U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

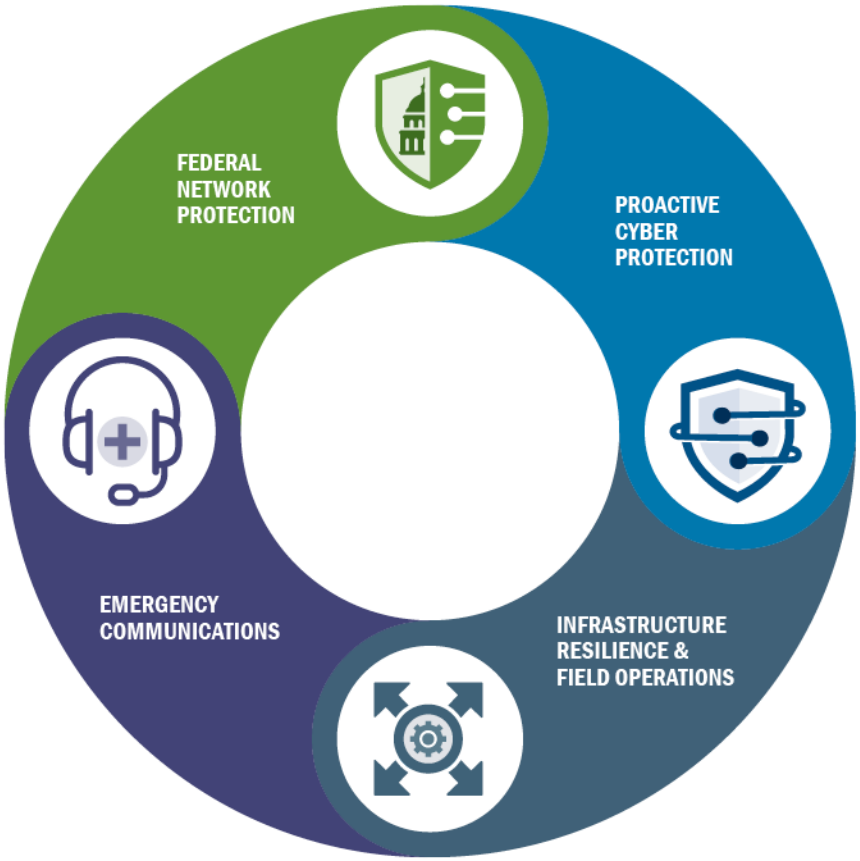
CISA
CYBER+INFRASTRUCTURE

Klint Walker
Cyber Security Advisor, Region IV

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

The Nation's Risk Managers

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



CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Who We Are

CISA works with public sector, private sector, and government partners to share information, build greater trust, and lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

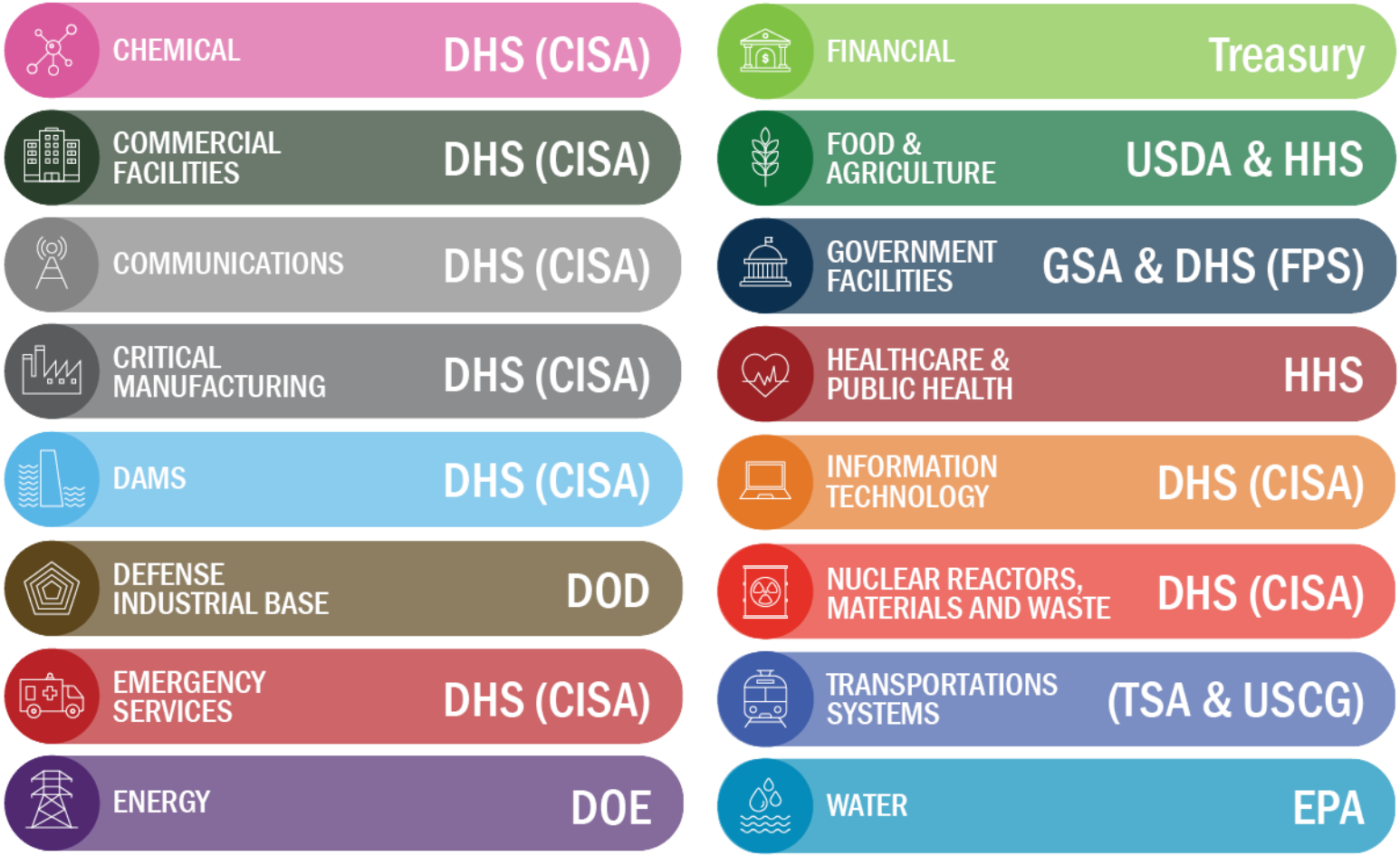
FEDERAL NETWORK PROTECTION

PROACTIVE CYBER PROTECTION

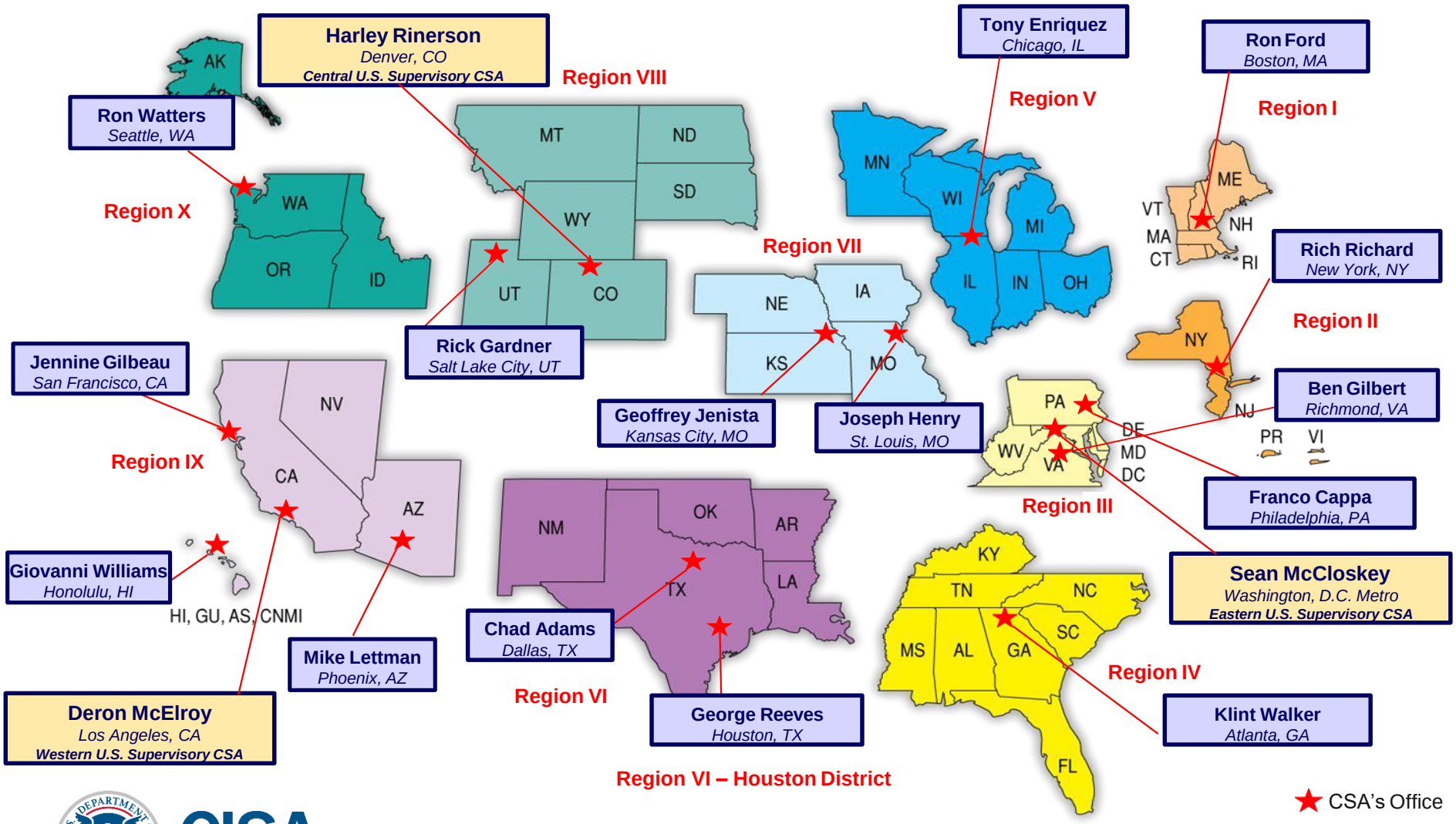
INFRASTRUCTURE RESILIENCE & FIELD OPERATIONS

EMERGENCY COMMUNICATIONS

16 Critical Infrastructure Sectors & Corresponding Sector-Specific Agencies



CSA Deployed Personnel



CISA
CYBER+INFRASTRUCTURE

CSA Program Mission

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, Territorial, and Tribal (SLTT) governments.

Cyber Security Advisor (CSA) Program in recognition that a regional and national focused cyber security presence is essential to protect critical infrastructure.

CSAs represent a front line approach and promote resilience of key cyber infrastructures throughout the U.S. and its territories.

CSA Program Activities

CSAs support four key DHS goals:

- Cyber Preparedness
- Risk Mitigation
- Incident & Information Coordination
- Cyber Policy Promotion & Situational Awareness

CSAs facilitate three assessments:

- Cyber Resilience Reviews (CRR)
- Cyber Infrastructure Surveys (C-IST)
- External Dependency Reviews (EDM)

CSAs participate in local / regional cyber working groups, mostly organized by Federal and state partners

Presidential Policy Directive 41 – Concurrent Lines of Effort

- **Threat Response**
  - **Threat response activities include conducting appropriate law enforcement and national security investigative activities; collecting evidence and gathering intelligence; providing attribution; linking related incidents; identifying additional affected entities; identifying threat pursuit and disruption opportunities; developing and executing courses of action to mitigate the immediate threat; and facilitating information sharing and operational coordination with asset response.**
- **Asset Response**
  - **Asset response activities include furnishing technical assistance to affected entities to protect their assets, mitigate vulnerabilities, and reduce impacts of cyber incidents; identifying other entities that may be at risk and assessing their risk to the same or similar vulnerabilities; assessing potential risks to the sector or region, including potential cascading effects, and developing courses of action to mitigate these risks; facilitating information sharing and operational coordination with threat response; and providing guidance on how best to utilize Federal resources and capabilities in a timely, effective manner to speed recovery.**
- **Intelligence Support**
  - **Intelligence support and related activities facilitate the building of situational threat awareness and sharing of related intelligence; the integrated analysis of threat trends and events; the identification of knowledge gaps; and the ability to degrade or mitigate adversary threat capabilities.**

Today's Risk Landscape

America remains at risk from a variety of threats:

ACTS OF TERRORISM

CYBER ATTACKS

EXTREME WEATHER

PANDEMICS

ACCIDENTS OR TECHNICAL FAILURES

Cyberspace: Foundational to Our World

- Automation, technology, and network communications have become increasingly essential to our daily lives.
- The amount of information and data stored electronically has grown.
- There is a vast interconnectedness of relationships and dependencies, for example
  - government – private sector – international
  - third-party vendors
  - linkages within organizations
- As a result, the country is dependent on the cyber resilience of its critical infrastructure, such as, the power grid, banking and financial systems, and telecommunications

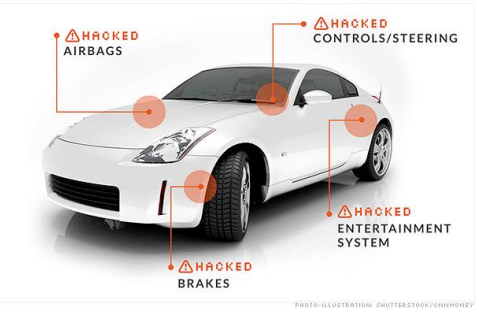
Homeland Security

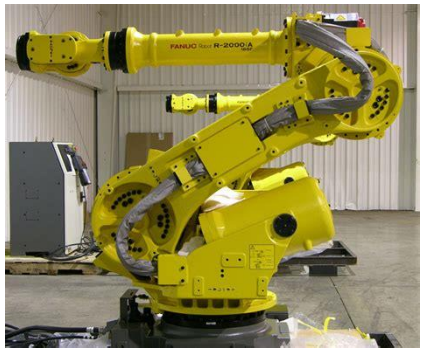
Cyber Security is Critical

- Smart cars, grids, medical devices, manufacturing, homes, buildings, smart everything!
- We bet our lives on these systems
  - cyber security ⇔ physical safety!
- Yet, much of CPS are “cobbled together from stuff found on the Web”!
- Who minds the shop?

Our buildings

Our transport





Our Production

Our health

Homeland Security

Vehicle Security – Many things to go wrong

200M lines of code in a modern vehicle!

- **Telematics**
  - Remote control (locks, start)
  - Remote diagnostics
  - Remote repair (updates)

- **System automation**
  - Dynamic EV charging
  - Computer control of engine, brakes, etc.

- **Driver support**
  - Navigation
  - Collision warning/avoidance
  - Augmented vision

- **Content and communication**
  - Voice and data
  - Information and entertainment

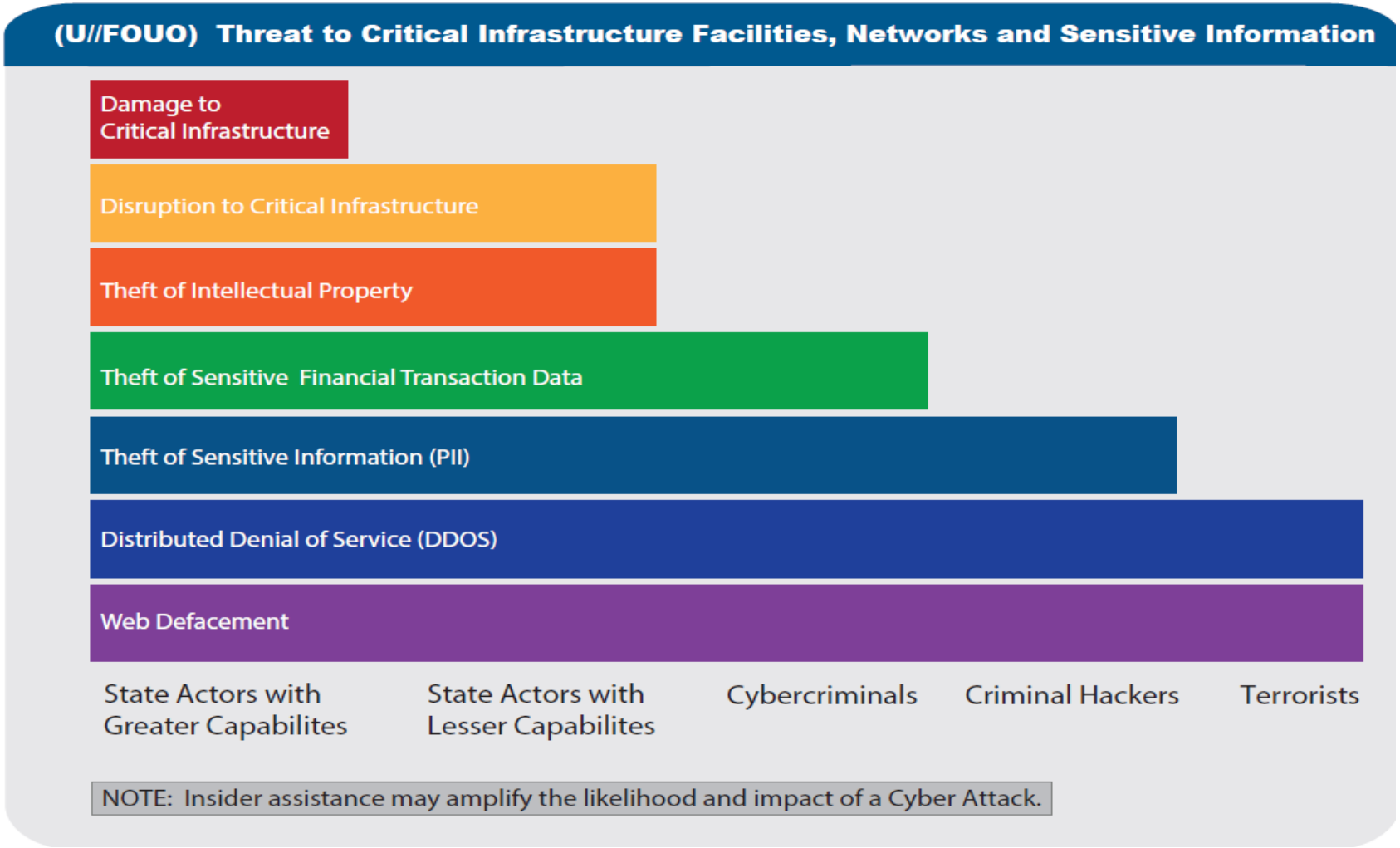
Homeland Security
Science and Technology

A Growing Challenge

- **Scale**: The number of cyber attacks has never been greater.
- **Sophistication** : Cyber attacks are increasing in complexity.
- **Trends**: Attackers are increasing their advantage.
- **Attack Surface**: Growing volumes of data = more targets.

Homeland Security

Threat Landscape



Homeland Security

IT vs. OT

SECURITY TOPIC	INFORMATION TECHNOLOGY	OPERATIONS TECHNOLOGY
ANTIVIRUS & MOBILE CODE COUNTER-MEASURES	Common & widely used	**Can be difficult to deploy**
SUPPORT TECHNOLOGY LIFETIME	3 to 5 years	**Up to 40+ years**
OUTSOURCING	Common/widely used	**Rarely used (vendor only)**
APPLICATION OF PATCHES	Regular/ scheduled	**Slow (vendor specific, compliance testing required)**
CHANGE MANAGEMENT	Regular/ scheduled	**Legacy based – unsuitable for modern security**

SECURITY TOPIC	INFORMATION TECHNOLOGY	OPERATIONS TECHNOLOGY
TIME CRITICAL CONTENT	Delays are usually accepted	**Critical due to safety**
AVAILABILITY	Delays are usually accepted	**24 x 7 x 365 x forever (Integrity also critical)**
SECURITY AWARENESS	Good in both private and public sector	**Generally poor inside the control zone**
SECURITY TESTING/ AUDIT	Scheduled and mandated	**Occasional testing for outages / audit for event recreation**
PHYSICAL SECURITY	Secure	**Traditionally good**

Cyber Supply Chain

Cybersecurity in the supply chain cannot be viewed as an IT only problem.

- Cyber supply chain risks include:
  - sourcing,
  - vendor management,
  - supply chain continuity and quality,
  - transportation security
  - and many other functions across the enterprise
- Cybersecurity is never just a technology problem, it's a people, processes and knowledge problem.
- Require a coordinated effort to address.

Cyber Supply Chain Attack Examples

- Target (2014) – HVAC security
- Equifax – 3rd Party Software flaw
- Verizon – Flawed Analytic software
- Paradise Papers – Data hacked from legal firms
- Domino's Pizza (Australia) – former 3rd party database hacked

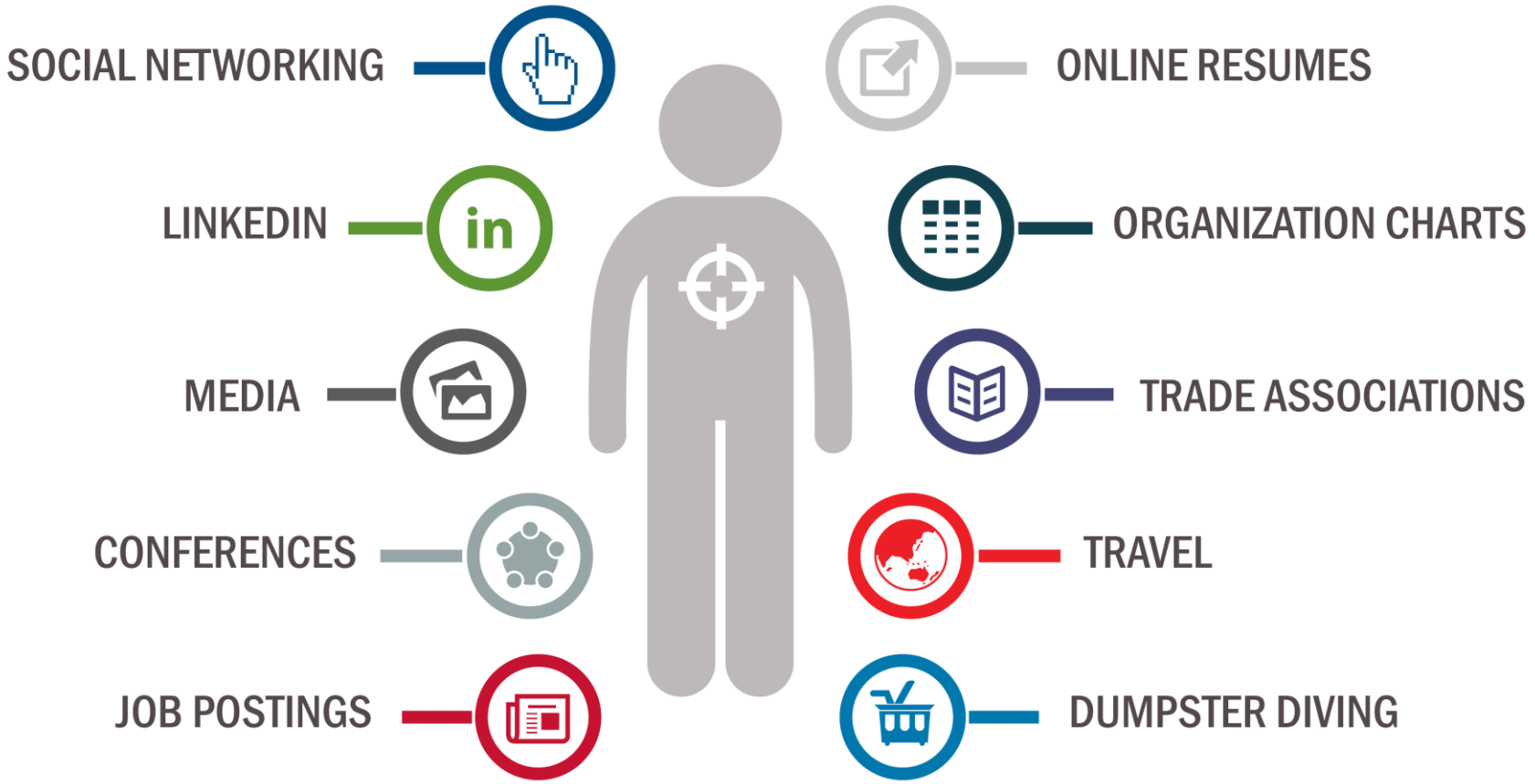
In a recent poll over 50 percent of organizations have had a breach that was caused by one of their vendors

Supply Chain Attacks Spiked 78 Percent in 2018, Cyber Researchers Found

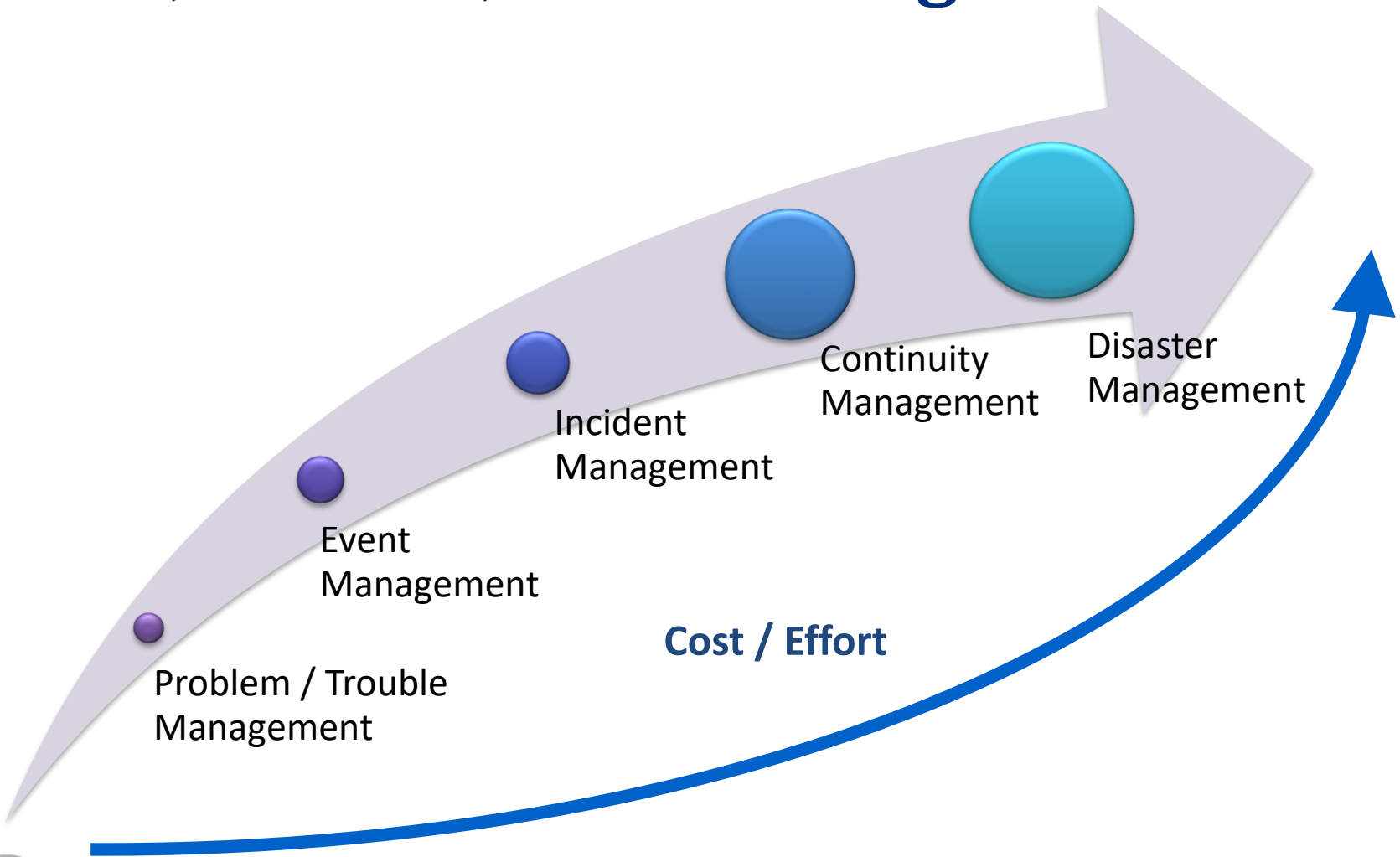
Cyber Supply Chain Threats

1. **Software service providers and outside contractors**
   - exploitation of smaller, typically less-secure companies who have access to or credentials for the networks of larger corporations
2. **Mergers and acquisitions**
   - Inheriting the (lack of) security for smaller companies
3. **Physical components**
   - hidden “backdoors” embedded in software or hardware
4. **Network services**
   - Do you know the route your digital traffic takes from one point to the next?
5. **IOT (internet of things)**
   - prioritize time-to-market over security

How Are You Targeted by Foreign Intel?



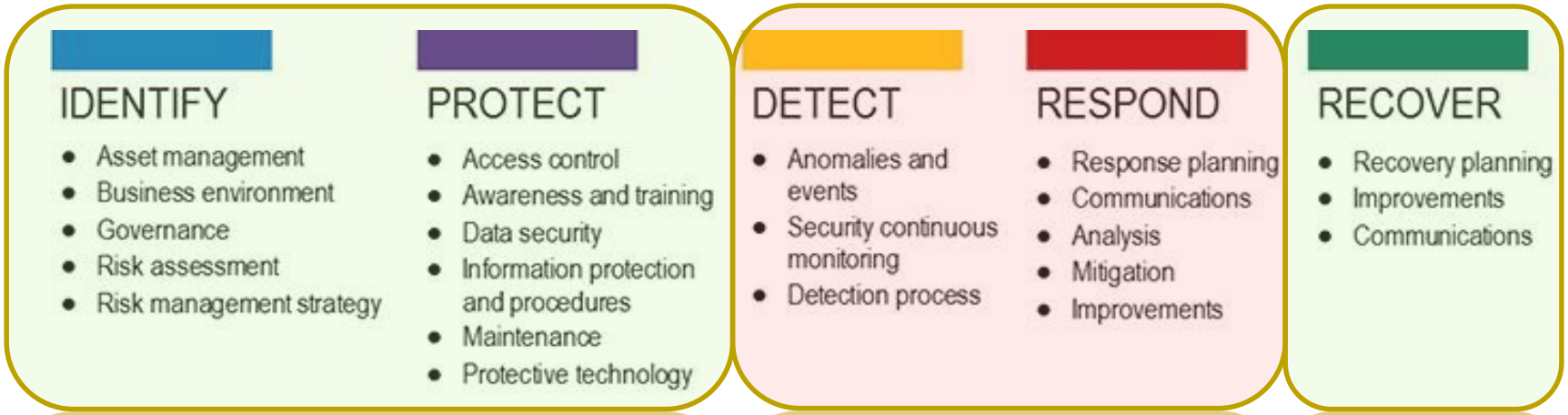
Operational Planning for Cyber Security Events, Attacks, and Contingencies



Homeland Security

CSF and the State of Cybersecurity Management

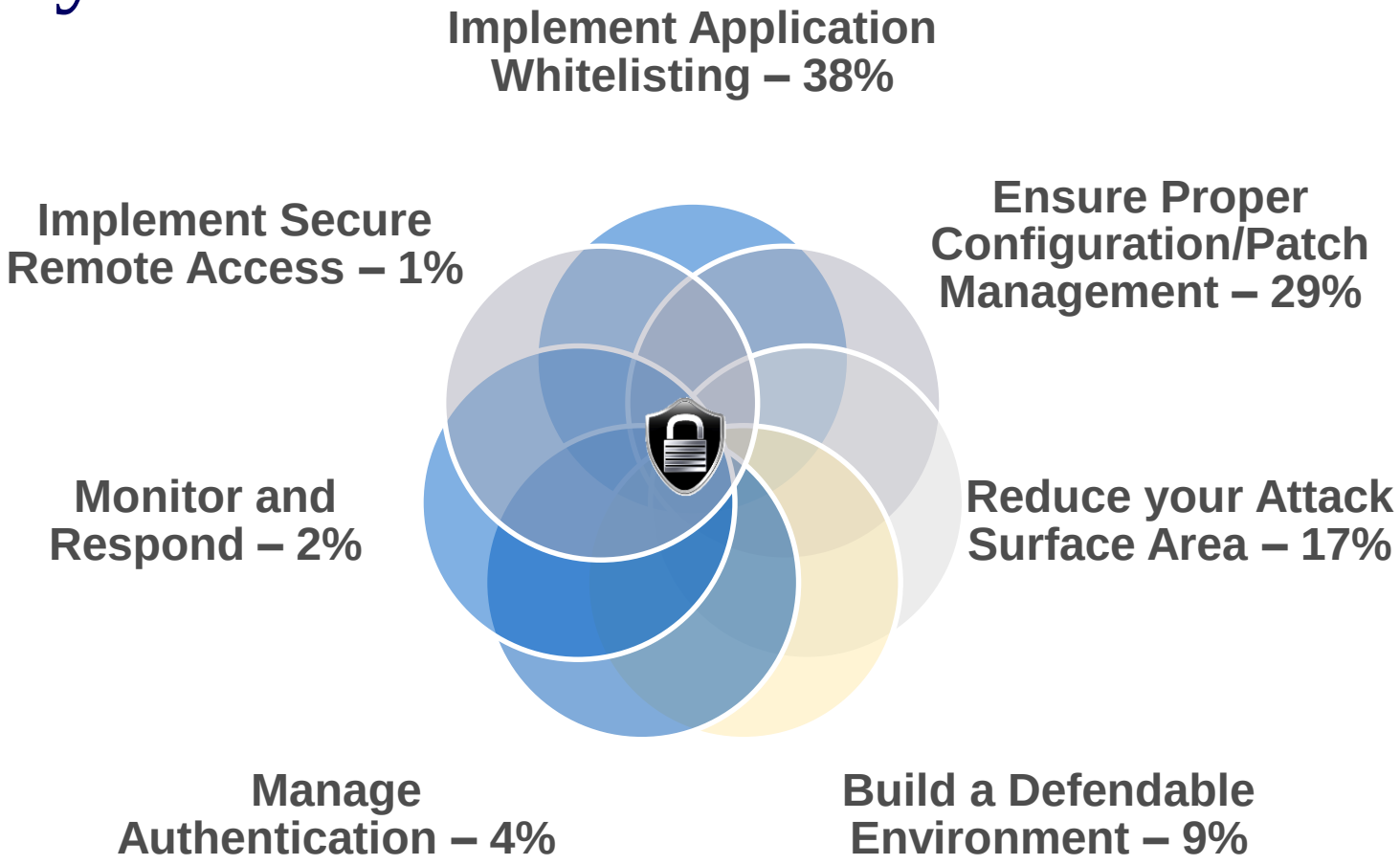
Status Quo: Practiced, Planned, & Resourced



Room for Improvement: Discussed but not Deliberate, Less Practiced, Planned, & Resourced

Homeland Security

Incident Response Root Cause Analysis*



*Based on FY14-15 ICS-CERT Incident Response Data

Homeland Security

A Wide Range of Offerings for Critical Infrastructure

- National Cybersecurity and Communications Integration Center (NCCIC)
  - US-CERT Operations Center
    - **Remote / On-Site Assistance**
    - **Malware Analysis**
    - **Incident Response Teams**
  - ICS-CERT Operations Center
    - **ICS-CERT Malware Lab**
    - **Incident Response Teams**
  - Cyber Exercise Program
- Cyber Security Advisors
- Protective Security Advisors
- Preparedness Activities
  - **National Cyber Awareness System**
  - **Vulnerability Notes Database**
  - **Security Publications**
  - **Technical Threat Indicators**
  - **Cybersecurity Training**
  - **Information Products and Recommended Practices**
- Control Systems Evaluations
  - **Cyber Security Evaluation Tool**
  - **ICS Design Architecture Reviews / Network Architecture Analysis**
- Other Cyber Security Evaluations
  - **Cyber Resilience Review**
  - **Cyber Infrastructure Survey**
  - **Cyber Hygiene service**
  - **Risk and Vulnerability Assessment (aka "Pen" Test)**

Homeland Security

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

Range of Cybersecurity Assessments

STRATEGIC
(C-Suite Level)

- Cyber Resilience Review (Strategic)----------
- External Dependencies Management (Strategic)----------
- Cyber Infrastructure Survey (Strategic)----------
- Cybersecurity Evaluations Tool Strategic/Technical)-----
- Phishing Campaign Assessment (EVERYONE)----------
- Vulnerability Scanning / Hygiene (Technical)----------
- Validated Architecture Design Review (Technical)-------
- Risk and Vulnerability Assessment (Technical)----------

TECHNICAL
(Network-Administrator Level)

CISA
CYBER+INFRASTRUCTURE

VULNERABILITY SCANNING

Vulnerability Scanning

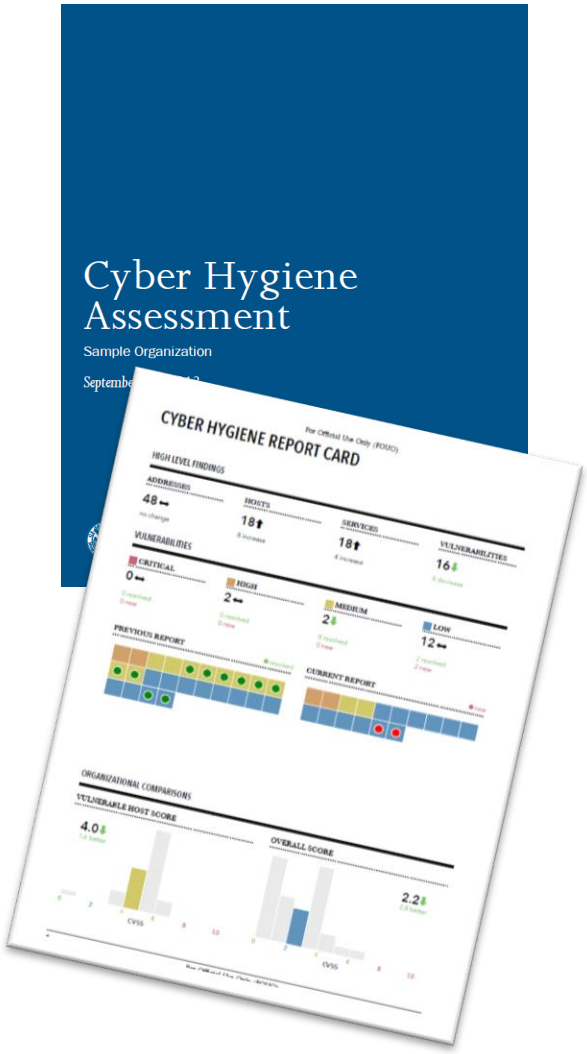
Purpose: Assess Internet-accessible systems for known vulnerabilities and configuration errors.

Delivery: 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

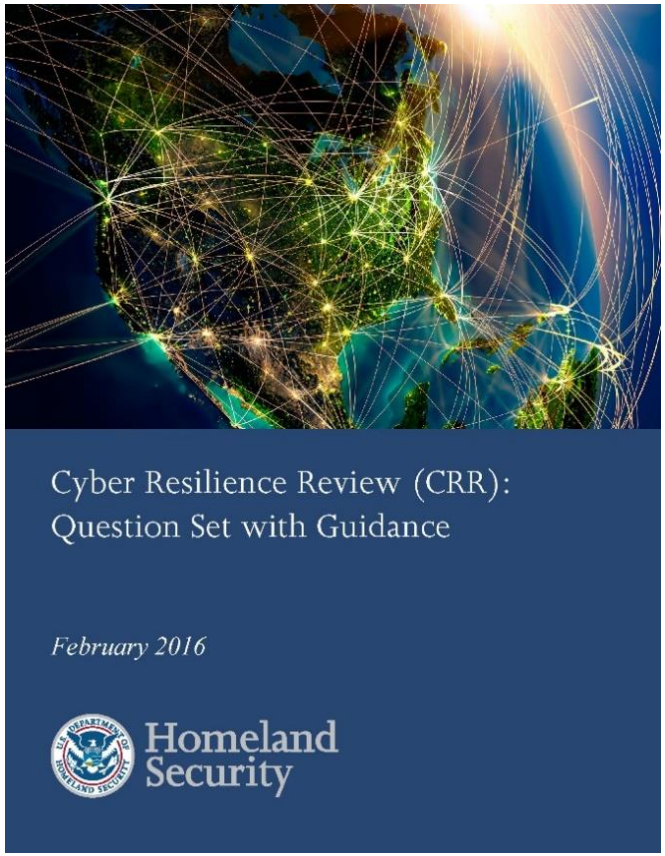
  - **Network Vulnerability & Configuration Scanning**
    - Identify network vulnerabilities and weakness



CYBER RESILIENCE REVIEW

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

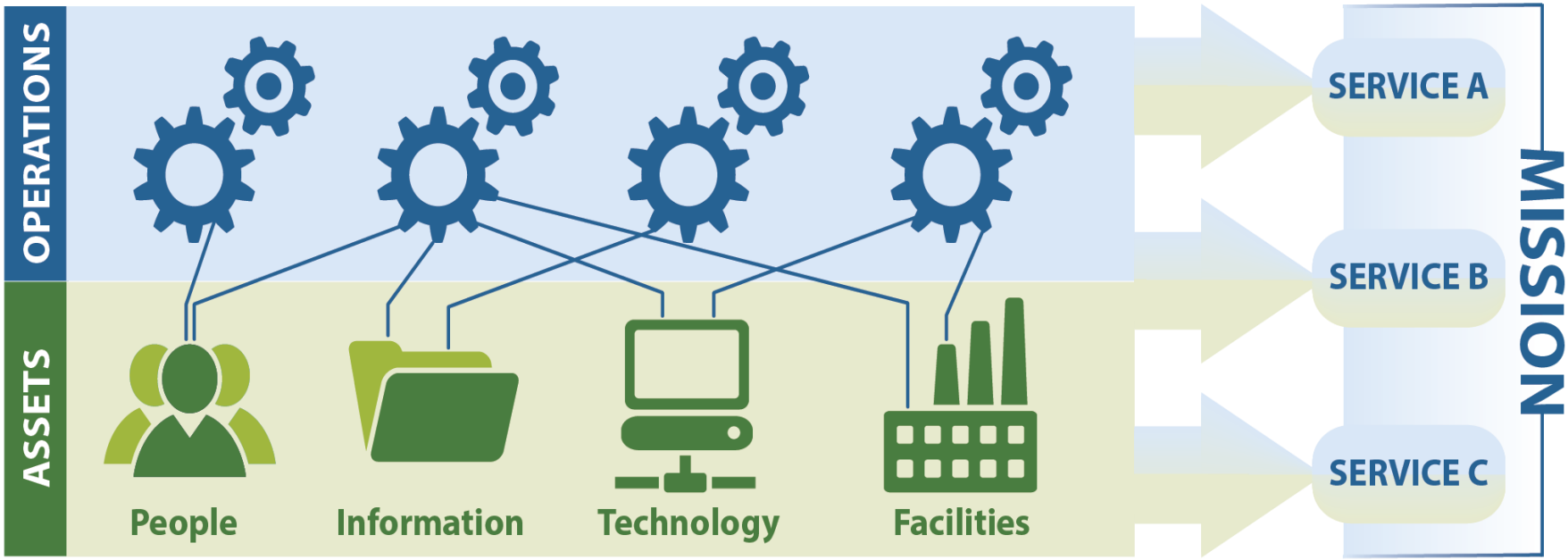


CRR Question Set & Guidance

CISA CYBER+INFRASTRUCTURE

Critical Service Focus

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



CISA
CYBER+INFRASTRUCTURE

Cyber Resilience Review Domains

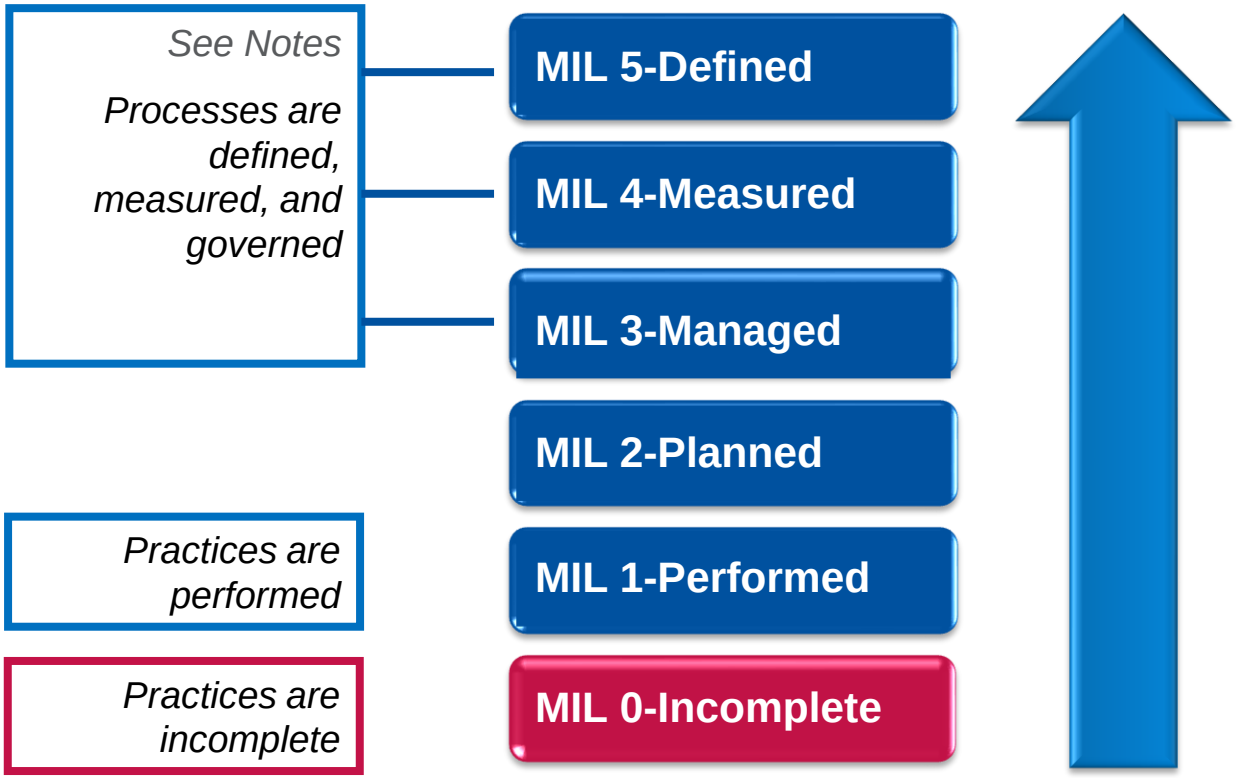
Asset Management Know your assets being protected & their requirements, e.g., CIA	**Risk Management** Know and address your biggest risks that considers cost and your risk tolerances
Configuration and Change Management Manage asset configurations and changes	**Service Continuity Management** Ensure workable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

For more information: http://www.us-cert.gov/ccubedvp

CISA
CYBER+INFRASTRUCTURE

Process Institutionalization

CRR maturity indicator levels (MILs) are to measure process institutionalization:



Higher MIL degrees translate to more stable processes that:

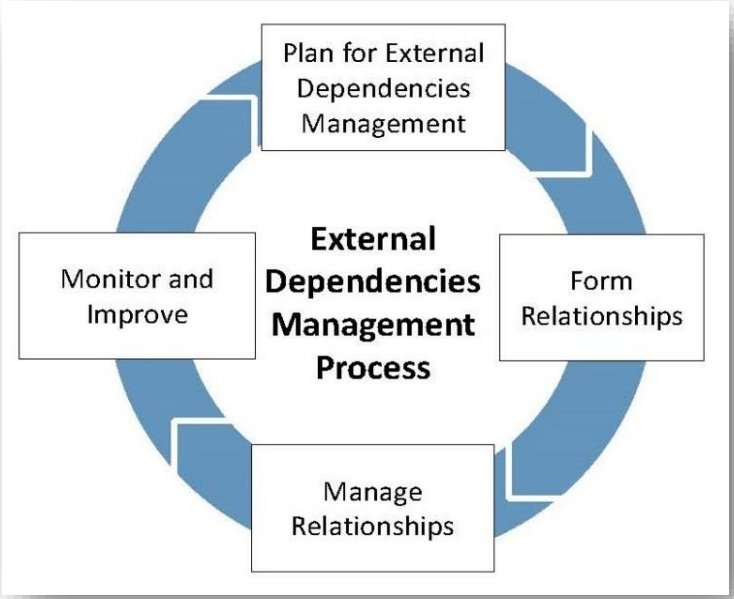
- Produce consistent results over time
- Are retained during times of stress

CISA CYBER+INFRASTRUCTURE

EXTERNAL DEPENDENCIES MANAGEMENT ASSESSMENT

External Dependencies Management Assessment

- **Purpose:** Evaluate an entity's management of their dependencies on third-party entities
- **Delivery:** CSA-facilitated
- **Benefits**:
  - Better understanding of the entity's cyber posture relating to external dependencies
  - Identification of improvement areas for managing third parties that support the organization



EDM process outlined per the External Dependencies Management Resource Guide

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

CYBER INFRASTRUCTURE SURVEY

Cyber Infrastructure Survey Highlights

- 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), and
  - Access to peer performance data visually depicted on the dashboard.

CISA
CYBER+INFRASTRUCTURE

Example of CIS Dashboard

Scenario:
- ❑ Where should we to invest?
- ❑ Weakest area in comparison to peers
- ❑ Show management improvement

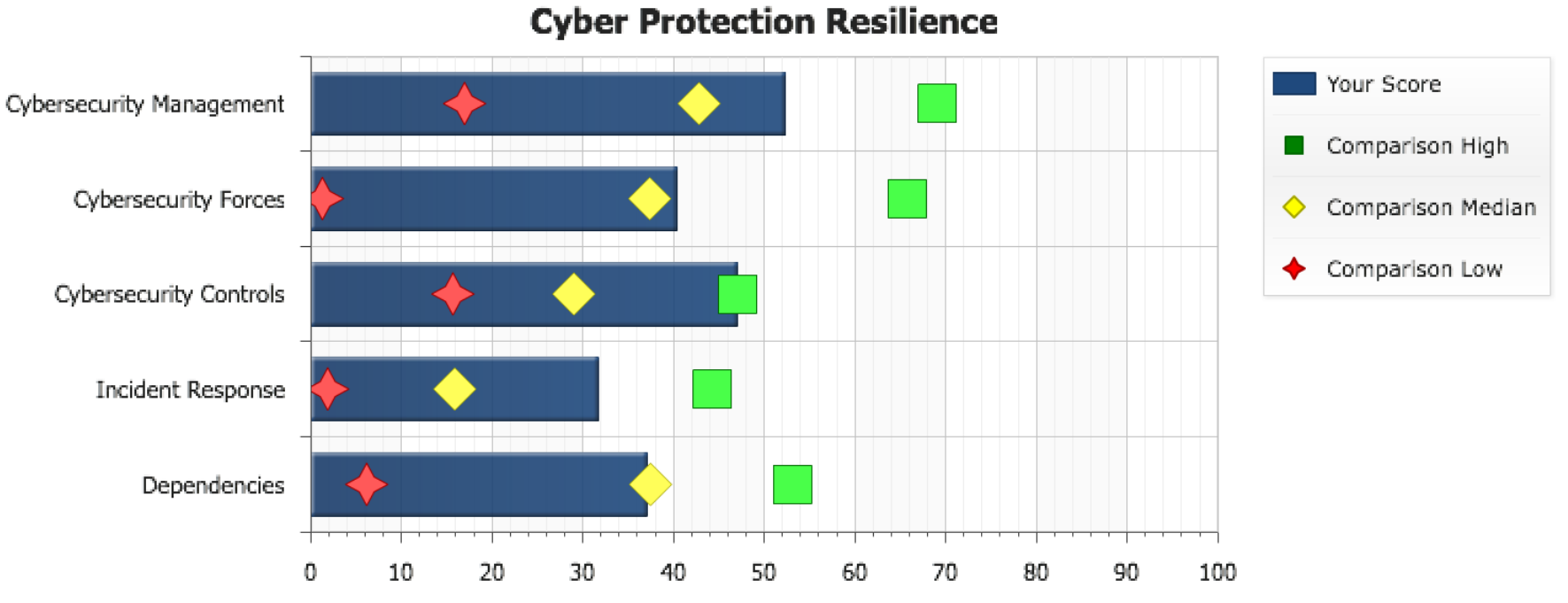
Threat-based PMI:
- ❑ Natural Disaster
- ❑ Distributed Denial-of-Service
- ❑ Remote Access Compromise
- ❑ System Integrity Compromise

Comparison:
- ❑ Low Performers
- ❑ Median Performers
- ❑ High Performers

CISA CYBER+INFRASTRUCTURE

CIS Dashboard - Comparison

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

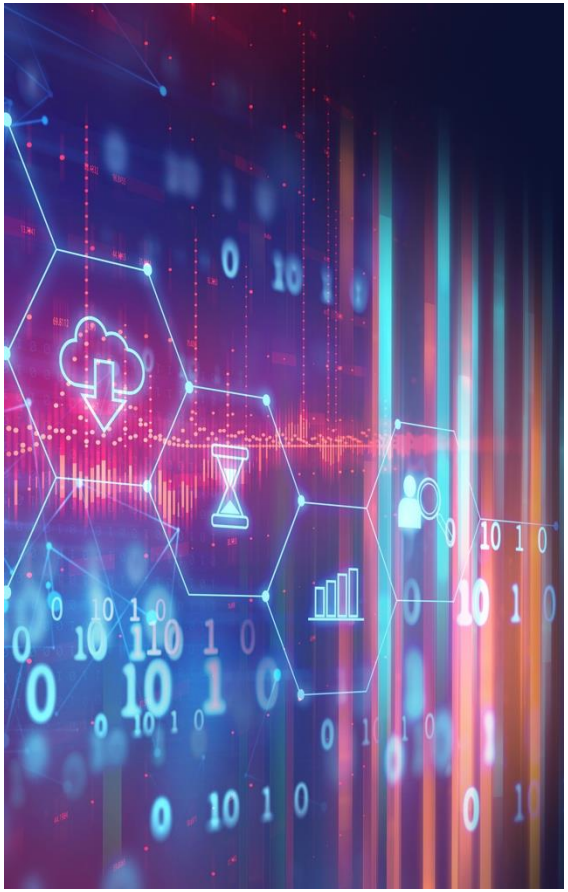


CISA
CYBER+INFRASTRUCTURE

CYBER SECURITY EVALUATION TOOL

Cyber Security Evaluation Tool

- **Purpose:** Assesses control system and information technology network security practices against industry standards.
- **Facilitated:** Self-Administered, undertaken independently
- **Benefits:**
  - Immediately available for download upon request
  - Understanding of operational technology and information technology network security practices
  - Ability to drill down on specific areas and issues
  - Helps to integrate cybersecurity into current corporate risk management strategy



CISA
CYBER+INFRASTRUCTURE

PHISHING CAMPAIGN ASSESSMENT

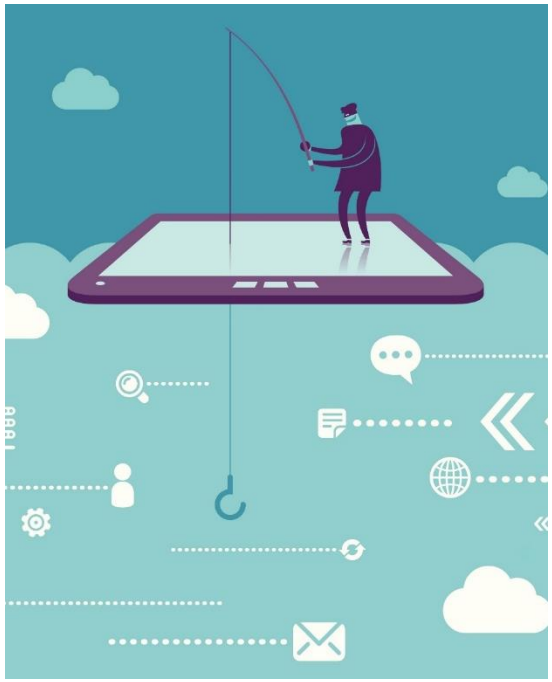
Phishing Campaign Assessment

Purpose: Test an organization's susceptibility and reaction to phishing emails.

Delivery: Online delivery by CISA

Benefits:

- Identify the risk phishing poses to your organization
- Decrease risk of successful malicious phishing attacks, limit exposure, reduce rates of exploitation
- Receive actionable metrics
- Highlight need for improved security training
- Increase cyber awareness among staff



CISA CYBER+INFRASTRUCTURE

Phishing Campaign Assessment Sample Email, 1 of 2

To: <Stakeholder List>

From: Apples Customer Relations <freeapplesforyou@[PCA-testing-site].org> Subject: Free iPad – Just Complete a Survey!

Want the new iPad or iPad Mini? I got mine free from this site: <fake link> !!!!!

We would like to invite you to be part of a brand new pilot program to get our new product in the hands of users before official release. This assures that any issues or errors are mitigated before the release. If you are accept to participate in this programall we ask is that you submit a survey at the end of the Pilot. You be able to keep iPad at the end for free!

Apples Customer Relationships Office

Apples Campus, Cupertino, California 95114

Phishing Campaign Assessment Sample Email, 2 of 2

To: <Stakeholder List>
From: OBRM <OBRM@[PCA-testing-site].org>
Subject: Future Budget Plans

In the coming weeks, our state's leadership will be working to draft a plan to prevent long term financial issues and ways to avoid human resource reductions. All departments within the State Government are being directed to draft a plan to help meet projected budget shortages and find ways to reduce spending within the State Government.

We have been asked to work more efficiently with less. As a result, many budgets and programs are also facing significant reduction. The Office of Budget and Resource Management has developed a draft plan that will address any potential budget shortcomings.

To learn more about the budget and how your program maybe affected, please visit <LINK>.

If you have any questions or concerns, we'd love to hear them. Please emails us here <embedded link>.

Office of Budget and Resource Management

VALIDATED ARCHITECTURE DESIGN REVIEW

CISA
CYBER+INFRASTRUCTURE

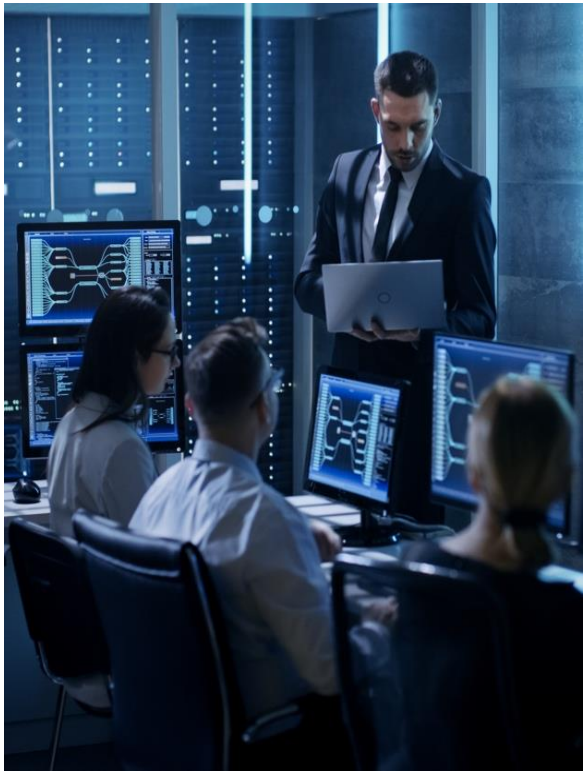
Validated Architecture Design Review

Purpose: Analyze network architecture, system configurations, log file review, network traffic and data flows to identify abnormalities in devices and communications traffic.

Delivery: CISA staff working with entity staff

Benefits:

- In-depth review of network and operating system
- Recommendations to improve an organization's operational maturity and enhancing their cybersecurity posture
- Evaluation of network architecture

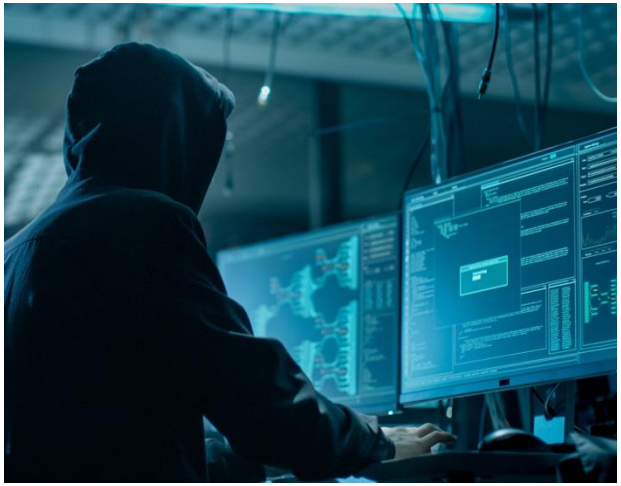


CISA
CYBER+INFRASTRUCTURE

RISK AND VULNERABILITY ASSESSMENT
[PENETRATION TEST]

Risk and Vulnerability Assessment

- **Purpose**: Perform network penetration and deep technical analysis of enterprise IT systems and an organization's external resistance to specific IT risks
- **Delivery**: Onsite by CISA
- **Benefits**:
  - Identification of vulnerabilities
  - Specific remediation recommendations
  - Improves an entity's cyber posture, limits exposure, reduces rates of exploitation
  - Increases speed and effectiveness of future cyber attack responses.



CISA CYBER+INFRASTRUCTURE

Risk and Vulnerability Assessment Specifics

Assessment Aspects

Service	Description
Vulnerability Scanning and Testing	Conduct Vulnerability Assessments
Penetration Testing	Exploit weakness, test responses in systems, applications, network, and security controls
Social Engineering	Craft e-mail at targeted audience to test security awareness, used as an attack sector to internal network
Wireless Discovery & Identification	Identify wireless signals and rogue wireless devices, and exploit access points
Web Application Scanning and Testing	Identify web application vulnerabilities
Database Scanning	Security Scan of database settings and controls
Operating System Scanning	Security Scan of operating system to do compliance checks

Incident Reporting

NCCIC (ICS-CERT/US-CERT) INCIDENT REPORTING INFORMATION

Homeland Security

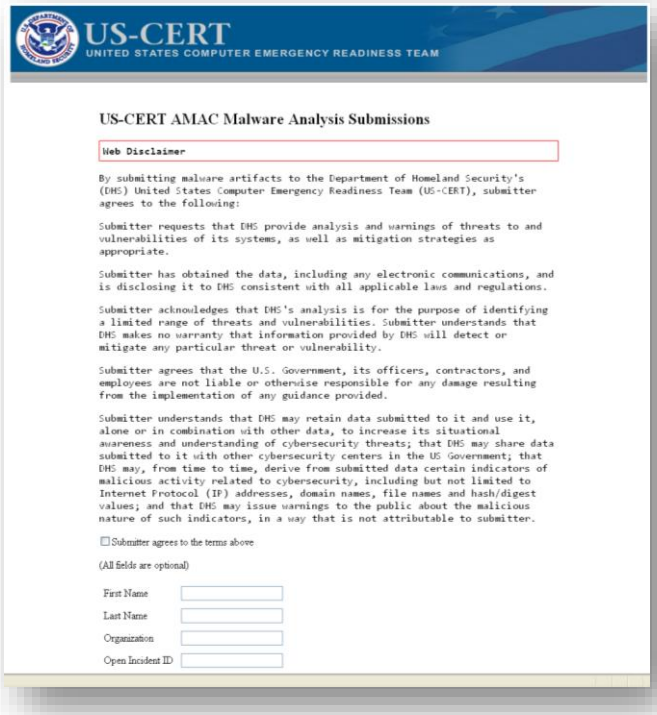
Additional - Incident Reporting

NCCIC provides real-time threat analysis and incident reporting capabilities

- 24x7 contact number: 1-888-282-0870

Malware Submission Process:

- Please send all submissions to AMAC at: submit@malware.us-cert.gov
- Must be provided in password-protected zip files using password “infected”
- Web-submission: https://malware.us-cert.gov


US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

US-CERT AMAC Malware Analysis Submissions

Web Disclaimer

By submitting malware artifacts to the Department of Homeland Security's (DHS) United States Computer Emergency Readiness Team (US-CERT), submitter agrees to the following:

Submitter requests that DHS provide analysis and warnings of threats to and vulnerabilities of its systems, as well as mitigation strategies as appropriate.

Submitter has obtained the data, including any electronic communications, and is disclosing it to DHS consistent with all applicable laws and regulations.

Submitter acknowledges that DHS's analysis is for the purpose of identifying a limited range of threats and vulnerabilities. Submitter understands that DHS makes no warranty that information provided by DHS will detect or mitigate any particular threat or vulnerability.

Submitter agrees that the U.S. Government, its officers, contractors, and employees are not liable or otherwise responsible for any damage resulting from the implementation of any guidance provided.

Submitter understands that DHS may retain data submitted to it and use it, alone or in combination with other data, to increase its situational awareness and understanding of cybersecurity threats; that DHS may share data submitted to it with other cybersecurity centers in the US Government; that DHS may, from time to time, derive from submitted data certain indicators of malicious activity related to cybersecurity, including but not limited to Internet Protocol (IP) addresses, domain names, file names and hash/digest values; and that DHS may issue warnings to the public about the malicious nature of such indicators, in a way that is not attributable to submitter.

☐ Submitter agrees to the terms above

(All fields are optional)

First Name

Last Name

Organization

Open Incident ID

Any Questions/Discussion?

- Web Resources and Contact CheatSheet:
- ICS-Cert: https://ics-cert.us-cert.gov/
- Stakeholder Engagement and Cyber Infrastructure Resilience:
  http://www.dhs.gov/stakeholder-engagement-and-cyber-infrastructure-resilience

Homeland Security

Contact Information

Evaluation Inquiries
cyberadvisor@hq.dhs.gov

General Inquiries
cyberadvisor@hq.dhs.gov

DHS Contact Information	
Bradford Willke Program Manager, Cyber Security Advisor Program	bradford.willke@hq.dhs.gov +1 412 375-4069
Klint Walker Cyber Security Advisor, Region IV	Klint.walker@hq.dhs.gov +1 404-895.1127

Department of Homeland Security
National Protection and Programs Directorate
Office of Cybersecurity and Communications

CYBER SECURITY SELF-TEST - 1

What role do you play in IT security, IT incident response, IT continuity of operations?

- Planner, Responder, Investigator?

How much emphasis do you place upon having up-to-date, documented plans versus having available, capable staff?

- What types of cyber hazards do these plans account for?

What requirements have you provided to IT security personnel and IT continuity planners, in terms of goals and objectives your agency/organization wants to achieve for cyber security?

- Do you have a procedures in-place that triggers your participation and coordination in incident response, continuity operations, etc?

How do you and do you test IT incident response and continuity plans beforehand?

- What makes a good test?
- How much are your disruptive scenarios based upon real-world threats?

CYBER SECURITY SELF-TEST - 2

How would law enforcement coordinate with you as an affected organizations, in the wake of cyber attacks?

Who in your agency or organization is (best) authorized to contact outsider partners (e.g., contracted, private, public, etc) for help, assistance, response, etc?

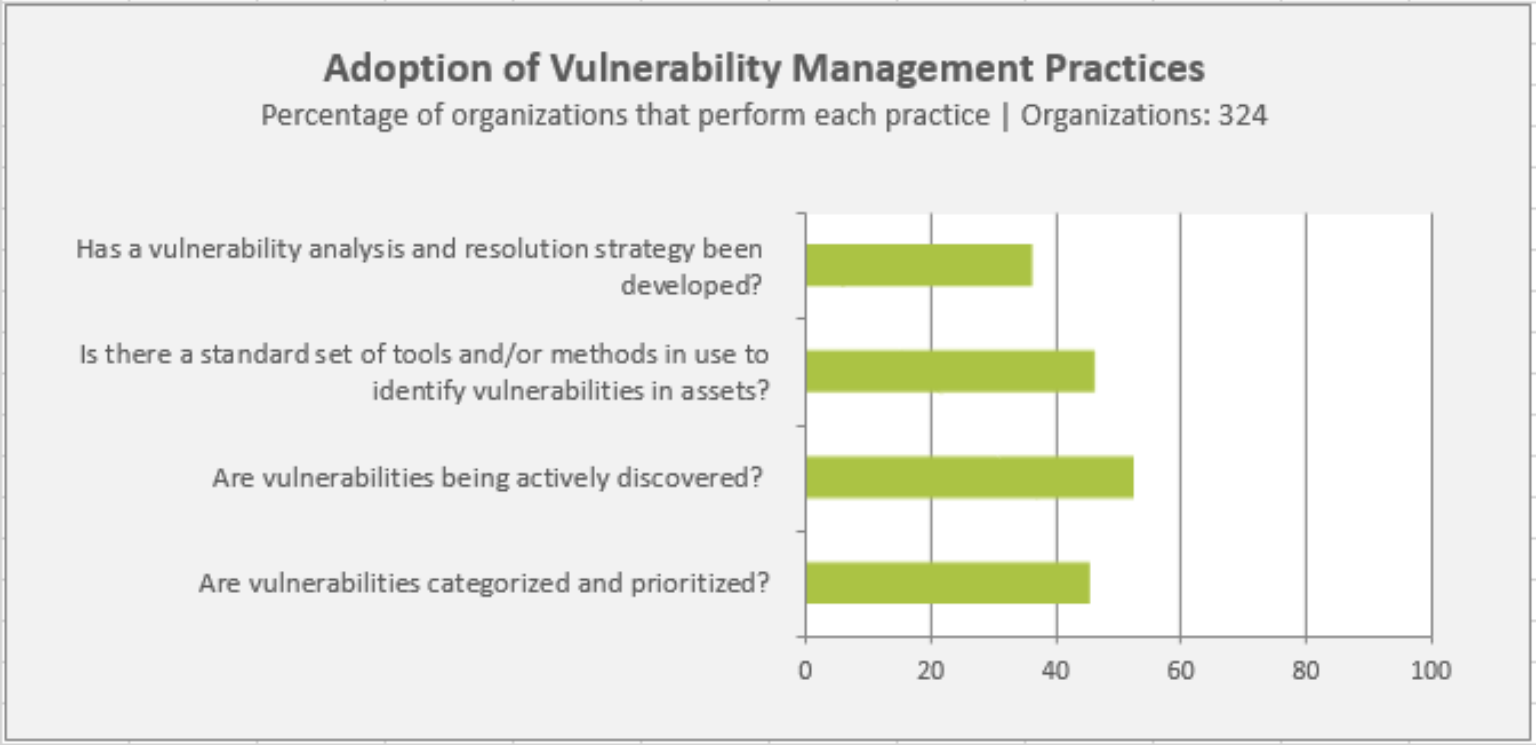
What do you want to know in the first 30 minutes of a disruptive cyber attack?

What are you willing to share within the first 30 minutes of a disruptive cyber attack?

What steps are you going to take in the next 30 days to improve cyber security … at the office … in your operations … at home?

Homeland Security

Vulnerability Management



- Approximately 35% of organizations have a strategy to guide their vulnerability management efforts.
- Roughly 45% of organizations have determined a standard set of tools or methods to assist in identifying vulnerabilities.

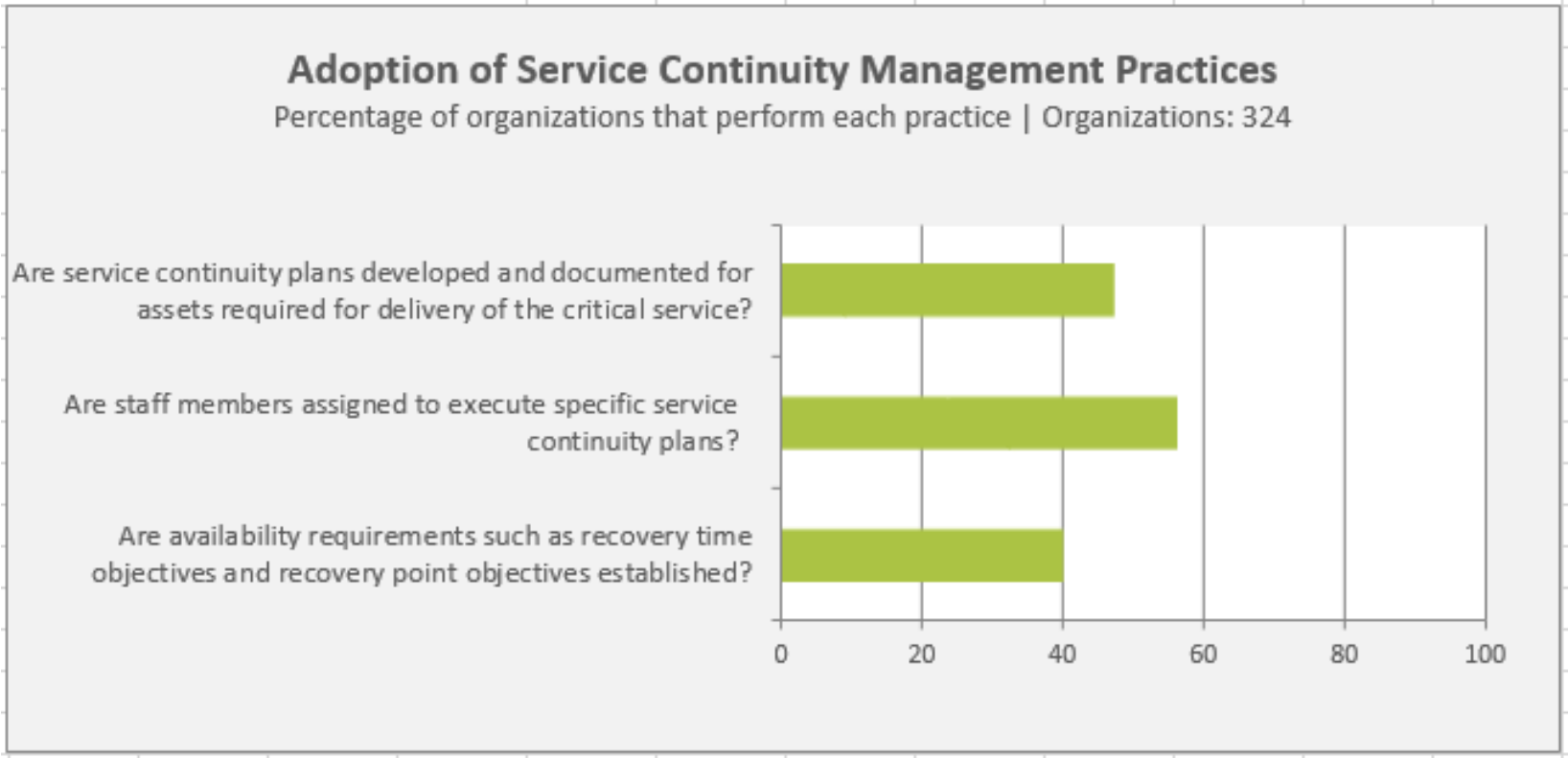
Homeland Security

Incident Management

- While roughly 70% of organizations perform event detection
  - 55% have a process to declare incidents
  - and only 35% have developed criteria to guide their staff

Homeland Security

Service Continuity



- Less than 50% of organizations have documented service continuity plans.
- Only 40% specify recovery time and recovery point objectives in their plans.

Homeland Security

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

CISA ASSESSMENTS

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services. The team also provides an objective third-party perspective of stakeholder operational cybersecurity posture and identifies security control strengths and weaknesses. CISA Assessments aggregates these insights into actionable reports that champion the implementation of mitigations and controls capable of positive impact toward overall risk reduction.

OBJECTIVES

- Reduce Stakeholder Risk
- Enable Data-Driven Decision
- Influence Operational Behaviors
- Increase National Resilience

SERVICE OFFERINGS

- **Vulnerability Scanning** is the persistent scanning of internet-accessible systems for vulnerabilities, configuration errors, and suboptimal security practices.
- **Phishing Campaign Assessments** measure propensity to click on email phishing lures which increases organizational training and awareness.
- **Remote Penetration Testing** focuses on testing a stakeholder's internet exposure.
- **Risk and Vulnerability Assessments** combine national threat information with data collected and vulnerabilities identified through on-site assessment activities to provide tailored risk analysis reports.
- **Red Team Assessments** closely mirror an attack by an advanced adversary to test operational capabilities and maturity.
- **Validated Architecture Design Review** evaluates the resiliency of a stakeholder's systems, networks and security services.
- **Third-Party Qualification** qualifies third-party organizations to perform assessments and technical services following CISA Assessments standards, process and procedures.
- **Critical Product Evaluations** assess, within an isolated environment, the "out-of-the-box" security of products and solutions relevant to critical infrastructure operations and national resilience.
- **Cyber Resilience Review** identifies and evaluates cyber security management capabilities, maturity, and capacity to manage cyber risk during normal operations and times of operational stress.
- **External Dependency Management** assesses the activities and practices utilized by an organization to manage risks arising from external dependencies.
- **Cyber Infrastructure Survey** identifies cybersecurity controls and protective measures in place and provides an interactive dashboard for comparative analysis and valuation.

ABOUT

Our Team

The CISA Assessments team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our Services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities.

Additional Information

CISA assessments' security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.

GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at **NCATS_INFO@hq.dhs.gov** to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.

MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

CYBER HYGIENE: VULNERABILITY SCANNING

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services.

CISA's Cyber Hygiene Vulnerability Scanning is "internet scanning-as-a-service." This service continuously assesses the "health" of your internet-accessible assets by checking for known vulnerabilities and weak configurations, and recommends ways to enhance security through modern web and email standards.

SCANNING OBJECTIVES

- Maintain enterprise awareness of your internet-accessible systems
- Provide insight into how systems and infrastructure appear to potential attackers
- Drive proactive mitigation of vulnerabilities and reduce risk

SCANNING PHASES AND STAGES

PHASES

- **Target Discovery:** Identify all active internet-accessible assets (networks, systems, and hosts) to be scanned
- **Vulnerability Scanning:** Initiate non-intrusive checks to identify potential vulnerabilities and configuration weaknesses

STAGES

Pre-Planning

- Request service
- Receive Cyber Hygiene brief
- Provide target list (scope)
- Sign and return documents

Planning

- Confirm scanning schedule
- Pre-scan notification

Execution

- Initial scan of submitted scope
- Rescan scope based on detected vulnerability severity:
  - 12 hours for "critical"
  - 24 hours for "high"
  - 4 days for "medium"
  - 6 days for "low"
  - 7 days for "no vulnerabilities"

Reporting

- Ongoing weekly summary report
- Vulnerability mitigation recommendations
- Detailed findings in consumable format

ABOUT

Our Team

The CISA Assessments team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities

Additional Information

CISA assessments' security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.

GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at **NCATS_INFO@hq.dhs.gov** to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.

MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

CYBER HYGIENE: WEB APPLICATION SCANNING (WAS)

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services.

CISA's Cyber Hygiene Web Application Scanning is "internet scanning-as-a-service." This service assesses the "health" of your publicly accessible web applications by checking for known vulnerabilities and weak configurations. Additionally, we can recommend ways to enhance security in accordance with industry and government best practices and standards.

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 AND OVERALL PROCESS

Scanning Phases

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

Overall Process

Planning
- Request service (Existing Cyber Hygiene Customers)
- Provide target list (scope)
- Confirm scanning schedule
- Pre-scan notification

Execution
- Initial discovery scan of submitted list
- Conduct vulnerability scan

Reporting
- Provide detailed report of findings
- Follow on discussion (if necessary) to review

ABOUT

Our Team

The CISA Assessments team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to Federal Government, SLTT and critical infrastructure networks.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities

Additional Information

CISA assessments' security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.

GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is currently limited to existing CISA customers. Contact us at NCATS_INFO@hq.dhs.gov to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.

MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

PHISHING CAMPAIGN ASSESSMENT

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services.

CISA Assessments' Phishing Campaign Assessment (PCA) measures an organization's propensity to click on email phishing lures, commonly used to collect sensitive information or as initial access to a network. Based on CISA Assessments' testing, email phishing is the number one means of initial access into a private network. PCA results can be used to provide guidance for anti-phishing training and awareness.

CAPABILITIES

Test: Assess the behavioral responses of a specified target user base when presented with expertly crafted phishing emails emulating real world threats.

Inform: Provide leadership information on potential training and awareness improvements based on the metrics gathered through the course of the assessment.

ASSESSMENT OBJECTIVES

- Reduce risk to malicious phishing email attempts by testing and informing users
- Understand how users are enticed to click on links and report suspicious activity
- Properly emulate malicious phishing activity to provide a quality learning experience

ASSESSMENT TIMELINE

Pre-Planning

- Request assessment
- Receive PCA briefing documents
- Sign and return forms

Planning

- Confirm schedule
- Approve email templates
- Test email delivery/receipt

Execution (Six weeks)

- Receive increasingly deceptive phishing emails from pre-approved templates

Post-Execution

- Receive weekly click-rate summaries
- Final report review and receipt
- Optional retest available

ABOUT

Our Team

The CISA Assessments team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities.

Additional Information

CISA assessments' security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.

GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at **NCATS_INFO@hq.dhs.gov** to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.

MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

RISK AND VULNERABILITY ASSESSMENT

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services.

CISA Assessments' Risk and Vulnerability Assessment (RVA) is a one-on-one engagement with stakeholders that combines open-source national threat and vulnerability information with data collected through remote and onsite assessment activities to provide actionable risk analysis reports with remediation recommendations prioritized by severity and risk.

CAPABILITIES

Penetration Testing: CISA Assessments conducts an array of tests to determine susceptibility to an actual real-world attack by infiltrating the target environment using current tactics, techniques, and procedures. Specific types of testing and assessments include network, web application, wireless, war dial, and social engineering in the form of an email phishing campaign.

Configuration Review: CISA Assessments reviews and analyzes operating system and database settings and configurations, which the team compares to industry standards, guidelines, and best practices to identify security issues.

ASSESSMENT OBJECTIVES

- Identify weaknesses through network, system, and application penetration testing
- Test stakeholders using a standard, repeatable methodology to deliver actionable findings and recommendations
- Analyze collected data to identify security trends across all RVA stakeholder environments

ASSESEMENT TIMELINE

Pre-Planning

- Request RVA
- Receive RVA brief
- Sign and return documents

Planning

- Confirm schedule
- Establish Trusted Point of Contact
- Determine RVA services, scope, and logistics during pre-assessment call(s)

Execution (Ten Days)

- One week external testing
- One week internal testing
- Remote Penetration Testing – external only

Post-Execution

- Out-Brief – provide initial findings
- Report review and receipt – 10 days
- Follow-up on remediation actions – 180 day

ABOUT

Our Team

The CISA Assessments team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities

Additional Information

CISA assessments' security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.

GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at **NCATS_INFO@hq.dhs.gov** to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.

MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

REMOTE PENETRATION TESTING

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services.

CISA Assessments' Remote Penetration Test (RPT) utilizes a dedicated remote team to assess and identify vulnerabilities and work with customers to eliminate exploitable pathways. RPTs are similar to risk and vulnerability assessments but focus only on externally accessible systems with a tradeoff made for more service capacity at the expense of assessment scope. As a remote service, it is less costly and more scalable than on-site offerings; however, it is more limited in organizational insight and context.

SCENARIOS

External Penetration Test: Verifying if the stakeholder network is accessible from the public domain by an unauthorized user by assessing open ports, protocols, and services.

External Web Application Test: Evaluating web applications for potential exploitable vulnerabilities; the test can include automated scanning, manual testing, or a combination of both methods.

Phishing Assessment: Testing through carefully crafted phishing emails containing a variety of malicious payloads to the trusted point of contact.

ASSESSMENT OBJECTIVES

- Conduct assessments to identify vulnerabilities and work with customers to eliminate exploitable pathways.
- Simulate the tactics and techniques of real-world threats and malicious adversaries.
- Test centralized data repositories and externally accessible assets/resources.
- Avoid causing disruption to the customer's mission, operation, and network infrastructure.

ASSESMENT TIMELINE

Pre-Planning

- Request RPT
- Receive RPT Capabilities Brief
- Sign and return RPT Rules of Engagement

Planning

- Confirm schedule
- Establish trusted points of contact
- Determine RPT services, scope, and logistics during pre-assessment call(s)

Execution (Up to Six Weeks)

- Dependent on resource availability
- Critical findings are immediately disclosed

Reporting

- Briefing and initial recommendations
- Final report review and receipt – 10 days
- Follow-up on mitigation actions – 180 day

ABOUT

Our Team

The CISA Assessments team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities

Additional Information

CISA assessments' security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.

GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at **NCATS_INFO@hq.dhs.gov** to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.

MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

RED TEAM ASSESSMENT

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services.

CISA Assessments' Red Team Assessment (RTA) is a comprehensive evaluation of an information technology (IT) environment. Simulation of advanced persistent threats (APTs) can assist stakeholders in determining their security posture by testing the effectiveness of response capabilities to a determined adversarial presence. RTAs are crafted specifically to test the people, processes, and technologies defending a network.

ASSESSMENT PHASES

Threat Simulation: CISA Assessments simulate APT tactics, techniques, and procedures using publicly available tools and data to access, navigate, and persist in a stakeholder's environment.

Measureable Events: Once entrenched in the network, a series of events are initiated, specifically intended to provoke a security response. Measured effectiveness of the people, processes, and technologies defending a stakeholder's network is determined by observable response-driven metrics.

ASSESSMENT OBJECTIVES

- Evaluate people, processes, and technologies responsible for defending the stakeholder's network.
- Provide stakeholder executives actionable insight to their cybersecurity posture and practical training for technical personnel.

ASSESMENT TIMELINE

Pre-Planning

- Request assessment
- Receive RTA brief
- Sign and return documents

Planning

- Confirm schedule
- Define scope
- Establish trusted points of contact

Execution (90 Days)

- Open-source intelligence
- Simulate APT
- Security response testing through activation of measurable Events

Post-Execution

- On-site out-brief and training

ABOUT

Our Team

The CISA Assessments team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities.

Additional Information

CISA assessments' security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.

GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at **NCATS_INFO@hq.dhs.gov** to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.

MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

CRITICAL PRODUCT EVALUATION

The CISA Assessments team supports Federal, State, Local, Tribal and Territorial Governments and Critical Infrastructure partners by providing proactive testing and assessment services.

CISA Assessments' Critical Product Evaluation (CPE) is a multi-week, comprehensive evaluation of a vendor's solution or appliance that ubiquitously supports critical infrastructure operations or other national endeavors to improve the "out of the box" and recommended security implementation of the product, ultimately improving our national resiliency.

ASSESSMENT OBJECTIVES

- Enumerate the vulnerabilities associated with the product's in-scope software, firmware, hardware
- Attempt exploitation of vulnerabilities that present the greatest risk using known exploits, or, if practical, develop new code or technique
- Capture indicators-of-compromise information to help incident responders determine the existence or extent of an incident
- Capture assessment methods
- Assist in developing remediation or mitigation strategies.

ASSESSMENT PHASES AND TIMELINE

Pre-Planning

- Request assessment
- Receive CPE brief
- Sign and return documents

Planning

- Define scope and confirm schedule
- Coordinate delivery of the system(s)-under-test (SUT)

Execution (Tailored*)

- Check-in and Configuration: setup and configure for normal operation
- Enumeration: list software and hardware interfaces
- Deconstructive Testing: mapping the attack surface and developing threat scenarios
- Target Analysis: execute attack vector testing and attempt exploitation

Post-Execution

- Coordinate SUT return**
- Report generation
- Out-brief with evaluation team

* Length of time for a CPE is based on the complexity of the SUT. Generally, eight-weeks is the starting point, however, this time can be amended during the scoping meetings or during the course of the evaluation.

** Equipment may become damaged during the course of testing.

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

ABOUT CISA ASSESSMENTS

Our Team

The CISA Assessments team is a group of highly trained information security experts. Our mission is to measurably reduce cybersecurity risks to our Nation.

CISA leads the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

Our services provide:

- **A proactive, risk-based approach** to analyzing stakeholder systems
- **Expertise** in identification of vulnerabilities, risk evaluation, and prioritized mitigation guidance
- **Comprehensive services that empower stakeholders** to increase speed and effectiveness of their cyber response capabilities.

Additional Information

CISA assessments' security services are available at no cost. Stakeholders include Federal, State, Local, Tribal and Territorial governments, as well as Critical Infrastructure private sector companies. CISA does not share attributable information without written and agreed consent from the stakeholder. CISA uses anonymized data to develop non-attributed reports for trending and analysis purposes.

GET STARTED

Capabilities and service delivery timelines are available upon request. Service availability is limited. Contact us at **NCATS_INFO@hq.dhs.gov** to get started. Service delivery queues are prioritized on a continuous basis to ensure no stakeholder or sector receives a disproportionate amount of resources and that the data collected is a diverse representation of the nation.

MISSION AND VISION

Mission: *Providing cybersecurity assessments to facilitate the identification of risk for the purpose of protecting the Nation's cyber infrastructure.*

Vision: *To be the preeminent government leader providing comprehensive, innovative, and dynamic cybersecurity assessments for the purpose of facilitating and protecting the federal, state, private sector and critical infrastructure networks of the United States, reducing attack surfaces, eliminating threats, and fostering partnerships across the government landscape.*

Homeland Security

Hunt and Incident Response Team (HIRT)

THE NATIONAL CYBERSECURITY & COMMUNICATIONS INTEGRATION CENTER (NCCIC) OPERATES AT THE INTERSECTION OF THE PRIVATE SECTOR, CIVILIAN, LAW ENFORCEMENT, INTELLIGENCE, AND DEFENSE COMMUNITIES, APPLYING UNIQUE ANALYTIC PERSPECTIVES, ENSURING SHARED SITUATIONAL AWARENESS, AND ORCHESTRATING SYNCHRONIZED RESPONSE EFFORTS WHILE PROTECTING THE CONSTITUTIONAL AND PRIVACY RIGHTS OF AMERICANS IN BOTH THE CYBERSECURITY AND COMMUNICATIONS DOMAINS.

The NCCIC HIRT provides expert intrusion analysis and mitigation guidance to clients who lack in-house capability or require additional assistance with responding to a cyber incident. HIRT supports federal departments and agencies, state and local governments, the private sector (industry and critical infrastructure asset owners and operators), academia, and international organizations.

NCCIC HIRT performs both on-site and remote cybersecurity incident response. A typical engagement includes log, network traffic, and host analysis. The goal is to discover malicious actors, acquire, and analyze the malicious tools, and provide mitigation guidance.

NCCIC HIRT is uniquely positioned with knowledge of both unclassified and classified actor tactics, techniques, and procedures compiled from public and private sector partners. HIRT works closely with law enforcement, the intelligence community, and international partners to provide a coordinated and comprehensive response. The NCCIC HIRT provides on-site support for numerous large-scale engagements each year, covering a wide variety of organizations.

HUNT

The goal of a hunt is to use tools and techniques to proactively check for and mitigate against malicious actor activity. More specifically, it will be charged to search for exploitation tools, tactics, procedures and their associated artifacts. Performed from within the customer environment on internal networks and hosts, it will encompass any systems that were identified by a Risk Review. Hunts are scoped to those systems that are part of a risk vetting process. The initial hunt will be targeted and precise, but results of an initial analysis may warrant the expansion of its scope to include additional systems, segments or environments. Ultimately, the analysis will further measure potential risks to the integrity, confidentiality, and availability of systems that need immediate attention. If evidence of a potential compromise is recognized, the Incident Response Team (IRT) will review agency materials and conduct interviews with technical staff, management, and senior leadership to further understand possible security gaps, thus allowing for more effective mitigation. As part of this mitigation response, a document incorporating actionable guidance will be provided.

INCIDENT RESPONSE

If evidence of a potential compromise is recognized, the Incident Response Team (IRT) will review agency materials and conduct interviews with technical staff, management, and senior leadership to further understand possible security gaps, thus allowing for more effective mitigation. As part of this mitigation response, a document incorporating actionable guidance will be provided.

TOOLS, TECHNIQUES, AND ARTIFACTS

A hunt and incident response will utilize tools, techniques, and artifacts to determine where a system has been compromised. They are listed as follows:

- Existing documentation to include policies, procedures and processes
- System owner interviews
- Existing customer documentation
- Host-based analysis
- Review of existing customer logs
- Network traffic analysis
- Network infrastructure analysis
- Data mappings and other diagrams

ADVANTAGES

- HIRT improves in-house lab capabilities and onsite processes
- HIRT utilizes defined, repeatable processes
- HIRT leverages total HIRT, US-CERT, ICS-CERT, and NCCIC capabilities to assist the client
- HIRT is able to create customized mitigation plan for the client

SERVICE OFFERINGS

The HIRT works onsite and remotely to provide services to eligible clients. All of the following are offered on a voluntary basis:

Incident Triage: Process taken to scope the severity of an incident and determine required resources for action

Network Topology Review: Assessment of network ingress, egress, remote access, segmentation, and interconnectivity, with resulting recommendations for security enhancements

Infrastructure Configuration Review: Analysis of core devices on the network which are or can be used for network security (e.g., prevention, monitoring, or enforcement functions)

Log Analysis: Examination of logs from network and security devices to illuminate possible malicious activity

Incident Specific Risk Overview: Materials and in-person briefings for technical, program manager, or senior leadership audience; cover current cyber risk landscape, including classified briefings to cleared staff when appropriate

Hunt Analysis: Deployment of network hunting tools to proactively detect indicators of compromise (IOC)

Security Program Review: A review of the client's existing security roles, responsibilities, and policies to identify possible organizational or information-sharing gaps

Malware Analysis: Reverse engineering of malware artifacts to determine functionality and build indicators

Mitigation: Actionable guidance to improve the organization's security posture, including incident-specific recommendations, security best practices, and recommended tactical measures

Digital Media Analysis: Technical forensic examination of digital artifacts to detect malicious activity and develop further indicators

Control Systems Incident Analysis: Analysis of supervisory control and data acquisition devices, process control, distributed control, and any other systems that control, monitor, and manage critical infrastructure

SEND REPORTS TO NCCIC

HIRT encourages reports of cybersecurity incidents, possible malicious code, vulnerabilities, and phishing attacks. Submit a report via phone: 1-888-282-0870 or email: *NCCICCustomerService@hq.dhs.gov*.

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

CYBERSECURITY ASSESSMENTS SUMMARY

Name	Validated Architecture Design Review (VADR)	Phishing Campaign Assessment (PCA)	Vulnerability Scanning (Formally Cyber Hygiene)	Remote Penetration Test (RPT)	Network Risk and Vulnerability Assessment (RVA)
Purpose	Provide analysis and representation of asset owner's network traffic, data flows, and device relationships and identifies anomalous communications flows.	Measure the susceptibility of an organization's personnel to social engineering attacks, specifically email phishing attacks.	Identify public-facing Internet security risks, through service enumeration and vulnerability scanning	Perform external penetration testing and security services to identify risks and externally exploitable pathways into systems, networks and applications.	Perform penetration testing and security services to identify risks and vulnerabilities within IT systems, networks and applications
Scope	Industrial Control Systems / Network Architecture/ Network Traffic	Organization / Business Unit / Email Service	Public-Facing, Network-Based IT Service	Organization / Business Unit / Network-Based IT Service	Organization / Business Unit / Network-Based IT Service
Time to Execute	Variable (Hours to Days)	Approximately 6 Weeks	Continuous	Up to 6 weeks	Two weeks of testing
Information Sought	Network design, system configurations, log files, interdependencies, and its applications	Phishing "click rate" metrics compared to attack sophistication	Network service and vulnerability information	Network, Database, Application scope and/or access to be tested with various security tools	Network, Database, Application scope and/or access to be tested with various security tools
Preparation	Coordinated via Email. Planning calls	Formal rules of engagement and pre-planning	Signed agreement letter and IP address scope to be tested	Formal rules of engagement and extensive pre-planning	Formal rules of engagement and extensive pre-planning
Participants	Control system operators/ engineers, IT personnel, and OT personnel	IT/Security Manager, Network Administrators, end users	IT/Security Manager and Network Administrators	Management stakeholders, IT/Security Manager, Network Administrators & System Owners.	Management stakeholders, IT/Security Manager, Network Administrators, and System Owners.
Delivered By	Contact the Cybersecurity Advisor mailbox at cyberadvisor@hq.dhs.gov for more information or to request services				

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

CYBERSECURITY ADVISORS

THE CYBERSECURITY AND INFRASTRUCTURE AGENCY'S (CISA) CYBERSECURITY ADVISOR (CSA) PROGRAM OFFERS CYBERSECURITY ASSISTANCE ON A VOLUNTARY, NO-COST BASIS TO CRITICAL INFRASTRUCTURE ORGANIZATIONS, TO INCLUDE STATE, LOCAL, TRIBAL, AND TERRITORIAL (SLTT) GOVERNMENTS. THROUGH THE CSA PROGRAM, YOUR ORGANIZATION CAN PREPARE FOR AND PROTECT AGAINST CYBERSECURITY THREATS TO CRITICAL INFRASTRUCTURE.

GOALS

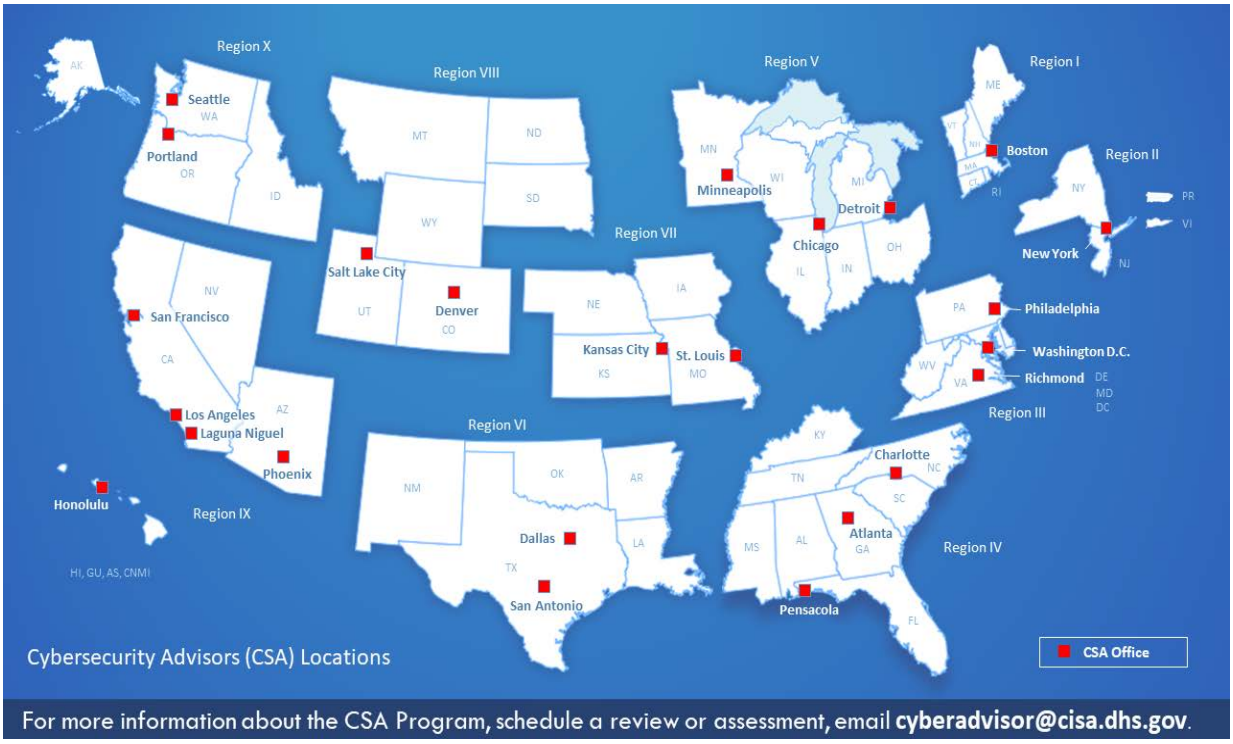
The goal of the CSA program is to promote cybersecurity preparedness, risk mitigation, and incident response capabilities of public and private sector owners and operators of critical infrastructure, as well as SLTT bodies, through stakeholder partnerships and direct assistance activities.

APPROACH

The CSA program maintains regional subject matter experts throughout DHS emergency management and protection regions. Regional CSAs cultivate partnerships with participating organizations and initiate information sharing. CSAs introduce organizations to various no-cost DHS cybersecurity products and services, along with other public and private resources, and act as liaisons to other DHS cyber programs and leadership. CSAs also collaborate with local and federal entities to facilitate delivery of cybersecurity services across the United States.

Service	What CSAs Offer	What Value Our Partners Receive
Cyber Preparedness	On-site preparedness and protective visits, work- shops, and engaging activities	Cybersecurity ideas, advice, and best practices and a formal exchange to raise awareness of DHS cybersecurity products, services, and information resources relative to critical infrastructure and partnerships
Strategic Messaging	DHS cybersecurity briefings, keynote addresses, and panel discussions	Improved cybersecurity awareness and collaboration potential, to convey timely and relevant information on DHS programs and operational activities
Working Group Support	Leadership at existing forums and working groups, engaging stakeholders with in-place cybersecurity initiatives and information sharing groups	Improved coordination with DHS on cybersecurity policy, procedures, and best practices; and an opportunity to exchange lessons-learned and identify areas of mutual interest
Partnership Development	Engagements to develop, build capacity in, and strengthen private-public cybersecurity partner- ships	Help initiating cybersecurity partnerships, establishing charter objectives and milestones, and maturing local and regional cybersecurity posture — in order to move partnerships from awareness building to operational capabilities

Cyber Assessments	Cyber Infrastructure Survey (CIS)	Assessment of more than 80 cybersecurity controls in five domains: cybersecurity management, cybersecurity forces, cybersecurity controls, cyber incident response, and cyber dependencies, resulting in an interactive decision support tool
	Cyber Resilience Review (CRR)	Assessment of cybersecurity management capabilities and maturity aspects of an organization's critical information technology (IT) services and associated assets — and in the context of the NIST Cybersecurity Frame- work (CSF)
	External Dependency Management (EDM)	Assessments of management activities and practices used to identify, analyze, and reduce risks arising from third parties
Incident Coordination and Support	Direct assistance and resourcing support, con- ducted in times of cyber threat, disruption, and attack	Facilitated cyber incident response and resource coordination, information de-confliction, and information request assistance



CYBER RESILIENCE REVIEW

THE PRESIDENTIAL POLICY DIRECTIVE (PPD) 41, UNITED STATES CYBER INCIDENT COORDINATION, SETS FORTH THE PRINCIPLES GOVERNING THE FEDERAL GOVERNMENT'S RESPONSE TO CYBER INCIDENTS AND ESTABLISHES LEAD AGENCIES AND PLANS FOR COORDINATING THE BROADER FEDERAL GOVERNMENT RESPONSE FOR THE AFFECTED ENTITIES, OR VICTIMS, OF SUCH INCIDENTS.

FORMAT AND GOAL

CISA offers two options for the CRR: a downloadable self-assessment and a facilitated six-hour session with trained DHS representatives at your locations.

Through the CRR, the organization will develop an understanding of its operational resilience and ability to manage cyber risk during normal operations and times of operational stress and crisis.

APPROACH

The CRR is derived from the CERT Resilience Management Model (CERT-RMM), a process improvement model developed by Carnegie Mellon University's Software Engineering Institute for managing operational resilience. The CRR is based on the premise that an organization deploys its assets (people, information, technology, and facilities) to support specific critical services or products. Based on this principle, the CRR evaluates the maturity of your organization's capacities and capabilities in performing, planning, managing, measuring and defining cybersecurity capabilities across 10 domains:

- Asset Management,
- Controls Management,
- Configuration and Change Management,
- Vulnerability Management,
- Incident Management,
- Service Continuity Management,
- Risk Management,
- External Dependencies Management,
- Training and Awareness, and
- Situational Awareness.

PARTICIPANTS

To conduct a CRR, CISA recommends that you involve a cross-functional team representing business, operations, security, information technology, and maintenance areas, including those responsible for the functions below:

- IT policy and governance (e.g., Chief Information Security Officer)
- IT security planning and management (e.g., Director of Information Technology)
- IT infrastructure (e.g., network/system administrator)

- IT operations (e.g., configuration/change managers)
- Business operations (e.g., operations manager)
- Business continuity and disaster recovery planning (e.g., BC/DR manager)
- Risk management (e.g., enterprise/operations risk manager)
- Procurement and vendor management (e.g., contracts and legal support managers)

BENEFITS AND OUTCOMES

The CRR provides a better understanding of an organization's cybersecurity posture. The review provides an improved organization-wide awareness of the need for effective cybersecurity management; a review of capabilities most important to ensuring the continuity of critical services during times of operational stress and crisis; a verification of management success; a catalyst for dialog between participants from different functional areas within your organization; and a comprehensive final report that maps the relative maturity of the organizational resilience processes in each of the 10 domains, and that includes improvement options for consideration, using recognized standards and best practices as well as references to the CERTRMM.

DATA PRIVACY

The CRR report is created exclusively for your organization's internal use. All data collected and analysis performed during a CRR assessment is afforded protection under the DHS Protected Critical Infrastructure Information (PCII) Program. PCII program protection means that DHS employees are trained in the safeguarding and handling of PCII, DHS cannot publicly disclose PCII, and PCII cannot be used for regulatory purposes. To learn more, please visit www.dhs.gov/pcii.

ASSOCIATION TO THE CYBERSECURITY FRAMEWORK

The principles and recommended practices within the CRR align with the Cybersecurity Framework (CSF) developed by the National Institute of Standards and Technology (NIST). After performing a CRR, your organization can compare the results to the criteria of the NIST CSF to identify gaps and, where appropriate, recommended improvement efforts. A reference crosswalk mapping the relationship of the CRR goals and practices to the NIST CSF categories and subcategories is included in the CRR self-assessment kit. An organization's assessment of CRR practices and capabilities may or may not indicate that the organization is fully aligned to the NIST CSF.

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

CYBER INFRASTRUCTURE SURVEY

THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) OFFERS THE CYBER INFRASTRUCTURE SURVEY (CIS) ON A VOLUNTARY, NO-COST BASIS FOR CRITICAL INFRASTRUCTURE ORGANIZATIONS AND STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS. ADMINISTED BY REGIONALLY-LOCATION CYBERSECURITY ADVISORS, A CIS EVALUATES THE EFFECTIVENESS, RESILIENCE AND CYBERSECURITY PREPAREDNESS OF AN ORGANIZATION'S SECURITY CONTROLS.

FORMAT AND GOAL

A CIS is a facilitated, expert-led assessment with cybersecurity personnel from your organization (e.g., Chief Information Security Officer, ICS/SCADA Security Manager, IT Security Manager). This informal interview typically takes 2½ to 4 hours in length.
Its goal is to assess the foundational and essential cybersecurity practices of an organization's critical service to identify dependencies, capabilities and emerging effects of the current cybersecurity posture. After the survey, DHS will provide an interactive dashboard for scenario planning.

APPROACH

CIS focuses on a service-based-view versus a programmatic-view of cybersecurity. Critical services are assessed against more than 80 cybersecurity controls grouped under five top-level domains: cybersecurity management, cybersecurity forces, cybersecurity controls, cyber incident response, and cyber dependencies.
Following the assessment, DHS will provide a user friendly dashboard for reviewing and interacting with the survey findings. Your organization can use the dashboard to compare its results against its industry peers, review results in the context of specific cyber and physical threat scenarios, and dynamically adjust the importance of in-place practices to see the effects on overall cyber protection.

CYBERSECURITY FRAMEWORK

The cybersecurity controls surveyed within the CIS broadly align to the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF), but does not show an organization's adherence to the NIST CSF. The CIS computes a unique, service-specific cyber protective resilience index based on only a narrow set of cyber protection and resilience measures. The NIST CSF is a comprehensive framework and should be considered as a next step after leveraging the CIS results.

BENEFITS AND OUTCOMES

A CIS provides your organization with:

* An effective assessment of cybersecurity controls in-place for critical service;
* A user friendly, interactive dashboard to support cybersecurity planning and resource allocation; and
* Access to peer performance data, visually depicted on the dashboard.

DATA PRIVACY

The CIS dashboard is for your organization's exclusive use. All data collected and analysis performed during the CIS is afforded protection under the DHS Protected Critical Infrastructure Information (PCII) Program. PCII program protection means that DHS employees are trained in the safeguarding and handling of PCII, DHS cannot publicly disclose PCII, and PCII cannot be used for regulatory purposes. To learn more, please visit www.dhs.gov/pcii.

CIS Survey Question Domains

CIS Domains

Cybersecurity Forces
- Personnel
- Cybersecurity Training

Cybersecurity Controls
- Authentication and Authorization Controls
- Access Controls
- Cybersecurity Measures
- Information Protection
- User Training
- Defense Sophistication and Compensating Controls

Incident Response
- Incident Response Measures
- Alternate Site and Disaster Recovery

Cybersecurity Management
- Cybersecurity Leadership
- Cyber Service Architecture
- Change Management
- Lifecycle Tracking
- Assessment and Evaluation
- Cybersecurity Plan
- Cybersecurity Exercises
- Information Sharing

Dependencies
- Data at Rest
- Data in Motion
- Data in Process
- End Point Systems

EXTERNAL DEPENDENCIES MANAGEMENT ASSESSMENT

THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY (CISA) OFFERS THE EXTERNAL DEPENDENCIES MANAGEMENT (EDM) ASSESSMENT ON A VOLUNTARY, NO-COST BASIS FOR CRITICAL INFRASTRUCTURE ORGAIZATIONS AND STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS. ADMINISTERED BY REGIONALLY-LOCATED CYBERSECURITY ADVISORS, THE ASSESSMENT PROVIDES AN ORGANIZATION WITH A BETTER UNDERSTANDING OF HOW THEY MANAGE RISKS ARISING FROM DEPENDENCES ON THE INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) SUPPLY CHAIN.

FORMAT AND GOALS

The EDM Assessment is conducted as a four-hour session at a location of your choosing and facilitated by trained DHS representatives. Your organization can use the assessment by itself and as the first step in an improvement effort. You also may use it in conjunction with CISA's External Dependencies Management Method, which provides a rigorous, repeatable way to identify and manage specific suppliers or other external entities that your organization depends on to support its mission.

The goals of the assessment are to:

- Evaluate the activities and practices your organization uses to manage risks arising from external dependencies.
- Provide an objective review of your organization's capabilities in the assessed areas and recommendations offering a roadmap for improvement based on industry-leading practices.

APPROACH

Risks associated with the ICT supply chain have grown dramatically with expanded outsourcing of technology and infrastructure. Failures in managing these risks have resulted in incidents affecting millions of people.

The EDM Assessment focuses on the relationship between your organization's high-value services and assets (people, technology, facilities, and information) and evaluates how you manage risks incurred from using the ICT supply chain to support these high-value services. The ICT supply chain consists of outside parties that operate, provide, or support information and communications technology. Common examples include externally provided web and data hosting, telecommunications services, and data centers, as well as any service that depends on the secure use of ICT.

Through the EDM Assessment, your organization will evaluate:

- Relationship Formation – how your organization considers third-party risks, selects external entities, and forms relationships with them so that risk is managed from the start.
- Relationship Management and Governance – how your organization manages ongoing relationships with external entities to support and strengthen your critical services at a managed level of risk and costs.

- Service Protection and Sustainment – how your organization plans for, anticipates, and manages disruption or incidents related to external entities.

The EDM Assessment evolved from the DHS Cyber Resilience Review (CRR) and, like the CRR, is based on the CERT Resilience Management Model (CERT-RMM), a process improvement model developed by Carnegie Mellon University's Software Engineering Institute.

BENEFITS AND OUTCOMES

Through an EDM Assessment, your organization will gain a better understanding of your cybersecurity posture relating to external dependencies. The assessment provides:

- An opportunity for participants from different parts of you organization to discuss issues relating to vendors and reliance on external entities;
- Options for consideration that guide improvement efforts, using recognized standards and best practices drawn from such sources as the CERT-RMM, NIST standards, and the NIST Cybersecurity Framework; and
- A comprehensive report on your third-party risk management practices and capabilities.

DATA PRIVACY

The EDM Assessment report is created exclusively for your organization's internal use. All data collected and analysis performed during an EDM assessment is afforded protection under the CISA Protected Critical Infrastructure Information (PCII) Program. PCII program protection means that CISA employees are trained in the safeguarding and handling of PCII, CISA cannot publicly disclose PCII, and PCII cannot be used for regulatory purposes. To learn more, please visit www.dhs.gov/pcii.

PARTICIPANTS

To conduct an EDM assessment, CISA recommends that you involve a cross-functional team that includes those responsible for the functions shown in the following.

- IT security planning and management (e.g., Director of Information Technology)
- IT operations (e.g., configuration/change managers)
- Risk managers, in particular operations risk (e.g., enterprise/operations risk manager)
- Business continuity and disaster recovery planning (e.g., BC/DR manager)
- IT policy and governance (e.g., Chief Information Security Officer)
- Business management (e.g., operations manager)
- Procurement and vendor management (e.g., contracts and legal support managers)
- Legal

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

CYBER RESILIENCE WORKSHOP

THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY'S (CISA) CYBERSECURITY ADVISOR (CSA) PROGRAM OFFERS CYBER RESILIENCE WORKSHOPS ON A VOLUNTARY, NO-COST BASIS FOR CRITICAL INFRASTRUCTURE ORGANIZATIONS, TO INCLUDE STATE, LOCAL, TRIBAL, AND TERRITORIAL GOVERNMENTS. THROUGH THE WORKSHOP, YOUR ORGANIZATION WILL BE INTRODUCED TO CYBER RESILIENCE CONCEPTS AND WAYS TO IMPROVE MANAGEMENT OF CYBER RESILIENCE.

FORMAT

The Cyber Resilience Workshop is a four-hour collaborative session led by CISA representatives. Each workshop is tailored to the concerns and threats of a specific sector and provides an opportunity for professionals to learn together. Workshops are held on demand (based on availability) at locations convenient to participants.

GOAL

The goal of the workshop is to provide your organization with tangible, useful take-away information related to risk-based decision making and security planning for critical services.

APPROACH

Through the workshop, your organization will be introduced to cyber resilience concepts and capability-building activities in key performance areas such as cybersecurity, IT operations, and business continuity. The workshop will address both operational risk management and emergency/crisis management. Structured drills and scenarios will help your organization examine capability building in operational resilience practices, going well beyond discussions of IT security controls and countermeasures. Content and threat examples specific to your sector or industry will be emphasized.

PARTICIPANTS

CISA recommends that a cross-functional team from your organization's business and operations attend the workshop, including those responsible for the functions below:

- IT policy and governance (e.g., Chief Information Security Officer)
- IT security planning and management (e.g., Director of Information Technology)
- IT infrastructure (e.g., network/system administrator)
- IT operations (e.g., configuration/change managers)
- Business operations (e.g., operations manager)
- Business continuity and disaster recovery planning (e.g., BC/DR manager)
- Risk management (e.g., enterprise/operations risk manager)
- Procurement and vendor management (e.g., contracts and legal support managers)

BENEFITS AND OUTCOMES

The Cyber Resilience Workshop is designed to keep communities-of-interest informed on national cybersecurity, policies, initiatives, and federal capabilities, and to encourage working partnerships with these communities on matters of cybersecurity. The workshop will provide your organization with a greater awareness of:

- Federal initiatives affecting critical infrastructure protection and realistic practices for improving operational resilience;
- Gaps in cyber management practices and potential process improvements;
- Cybersecurity best practices and operational resilience concepts;
- Processes to maintain and repeatedly carry out protection and sustainment activities for critical assets and services;
- Ways to enhance cyber incident response and business continuity capabilities; and
- Federal coordination for incident notification, containment, and recovery.

FOR INFORMATION AND SCHEDULING

The Cyber Resilience Workshop is facilitated by regional personnel of the Cybersecurity Advisor (CSA) Program. Email cyberadvisor@hq.dhs.gov for more information on the Cyber Resilience Workshop and on the schedules and locations of upcoming sessions.

CISA
CYBER+INFRASTRUCTURE

DEFEND TODAY. SECURE TOMORROW.

CYBERSECURITY ASSESSMENTS SUMMARY

Name	Cyber Resilience Review (CRR)	External Dependency Management (EDM)	Cyber Infrastructure Survey (CIS)	Onsite Cyber Security Evaluation Tool (CSET)
Purpose and Value Proposition	Identifies and evaluates cyber security management capabilities, maturity, and capacity to manage cyber risk during normal operations and times of operational stress.	Assesses the activities and practices utilized by an organization to manage risks arising from external dependencies.	Identifies cybersecurity controls and protective measures in place and provides an interactive dashboard for comparative analysis and valuation.	Provides a detailed, effective, and repeatable tool for assessing systems security against established industry standards and guidance
Scope	Critical Service view	Critical Service view	Critical Service view	Information Technology and Operational Technology systems
Time to Execute/	5 to 6 Hours	3 – 4 Hours	2 ½ to 4 Hours	Varies greatly (min 2 Hours) (self-assessment)
Information Sought	Capabilities and maturity indicators in 10 security domains	Capabilities and maturity indicators across third party relationship management lifecycle domains	Protective measures in-place	Architecture diagrams, infrastructure, policies, and procedures documents
Preparation	Planning call to scope evaluation	Planning call to scope evaluation	Planning call to scope evaluation	Self-assessment available from web site and utilized locally
Participants	IT/Security Manager, Continuity Planner, and Incident Responders	IT/Security Manager, Continuity Planner, with Contract Management	IT/Security Manager	Operators, engineers, IT staff, policy/ management personnel, and subject matter experts
All Assessments Delivered By	Contact the Cybersecurity Advisor mailbox at cyberadvisor@hq.dhs.gov for more information or to request services			