CISA CYBERSECURITY SERVICES

Sean McCloskey
Chief of Cybersecurity
CISA Region 4
Cybersecurity and Infrastructure Security Agency

February 16, 2023

WHO WE ARE

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

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

A Nation with secure and resilient critical infrastructure that ensures our security, economic prosperity, and way of life.

MISSION

Strengthen the Nation's cyber and physical infrastructure by managing and reducing systemic and catastrophic risk in partnership with the private sector, collaboration with the public sector, and protection of federal government networks.

CYBERSECURITY ADVISOR PROGRAM

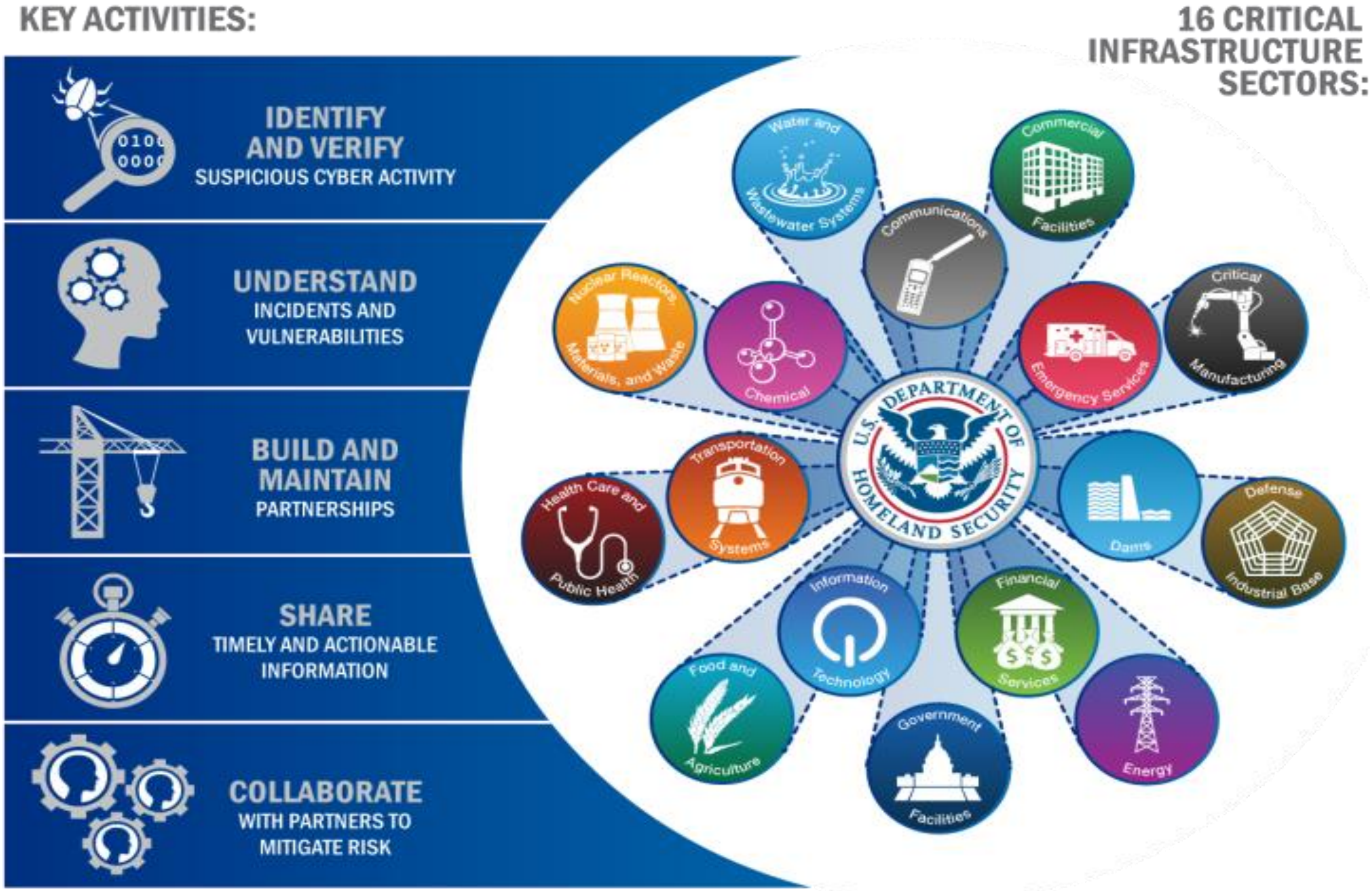
Cybersecurity Advisor Program

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.

Serving Critical Infrastructure



KEY ACTIVITIES:

IDENTIFY AND VERIFY SUSPICIOUS CYBER ACTIVITY

UNDERSTAND INCIDENTS AND VULNERABILITIES

BUILD AND MAINTAIN PARTNERSHIPS

SHARE TIMELY AND ACTIONABLE INFORMATION

COLLABORATE WITH PARTNERS TO MITIGATE RISK

16 CRITICAL INFRASTRUCTURE SECTORS:

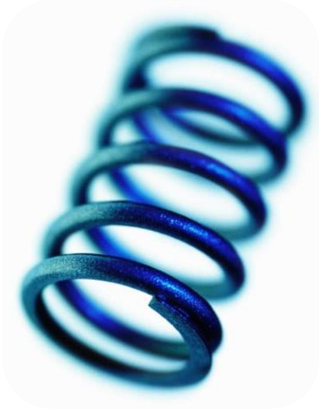
CISA
CYBER+INFRASTRUCTURE

CYBERSECURITY AND RESILIENCE

Resilience Defined

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

- Presidential Policy Directive 21
February 12, 2013



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

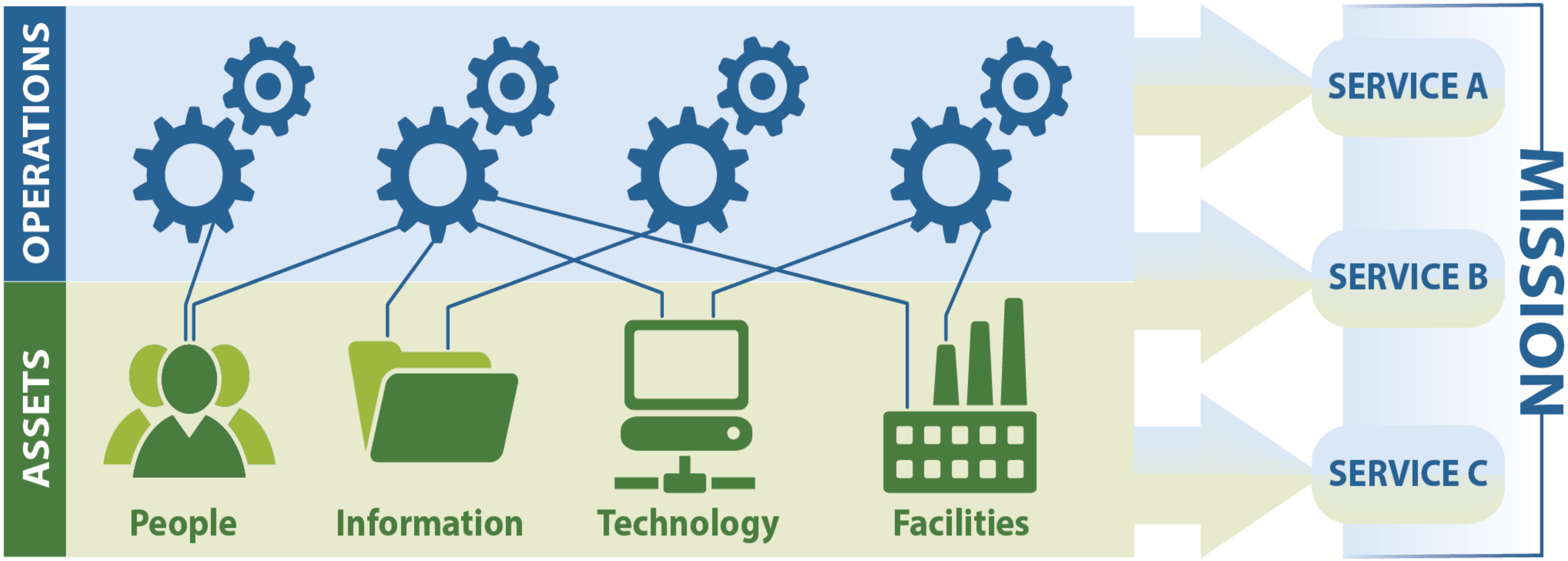
Operational Resilience in Practice

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.

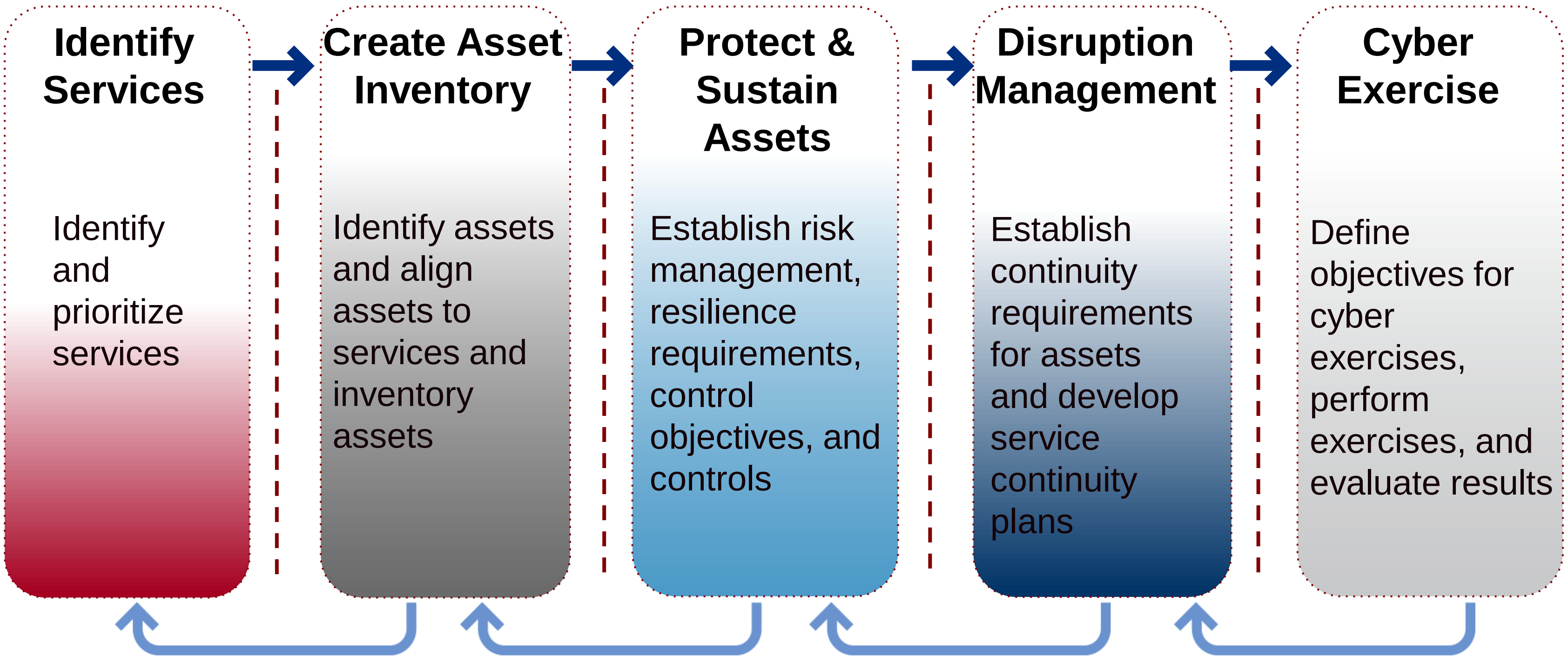
Cybersecurity Assets and Services

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



Working toward Cyber Resilience

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



Identify Services

Identify and prioritize services

Create Asset Inventory

Identify assets and align assets to services and inventory assets

Protect & Sustain Assets

Establish risk management, resilience requirements, control objectives, and controls

Disruption Management

Establish continuity requirements for assets and develop service continuity plans

Cyber Exercise

Define objectives for cyber exercises, perform exercises, and evaluate results

Process Management and Improvement

CISA CYBER ESSENTIALS

BOOTING UP

Things to Do First ▸

✓ Backup Data

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

✓ Multi-Factor Authentication

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

✓ Patch & Update Management

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

ESSENTIALS VOL.1

THE IT PROFESSIONAL'S GUIDE

✓ *Actions for leaders.*

✓ *Discuss with IT staff or service providers.*

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

Yourself

Drive cybersecurity strategy, investment and culture

Organizations living the culture have:

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

Your Staff

Develop security awareness and vigilance

Organizations living the culture have:

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

Your Systems

Protect critical assets and applications

Organizations living the culture have:

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

Your Surroundings

Ensure only those who belong on your digital workplace have access

Organizations living the culture have:

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

Your Data

Make backups and avoid loss of info critical to operations

Organizations living the culture have:

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

Your Actions Under Stress

Limit damage and quicken restoration of normal operations

Organizations living the culture have:

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

VOL.1 FALL 2019

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

CISA Cyber Essentials (1 of 6)

Essential Practice 1: Drive Strategy, Investment, and Culture

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

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

CISA
CYBER+INFRASTRUCTURE

CISA Cyber Essentials (2 of 6)

Essential Practice 2: Develop Security Awareness and Vigilance

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

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

CISA Cyber Essentials (3 of 6)

Essential Practice 3: Protect Critical Assets and Applications

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

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

CISA
CYBER+INFRASTRUCTURE

CISA Cyber Essentials (4 of 6)

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

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

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

CISA
CYBER+INFRASTRUCTURE

CISA Cyber Essentials (5 of 6)

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

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

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

CISA
CYBER+INFRASTRUCTURE

CISA Cyber Essentials (6 of 6)

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

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

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

CISA
CYBER+INFRASTRUCTURE

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
    - External Dependency Management Reviews
    - Cyber Security Evaluation Tool (CSET™)

- **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

VULNERABILITY SCANNING / HYGIENE

Vulnerability Scanning / Hygiene

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

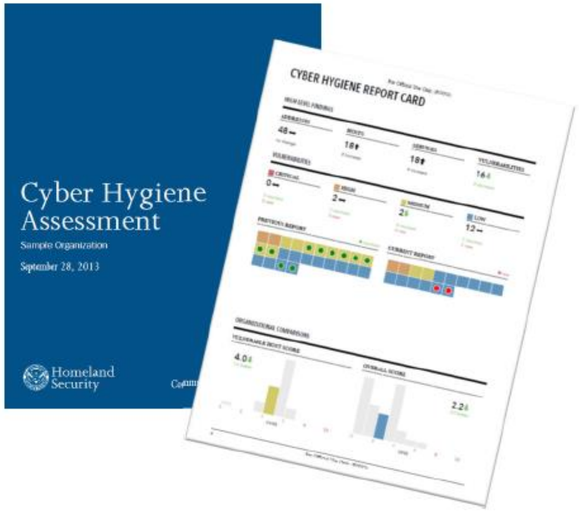
Delivery: Identify public-facing Internet security risks, through service enumeration and vulnerability scanning online by CISA.

Benefits:

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

Network Vulnerability & Configuration Scanning:

- Identify network vulnerabilities and weakness



Cyber Hygiene Assessment

Sample Organization

September 28, 2013

Homeland Security

CYBER HYGIENE REPORT CARD

HIGH LEVEL FINDINGS

ADDRESSES 48

HOSTS 18

SERVICES 18

VULNERABILITIES 16

VULNERABILITIES

CRITICAL 0

HIGH 2

MEDIUM 2

LOW 12

PREVIOUS REPORT

CURRENT REPORT

ORGANIZATIONAL COMPARISONS

VULNERABLE HOST SCORE 4.0

OVERALL SCORE 2.2

Vulnerability Scanning Report Card

High Level Findings

□ Latest Scans

□ Addresses Owned

□ Addresses Scanned

□ Hosts

□ Services

□ Vulnerable Hosts

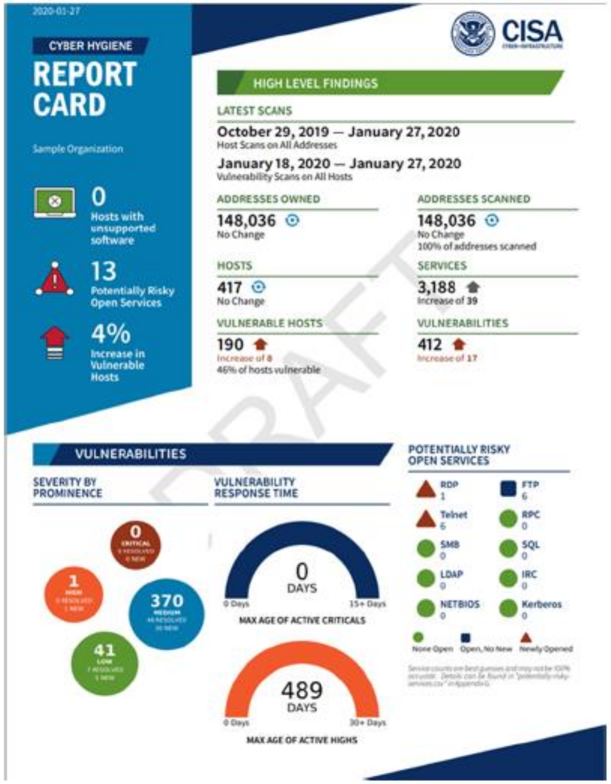
□ Vulnerabilities

Vulnerabilities

□ Severity by Prominence

□ Vulnerability Response Time

□ Potentially Risky Open Services



2020-01-27

CYBER HYGIENE

REPORT CARD

Sample Organization

CISA

0 Hosts with unsupported software

13 Potentially Risky Open Services

4% Increase in Vulnerable Hosts

HIGH LEVEL FINDINGS

LATEST SCANS

October 29, 2019 — January 27, 2020
Host Scans on All Addresses

January 18, 2020 — January 27, 2020
Vulnerability Scans on All Hosts

ADDRESSES OWNED
148,036
No Change

ADDRESSES SCANNED
148,036
No Change
100% of addresses scanned

HOSTS
417
No Change

SERVICES
3,188
Increase of 39

VULNERABLE HOSTS
190
Increase of 8
46% of hosts vulnerable

VULNERABILITIES
412
Increase of 17

VULNERABILITIES

SEVERITY BY PROMINENCE

VULNERABILITY RESPONSE TIME

MAX AGE OF ACTIVE CRITICALS

MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

▲ RDP 1	■ FTP 6
▲ Telnet 6	● RPC 0
● SMB 0	● SQL 0
● LDAP 0	● IRC 0
● NETBIOS 0	● Kerberos 0

● None Open ■ Open, No New ▲ Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

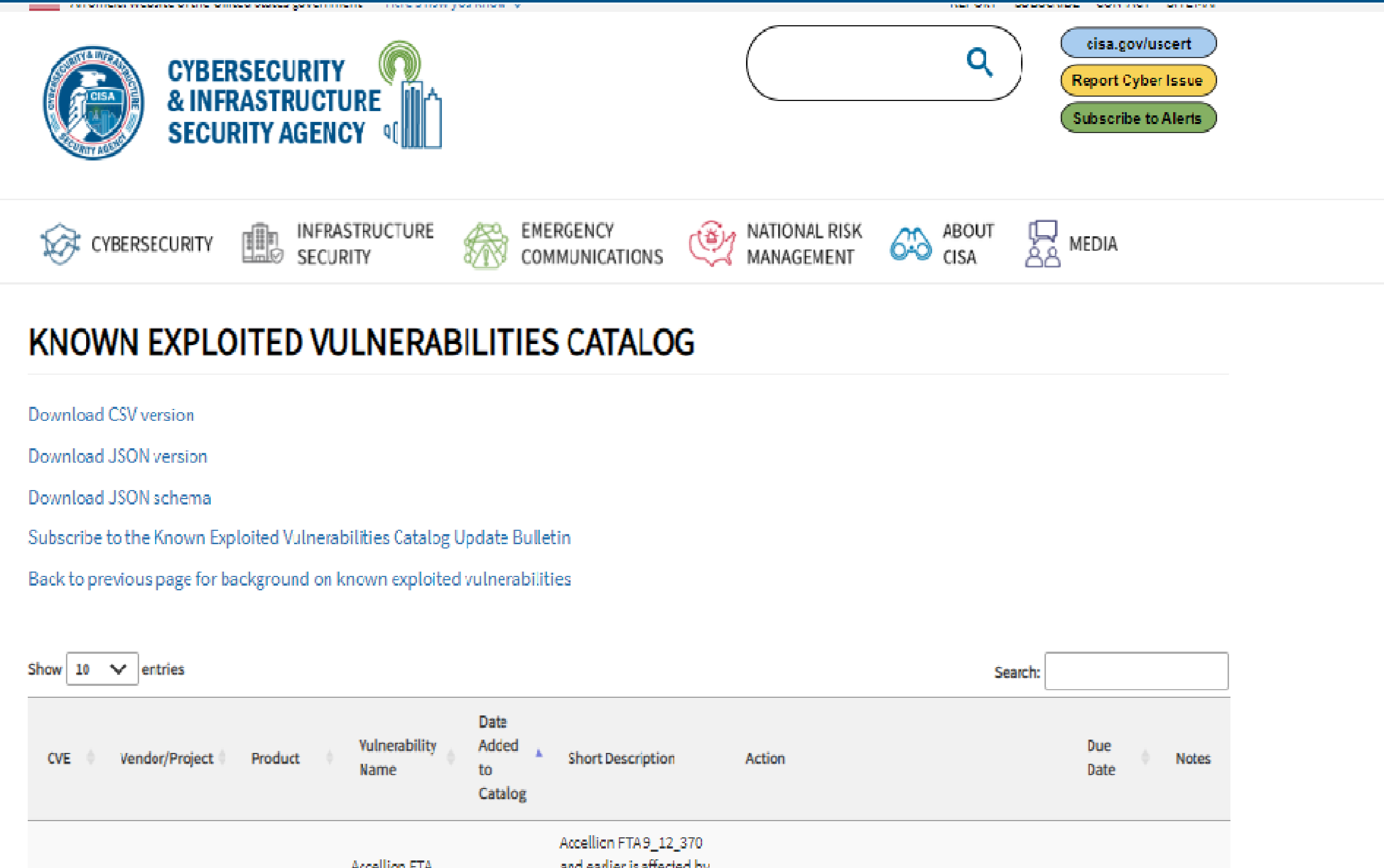
CISA Shields Up

CISA Shields Up Portal

CISA Cyber Resource Hub

CISA Cyber Resource Hub

CISA Known Exploited Vulnerabilities Catalog (KEV)



KNOWN EXPLOITED VULNERABILITIES CATALOG

Download CSV version

Download JSON version

Download JSON schema

Subscribe to the Known Exploited Vulnerabilities Catalog Update Bulletin

Back to previous page for background on known exploited vulnerabilities

Show 10 entries

Search:

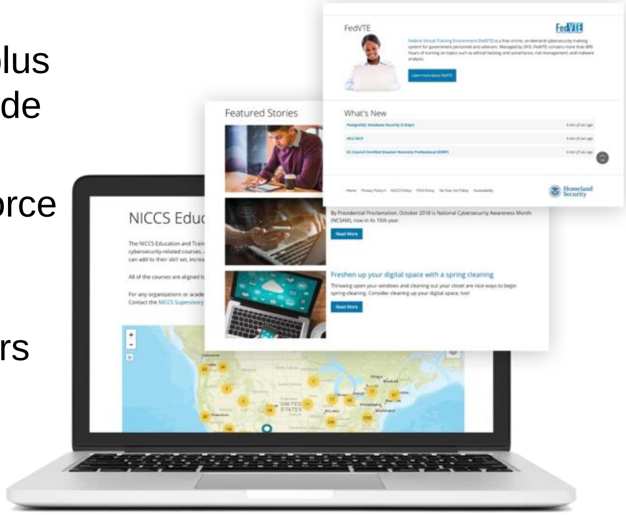
CVE	Vendor/Project	Product	Vulnerability Name	Date Added to Catalog	Short Description	Action	Due Date	Notes
			Accellion FTA		Accellion FTA9_12_370 and earlier is affected by			

Cybersecurity Training Resources

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

The NICCS website includes:

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



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

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

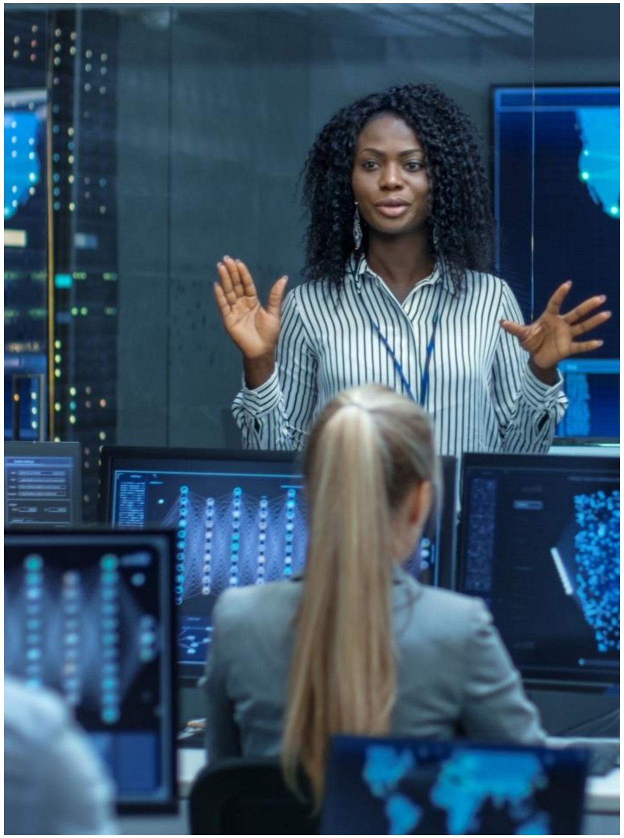
Collect & Operate

Oversight & Development

Protect & Defend

Investigate

Contact



General Inquiries

CISARegion4@hq.dhs.gov

CISA Contact Information

Sean McCloskey Chief of Cybersecurity CISA Region 4	**Sean.McCloskey@hq.dhs.gov**

Incident Reporting

central@cisa.gov

Cybersecurity and Infrastructure Security Agency

CISA
CYBER+INFRASTRUCTURE

U.S. DEPARTMENT OF HOMELAND SECURITY

CISA

CYBER+INFRASTRUCTURE