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] Prioritize 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) | |

!--SAMPLE--!

| 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) | |

!--SAMPLE--!

# EDM Assessment Organization and Structure

- Structure and scoring similar to Cyber Resilience Review
- Uses one Maturity Indicator Level (MIL) scale with three lifecycle domains.

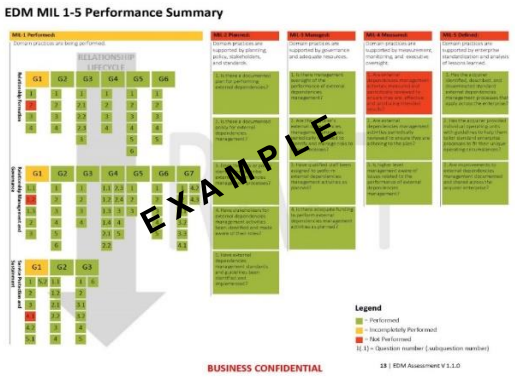
| |
|---|
| **Relationship Formation**<br><br>*Assesses whether the acquirer evaluates and controls the risks of relying on external entities before entering into relationships with them.* |
| **Relationship Management and Governance**<br><br>*Assesses whether the acquirer manages ongoing relationships to maintain the resilience of the critical service and mitigate dependency risk.* |
| **Service Protection and Sustainment**<br><br>*Assesses whether the acquirer accounts for its dependence on external entities as part of its operational activities around managing incidents, disruptions, and threats.* |

CISA CYBER+INFRASTRUCTURE

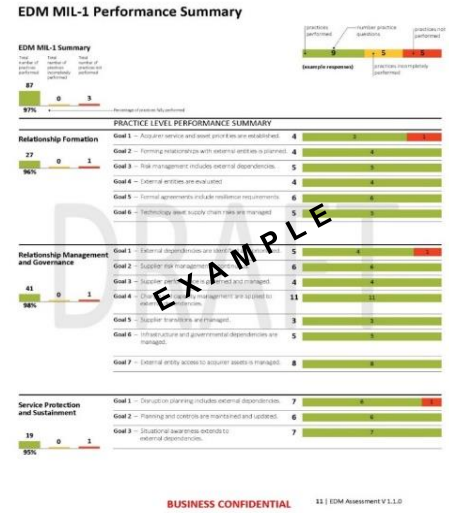
# EDM Assessment Report

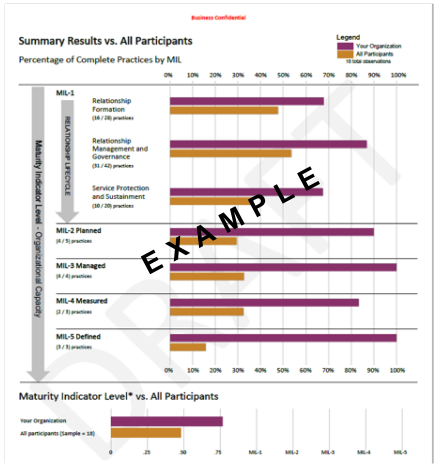
## Each EDM report includes:

- Performance summary of existing capability managing external dependencies

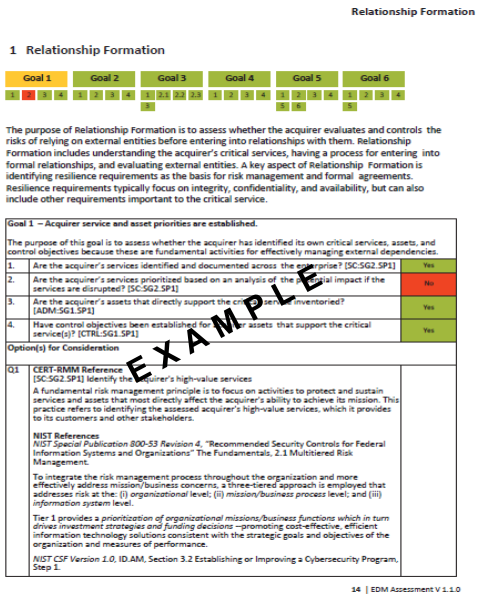



- Comparison data with other EDM participants




- Sub-domain performance of existing capability managing external dependencies and options for consideration for all responses



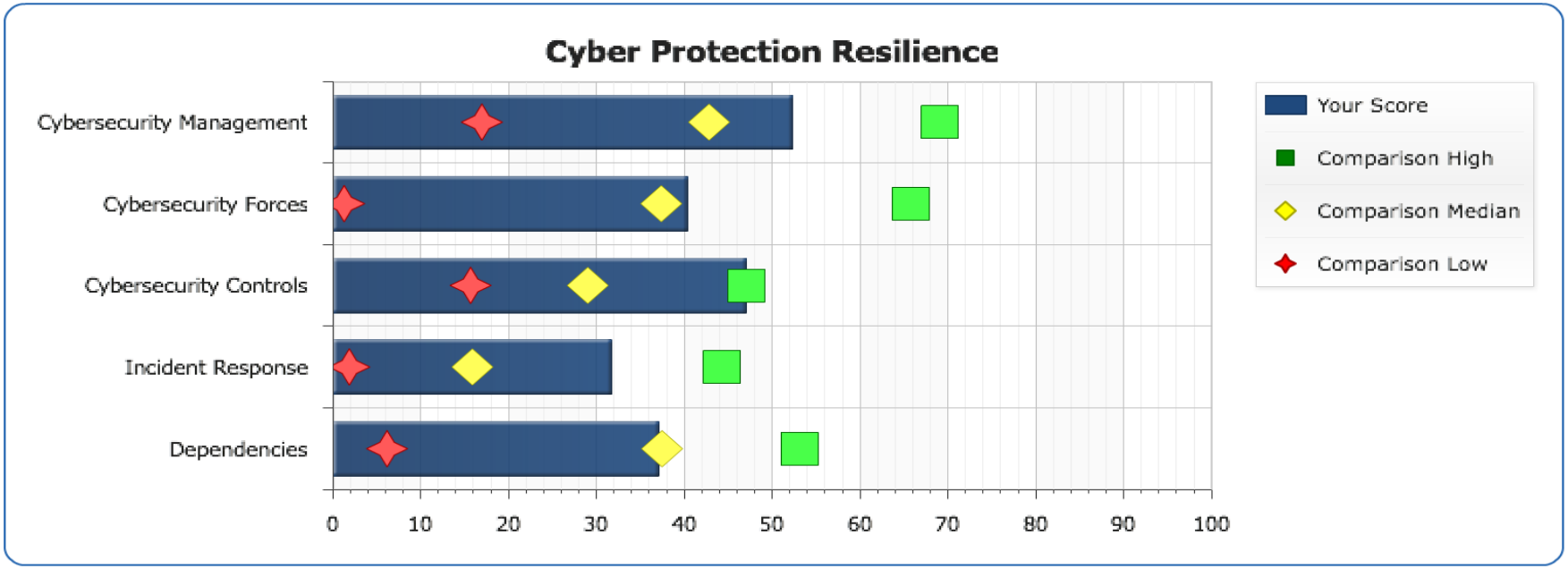

CISA CYBER+INFRASTRUCTURE

# Cyber Infrastructure Survey (CIS)

- Purpose: Evaluate security controls, cyber preparedness, overall resilience.
- Delivery: CSA-facilitated
- Benefits:
  - Effective assessment of cybersecurity controls in place for a critical service,
  - Easy-to-use interactive dashboard to support cybersecurity planning and resource allocation.

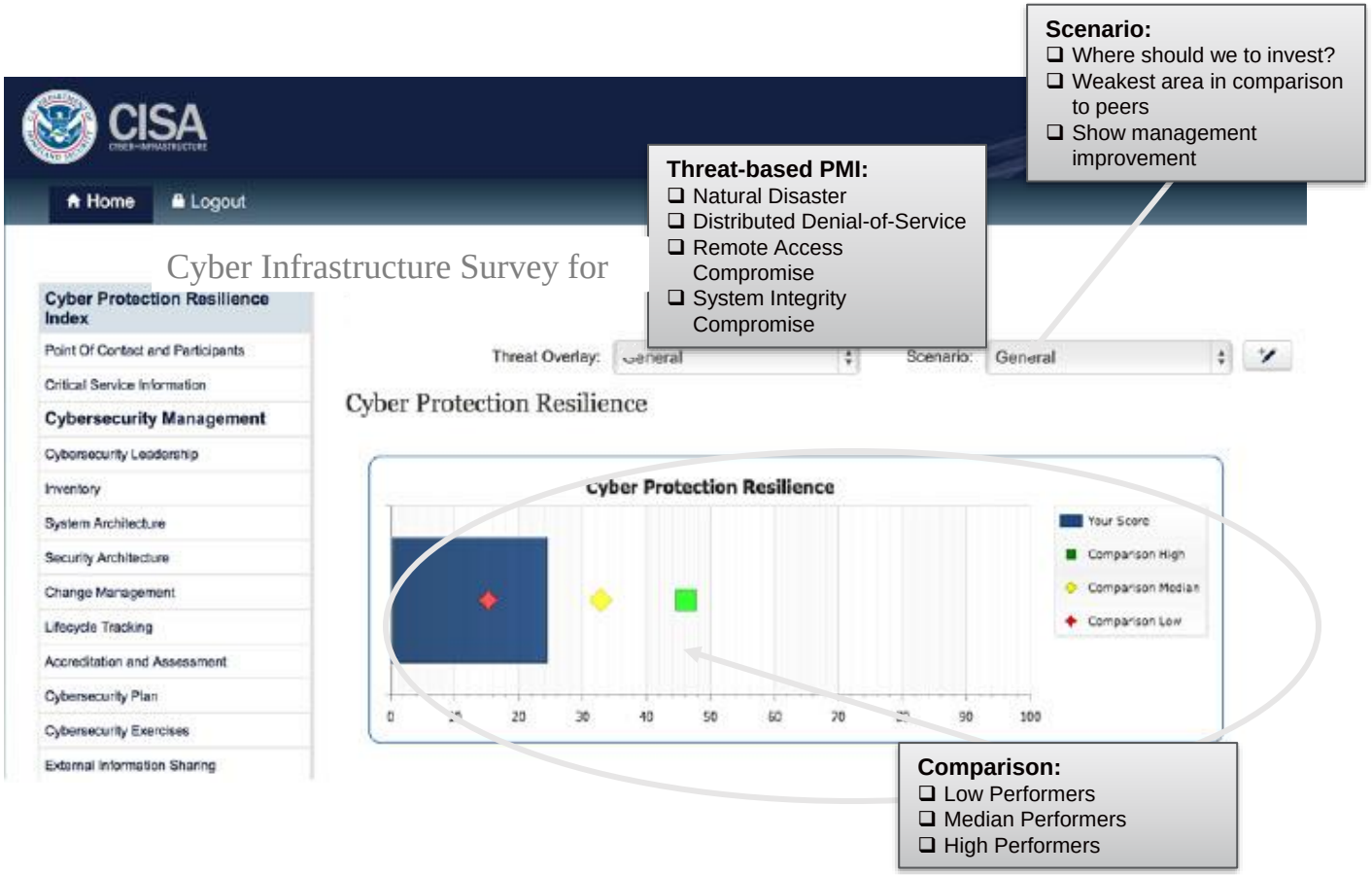
# CIS Dashboard - Comparison

- Shows the low, median, and high performers
- Compares your organization to the aggregate




CISA
CYBER+INFRASTRUCTURE

# Example of CIS Dashboard



# TRAINING RESOURCES

# Resource Guides

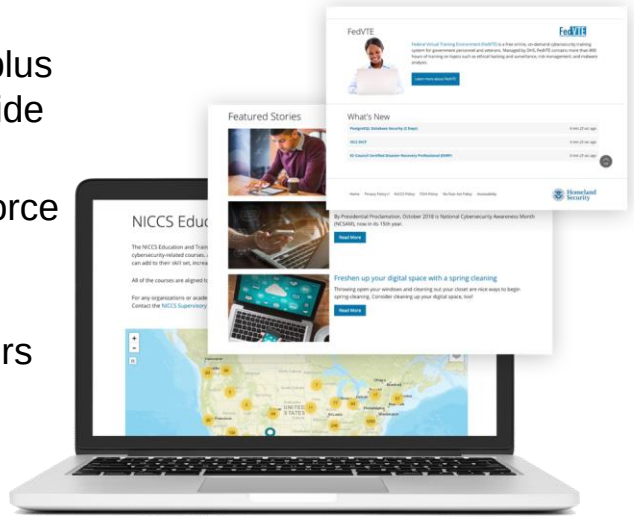
- **Resource Guides:** Created to help organizations enhance their resilience in specific Cyber Resilience Review (CRR) domains.
- **CRR Tools:** Helps move organizations from initial capability to well-define capability in security management areas
- **CRR Domains**: Includes the CRR 10 “domains” each representing a capability area foundational to an organization’s cyber resilience.
- **Content**: While the guides were developed for organizations to utilize after conducting a CRR, these publications provide content useful for all organizations with cybersecurity equities.
- **Flexibility in Use**: Moreover, the guides can be utilized as a full set or as individual components, depending on organizational preference and/or need.
- For more information, visit CRR Supplemental Resource Guides | CISA

# Cybersecurity Training Resources

**CISA offers easily accessible education and awareness resources through the National Initiative for Cybersecurity Careers and Studies (NICCS) website.**

The NICCS website includes:

- Searchable Training Catalog with 4,400 plus cyber-related courses offered by nationwide cybersecurity educators
- Interactive National Cybersecurity Workforce Framework
- Cybersecurity Program information: FedVTE, Scholarships for Service, Centers for Academic Excellence, and Cyber Competitions
- Tools and resources for cyber managers
- Upcoming cybersecurity events list




**For more information, visit https://niccs.us-cert.gov/training/search**

CISA CYBER+INFRASTRUCTURE

# Our Nation's Cyber Workforce Foundation

The **National Cybersecurity Workforce Framework** is a collection of definitions that describe types of cybersecurity work and skills requires to perform it.

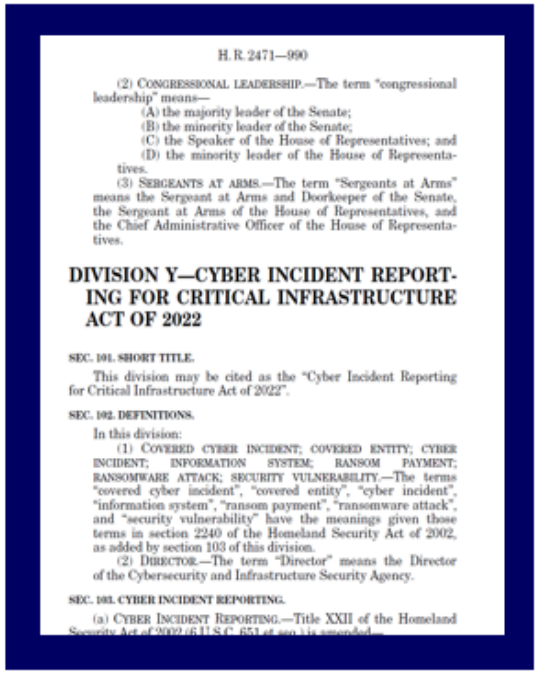
- ✓ When used nationally, the definitions help establish universally applicable cybersecurity skills, training/development, and curricula
- ✓ 7 Categories, 30+ Specialty Areas
- ✓ Baselines knowledge, skills, and abilities & tasks

**Operate & Maintain** | **Securely Provision** | **Analyze** | **Collect & Operate** | **Oversight & Development** | **Protect & Defend** | **Investigate**

CISA CYBER+INFRASTRUCTURE

# CIRCIA Overview

- In March 2022, Congress enacted the ***Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)***



H. R. 2471—990

(2) CONGRESSIONAL LEADERSHIP.—The term "congressional leadership" means—
(A) the majority leader of the Senate;
(B) the minority leader of the Senate;
(C) the Speaker of the House of Representatives; and
(D) the minority leader of the House of Representatives.
(3) SERGEANTS AT ARMS.—The term "Sergeants at Arms" means the Sergeant at Arms and Doorkeeper of the Senate, the Sergeant at Arms of the House of Representatives, and the Chief Administrative Officer of the House of Representatives.

**DIVISION Y—CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022**

**SEC. 101. SHORT TITLE.**

This division may be cited as the "Cyber Incident Reporting for Critical Infrastructure Act of 2022".

**SEC. 102. DEFINITIONS.**

In this division:
(1) COVERED CYBER INCIDENT; COVERED ENTITY; CYBER INCIDENT; INFORMATION SYSTEM; RANSOM PAYMENT; RANSOMWARE ATTACK; SECURITY VULNERABILITY.—The terms "covered cyber incident", "covered entity", "cyber incident", "information system", "ransom payment", "ransomware attack", and "security vulnerability" have the meanings given those terms in section 2240 of the Homeland Security Act of 2002, as added by section 103 of this division.
(2) DIRECTOR.—The term "Director" means the Director of the Cybersecurity and Infrastructure Security Agency.

**SEC. 103. CYBER INCIDENT REPORTING.**

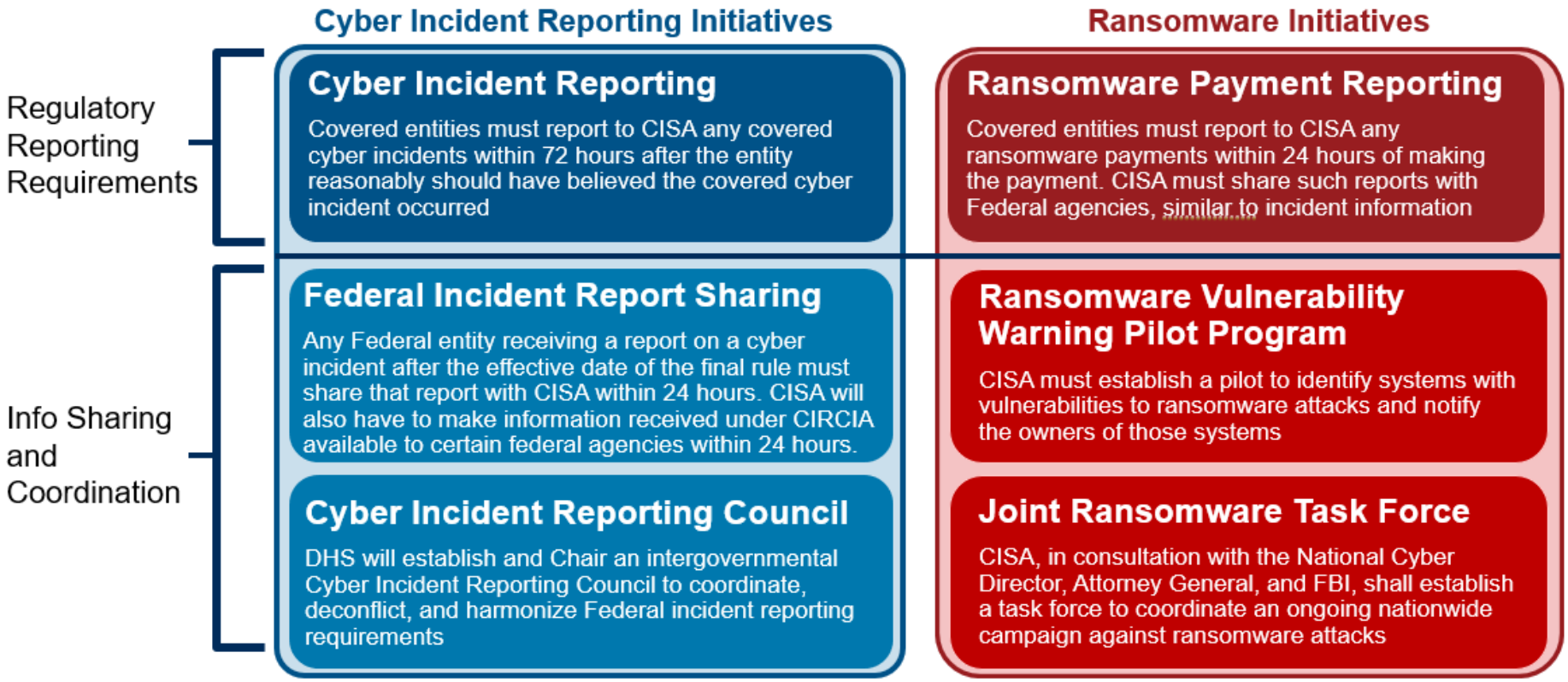
(a) CYBER INCIDENT REPORTING.—Title XXII of the Homeland Security Act of 2002 (6 U.S.C. 651 et seq.) is amended—

- Requires the Cybersecurity and Infrastructure Security Agency (CISA) to coordinate with Federal partners and others on various cyber incident reporting and ransomware related activities
- Requires CISA to establish a new regulatory program requiring reporting of certain cybersecurity related items

CISA
CYBER+INFRASTRUCTURE

# CIRCIA Overview

## CIRCIA Key Elements




CISA
CYBER+INFRASTRUCTURE


CYBERSECURITY AWARENESS MONTH 2022

# Theme

The 2022 Campaign theme, See Yourself in Cyber, emphasizes that while cybersecurity may seem like a complex subject, ultimately, it's really all about people. This October, we will focus on the "people" part of cybersecurity, providing information and resources to help Americans make smart decisions on the job, at home, at school, and in the future.



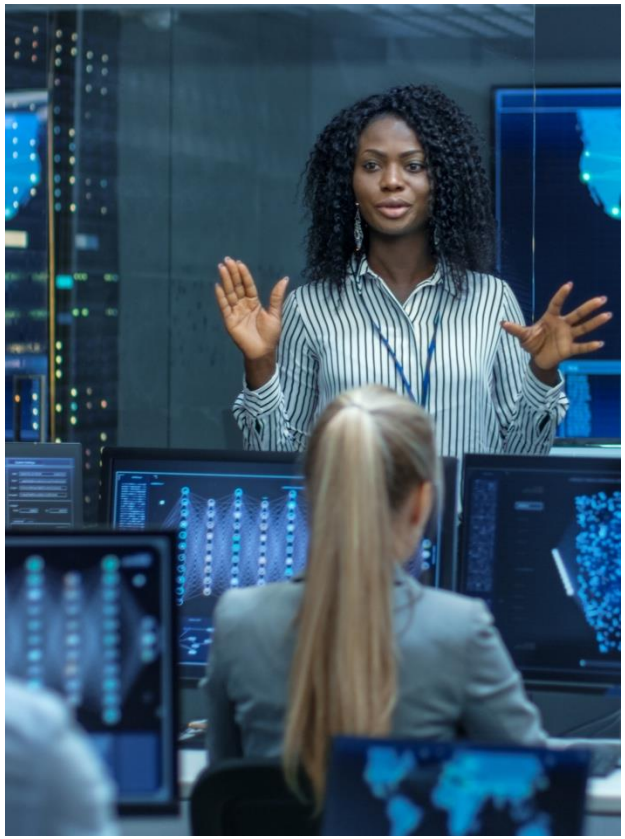

CYBERSECURITY AWARENESS MONTH 2022

# Action Steps

This year's campaign goal is to have everyone implement these four action steps to increase online security:

- **Enable Multi-Factor Authentication**: You need more than a password to protect your online accounts, and enabling MFA makes it 99% less likely you will get hacked
- **Use Strong Passwords**: Use passwords that are long, unique, and randomly generated.
- **Recognize and Report Phishing**: If a link looks a little off, think before you click. It could be an attempt to get sensitive information or install malware.
- **Update Your Software**: Don't delay – if you see a software updated notification, act promptly. Better yet, turn on automatic updates.

# Contact



## General Inquiries

**central@cisa.gov**

## CISA Contact Information

| | |
|---|---|
| **Sean McCloskey**<br>**Chief of Cybersecurity**<br>**CISA Region 4** | **Sean.McCloskey@hq.dhs.gov** |
| **Greg Mallette**<br>**CISA Cyber State Coordinator, Mississippi** | **William.Mallette@cisa.dhs.gov** |

## Incident Reporting

www.cisa.gov/report

Email: report@cisa.gov

**Cybersecurity and Infrastructure Security Agency**


CISA

CYBER+INFRASTRUCTURE