SERVICES FOR BUILDING RESILIENCE

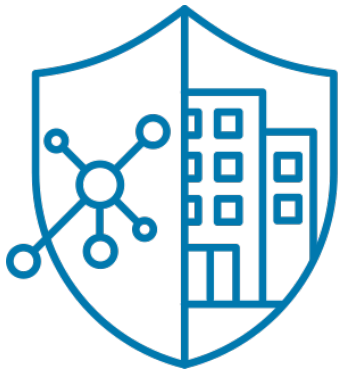
Kyle Wolf & Colin Glover
Cybersecurity and Infrastructure Security Agency

3/29/2022

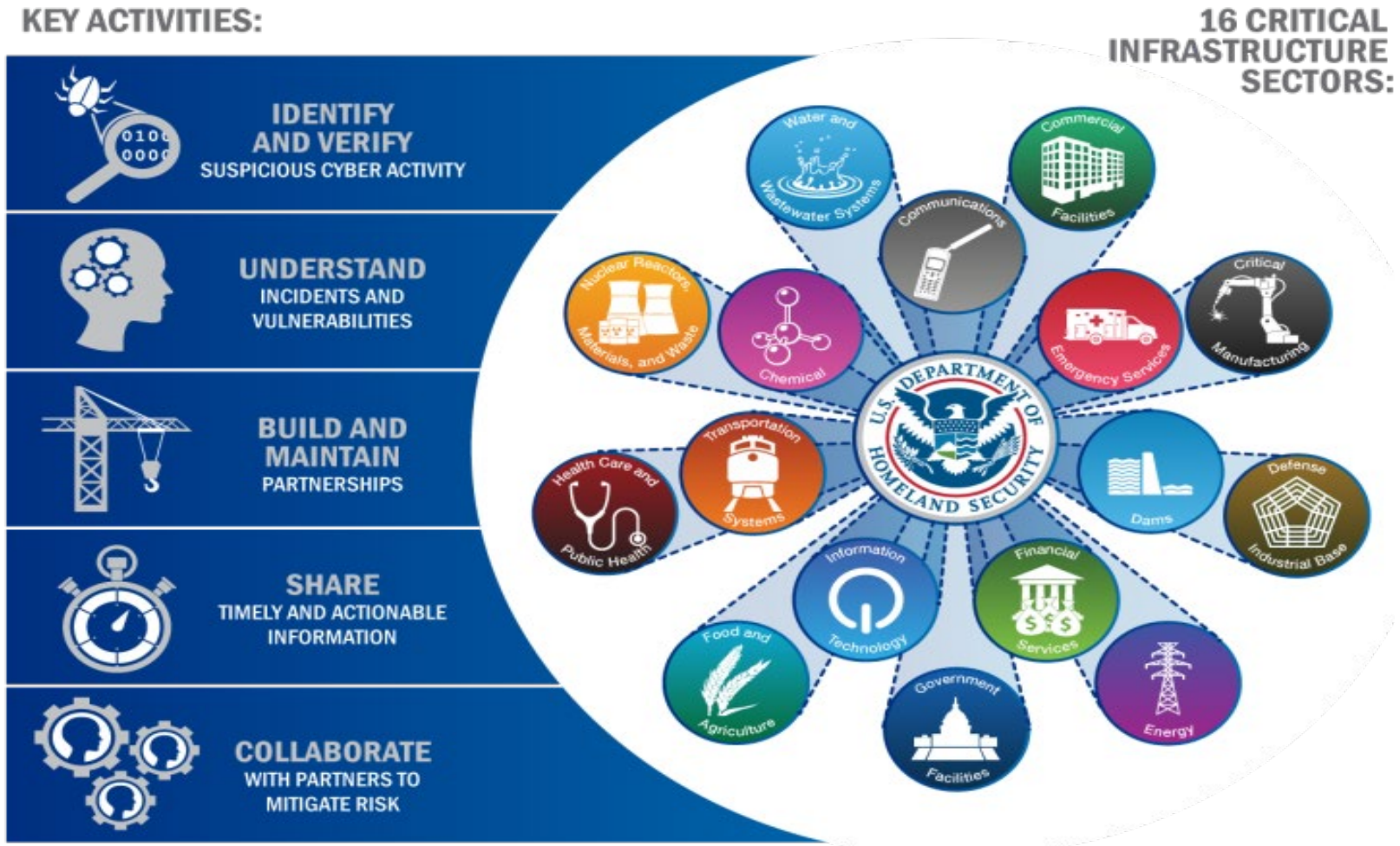
WHO WE ARE

CISA Mission and Vision

- Cybersecurity and Infrastructure Security Agency (CISA) mission:
  - Lead the collaborative national effort to strengthen the security and resilience of America's critical infrastructure
- CISA vision:
  - A Nation with secure, resilient, and reliable critical infrastructure upon which the American way of life can thrive



Serving Critical Infrastructure

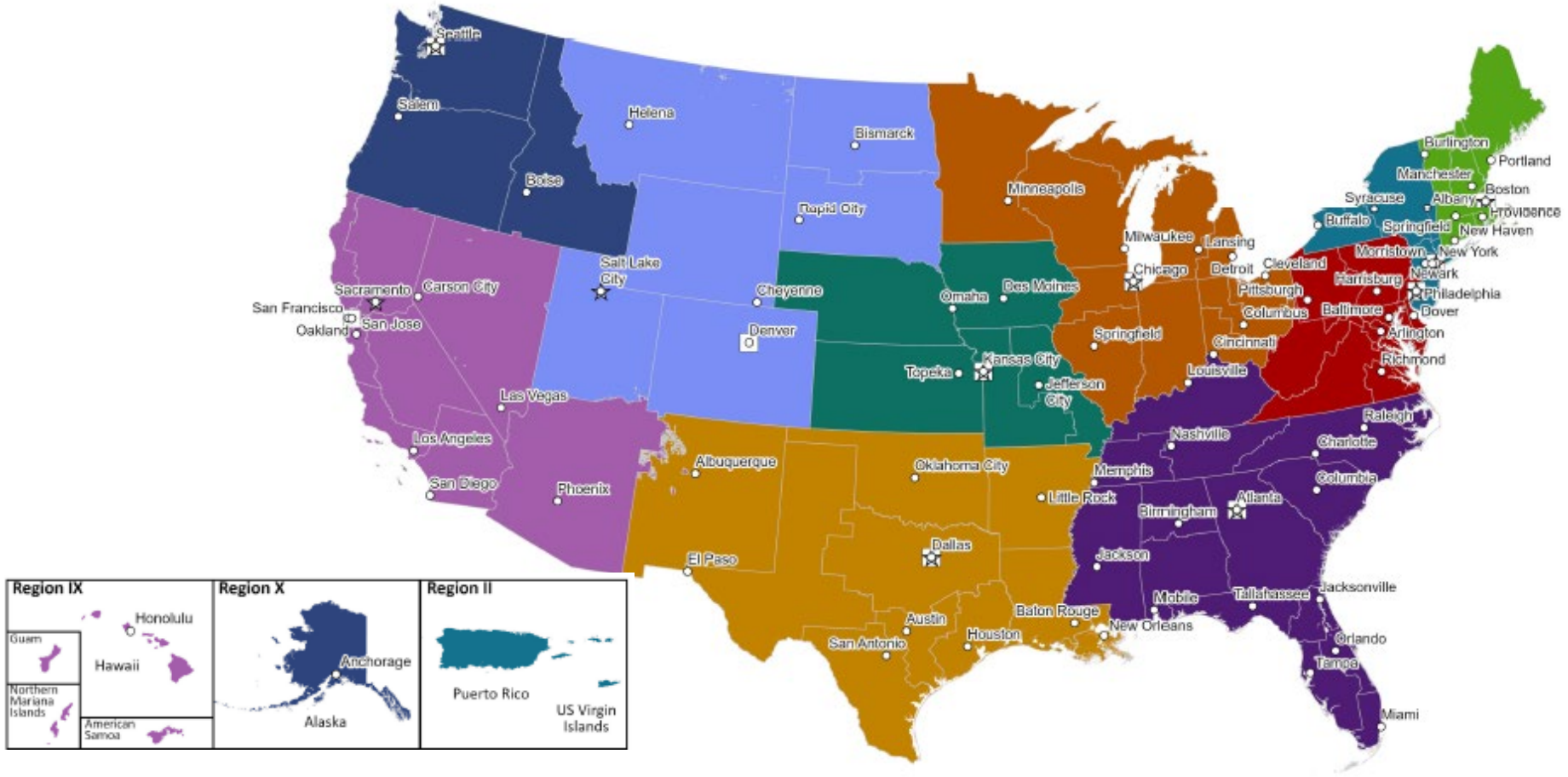


PROTECTIVE SECURITY ADVISOR

2022

Presenter's Name
April 7, 2022

PSA Locations



Kentucky PSA

- PSAs are field-deployed personnel who serve as critical infrastructure security specialists
- State, local, tribal, and territorial (SLTT) and private sector link to DHS infrastructure protection resources

PSA Mission Areas

OUTREACH ACTIVITIES

PSAs conduct outreach activities with critical infrastructure owners and operators, community groups, and faith-based organizations in support of CISA priorities.

SURVEYS AND ASSESSMENTS

PSAs conduct voluntary, non-regulatory security surveys and assessments on critical infrastructure assets and facilities within their respective regions.

SPECIAL EVENT SUPPORT

PSAs support Federal, State, and local officials responsible for planning, leading, and coordinating NSSE and SEAR events.

INCIDENT RESPONSE

PSAs plan for and, when directed, deploy in response to natural or man-made incidents.

BOMBING PREVENTION AND AWARENESS

PSAs work in conjunction with CISA's Office for Bombing Prevention by coordinating training and materials for partners to assist in deterring, detecting, preventing, protecting against, and responding to improvised explosive device threats.

Assist Visits (Outreach)

- Establish and enhance CISA's relationship with critical infrastructure owners and operators; inform them of the importance of their facilities, and reinforce the need for continued vigilance
- During an Assist Visit, PSAs focus on coordination, outreach, training, and education
- Assist Visits are often followed by security or delivery of other CISA services

Surveys and Assessments

- Physical security/resilience surveys identify infrastructure vulnerabilities and trends across sectors
- Facilitates the consistent collection of security information

- Physical Security
- Security Force
- Security Management
- Information Sharing
- Protective Measures
- Dependencies

IST Deliverables

Table 2 Facility and SAA Vulnerabilities and Options for Consideration

	Category	Vulnerability	Option(s) for Consideration
	Security Management Profile	The facility's security plan is missing key elements.	Update the security plan to include the following: • Illumination[3] • Security force staffing[4] • Security force training[5] • Access control procedures for contractors • A security awareness training program that addresses internal disturbances (e.g., workplace violence) – Develop a protocol to respond to workplace violence. Refer to the Federal Bureau of Investigation (FBI) Website for resources, such as the January 2011 *FBI Law Enforcement Bulletin: Workplace Violence Prevention*, available at http://www.fbi.gov/stats-services/publications/law-enforcement-bulletin/january2011/january_2011. – Include policies and procedures to respond to workplace violence threats and incidents in the security plan. – Provide training on workplace violence to all personnel at initial hire and annually thereafter. • A security awareness training program that addresses security communications policy or procedures • A security awareness training program that addresses information protection/operation security • A security awareness training program that addresses hostage situations • Liaison with response agencies • Exercising the plan • Plan maintenance (e.g., review and revision)
	Security Management Profile	Background checks are not conducted on contractors.	• Require contracting companies to conduct background checks on their personnel who will work at the facility and to make such records available for audit.[6]

IST Dashboards

SAFE Tool

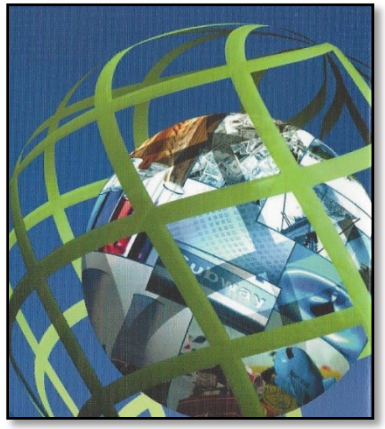
- The Security Assessment at First Entry (SAFE) tool is designed to assess the current security posture and identify options for facility owners and operators to mitigate relevant threats
- The SAFE tool is suited for all facilities, including smaller ones such as rural county fairgrounds, houses of worship with only weekend services and few members, and small health clinics

Infrastructure Visualization Platform

- Infrastructure Visualization Platform (IVP) is a data collection and presentation medium
  - Supports critical infrastructure security, special event planning, and response operations
  - Integrates assessment data with immersive video and geospatial and hypermedia data

Protected Critical Infrastructure Information Program

- The Protected Critical Infrastructure Information (PCII) Program protects critical infrastructure information voluntarily shared with the federal government for homeland security purposes
- PCII protects from release through:
  - Freedom of Information Act disclosure requests
  - State, local, tribal, territorial disclosure laws
  - Use in civil litigation
  - Use for regulatory purposes



Counter-IED Risk Mitigation Training

CISA's Office for Bombing Prevention delivers a diverse curriculum of accredited training to build nationwide C-IED awareness and capabilities among stakeholders.

OBP is accredited by the International Association for Continuing Education and Training (IACET) to issue the IACET Continuing Education Unit (CEU).

Diverse Curriculum

Diverse curriculum of training designed to build counter-IED core capabilities, such as

- IED Awareness
- VBIED Detection
- Bomb Threats
- Surveillance Detection
- Protective Measures
- Suspicious Items/Activity

Participants

- State and local law enforcement
- Federal agencies
- First responders and First Receivers
- Private sector partners

Access Training

- In-Person Instructor Led Training – 9 courses
- Virtual Instructor-Led Training – 6 courses
- Web-Based Training – 5 courses

Access courses at www.cisa.gov/bombing-prevention-training-courses

Active Shooter Preparedness

CYBERSECURITY ADVISOR PROGRAM

Cybersecurity Advisor Program

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

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

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

CISA Central

CISA Central works to reduce the risk of systemic cybersecurity and communications challenges in our role as the Nation's flagship cyber defense, incident response, and operational integration center.

Core efforts include:

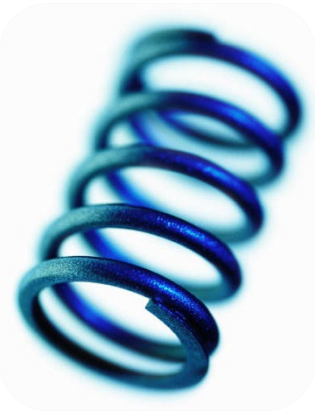
- Information exchange
- Training and exercises
- Risk and vulnerability assessments
- Data synthesis and analysis
- Operational planning and coordination
- Watch operations
- Incident response and recovery

CYBERSECURITY AND RESILIENCE

Resilience Defined

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

- Presidential Policy Directive 21
February 12, 2013



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

Emergent Property of Operational Resilience

- The **emergent property** of infrastructure requires an entity to
  - Prevent disruptions from occurring and
  - Respond quickly and recover from disruptions in its most critical business processes.
- Emergent property of operational resilience is essential to critical infrastructure.

What Is An Emergent Property?

- Consider your health.
  - How do you become healthy?
  - Can you buy good health?
  - Can you “manufacture” good health?
- *Good health* and *resilience* are both emergent properties.
- They develop – or emerge – from what we do.

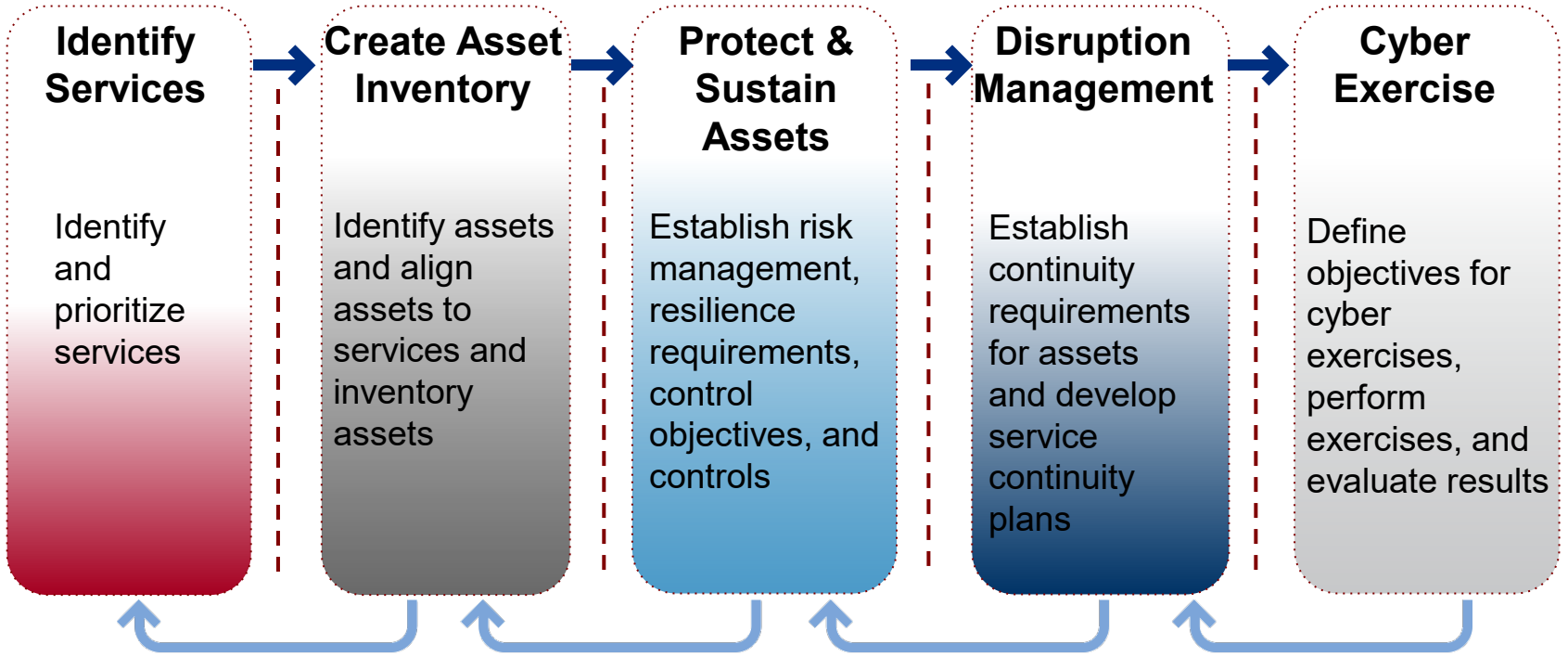
Operational Resilience in Practice

Operational resilience emerges from what we do, such as:

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

Working toward Cyber Resilience

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



CISA
CYBERSECURITY SERVICES

Cybersecurity Services for All

- Cybersecurity Advisors
- State, Local, Tribal, and Territorial engagements
- Cyber Resilience Reviews (CRR™)
- External Dependencies Management (EDM) Assessments
- Cyber Infrastructure Surveys
- Cyber Education and Awareness
- Federal Virtual Training Environment (Fed VTE)
- National Initiative for Cybersecurity Careers and Studies (NICCS)
- Stop. Think. Connect.™

CISA Central

CISA Central is CISA's hub for staying on top of threats and emerging risks to our nation's critical infrastructure, whether they're of cyber, communications or physical origin**:**

CYBER RESOURCE HUB

- RVA Mapped to the MITRE ATT&CK Framework Infographic
- Vulnerability Scanning
- Phishing Campaign Assessment
- Risk and Vulnerability Assessment
- Cyber Resilience Review (CRR)
- CRR Downloadable Resources
- External Dependencies Management Assessment (EDM)
- EDM Downloadable Resources
- Cyber Infrastructure Survey
- Remote Penetration Testing
- Web Application Scanning
- Cyber Security Evaluation Tool (CSET®)
- Validated Architecture Design Review (VADR)

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 Dependencies 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

ASSESSMENTS

Criticality of Periodic Assessments

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

Range of Cybersecurity Assessments

- 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)

Protected Critical Infrastructure Information Program

Protected Critical Infrastructure Information (PCII) Program Guards Your Information

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

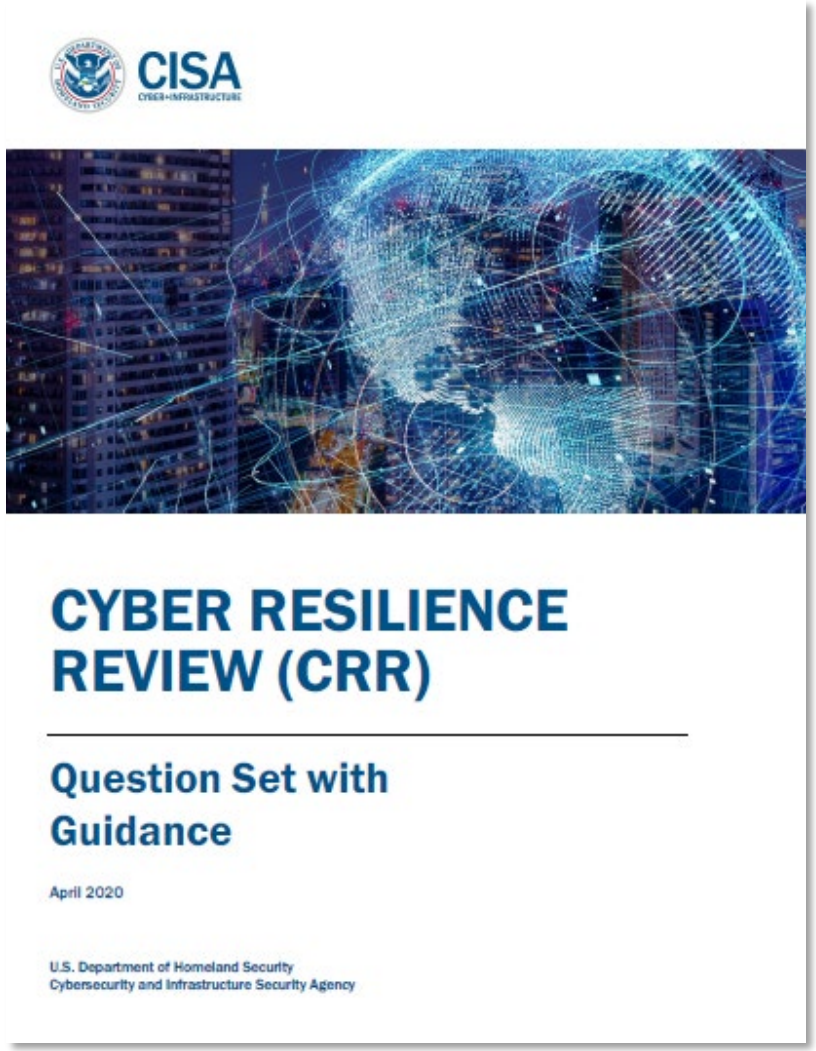
CYBER RESILIENCE REVIEW

Cyber Resilience Review

- **Purpose:** Evaluates that maturity of an organization's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity capabilities across the following 10 domains:

Asset Management	Service Continuity Management
Controls Management	Risk Management
Configuration and Change Management	External Dependency Management
Vulnerability Management	Training and Awareness
Incident Management	Situational Awareness

- Benefits include: Helps public and private sector partners understand and measure cybersecurity capabilities as they relate to operational resilience and cyber risk



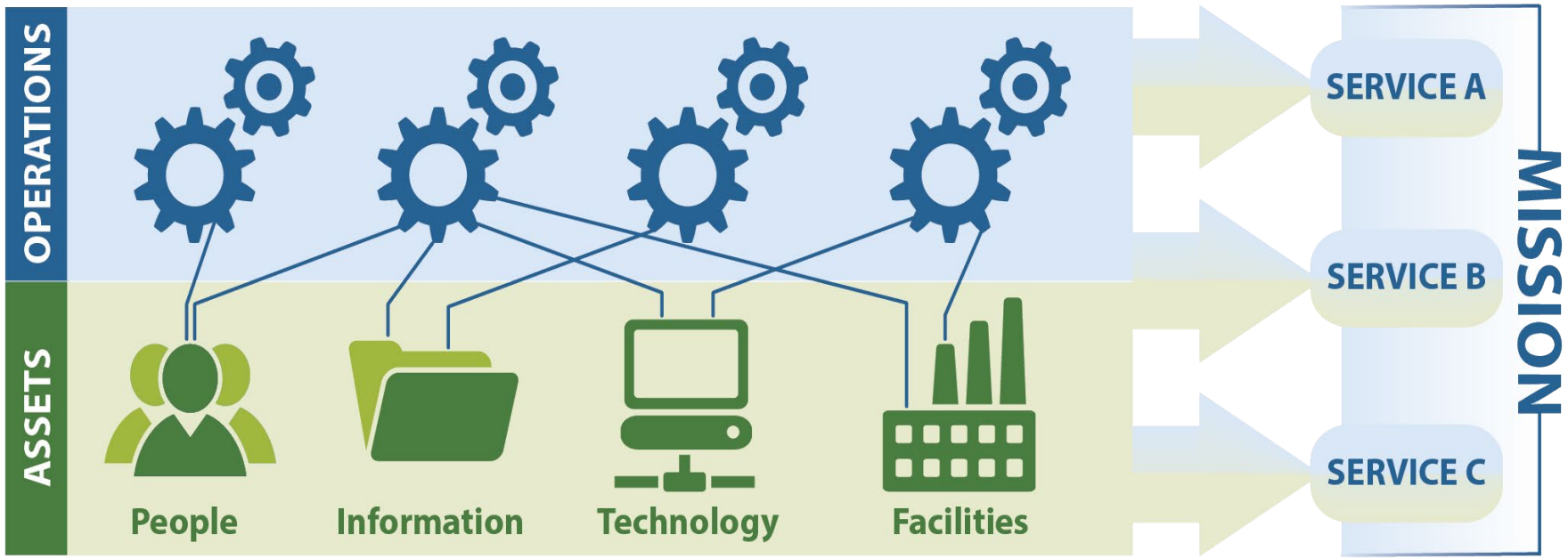
Cyber Resilience Review Domains

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: https://www.cisa.gov/cisa-cybersecurity-resources

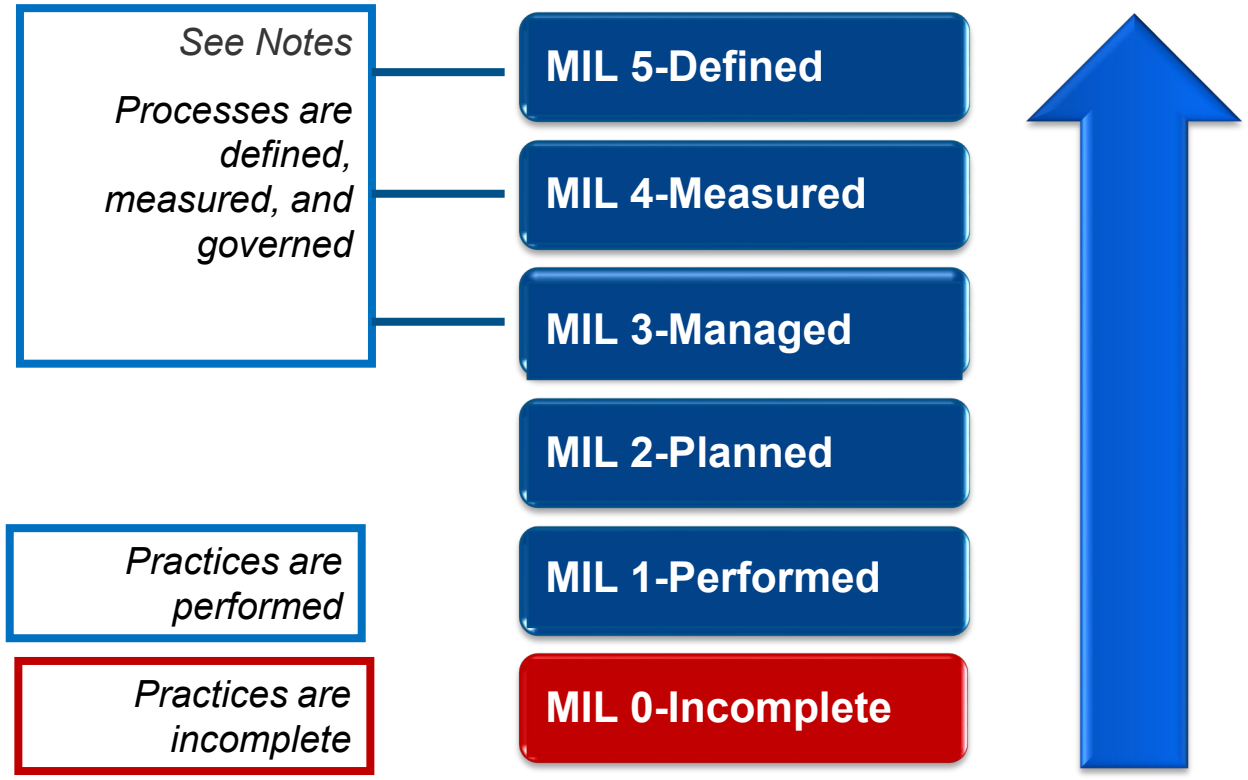
Critical Service Focus

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



Process Institutionalization

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



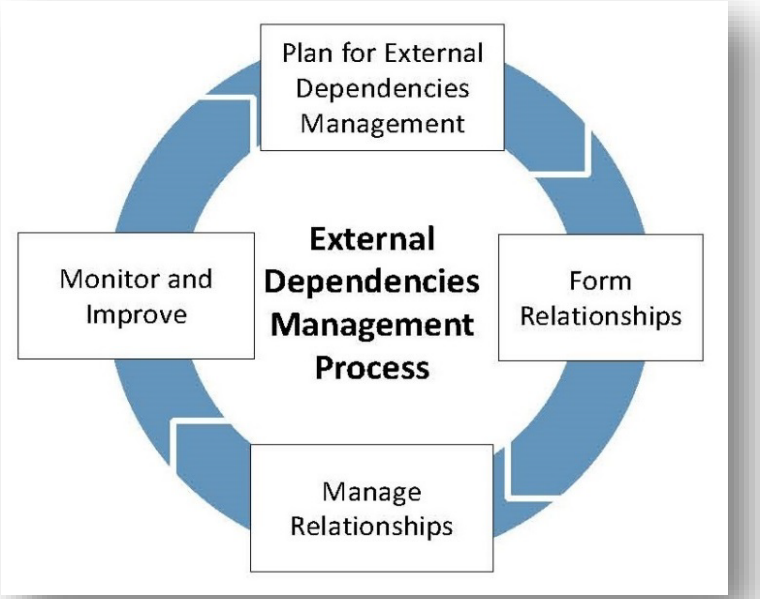
Higher MIL degrees translate to more stable processes that:

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

EXTERNAL DEPENDENCIES MANAGEMENT ASSESSMENTS

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

Note: graphic edits will need time to be recreated and adjusted.

EDM Assessment Organization and Structure

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

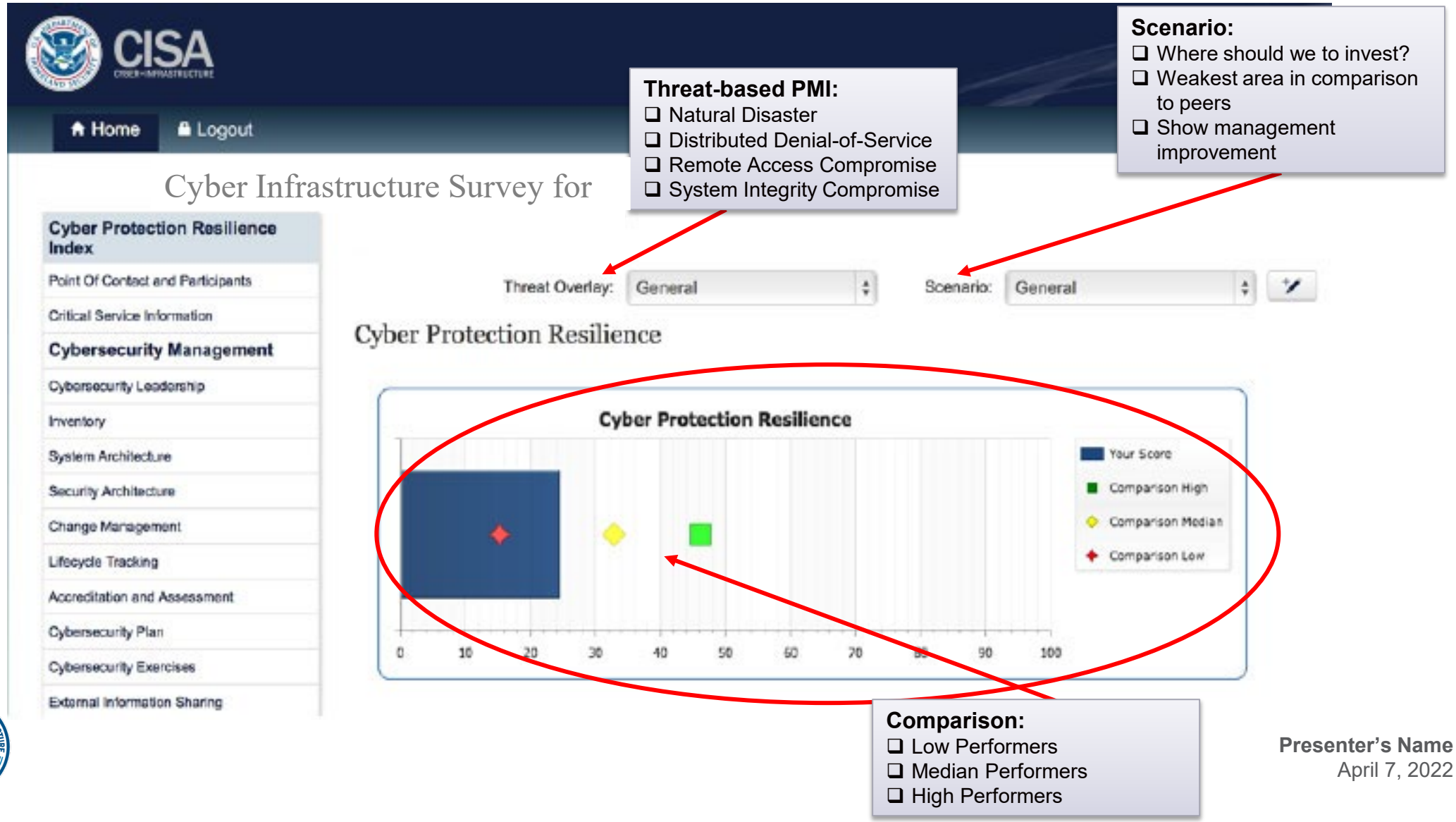
Relationship Formation *Assesses whether the acquirer evaluates and controls the risks of relying on external entities before entering into relationships with them.*
Relationship Management and Governance *Assesses whether the acquirer manages ongoing relationships to maintain the resilience of the critical 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

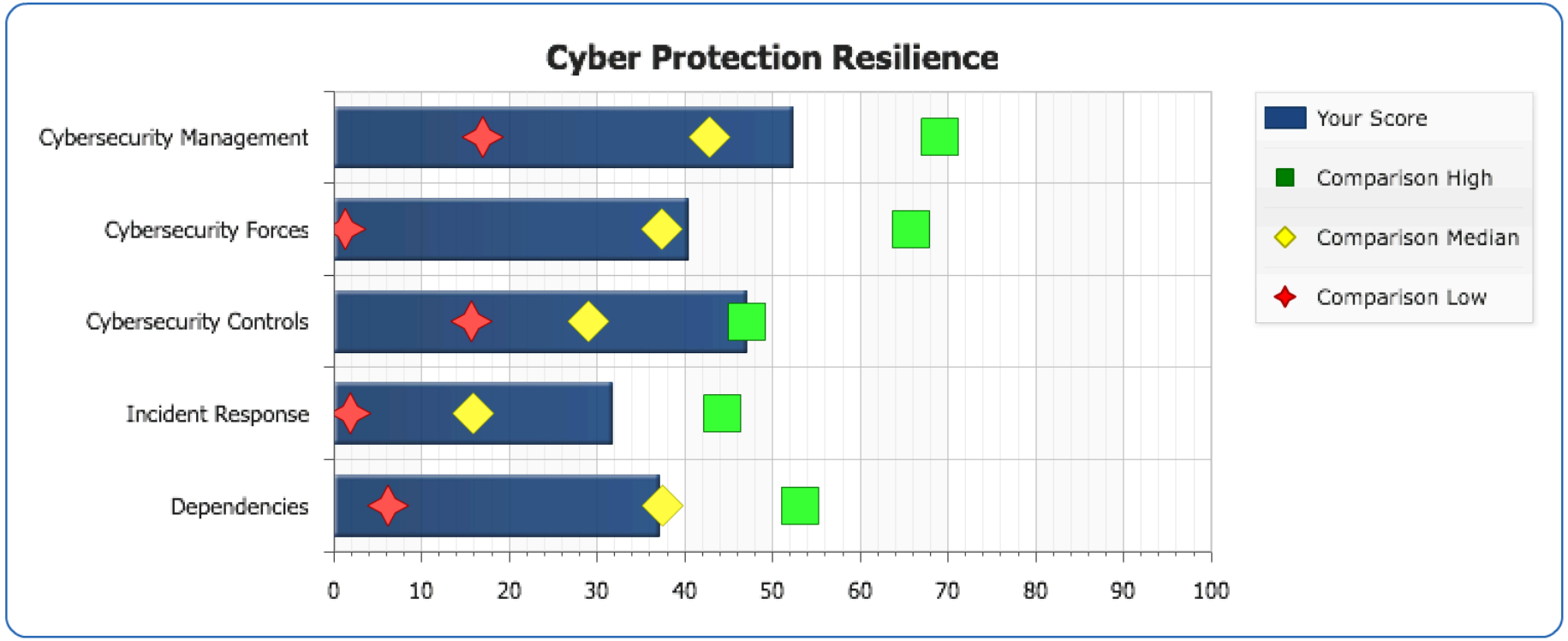
- Purpose: Evaluate security controls, cyber preparedness, overall resilience.
- Delivery: CSA-facilitated
- Benefits:
  - Effective assessment of cybersecurity controls in place for a critical service,
  - Easy-to-use interactive dashboard to support cybersecurity planning and resource allocation),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

Example of CIS Dashboard



CIS Dashboard - Comparison

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



CYBER SECURITY EVALUTION 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

PHISHING CAMPAIGN ASSESSMENT

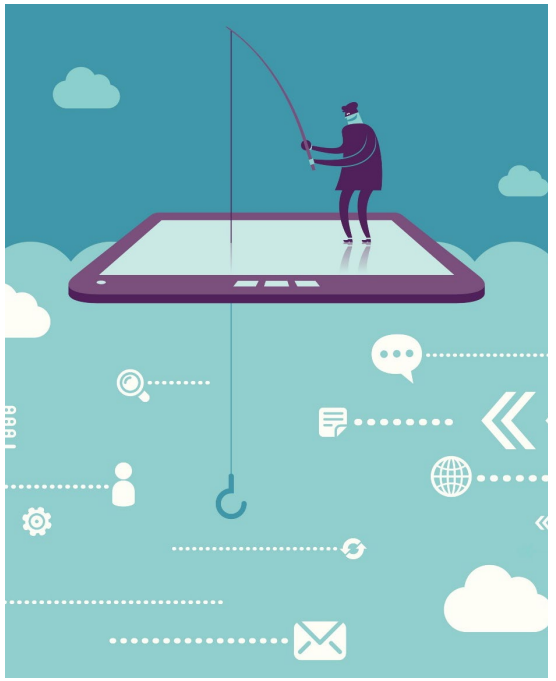
Phishing Campaign Assessment

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



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

CYBER HYGIENE: WEB APPLICATION SCANNING (WAS)

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

REMOTE PENETRATION TESTING

Remote Penetration Testing

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 the stakeholder email infrastructure through carefully crafted phishing emails containing a variety of malicious payloads to the trusted point of contact.
- **Open-Source Information Gathering:** Identify publicly available information about the stakeholder environment which may be useful in preparing for an attack.

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.

ASSESSMENT TIMELINE

Pre-Planning
- Request RPT
- Receive RPT Capabilities Brief
- Sign and return RPT Rules of Engagement
- Determine RPT services, scope, and logistics during pre-assessment call(s)

Planning
- Confirm schedule
- Establish trusted points of contact

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

VULNERABILITY SCANNING

Vulnerability Scanning

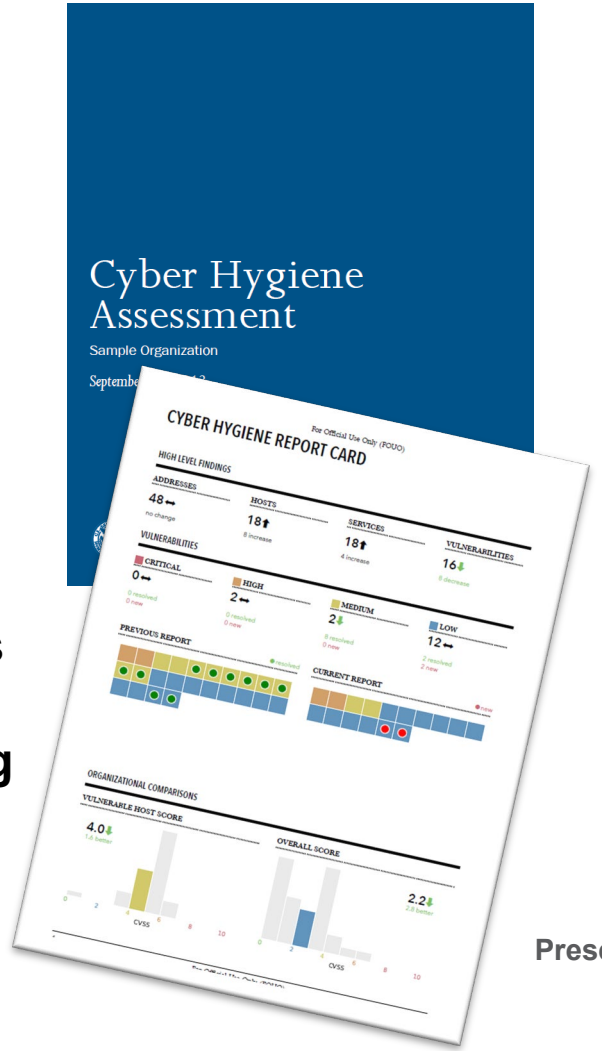
Purpose: Assess Internet-accessible systems for known vulnerabilities and configuration errors.

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



VALIDATED ARCHITECTURE DESIGN REVIEW

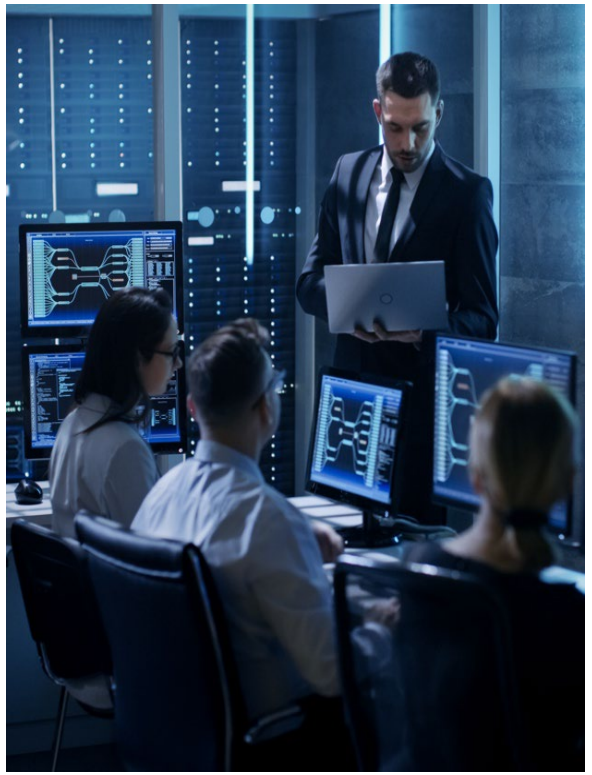
Validated Architecture Design Review

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

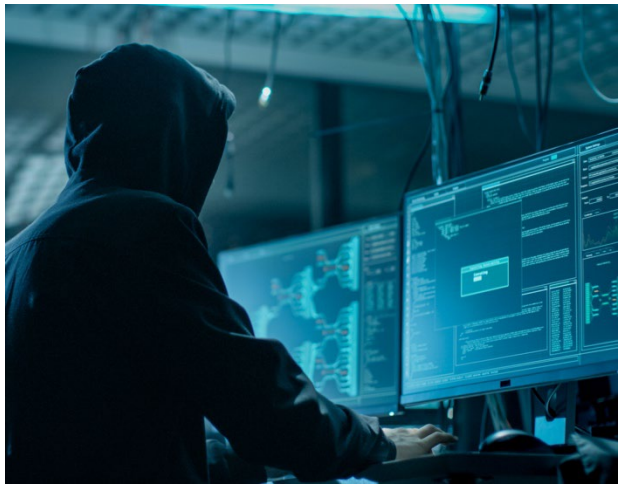


RISK AND VULNERABILITY ASSESSMENT

[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.



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

CISA Cyber Assessments in Brief, 1 of 2

Name	Cyber Resilience Review	Cyber Infrastructure Survey	External Dependencies Management Review	Cybersecurity Evaluation Tool Assessment
Purpose	Identify cybersecurity management capabilities and maturity	Calculate a comparative analysis and valuation of protective measures in-place	Assess the activities and practices utilized by an organization to manage risks arising from external dependencies	Provide detailed, effective, and repeatable methodology for assessing control systems security encompassing the organization's infrastructure, policies, and procedures
Scope	Critical service view	Critical service view	Critical service view	Information Technology and Operational Technology systems
Time to Execute	8 Hours (1 business day)	2 ½ to 4 Hours	2 ½ to 4 Hours	Varies greatly (min 2 Hours), unknown for self-assessment
Information Sought	Capabilities and maturity indicators in 10 security domains	Protective measures in-place	Capabilities and maturity indicators across third-party relationship management lifecycle domains	Architecture diagrams, infrastructure, policies, and procedures documents
Preparation	1-hour questionnaire and planning call(s)	Planning call to scope evaluation	Planning call to scope evaluation	Self-assessment available from web site and used locally
Participants	IT / Security Manager, Continuity Planner, and Incident Responders	IT / Security Manager	IT / Security Manager with Continuity Planner and Contract Management	Operators, engineers, IT staff, policy / management personnel, and subject matter experts
Delivered By	CSAs iodregionaloperations@cisa.dhs.gov	CSAs iodregionaloperations@cisa.dhs.gov	CSAs iodregionaloperations@cisa.dhs.gov	Self-administered / CSAs https://ics-cert.us-cert.gov/

CISA Cyber Assessments in Brief, 2 of 2

Name	Validated Architecture Design Review	Phishing Campaign Assessment	Risk and Vulnerability Assessment	Vulnerability Scanning
Purpose	Provide analysis and representation of asset owner's network traffic, data flows, and relationships between devices and identifies anomalous communications flows.	Measure the susceptibility of an organization's personnel to social engineering attacks, specifically email phishing attacks.	Perform penetration and deep technical analysis of enterprise IT systems and an organization's external resistance to specific IT risks	Identify public-facing Internet security risks, at a high-level, through service enumeration and vulnerability scanning
Scope	Industrial Control Systems / Network Architecture, Traffic	Organization / Business Unit / Email Exchange Service	Organization / Business Unit / Network-Based IT Service	Public-Facing, Network-Based IT Service
Time to Execute	Variable (Hours to Days)	Approximately 6 Weeks	Variable (Days to Weeks)	Variable (Hours to Continuous)
Information Sought	Network design, configurations, log files, interdependencies, data flows and its applications	Click rate metrics gathered during phishing assessment	Low-level options and recommendations for improving IT network and system security	High-level network service and vulnerability information
Preparation	Coordinated via Email. Planning call(s).	Formal rules of engagement and pre-planning	Formal rules of engagement and extensive pre-planning	Formal rules of engagement and extensive pre-planning
Participants	Control system operators/ engineers, IT personnel, and ICS network, architecture, and topologies SMEs	IT/Security Manager and Network Administrators, end users	IT/Security Manager and Network Administrators	IT/Security Manager and Network Administrators
Delivered By	VM VM@CISA.DHS.GOV	VM VM@CISA.DHS.GOV	VM VM@CISA.DHS.GOV	VM VM@CISA.DHS.GOV

INFORMATION SHARING

AUTOMATED INDICATOR SHARING

Automated Indicator Sharing

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

AIS Benefits: Forewarned Is Forearmed

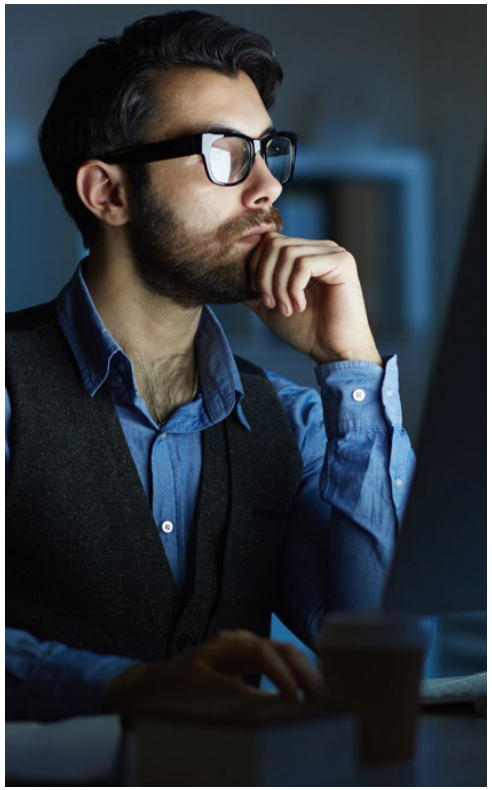
Why do I want these indicators?

- Receiving cyber threat indicators and defensive measures enables organizations to improve network defenses faster and forces adversaries to change their infrastructure, tactics, etc.

- If your organization cannot use AIS indicators directly (e.g., outsourced infrastructure), you should make sure your service provider is receiving and using.

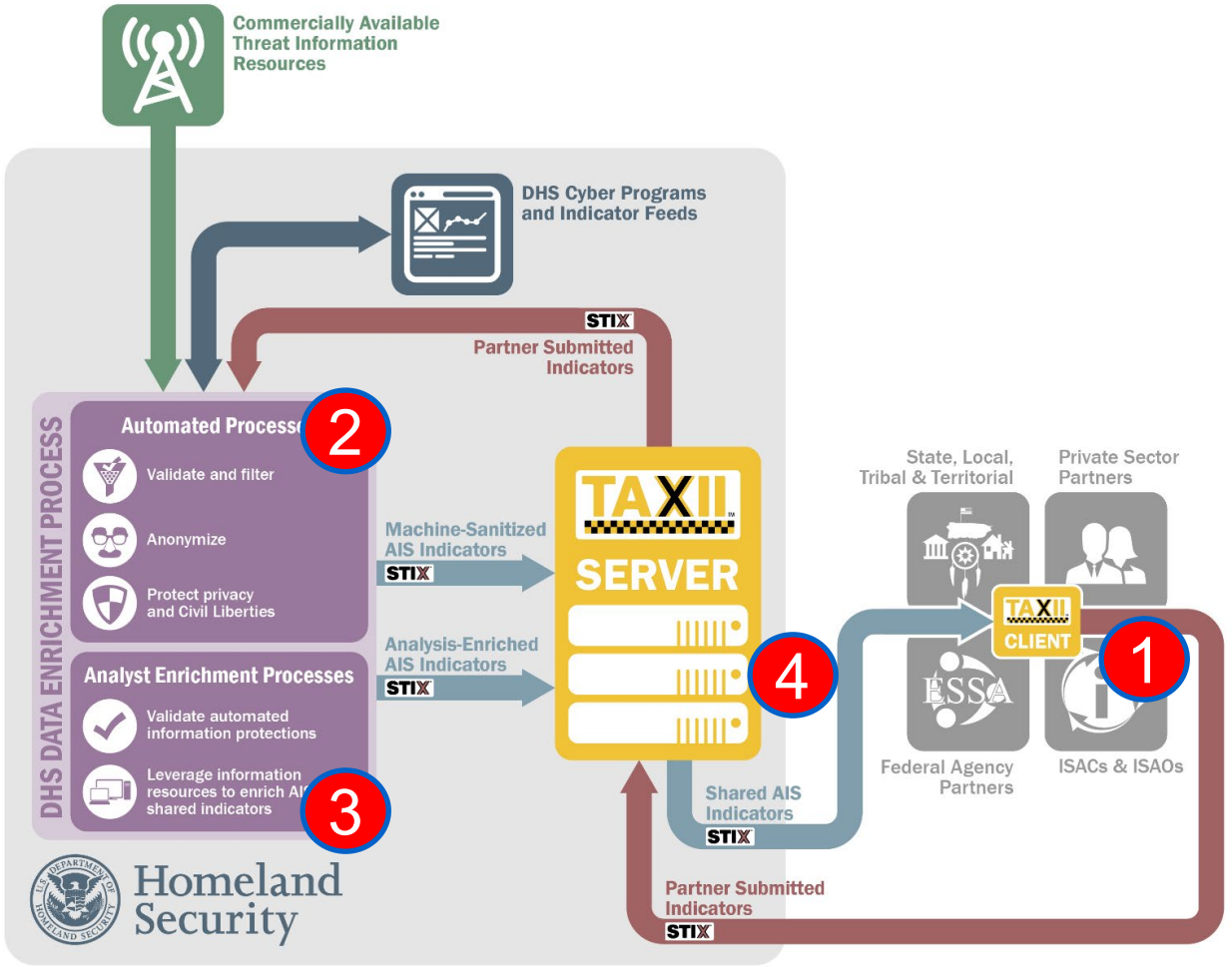
And why do I want to share indicators back?

- Your detection can become someone else's prevention and makes the entire community stronger.



How AIS Works

1. Entities format cyber threat indicators in STIX and submit via TAXII to DHS server.
2. Server code reviews submission to validate, anonymize (if requested), conduct automated privacy review and enrich.
3. Indicators requiring review go to DHS analysts.
4. Finally, indicators are published back out to everyone connected to the DHS server.



CISA's Approach to AIS and Privacy

Goal:

- Remove ***any*** personal information **not required** to understand the cyber threat.

Process:

- Automated technical and manual reviews/mitigations will ensure information is sanitized.
- Auditing is an important step to ensure the guidance regarding minimizing/redaction and tagging is appropriately being implemented.

Liability Protection for AIS Participants

By law, organizations receive liability protection when sharing threat indicators:

SEC. 106. PROTECTION FROM LIABILITY.
(a) MONITORING OF INFORMATION SYSTEMS.—No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the monitoring of an information system and information…

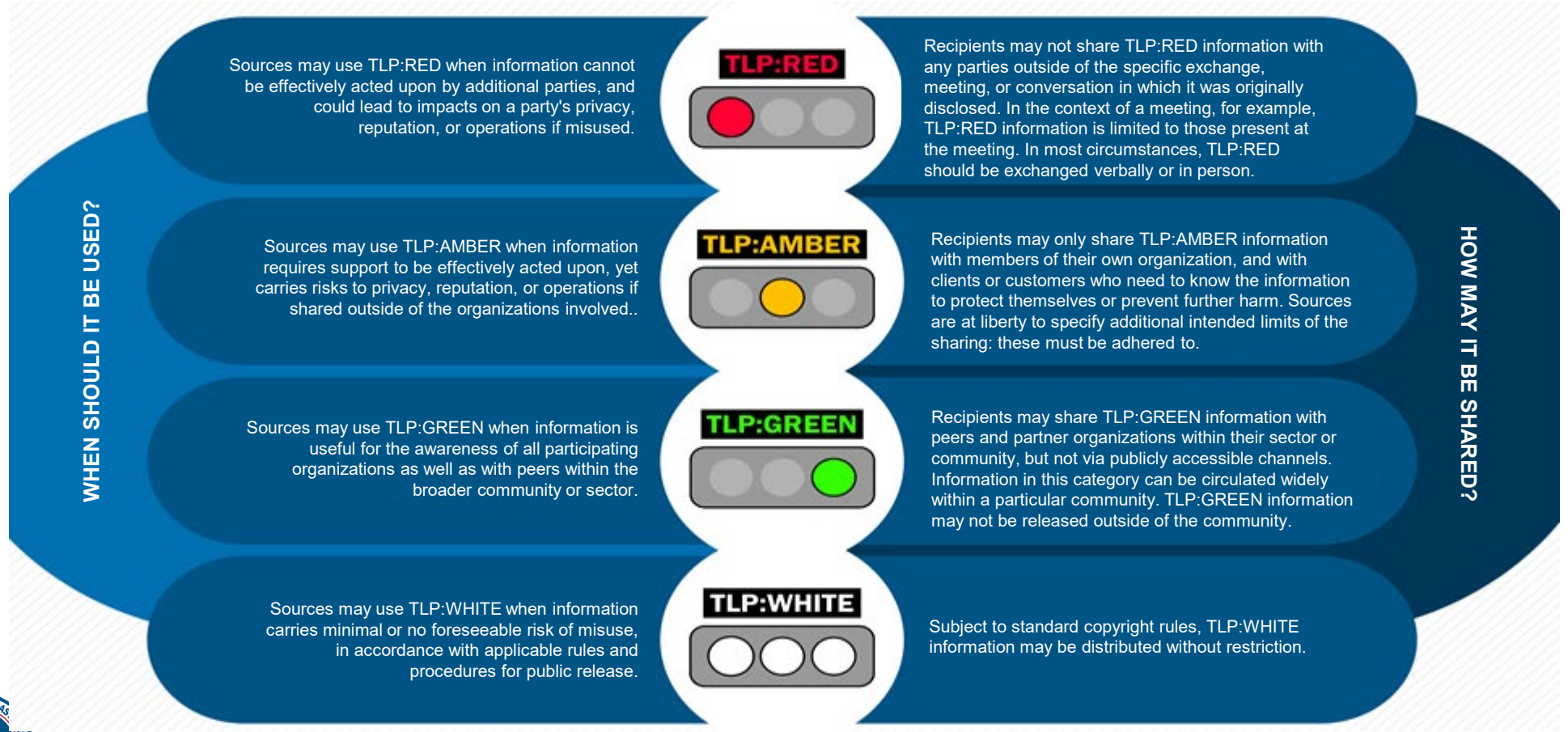
(b) SHARING OR RECEIPT OF CYBER THREAT INDICATORS.—No cause of action shall lie or be maintained in any court against any private entity, and such action shall be promptly dismissed, for the sharing or receipt of a cyber threat indicator or defensive measure…

Cybersecurity Information Sharing Act of 2015

- AIS participants are protected from liability charges as long as the sharing is in accordance with the law.

Share Your Identity as You Wish in AIS

Using TLP, submitters mark whether they will allow DHS to share their identity with everyone, only the Federal Government, or no one.



AIS Today

More than 260 Federal and non-Federal entities are connected to AIS (about 190 non-Federal).

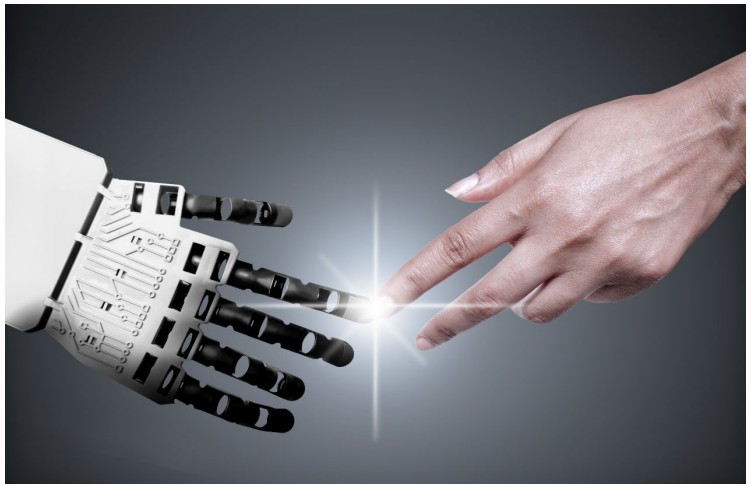
Of non-Federal connections, about 30 are Information Sharing and Analysis Centers, Information Sharing and Analysis Organizations, or managed security providers, who further distribute AIS indicators to members or customers.

Eleven international computer emergency response teams connect to our AIS server.

Six non-Federal entities share indicators under AIS.

Overall, more than 3 million unique indicators have been shared through AIS since implementation in 2016.

Join us!



Additional Information Sharing Opportunities, 1 of 2

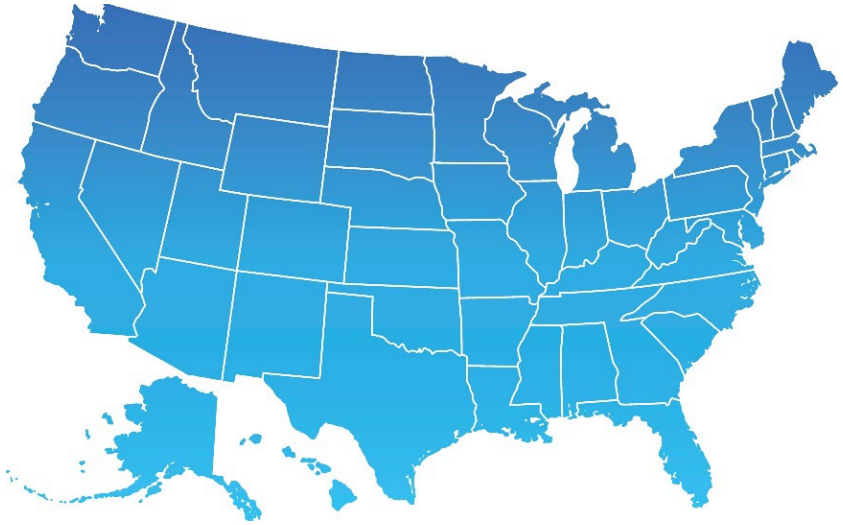
- **Cyber Information Sharing and Collaboration Program (CISCP)**
  - Enhances cyber collaboration between CISA and critical infrastructure owners and operators, uses government and industry subject matter experts to collaboratively respond to incidents.
  - Supports data flow and analytical collaboration to support threat sharing across all sectors.
  - Provides timely, actionable products including threat/vulnerability indicators, early warnings and alerts focused on single threats/vulnerabilities expected to impact critical infrastructure, and recommended practices.
  - For more CISCP information, email ciscp_coordination@hq.dhs.gov.

Additional Information Sharing Opportunities, 1 of 2

- **Enhanced Cybersecurity Services (ECS) program**
  - Improves protection of critical infrastructure systems from unauthorized access, exploitation, or data exfiltration. Cyber threat information shared with qualified commercial service providers.
  - Operationalizes sensitive or classified information
  - For more ECS information, visit http://www.dhs.gov/enhanced-cybersecurity-services, or email ECS_Program@HQ.DHS.gov.

Additional Information Sharing Opportunities, 2 of 2

- Multi-State Information Sharing and Analysis Center
  - Focal point for cyber threat prevention, protection, response and recovery for state, local, tribal, and territorial governments.
  - Operates 24 x7 cyber security operations center, providing real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response. For more information, visit www.cisecurity.org/ms-isac or email info@msisac.org



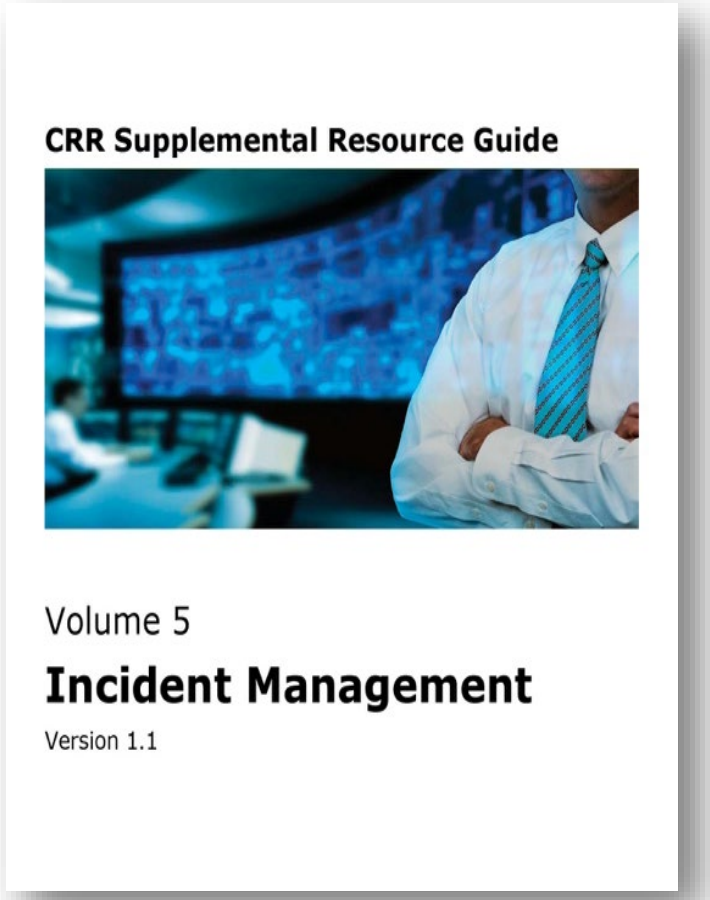
- ISACs and ISAOs
  - **Information Sharing and Analysis Centers** (ISACs) or **Organizations** (ISAOs) are communities of interest sharing cybersecurity risk, threat information, and incident management to members. For more information on ISACs, visit www.nationalisacs.org. For more on ISAOs visit www.isao.org/about.

INCIDENT MANAGEMENT

Incident Management Planning Helps Mitigate Effects

1. Get leadership support for incident management planning.
2. Establish an event-detection process.
3. Establish a triage-and-analysis process.
4. Establish an incident-declaration process.
5. Establish an incident-response and recovery process.
6. Establish an incident-communications process.
7. Assign roles and responsibilities for incident management.
8. Establish a post-incident analysis and improvement process.

Resource: CRR Supplemental Resource Guide, Incident Management.



Federal Incident Response, 1 of 2

Federal Incident Response

- **Threat Response:** Attributing, pursuing, and disrupting malicious cyber actors and malicious cyber activity. Conducting criminal investigations and other actions to counter the malicious cyber activity.
- **Asset Response:** Protecting assets and mitigating vulnerabilities in the face of malicious cyber activity, reducing the impact to systems and data; strengthening, recovering, and restoring services; identifying other entities at risk; and assessing potential risk to broader community.

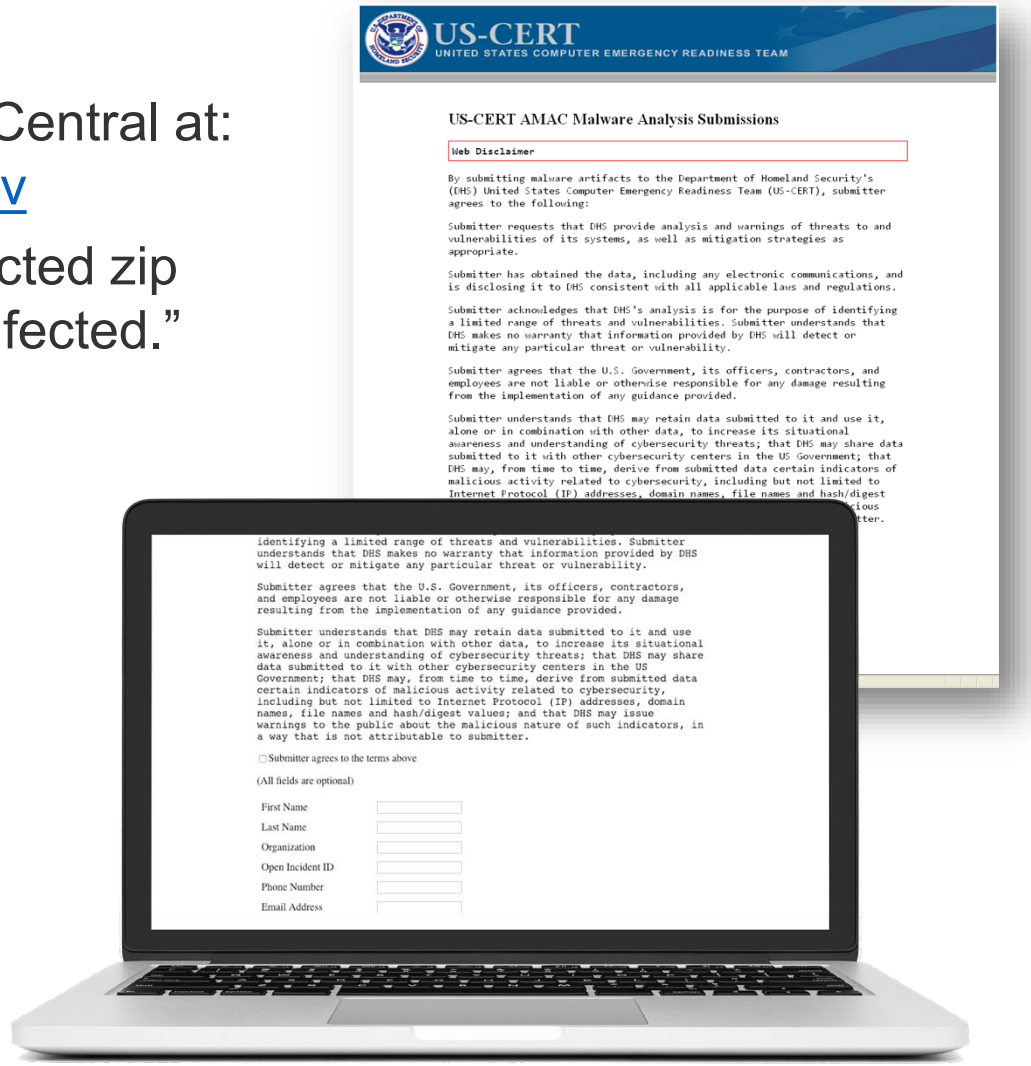
Federal Incident Response, 2 of 2

Threat Response	Asset Response
Federal Bureau of Investigation 855-292-3937 or cywatch@ic.fbi.gov	**CISA Central** 888-282-0870 or central@cisa.DHS.gov Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.
U.S. Secret Service secretservice.gov/contact/field-offices	
Immigration and Customs Homeland Security Investigations 866-347-2423 or ice.gov/contact/hsi	**Report Internet Crimes**: FBI Internet Crime Complaint Center ic3.gov

Malware Analysis

To submit malware:

- Email submissions to CISA Central at: submit@malware.us-cert.gov
  - Send in password-protected zip file(s). Use password “infected.”
- Upload submission online: https://malware.us-cert.gov



ADDITIONAL CYBERSECURITY RESOURCES

Cyber Exercises and Planning

CISA's National Cyber Exercise and Planning Program develops, conducts, and evaluates cyber exercises and planning activities for state, local, tribal and territorial governments and public and private sector critical infrastructure organizations.

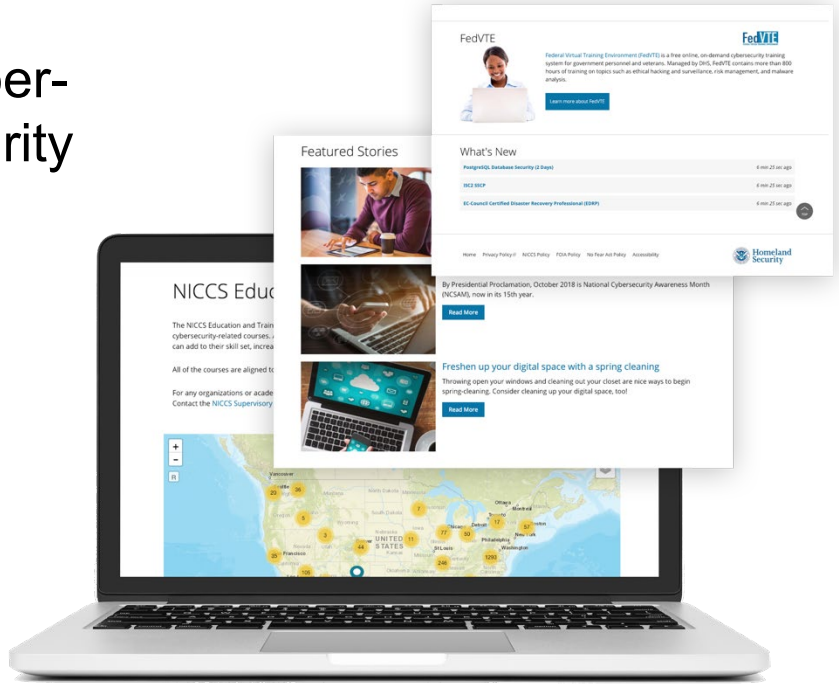
- Cyber Storm Exercise – DHS's flagship national-level biennial exercise
- Exercise Planning and Conduct
- Cyber Exercise Consulting and Subject Expertise Support
- Cyber Planning Support
- Off-the-Shelf Resources

Cybersecurity Training Resources

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

The NICCS website includes:

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



For more information, visit NICC.US-CERT.gov

Our Nation's Cyber Workforce Foundation

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

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

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

Free Federal Cyber Training

FedVTE enables cyber professionals to continue growing skills.

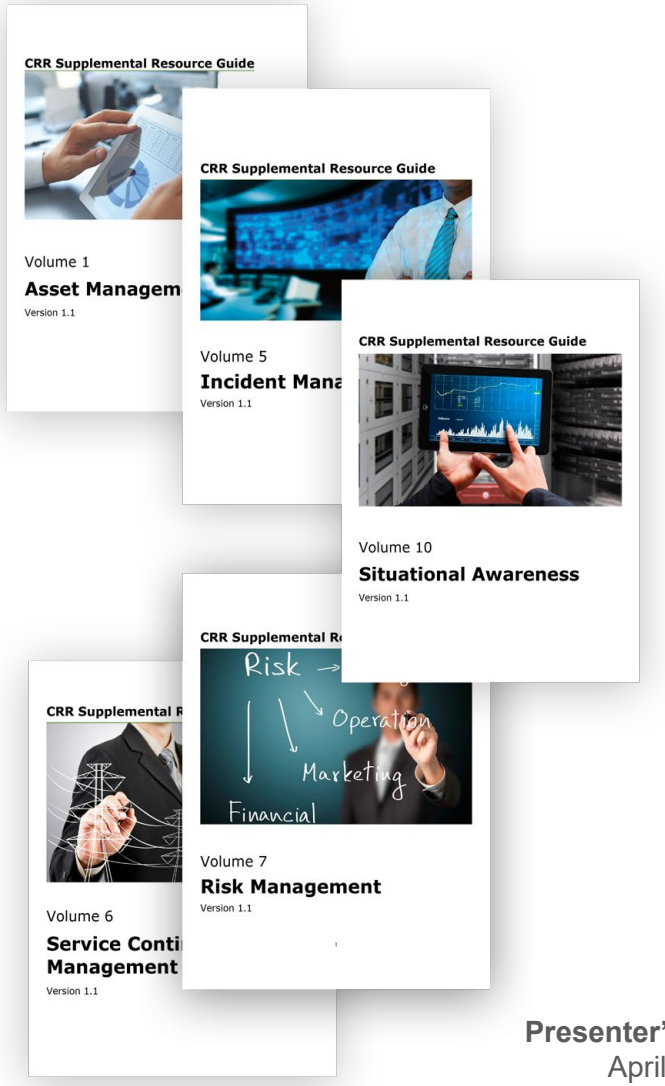
FedVTE is an online, on-demand training center that provides **free** cybersecurity training for U.S. veterans and federal, state, local, tribal, and territorial government employees. **As of January 2017,** there are:

- Over 140,000 registered users, including employees at all levels of government
- Over 18,000 veteran users (through non-profit partner, Hire Our Heroes™)
- Over 5,000 SLTT registered users

FedVTE FEDERAL VIRTUAL TRAINING ENVIRONMENT

Resource Guides

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



NIST CYBERSECURITY FRAMEWORK

NIST Cybersecurity Framework

- The Cybersecurity Framework
  - Establishes a common perspective and vernacular,
  - Provides risk-based guidelines,
  - Is collaboration-oriented, and
  - Is internationally recognized.

- For more information, visit nist.gov/cyberframework

Functions	*Categories*
IDENTIFY (ID)	Asset Management (AM)
	Business Environment (BE)
	Governance (GV)
	Risk Assessment (RA)
	Risk Management Strategy (RM)
PROTECT (PR)	Access Control (AC)
	Awareness and Training (AT)
	Data Security (DS)
	Information Protection Processes and Procedures (IP)
	Maintenance (MA)
	Protective Technology (PT)
DETECT (DE)	Anomalies and Events (AE)
	Security Continuous Monitoring (CM)
	Detection Processes (DP)
RESPOND (RS)	Incident Response Planning (RP)
	Communications (CO)
	Analysis (AN)
	Mitigation (MI)
	Improvements (IM)
RECOVER (RC)	Recovery Planning (RP)
	Improvements/Gap Remediation (IM)
	Communications (CO)

Contact

General Inquiries

iodregionaloperations@cisa.dhs.gov

CISA Contact Information

Name **Title**	**@cisa.dhs.gov** **Number**
Number	**@cisa.dhs.gov** **+1 202-380-6024**

Cybersecurity and Infrastructure Security Agency

For more information:
cisa.gov

Questions?

Email: kyle.wolf@hq.dhs.gov
Phone: 202-573-6237
Email: colin.glover@cisa.dhs.gov
Phone: 202-380-5741


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY