

U.S. Department of Homeland Security

---

# **CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY**



CYBERSECURITY &  
INFRASTRUCTURE  
SECURITY AGENCY

# Cybersecurity and Infrastructure Security Agency (CISA)

## VISION

Secure and resilient  
infrastructure for the  
American people.

## MISSION

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



## OVERALL GOALS

### GOAL 1

#### DEFEND TODAY

Defend against urgent  
threats and hazards

seconds | days | weeks

### GOAL 2

#### SECURE TOMORROW

Strengthen critical  
infrastructure and  
address long-term risks

months | years | decades

CYBERSECURITY &  
INFRASTRUCTURE  
SECURITY AGENCY

# Our Work

The Cybersecurity and Infrastructure Security Agency (CISA) works with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future



PARTNERSHIP  
DEVELOPMENT



INFORMATION AND  
DATA SHARING



CAPACITY BUILDING



INCIDENT  
MANAGEMENT  
& RESPONSE



RISK ASSESSMENT  
AND ANALYSIS
















NETWORK DEFENSE



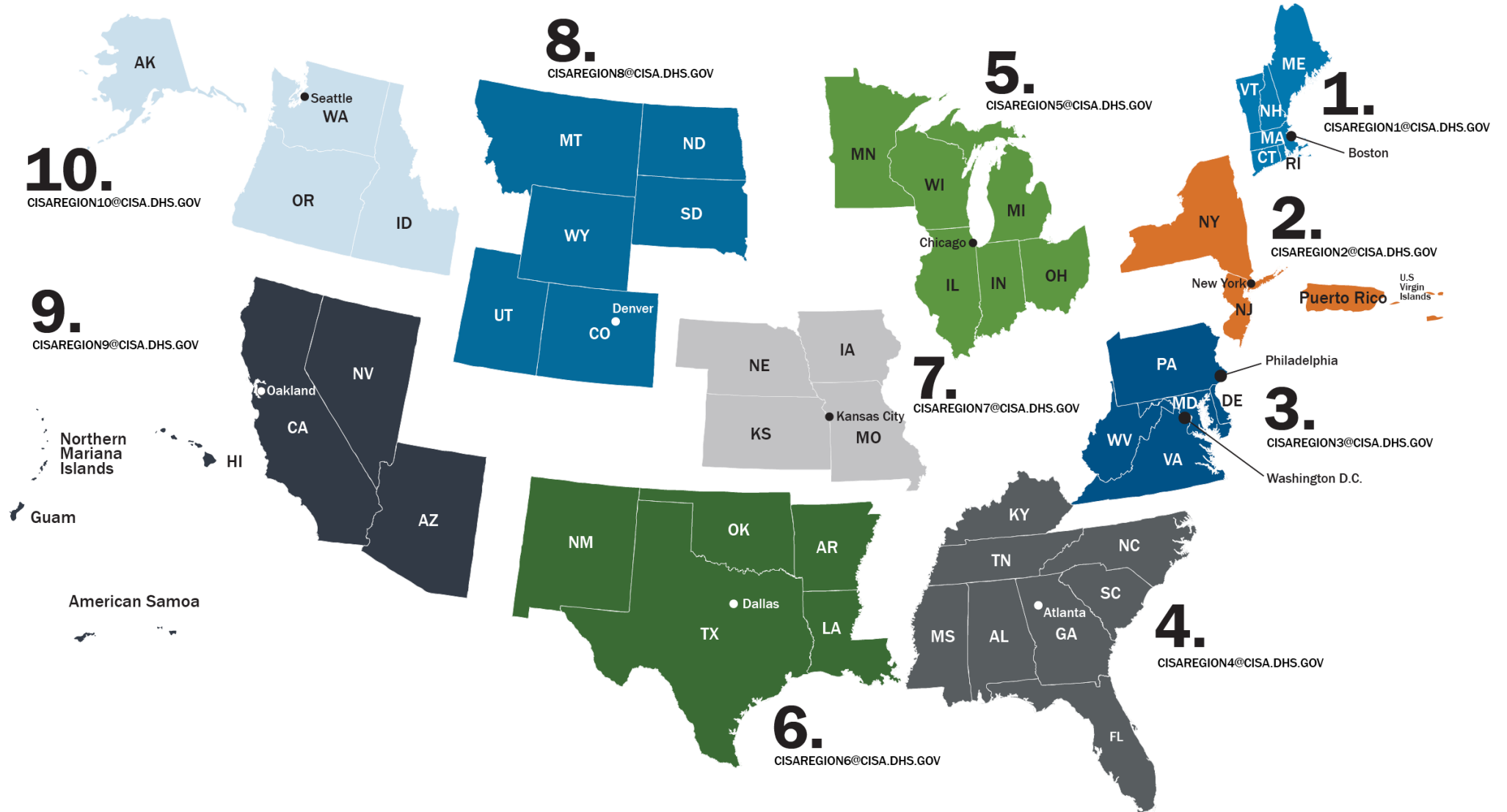
EMERGENCY  
COMMUNICATIONS

# 16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

 <b>CHEMICAL</b> <b>CISA</b>	 <b>FINANCIAL</b> <b>Treasury</b>
 <b>COMMERCIAL FACILITIES</b> <b>CISA</b>	 <b>FOOD &amp; AGRICULTURE</b> <b>USDA &amp; HHS</b>
 <b>COMMUNICATIONS</b> <b>CISA</b>	 <b>GOVERNMENT FACILITIES</b> <b>GSA &amp; FPS</b>
 <b>CRITICAL MANUFACTURING</b> <b>CISA</b>	 <b>HEALTHCARE &amp; PUBLIC HEALTH</b> <b>HHS</b>
 <b>DAMS</b> <b>CISA</b>	 <b>INFORMATION TECHNOLOGY</b> <b>CISA</b>
 <b>DEFENSE INDUSTRIAL BASE</b> <b>DOD</b>	 <b>NUCLEAR REACTORS, MATERIALS AND WASTE</b> <b>CISA</b>
 <b>EMERGENCY SERVICES</b> <b>CISA</b>	 <b>TRANSPORTATIONS SYSTEMS</b> <b>TSA &amp; USCG</b>
 <b>ENERGY</b> <b>DOE</b>	 <b>WATER</b> <b>EPA</b>

# CISA Regions

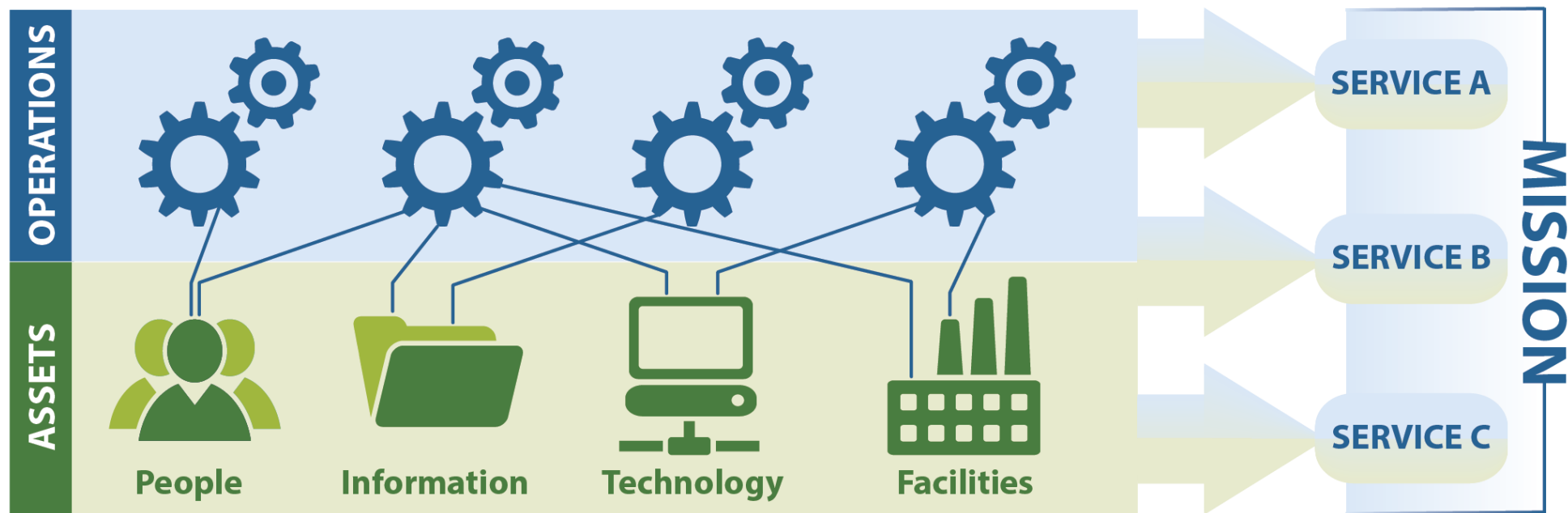
1. Boston, MA
2. New York, NY
3. Philadelphia, PA
4. Atlanta, GA
5. Chicago, IL
6. Dallas, TX
7. Kansas City, MO
8. Denver, CO
9. Oakland, CA
10. Seattle, WA



# Defining the Critical Services

## Conduct a Business Impact Analysis!

An organization uses its **assets (people, information, technology, and facilities)** to perform **productive activities** to provide operational **services** and accomplish the organization's **mission**.



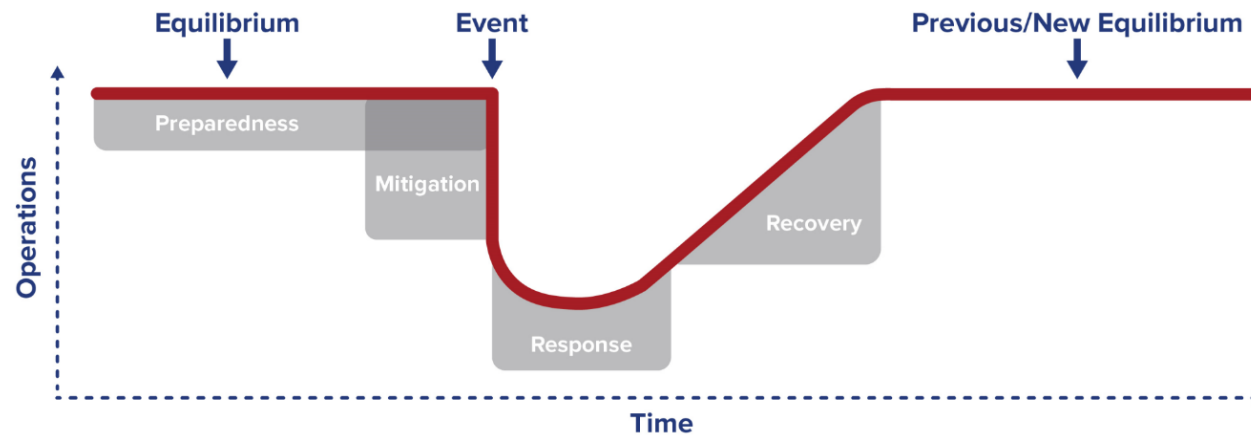
# Cyber Operational Buckets

## Bucket # 1 (left of bang)

Prevention, education and training, outreach, sharing best practices, and provide security resources.

## Bucket # 2 (right of bang)

Incident mitigation, investigations, reporting, recovery, and resiliency efforts



# Security Advisor Programs

**Security Advisors** are field-based critical infrastructure security specialists who link State, local, tribal, territorial (SLTT) & private sector stakeholders with infrastructure protection resources

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

**Protective Security Advisors (PSA):** Security, Emergency Preparedness, and Business Continuity Programs

**Cybersecurity Advisors (CSA):** Cybersecurity for Information Technology & Operational Technology networks





# Health Industry Cybersecurity Practices (HICP) 2023

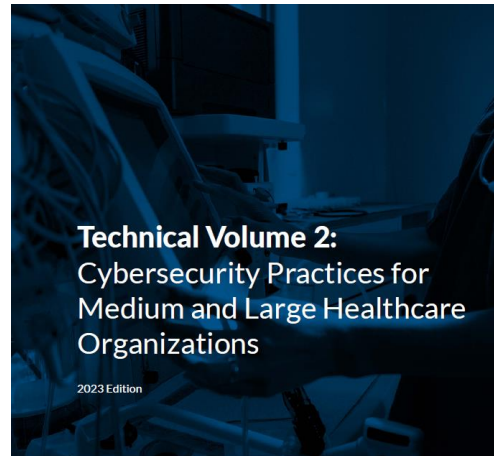
## 405(d)'s Cornerstone Publication

Cybersecurity threats evolve each year and with them comes new mitigating practices. The HICP 2023 Edition has been updated by industry and government professionals to include the most relevant and cost-effective ways to mitigate the current cybersecurity threats the HPH sector is facing. After significant analysis of the current cybersecurity issues facing the healthcare industry, the 405(d) Task Group agreed on the development of three HICP components—a main document and two technical volumes, and a robust appendix of resources and templates.

The **Main Document** examines cybersecurity threats and vulnerabilities that affect the healthcare industry. It explores five (5) current threats and presents ten (10) practices to mitigate those threats.

**Technical Volume 1** discusses these ten cybersecurity practices for small healthcare organizations.

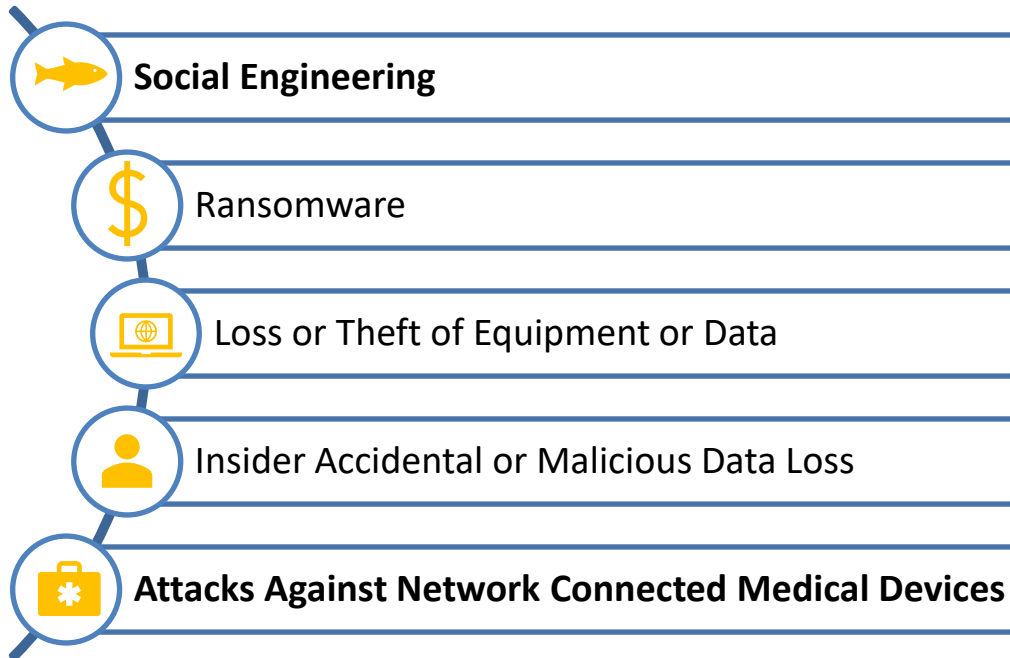
**Technical Volume 2** discusses these ten cybersecurity practices for medium and large healthcare organizations.



Healthcare & Public Health  
Sector Coordinating Council  
PUBLIC PRIVATE PARTNERSHIP

# HICP Top 5 Threats & Top 10 Practices

## Top 5 Threats



## Top 10 Practices

1. Email Protection Systems
2. Endpoint Protection Systems
3. Identity and Access Management
4. Data Protection and Loss Prevention
5. Asset Management
6. Network Management
7. Vulnerability Management
8. Security Operations Center and Incident Response
9. Network Connected Medical Device Security
- 10. Cybersecurity Oversight and Governance**

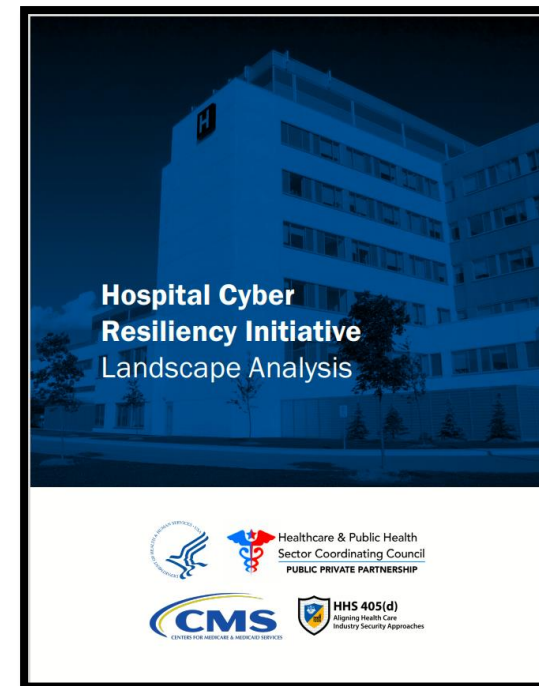


# Hospital Cyber Resiliency Initiative Landscape Analysis

The HPH Sector has faced dramatic increases in cyber-attacks intended to cause disruption to the care continuum. In response to this growing threat, the HHS 405(d) Program conducted Landscape Analysis, which reviewed active threats attacking hospitals and the cybersecurity capabilities of hospitals operating in the United States.

## Document Overview:

- **Executive Summary** –overview of key observations, HICP Practice Adoption and a note on Data sources
- **Threat Analysis** –overview of the evolving threat of ransomware and links between threats and mitigations
- **Capabilities and Performance Assessment**- covers staff analysis, cyber expense, coverage to NIST and HICP
- **Adoption of HICP Practices** – covers practices in HICP that have significant progress, need improvement, and need additional research, and non urgent items



\*Data Sources: The quantitative data was gathered by utilizing CHIME's Most Wired Surveys, a separate survey in partnership with Censinet and the American Hospital Association of 59 hospitals, and 20 conversations with geographically and demographically diverse hospitals

# Key Observations

HHS 405(d) analysis from the two (2) quantitative studies combined with participating hospital conversations resulted in a series of key observations - See below for a few

- 1. Directly targeted ransomware attacks aimed to disrupt clinical operations are an outsized and growing cyber threat to hospitals**
- 2. Variable adoption of critical security features and processes, coupled with a continually evolving threat landscape can expose hospitals to more cyber-attacks**
  1. Adoption of MFA is taking place in over 90% of surveyed hospitals- why not 100%?
  2. 89% of the hospitals surveyed indicated that they were conducting regular vulnerability scanning at least on a quarterly basis
  3. 86% of the hospitals surveyed responded that their users are informed and trained on performing their cybersecurity related duties and responsibilities
  4. The delivery of in-home care, accelerated by COVID-19, is growing and expanding the cyber threat landscape
- 3. Hospitals report measurable success in implementing email protections, which is a key attack vector**
- 4. Supply chain risk is pervasive for hospitals. Only 49% of hospitals state they have adequate coverage in managing risks to supply chain risk management**
- 5. Medical devices have not typically been exploited to disrupt clinical operations in hospitals.**



# Key Observations Continued...

## 6. There is significant variation in cybersecurity resiliency among hospitals

## 7. The use of antiquated hardware, systems, and software by hospitals is concerning

- 96% of small, medium, and large sized hospitals claim they were operating with end-of-life operating systems or software with known vulnerabilities, which is inclusive of medical devices.

## 8. Cybersecurity insurance premiums continue to rise

- On average, cybersecurity premiums increased by 46% in 2021. Five of fifty-six hospitals surveyed in 2022 experienced increases more than 100%, whereas 32 experienced increases just below 35%.

## 9. Securing cyber talent with requisite skills and experience is challenging

## 10. Adopting HICP improves cyber resiliency

- An interesting correlation that was uncovered during analysis was a strong connection between those who have adopted HICP and robust NIST CSF coverage. This indicates that organizations that focus on HICP Practices will gain value and benefit towards managing implementation of the NIST CSF cybersecurity framework.



# Threat Analysis

HHS 405(d) assessment, based on the data sources used, identified numerous cybersecurity threats to U.S. hospitals, such as:

1. Ransomware and Ransomware-as-a-Service (RaaS) attacks
2. Cloud exploitations by threat actors; with data suggesting a 95% increase from 2021 in cloud exploitation cases
3. Phishing/Spear-Phishing Attacks; specifically those attacks that overcome MFA through social engineering
4. Software and zero-day vulnerabilities
5. Distributed Denial of Service attacks (DDoS)

## Threat Analysis- Key Take Aways

- Human Directed Attacks make up 71% of attacks
- Access Broker theft up 112%, used by the human directed attacks
- Time to move off initial intrusion point is 1 hour 28 minutes (this is the lateral movement off the originally compromised host to another stage to obfuscate)





# 405(d) Knowledge on Demand

The 405(d) Program, in collaboration with industry, is launching a new cybersecurity training platform on its website—[405d.hhs.gov](https://405d.hhs.gov)—titled Knowledge on Demand. This new cybersecurity education platform will include multiple delivery methodologies to reach the varied size health care facilities across the country. The platform will include five cybersecurity awareness trainings that align with the top five cybersecurity threats outlined in the landmark 405(d) publication: The Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients (HICP) and its accompanying two volumes.

## The delivery methodologies for Knowledge on Demand include:



### Job Aids

These are single documents with key tips related to the topic. This format is meant to be used as an "on-the-job" resource tool. They can provide instructional steps if necessary to meet the training objectives.

**Key Benefits:** Job aids are useful since an employee can reference one throughout the day-to-day operations. They can also act as reminders about topics covered in more formal trainings.



### Learning Management System (LMS) File

Content intended for an LMS will be similar in look and experience as the previously discussed Interactive Training video. Content will be exported and saved to a file type compatible for import to an organization's LMS platform.

**Key Benefits:** This delivery method will allow larger organizations that already have an LMS platform and want to add our content directly to their system. This will be especially useful if they do not already have cybersecurity training courses.



### Interactive Training Videos

These videos are launched from the 405(d) KOD webpage but can also be downloaded by the end user. They include recorded audio to take the trainee through the video along with interactive content to include knowledge checks and animations.

**Key Benefits:** This interactive delivery method provides end users flexibility to access each threat topic at their own time due to the easy of access from the website.

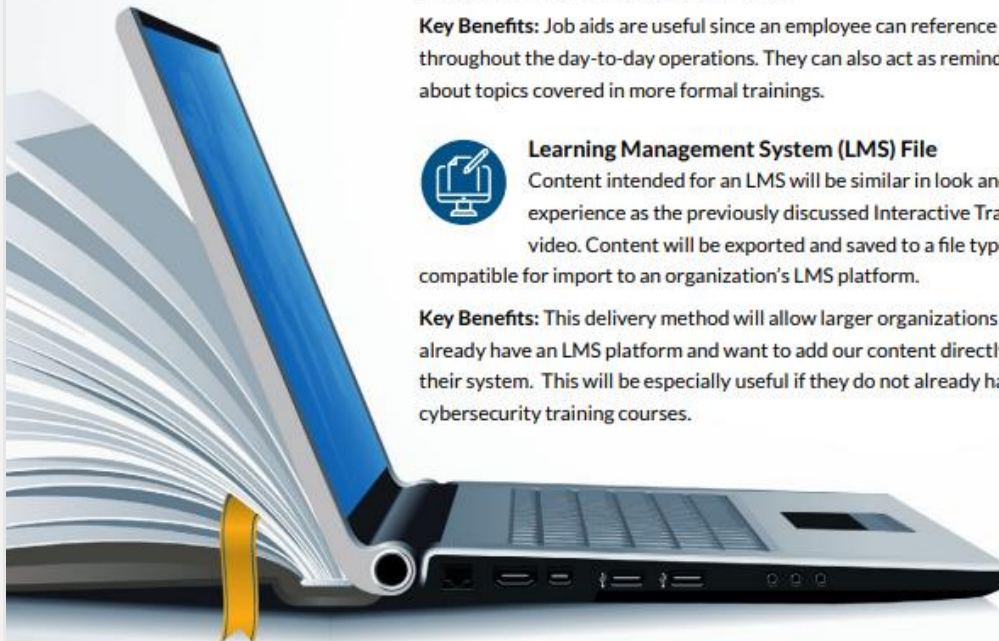


### PowerPoint Trainings

These can be leveraged for in person or on-site presentations. These will include facilitator notes with slide specific content and knowledge checks to reinforce learning. Such presentations can be delivered in presentation mode or in a "Lunch n Learn" format at your location.

**Key Benefits:** PowerPoint presentations are useful tools because they encourage discussion between employees and managers. It also allows the organization to better tailor their training to meet their specific needs.

Visit our website at [405d.hhs.gov/KOD](https://405d.hhs.gov/KOD) to experience this new learning platform and explore the ways you can integrate this platform into the awareness education for all employees at your healthcare organization.



# PSA Assessments



## Security Walk-Through Assessment

- Programs Reviewed
  - Security
  - Emergency Preparedness
  - Business Continuity
- Time Requirement = Site Dependent; Tour of facility(s) followed by conference room meeting
- Written report **NOT** provided

## Security Assessment at First Entry (SAFE)

- Programs Reviewed
  - Security
  - Emergency Preparedness
  - Business Continuity
- Time Requirement = Site Dependent; Tour of facility(s) followed by conference room meeting
- Written report provided

## Infrastructure Survey Tool (IST)

- Programs Reviewed
  - Security
  - Emergency Preparedness
  - Business Continuity
  - Dependencies/Interdependencies
  - Information Technology
- Time Requirement = Typically two full days
- Written report provided





# Cyber Services Planning - Initial

## Step One

### Cyber Protective Visit (CPV):

- Initial visit with a Cyber Security Advisor (CSA) to gauge interest in CISA services, understand the organization's needs, and develop the foundation for further engagements and offerings.

## Step Two

### Cyber Hygiene Vulnerability Scanning (CyHy):

- 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

### Cyber Performance Goals (CPGs):

- A set of high-impact security actions for critical infrastructure organizations that address both IT and OT/ICS considerations.
- Mapped to the relevant NIST Cybersecurity Framework subcategories, as well as other frameworks (e.g., IEC 62443).

## Step Three

### Ongoing Partnership:

- Information sharing
- **Assessments**
- Tabletop Exercises
- Presentations
- Connection to resources
- Incident Support



# Cyber Hygiene Services - Intermediate

## Web Application Scanning

**Services provided by invite only**

- **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



## Remote Penetration Testing (RPT)

**Services provided by invite only**

- **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.

# Cyber Hygiene Services - Advanced

## Risk and Vulnerability Assessment (RVA)

### Services provided by invite only

- **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

## Validated Architectural Design and Review (VADR)

### Services provided by invite only

- **Objectives**
- 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

## Critical Product Evaluation (CPE)

### Services provided by invite only

- **Objectives**
- Enumerate the vulnerabilities associated with the product's in-scope software, firmware, and hardware.
- Attempt exploitation of vulnerabilities that pose the greatest risk, using known exploits or new code/techniques.
- Assist in developing remediation or mitigation strategies.



# Protected Critical Infrastructure Information Program - PCII

## 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.



# Training and Presentations

- CISA 101
- Active Shooter
- Bombing Threat Management
- Bombing Prevention
- Insider Threat
- Cybersecurity Awareness
- Elections Security
- Targeted Violence
- De-Escalation Training for CI
- Securing Public Gatherings
- Hometown Security
- School Security
- Security of Soft Targets and Crowded Places
- See Something, Say Something
- Counter Unmanned Aircraft Systems
- Power of Hello
- Workplace Security
- Cyber Incident Response



# Exercises



## Discussion-based Exercises

Seminar

Workshop

Tabletop

## Operations-based Exercises

Drill

Functional

Full-Scale

---

### Examples

- Natural Hazards
- Active Shooter
- Complex Coordinated Terrorist Attack
- Vehicle Ramming
- Improvised Explosive Device (IED)
- Phishing
- Ransomware
- Loss of Personally Identifiable Information (PII)
- Industrial Control Systems Compromise



# Information Sharing & Analysis Centers (ISACs)

- American Chemistry Council
- Automotive ISAC
- Aviation ISAC
- Communications ISAC
- Downstream Natural Gas ISAC
- Elections Infrastructure ISAC
- Electricity ISAC
- Emergency Management & Response ISAC
- Financial Services ISAC
- Food and AG ISAC
- Healthcare Ready
- Health ISAC
- Information Technology ISAC
- Maritime Transportation System ISAC
- Media & Entertainment ISAC
- Multi-State ISAC
- National Defense ISAC
- Oil & Natural Gas ISAC
- Real Estate ISAC
- Research & Education Networks ISAC
- Retail & Hospitality ISAC
- Small Broadband ISAC
- Space ISAC
- Surface Transportation, Public Transportation & Over-the-Road Bus ISACS
- Water ISAC



# Multi-State - Infrastructure Information Sharing & Analysis Center (MS-ISAC)

<https://www.cisecurity.org/ms-isac>

## Services Included with Membership

- |                                                                   |                                               |
|-------------------------------------------------------------------|-----------------------------------------------|
| • 24/7 Security Operation Center                                  | • Weekly Top Malicious Domains/IP Report      |
| • Incident Response Services                                      | • Monthly Members-only Webcasts               |
| • Cybersecurity Advisories and Notifications                      | • Access to Cybersecurity Table-top Exercises |
| • Access to Secure Portals for Communication and Document Sharing | • Vulnerability Management Program (VMP)      |
| • Cyber Alert Map                                                 | • Nationwide Cyber Security Review (NCSR)     |
| • Malicious Code Analysis Platform (MCAP)                         | • Awareness and Education Materials           |

<https://learn.cisecurity.org/ms-isac-registration>





# Federal Incident 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.

## National Cyber Investigative Joint Task Force (NCIJTF)

CyWatch 24/7 Command Center: [cywatch@ic.fbi.gov](mailto: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.

## 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.

## CISA Central

(888) 282-0870 or

[Central@cisa.dhs.gov](mailto:Central@cisa.dhs.gov)

## Cybersecurity and Infrastructure Security Agency (CISA)

<https://www.cisa.gov/forms/report>

- The CISA Incident Reporting System provides a secure web-enabled means of reporting computer security incidents to CISA. This system assists analysts in providing timely handling of your security incidents as well as the ability to conduct improved analysis.

## 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](mailto:soc@msisac.org)**

## Center for Internet Security (CIS)

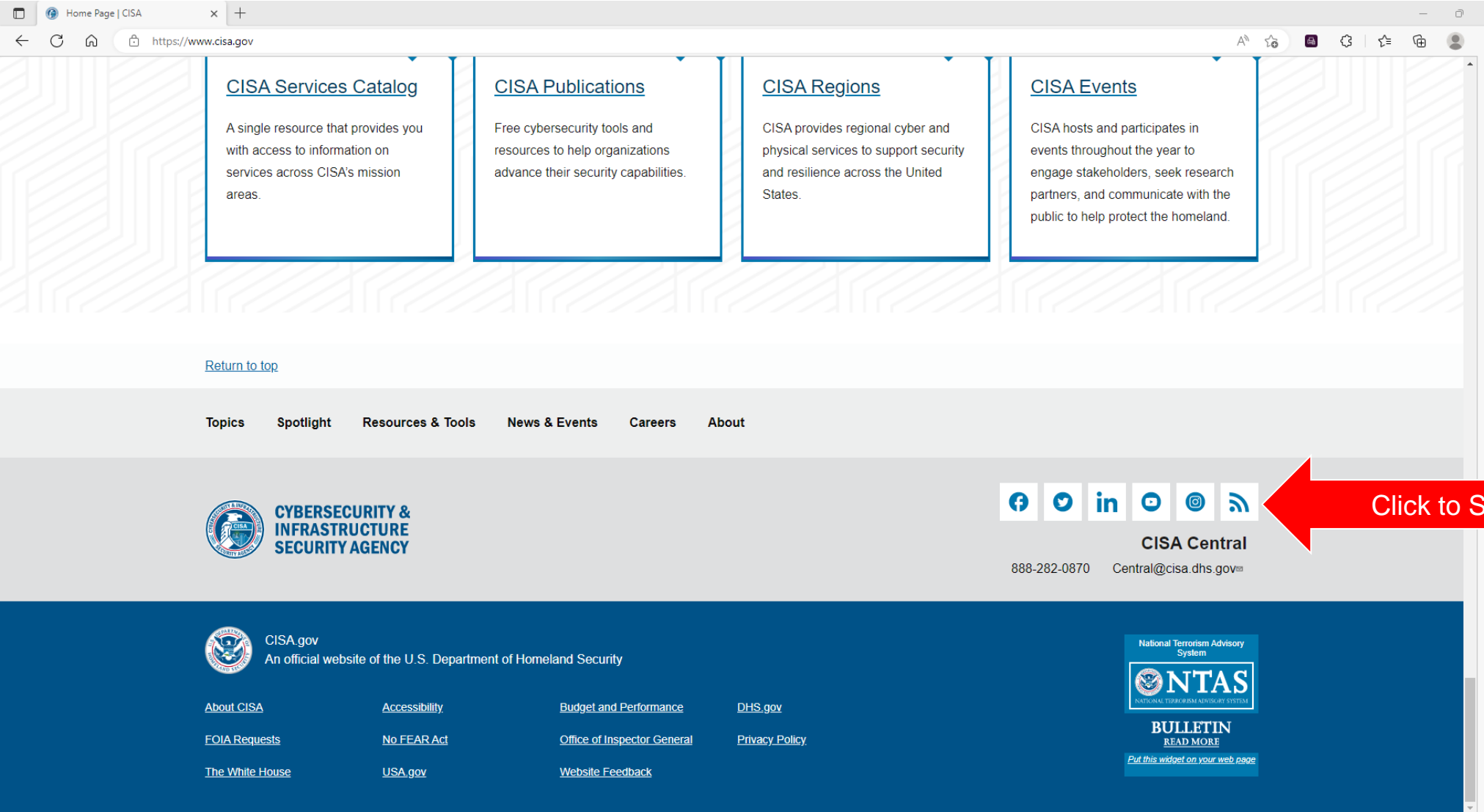
- Albert Sensors (Intrusion Detection)
- Vulnerability Management
- Baseline Configuration Guides
- Assessment Tools



# Available Cyber Services & Tools

- Cyber Hygiene Services
- Known Exploited Vulnerabilities (KEV) Catalog
- Bad Practices Catalog
- Get Your Stuff Off Search
- No Cost Tools & Service Catalog:
  - Antivirus
  - Malware Removal
  - Investigation
  - Log analysis
  - Scanning
  - Network packet captures
  - Protocol analyzer
  - Intrusion detection & prevention
  - Threat modeling
  - Backup







**WARREN HAGELSTIEN**

**Cybersecurity Advisor**

**Email: [warren.hagelstien@cisa.dhs.gov](mailto:warren.hagelstien@cisa.dhs.gov)**

**NICHOLAS BRAND**

**Cybersecurity Advisor**

**Email: [nicholas.brand@cisa.dhs.gov](mailto:nicholas.brand@cisa.dhs.gov)**

**GREGORY GOODWATER**

**Protective Security Advisor**

**Email: [gregory.goodwater@cisa.dhs.gov](mailto:gregory.goodwater@cisa.dhs.gov)**

