Homeland Security

Understanding Risk and Vulnerability:

DHS Services and Resources

CISA

Cyber + Infrastructure Security

J.D. Henry, M.B.A., CISSP, CISM, GCFA
Cybersecurity Advisor (CSA), Region VII (IA, KS, MO, NE)
Cyber Security Division

Agenda

- Cyber Security Advisor Program
- CISA Cyber Service Offerings
  - CSA Services
  - NCATS Services
  - Training, Awareness, & Reporting

Cyber Security Advisor Program

CISA
CYBER+INFRASTRUCTURE

CSA Program- Mission, Vision, and Goals

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 understands that a regional and national focus is essential to protect critical infrastructure through a sustained **cyber security presence.**

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:

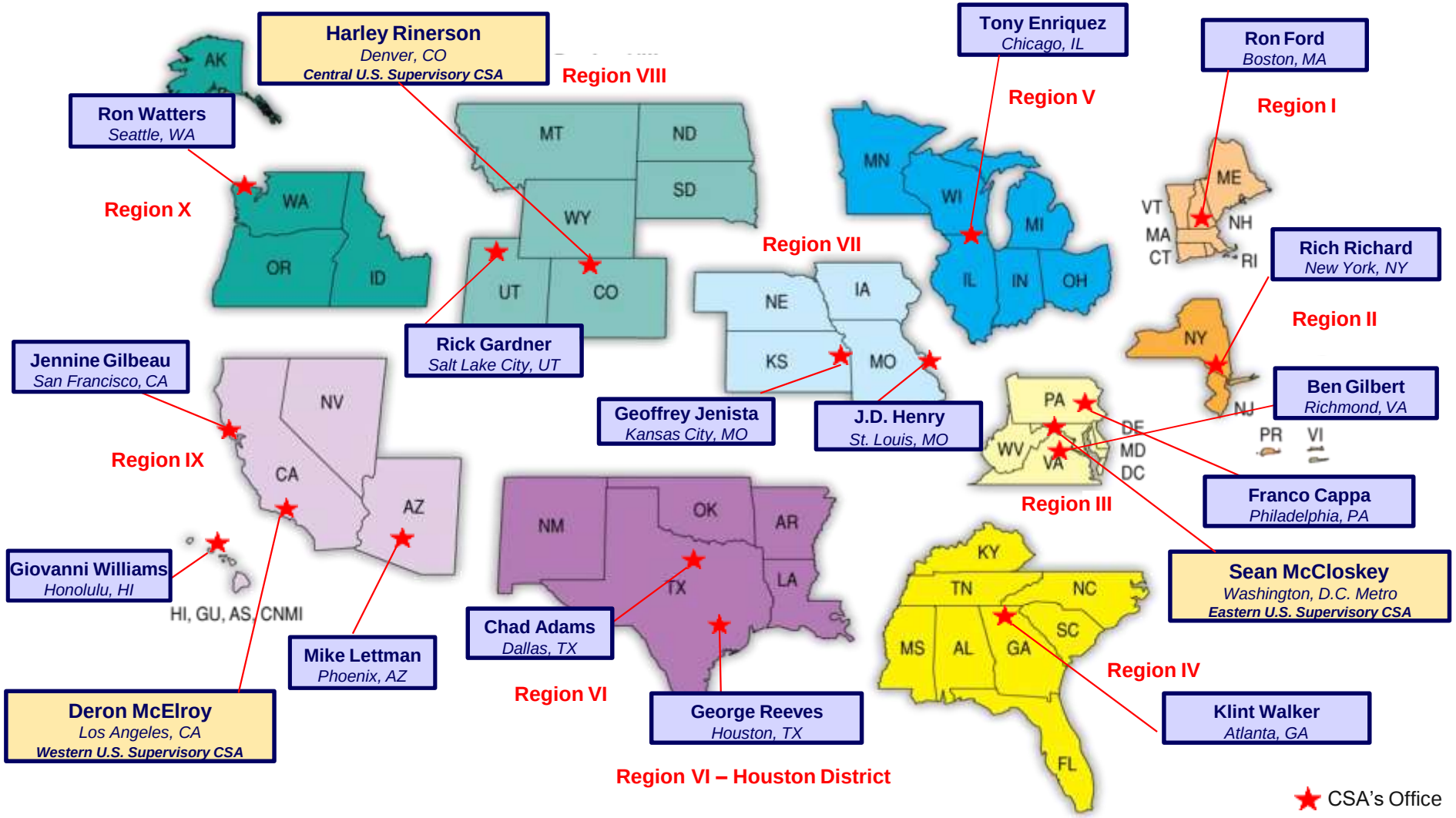
- Cyber Preparedness
- Risk Mitigation
- Incident & Information Coordination
- Cyber Policy Promotion & Situational Awareness

CSAs primarily 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

Cybersecurity Advisor (CSA) Locations



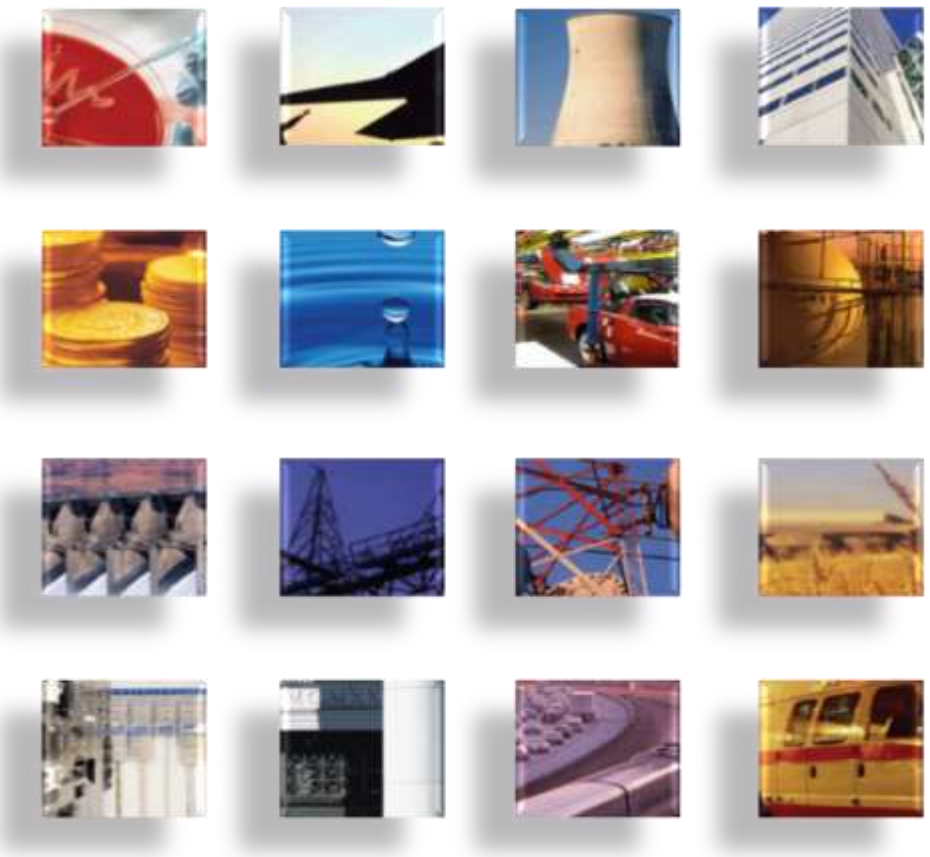
CISA
CYBER+INFRASTRUCTURE

Homeland Security

Critical Infrastructure Sectors

CSAs assists the public and private sectors secure its networks and focuses on organizations in the following 16 critical infrastructure sectors.

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food and Agriculture
- Government Facilities
  - Election Infrastructure
- Health Care & Public Health
- Information Technology
- Nuclear Reactors, Materials, & Waste
- Transportation Systems
- Water



What is Cyber Resilience

"… 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 – PPD 21
February 12, 2013

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

CISA
CYBER+INFRASTRUCTURE

CISA Service Offerings

Protections for Shared Information

Protected Critical Infrastructure Information (PCII)

The DHS Protected Critical Infrastructure Information (PCII) Program is an information protection program that enhances information sharing between the private sector and the government. The DHS and other federal, state and local analysts use PCII to analyze and secure critical infrastructure and protected systems, identify vulnerabilities and develop risk assessments, and enhance recovery preparedness measures.

If the information submitted satisfies the requirements of the CII Act of 2002, it is protected from:

- The Freedom of Information Act (FOIA)
- State and local disclosure laws
- Use in civil litigation

PCII cannot be used for regulatory purposes and can only be accessed in accordance with strict safeguarding and handling requirements. PCII may be accessed by federal, state or local government employees and their contractors who meet the requirements of the PCII Program standard access policy.

CISA Service Offerings

Cyber Security Advisors (CSAs)

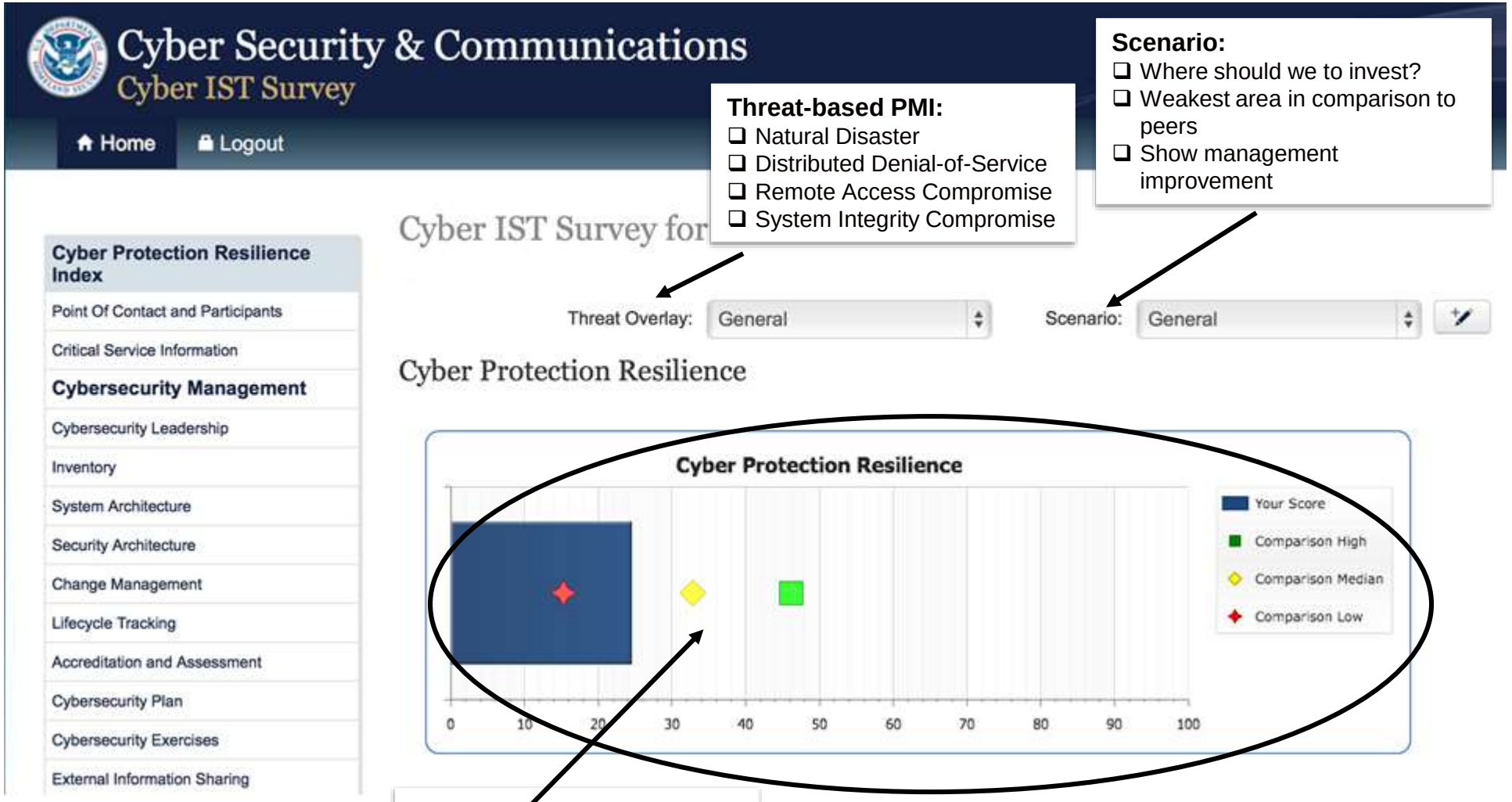
Cyber Infrastructure Survey (CIS)

- Structured, interview based assessment (2 ½ to 4 hours) of essential cybersecurity practices in-place for critical services within your organization
- Identifies interdependencies, capabilities, and the emerging effects related to current cybersecurity posture
- Focuses on protective measures, threat scenarios, and a service based view of cybersecurity in context of the surveyed topics
- Broadly aligns to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF)

CIS Survey Question Domains

CIS Domains	
Cybersecurity Forces	**Cybersecurity Management**
* Personnel	* Cybersecurity Leadership
* Cybersecurity Training	* Cyber Service Architecture
Cybersecurity Controls	* Change Management
* Authentication and Authorization Controls	* Lifecycle Tracking
* Access Controls	* Assessment and Evaluation
* Cybersecurity Measures	* Cybersecurity Plan
* Information Protection	* Cybersecurity Exercises
* User Training	* Information Sharing
* Defense Sophistication and Compensating Controls	**Dependencies**
Incident Response	* Data at Rest
* Incident Response Measures	* Data in Motion
* Alternate Site and Disaster Recovery	* Data in Process
	* End Point Systems

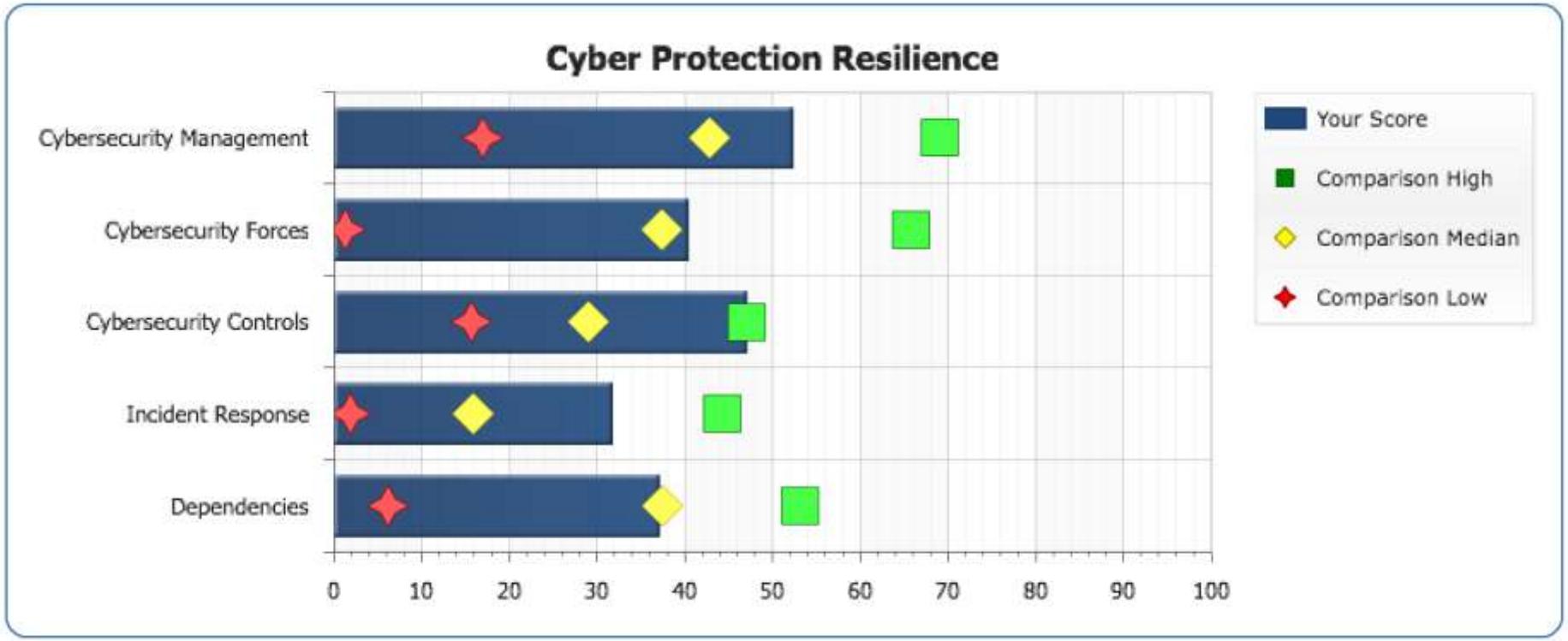
Example CIS Dashboard



CISA
CYBER+INFRASTRUCTURE

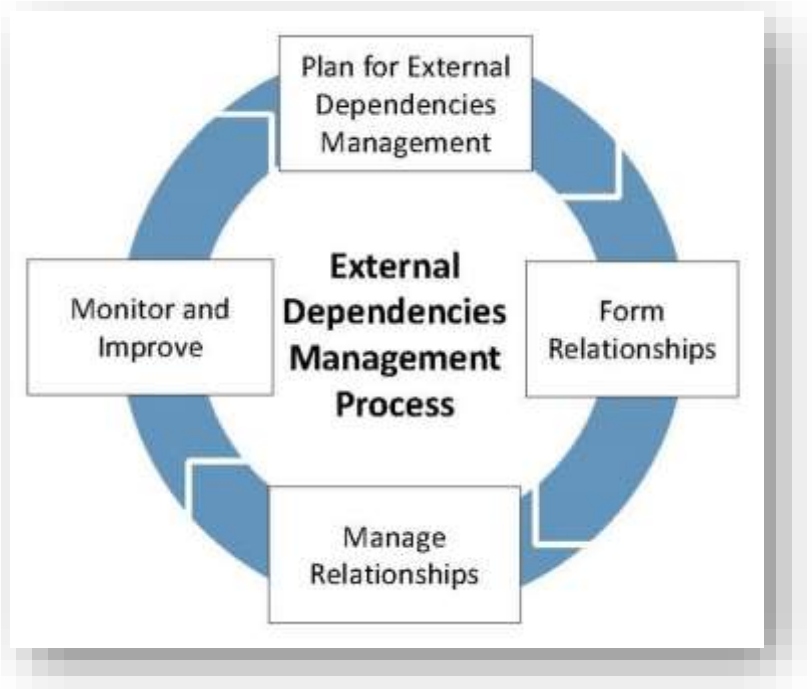
Example CIS Comparison

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



External Dependency Management (EDM)

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



EDM process outlined in the External Dependencies Management Resource Guide

The EDM Assessment provides stakeholders with a more in-depth examination of risks associated with their third-party entities.

External Dependency Management (EDM)

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

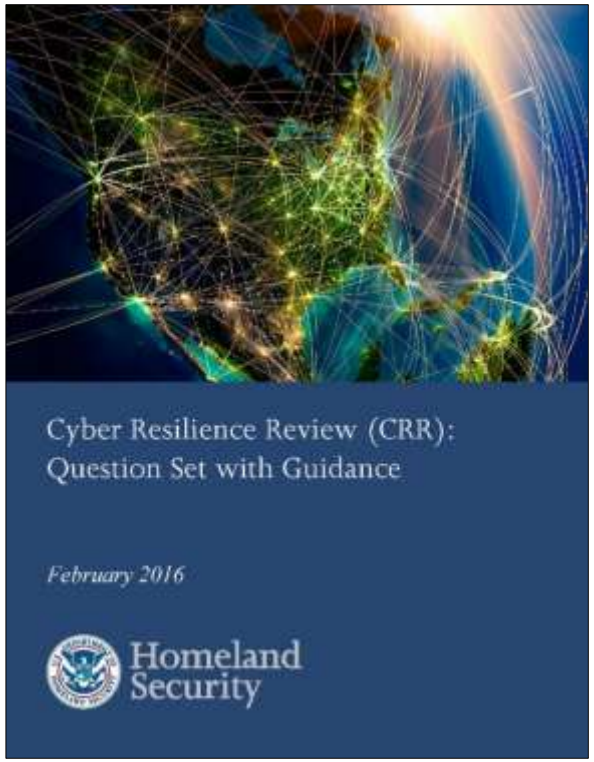
1. **RELATIONSHIP FORMATION –** how the organization considers third party risks, selects external entities, and forms relationships with them so that risk is managed from the start
2. **RELATIONSHIP MANAGEMENT AND GOVERNANCE–**how the organization manages ongoing relationships with external entities to support and strengthen its critical services at a managed level of risk and cost
3. **SERVICE PROTECTION AND SUSTAINMENT –** how the organization plans for, anticipates, and manages disruption or incidents related to external entities

Cyber Resilience Review (CRR)

- **Purpose:** The CRR is an assessment intended to evaluate an organization's operational resilience and cybersecurity practices of its **critical services**
- **Delivery:** The CRR can be
  - **Facilitated**
  - **Self-administered**

CRR Self-Assessment Package is available on the C-Cubed Voluntary Program website.

- Helps public and private sector partners understand and measure cyber security capabilities as they relate to operational resilience and cyber risk
- Based on the CERT ® Resilience Management Model (CERT® RMM))



CRR Question Set & Guidance

CISA CYBER+INFRASTRUCTURE

The CRR provides organizations with a no-cost method to assess their cybersecurity postures and measure against the NIST CSF.

Cyber Resilience Review (CRR) | Domains

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

- Documentation in place, and periodically reviewed & updated
- Communication and notification to all those who need to know
- Execution/Implementation & analysis in a consistent, repeatable manner
- Alignment of goals and practices within and across CRR domains

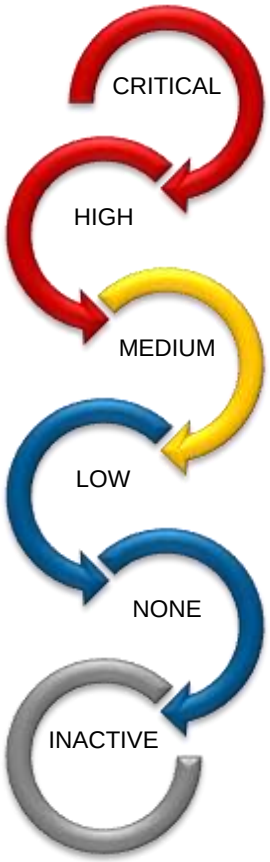
AM	**Asset Management** *identify, document, and manage assets during their life cycle*	SCM	**Service Continuity Management** *ensure continuity of IT operations in the event of disruptions*
CCM	**Configuration and Change Management** *ensure the integrity of IT systems and networks*	RISK	**Risk Management** *identify, analyze, and mitigate risks to services and IT assets*
CNTL	**Controls Management** *identify, analyze, and manage IT and security controls*	EXD	**External Dependency Management** *manage IT, security, contractual, and organizational controls that are dependent on the actions of external entities*
VM	**Vulnerability Management** *identify, analyze, and manage vulnerabilities*	TRNG	**Training and Awareness** *promote awareness and develop skills and knowledge*
IM	**Incident Management** *identify and analyze IT events, detect cyber security incidents, and determine an organizational response*	SA	**Situational Awareness** *actively discover and analyze information related to immediate operational stability and security*

CISA Service Offerings

National Cybersecurity Assessments and Technical Services (NCATS)

CISA
CYBER+INFRASTRUCTURE

Cyber Hygiene (CyHy)

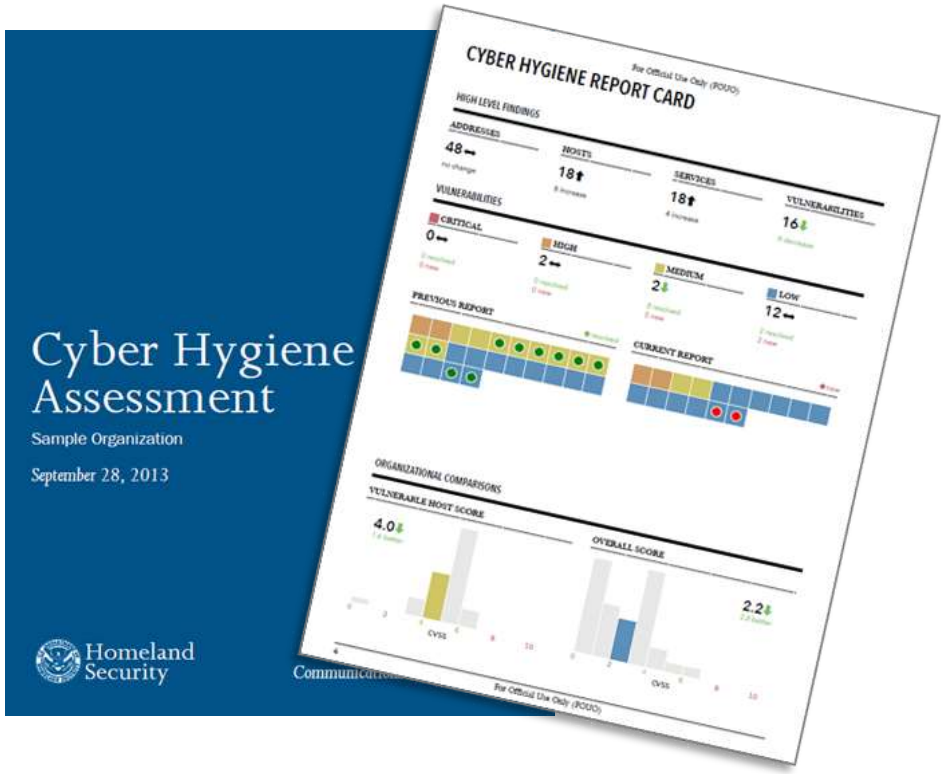


Assess Internet accessible systems for known vulnerabilities and configuration errors

Work with organization to proactively mitigate threats and risks to systems

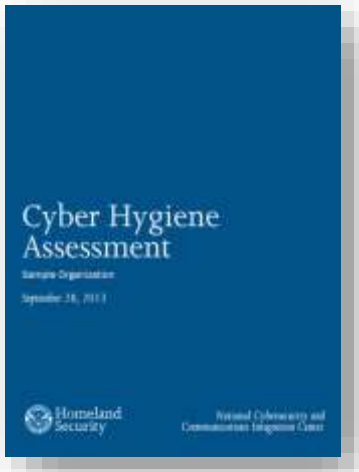
Activities include:

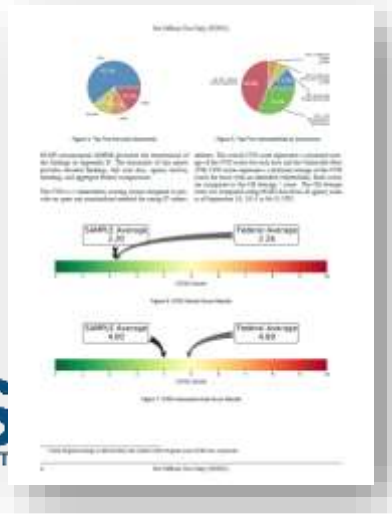
- Network Mapping
  - Identify public IP address space
  - Identify hosts that are active on IP address space
  - Determine the O/S and Services running
  - Re-run scans to determine any changes
  - Graphically represent address space on a map
- Network Vulnerability & Configuration Scanning
  - Identify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

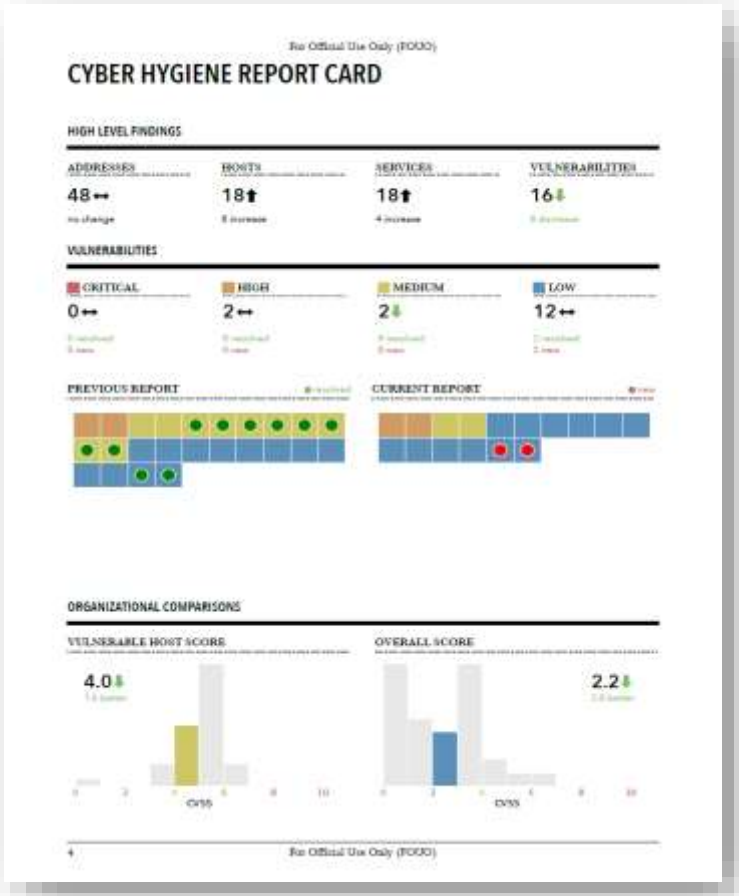


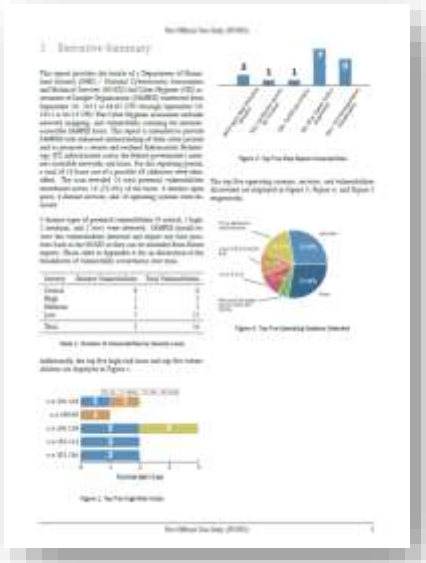
CISA
CYBER+INFRASTRUCTURE

Cyber Hygiene (CyHy)









Phishing Campaign Assessment (PCA)

Objectives:

- Increase cybersecurity awareness within stakeholder organizations
- Decrease risk of successful malicious phishing attacks, limit exposure, reduce rates of exploitation

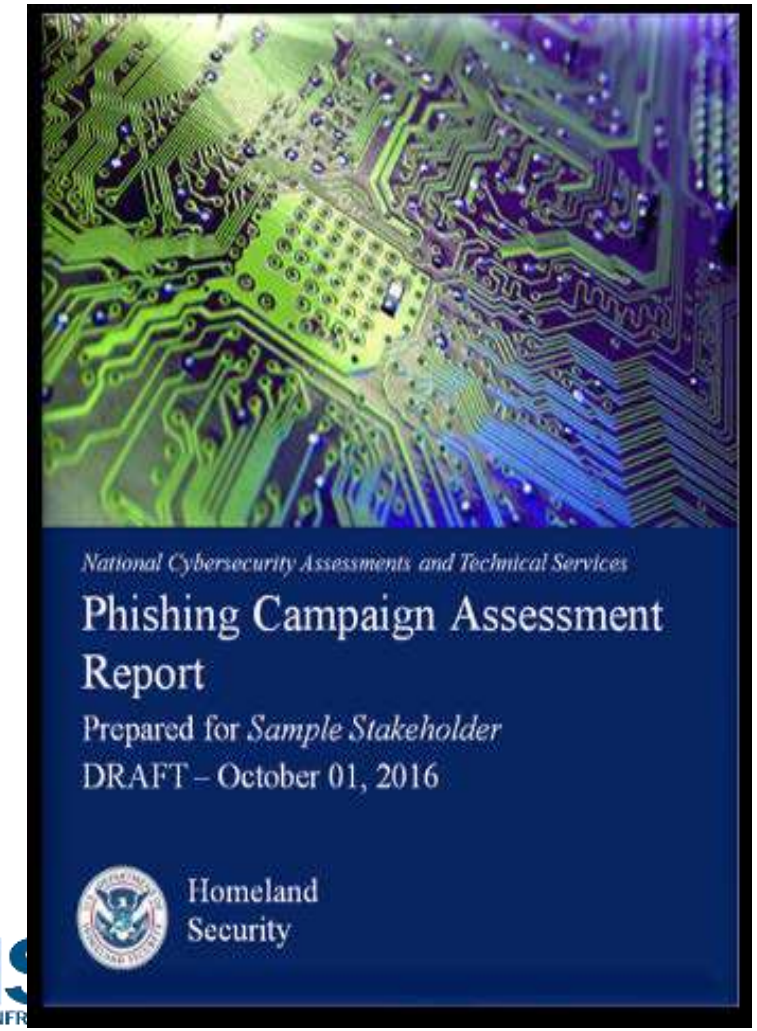
Benefits:

- Receive actionable metrics
- Highlight need for improved security Training

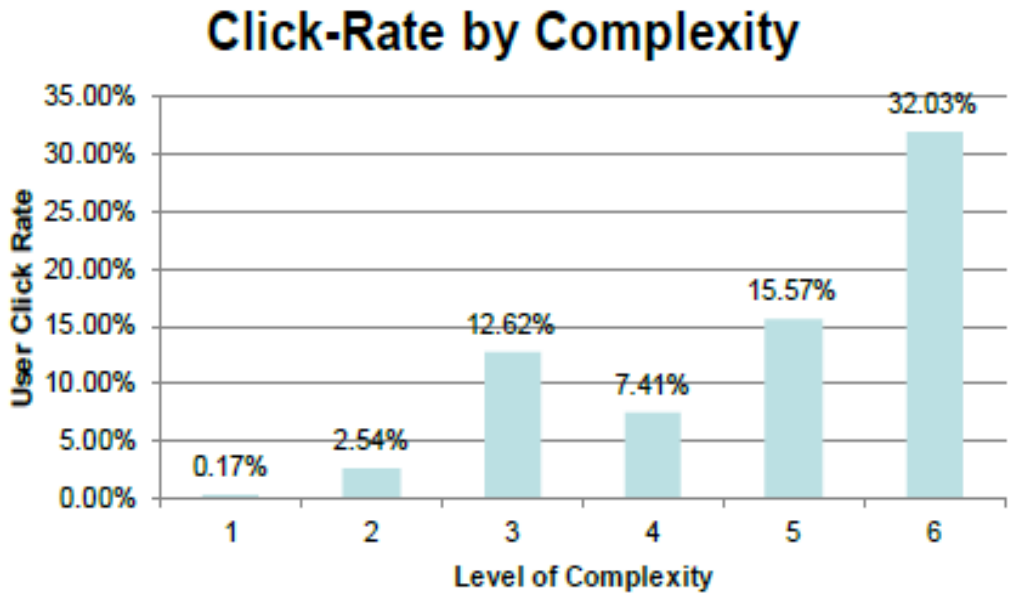
Scope:

- 6-week engagement period
- Phishing emails capture click-rate only, no payloads will be used
- Varying Levels of Complexity -- Levels 1 - 6 (Easy to Difficult)

Phishing Campaign Assessment (PCA)



Week	Campaign	Date Sent	Complexity Level	User Click Rate	# Emails Sent
1	Please Help!	3/18/16	1	0.17%	401
2	Reveal Your Past	3/31/16	2	2.54%	402
3	Password Expire Alert	4/6/16	3	12.62%	401
4	Severe Weather Checklist	4/15/16	4	7.41%	402
5	Federal Employee Survey	4/20/16	5	15.57%	401
6	Salary Guidelines	4/27/16	6	32.03%	402



Validated Architecture Design Review (VADR)

Overview:

The Validated Architecture Design Review (VADR) is an assessment based on Federal and industry standards, guidelines, and best practices. Assessments can be conducted on Information Technology (IT) or Operational Technology (OT) infrastructures (ICS-SCADA).

Assessment Objectives:

- Reduce risk to the Nation's Critical Infrastructure components
- Analyze systems based on standards, guidelines, and best practices
- Ensure effective defense-in-depth strategies
- Provide findings and practical mitigations for improving operational maturity and enhancing cybersecurity posture

Validated Architecture Design Review (VADR)

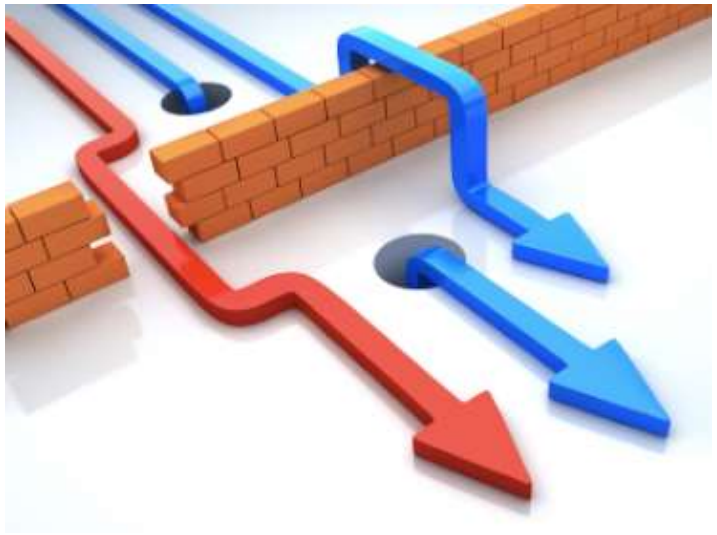
ICS-CERT's assessment team works interactively with your IT and operations personnel to focus on **three key areas**:

- **Evaluation of Architecture**
  - An in-depth review and evaluation of the network design, configuration, and inter-connectivity to internal and external systems focused on defensive strategies
- **Analysis of Network Traffic**
  - Utilizes a combination of open source and commercial tools to identify anomalous communication which could indicate suspicious activity or misconfiguration
- **Systems Log Review and Analysis**
  - Detailed review of system settings and activity to determine the susceptibility to potential attacks and baseline normal behavior to find anomalies

Risk and Vulnerability Assessment (RVA)

A penetration test, or the short form pentest, is an attack on a computer system with the intention of finding security weaknesses, potentially gaining access to it, its functionality and data.

- Involves identifying the target systems and the goal, then reviewing the information available and undertaking available means to attain the goal
- A penetration test target may be a white box (where all background and system information is provided) or black box (where only basic or no information is provided except the company name)
- A penetration test will advise if a system is vulnerable to attack, if the defenses were sufficient and which defenses (if any) were defeated in the penetration test



Risk and Vulnerability Assessment (RVA)

Conducts red-team assessments and provides remediation recommendations.

- Identify risks, and provide risk mitigation and remediation strategies
- Improves an agency's cybersecurity posture, limits exposure, reduces rates of exploitation, and increases the speed and effectiveness of future cyber attack responses.

Service	Description
Vulnerability Scanning and Testing	Conduct Vulnerability Assessments
Penetration Testing	Exploit weakness or test responses in systems, applications, network and security controls
Social Engineering	Crafted e-mail at targeted audience to test Security Awareness / Used as an attack sector to internal network
Wireless Discovery & Identification	Identify wireless signals (to include identification of 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 Service Offerings

Training, Awareness, & Reporting

Federal Virtual Training Environment

https://fedvte.usalearning.gov/

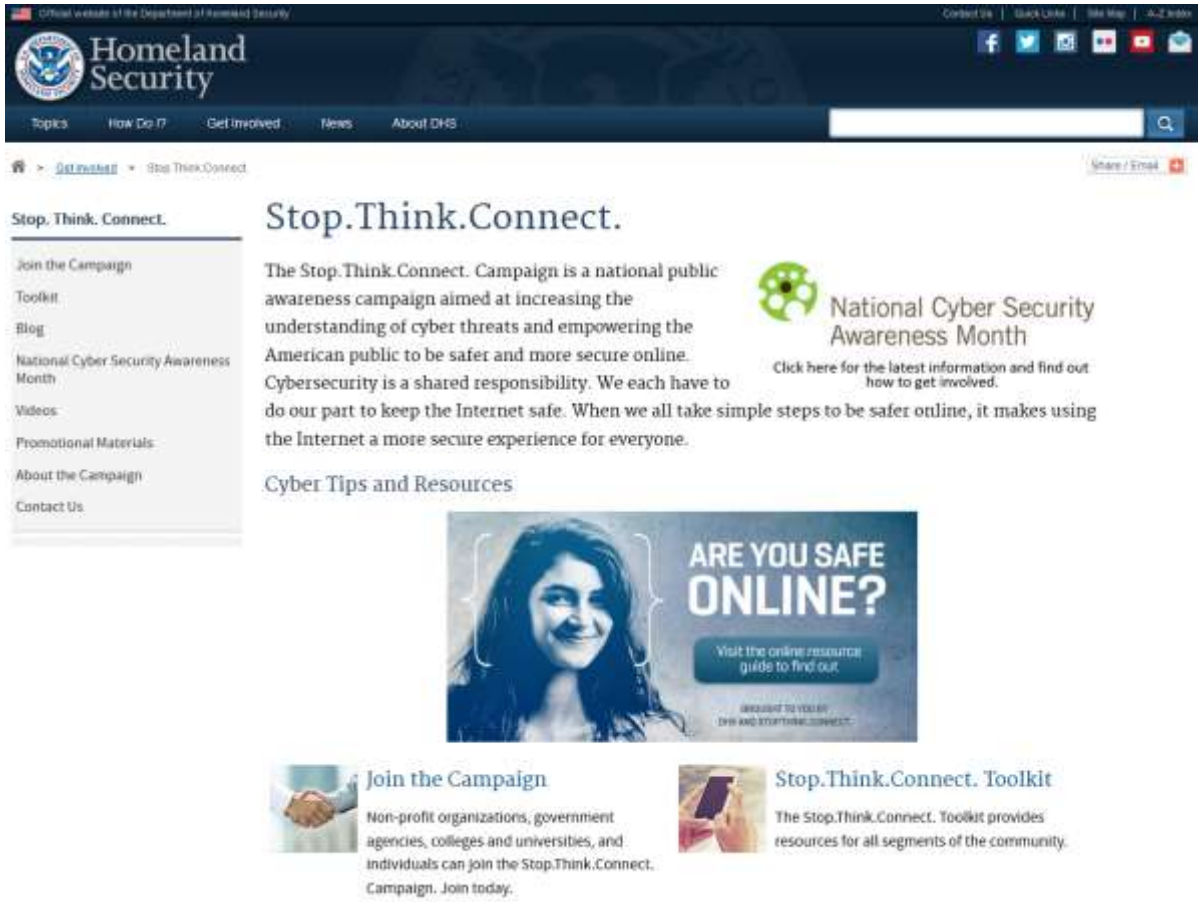
CISA
CYBER+INFRASTRUCTURE

Stop. Think. Connect

https://www.dhs.gov/stopthinkconnect

Toolkit Materials for Different Audiences

- *Students K-8, 9-12, and Undergraduate*
- *Parents and Educators*
- *Young Professionals*
- *Older Americans*
- *Government*
- *Industry*
- *Small Business*
- *Law Enforcement*



Toolkit Materials by Cyber Topic

Topics: Cybersecurity, Law Enforcement Partnerships

Attachment	Size
Social Media Guide	180.59 KB
Internet of Things Tip Card	146.25 KB
Cybersecurity While Traveling Tip Card	149.32 KB
Chatting with Kids about Being Online Booklet	4.89 MB
Parents and Educators Tip Card	154.11 KB
Mobile Security Tip Card	156.06 KB
Seguridad Cibernética Para Los Niños	281.79 KB
Best Practices for Creating a Password	262.54 KB
Best Practices for Using Public WiFi	215.71 KB
Identity Theft and Internet Scams	359.92 KB
Mobile Banking and Payments	227.88 KB
Online Gaming	301.16 KB
Online Privacy	226.48 KB
Reporting a Cybercrime Complaint	187.17 KB
Insider Threat	447.96 KB
Malware	354.77 KB
Five Every Day Steps Towards Online Safety	235.9 KB
Five Ways to be Cyber Secure at Work	232.38 KB
How to Recognize and Prevent Cybercrime	245.29 KB
Five Steps to Protecting Your Digital Home	202.05 KB
Your Part in Protecting Critical Infrastructure	446.68 KB
Phishing	253.68 KB

National Cyber Security Awareness Month

- National Cyber Security Awareness Month (NCSAM) — held annually in October — is a collaborative effort between government, industry and organizations of all sizes to help you — and everyone — stay safer and more secure online.

- NCSAM 2018 Themes
  - *Week 1: Oct. 1–5: Make Your Home a Haven for Online Safety*
  - Week 2: Oct. 8–12*: Millions of Rewarding Jobs: Educating for a Career in Cybersecurity*
  - Week 3: Oct. 15–19*: It's Everyone's Job to Ensure Online Safety at Work*
  - Week 4: Oct. 22–26*: Safeguarding the Nation's Critical Infrastructure*

CISA
CYBER+INFRASTRUCTURE

National Cybersecurity Awareness Month

NCCIC

The mission of the **National Cybersecurity and Communications Integration Center (NCCIC)** is to serve as a national center for reporting of and mitigating communications and cybersecurity incidents.

Incident Reporting/Response/Hunting

NCCIC's Hunt and Incident Response Team (HIRT)

Provides expert intrusion analysis and mitigation guidance to clients who lack the ability to respond to a cyber incident in-house or require additional assistance.

Supports federal departments and agencies, state and local governments, the private sector (such as, industry and critical infrastructure asset owners and operators), academia, and international organizations.

Services:

- Incident Triage
- Network Topology Review
- Infrastructure Configuration Review
- Log Analysis
- Incident Specific Risk Overview
- Hunt Analysis
- Security Program Review
- Malware Analysis
- Mitigation Analysis
- Digital Media Analysis
- Control Systems Incident Analysis

CISA
CYBER+INFRASTRUCTURE

Incident Reporting

NCCIC provides real-time threat analysis and incident reporting capabilities

- 24x7 contact number: 1-888-282-0870;
  - nccicustomerservice@hq.dhs.gov

When to Report:

If there is a suspected or confirmed cyber attack or incident that:

- ❖ Affects core government or critical infrastructure functions;
- ❖ Results in the loss of data, system availability; or control of systems;
- ❖ Indicates malicious software is present on critical systems

Malware Submission Process:

- Please send all submissions to the Advance Malware Analysis Center (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

CISA CYBER+INFRASTRUCTURE

Federal Incident Response

Threat Response	Asset Response
Federal Bureau of Investigation (FBI): FBI Field Office Cyber Task Forces: http://www.fbi.gov/contactus/field Internet Crime Complaint Center (IC3): http://www.ic3.gov ▪ Report cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity to FBI Field Office Cyber Task Forces. ▪ Report individual instances of cybercrime to the IC3, which accepts Internet crime complaints from both victim and third parties.	**United States Computer Emergency Readiness Team:** http://www.us-cert.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.
National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center: cywatch@ic.fbi.gov or (855) 292-3937 ▪ Report cyber intrusions and major cybercrimes that require assessment for action, investigation, and engagement with local field offices of Federal law enforcement agencies or the Federal Government.	**The Multi-State Information Sharing and Analysis Center (MS-ISAC)** is a voluntary and collaborative effort designated by the U.S. Department of Homeland Security as the key resource for cyber threat prevention, protection, response and recovery for the nation's State, Local, Tribal, and Territorial governments. **1.866.787.4722** **soc@msisac.org**
United States Secret Service (USSS) Secret Service Field Offices and Electronic Crimes Task Forces (ECTFs): http://www.secretservice.gov/contact/field-offices ▪ Report cybercrime, including computer intrusions or attacks, transmission of malicious code, password trafficking, or theft of payment card or other financial payment information.	**Center for Internet Security (CIS)** • Albert Sensors (Intrusion Detection) • Vulnerability Management • Baseline Configuration Guides • Assessment Tools
National Cybersecurity and Communications Integration Center (NCCIC) (888) 282-0870 or NCCIC@hq.dhs.gov	

CISA
CYBER+INFRASTRUCTURE

Questions / Discussion?

- Web Resources and Contact Cheat Sheet:
  - National Cybersecurity and Communications Integration Center

    https://www.dhs.gov/national-cybersecurity-and-communications-integration-center
  - Stakeholder Engagement and Cyber Infrastructure Resilience

    http://www.dhs.gov/stakeholder-engagement-and-cyber-infrastructure-resilience
  - Stop.Think.Connect

    https://www.dhs.gov/stopthinkconnect
  - Critical Infrastructure Cyber Community Voluntary Program (C3VP)

    https://www.us-cert.gov/ccubedvp
  - Federal Virtual Training Environment

    https://fedvte.usalearning.gov/

Region 7 Contact Information

Joseph "JD" Henry
Cybersecurity Advisor
(202) 860-7546
Joseph.Henry@hq.dhs.gov

Geoffrey F. Jenista
Cybersecurity Advisor
(913) 249-1539
Geoffrey.Jenista@hq.dhs.gov

Greg Hollingsead
Protective Security Advisor
(402) 981-8970
greg.hollingsead@hq.dhs.gov

For inquiries or further information,
contact cyberadvisor@dhs.gov