

# CISA CYBERSECURITY SERVICES

Joseph Frohlich  
Cybersecurity Coordinator, Montana



# CISA

**CYBERSECURITY &  
INFRASTRUCTURE  
SECURITY AGENCY**

# Cybersecurity and Infrastructure Security Agency (CISA)

## VISION

Secure and resilient infrastructure for the American people.

## MISSION

Lead the national effort to understand, manage, and reduce risk to the nation's cyber and physical infrastructure.



# CISA's Core Capabilities

## AT A GLANCE



PARTNERSHIP DEVELOPMENT



INFORMATION AND DATA SHARING



CAPACITY BUILDING



INCIDENT MANAGEMENT & RESPONSE



RISK ASSESSMENT AND ANALYSIS



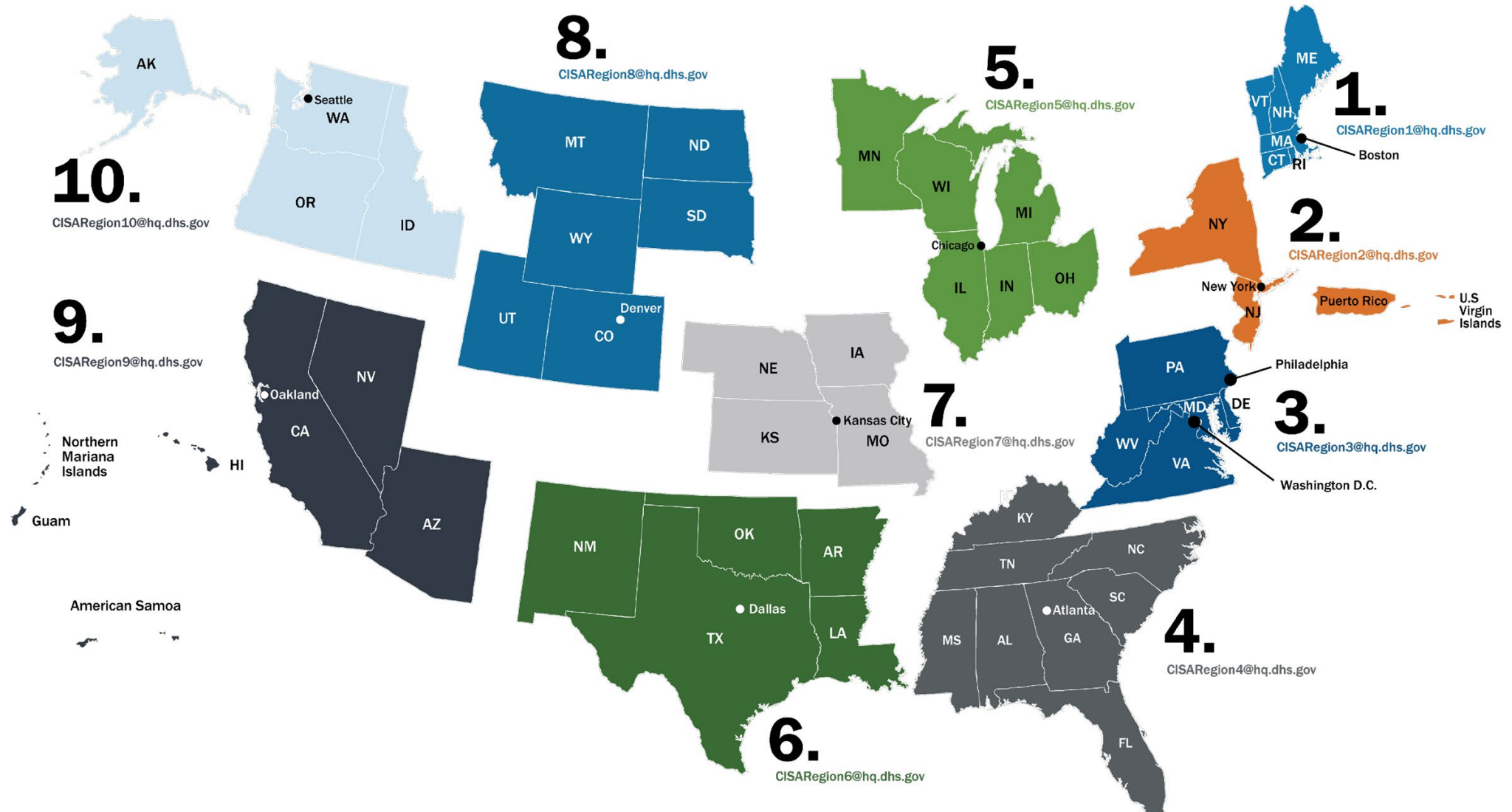
NETWORK DEFENSE



EMERGENCY COMMUNICATIONS

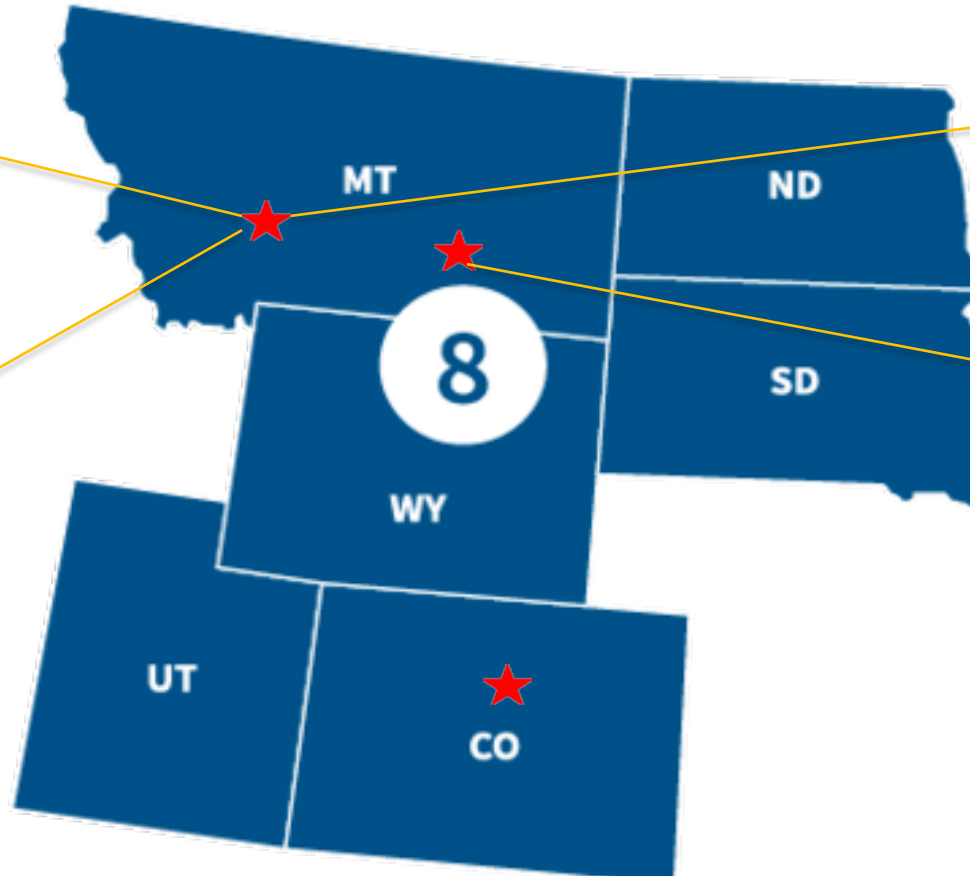
# CISA Regions

- 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



# CISA Region 8 – Montana Cadre

















CISA Cyber Security Advisors
<b>Joe Frohlich</b> <i>Cybersecurity State Coordinator (CSC)</i> <i>State &amp; Local Government,</i> <i>K-12, Higher Education</i> <i>Helena</i>
<b>Travis Light</b> <i>Cybersecurity Advisor (CSA)</i> <i>Critical Infrastructure Focus</i> <i>Helena</i>



CISA Protective Security Advisors
<b>Randy Middlebrook</b> <i>Protective Security Advisor (PSA)</i> <i>Helena</i>
<b>Albert Mendoza</b> <i>Protective Security Advisor (PSA)</i> <i>Billings</i>



# 16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

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



## Healthcare and Public Health Sector

The Healthcare and Public Health Sector focuses on population health and provides the response and recovery actions needed after large-scale hazards such as terrorism, infection disease, and natural disasters.



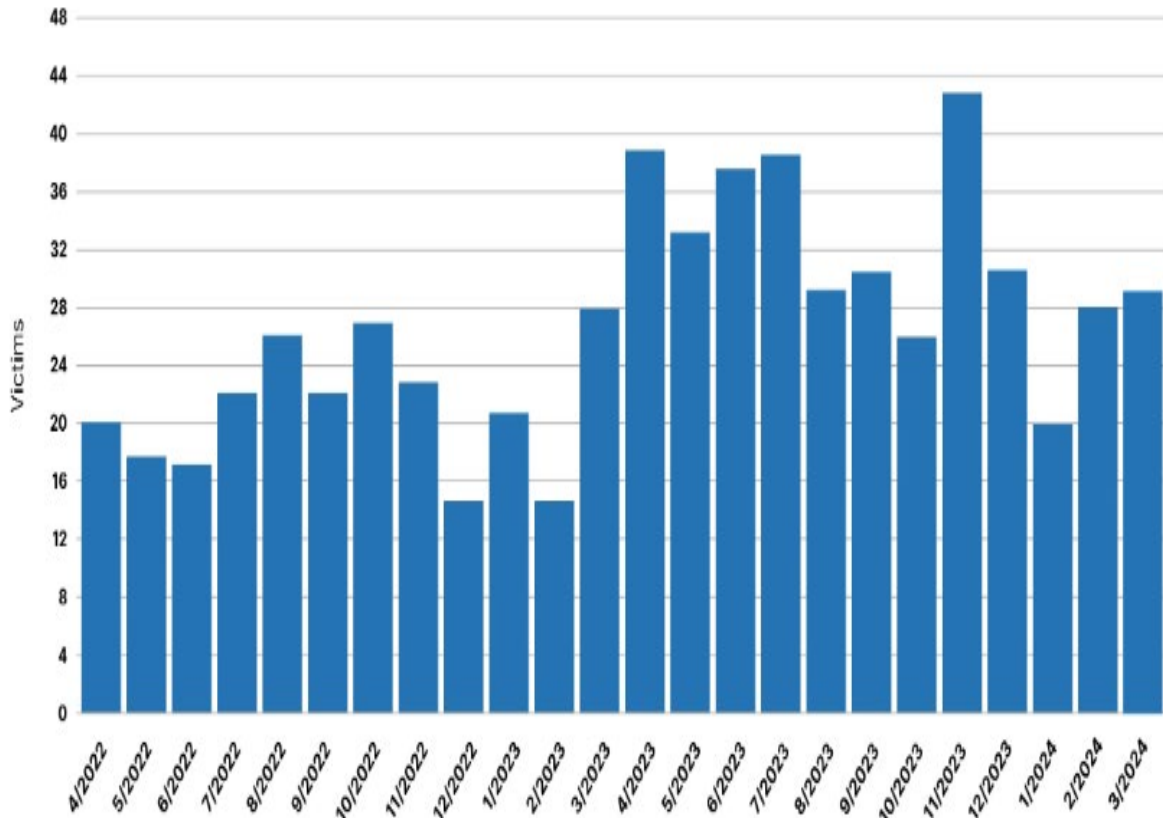
# Whose Job is Cybersecurity?



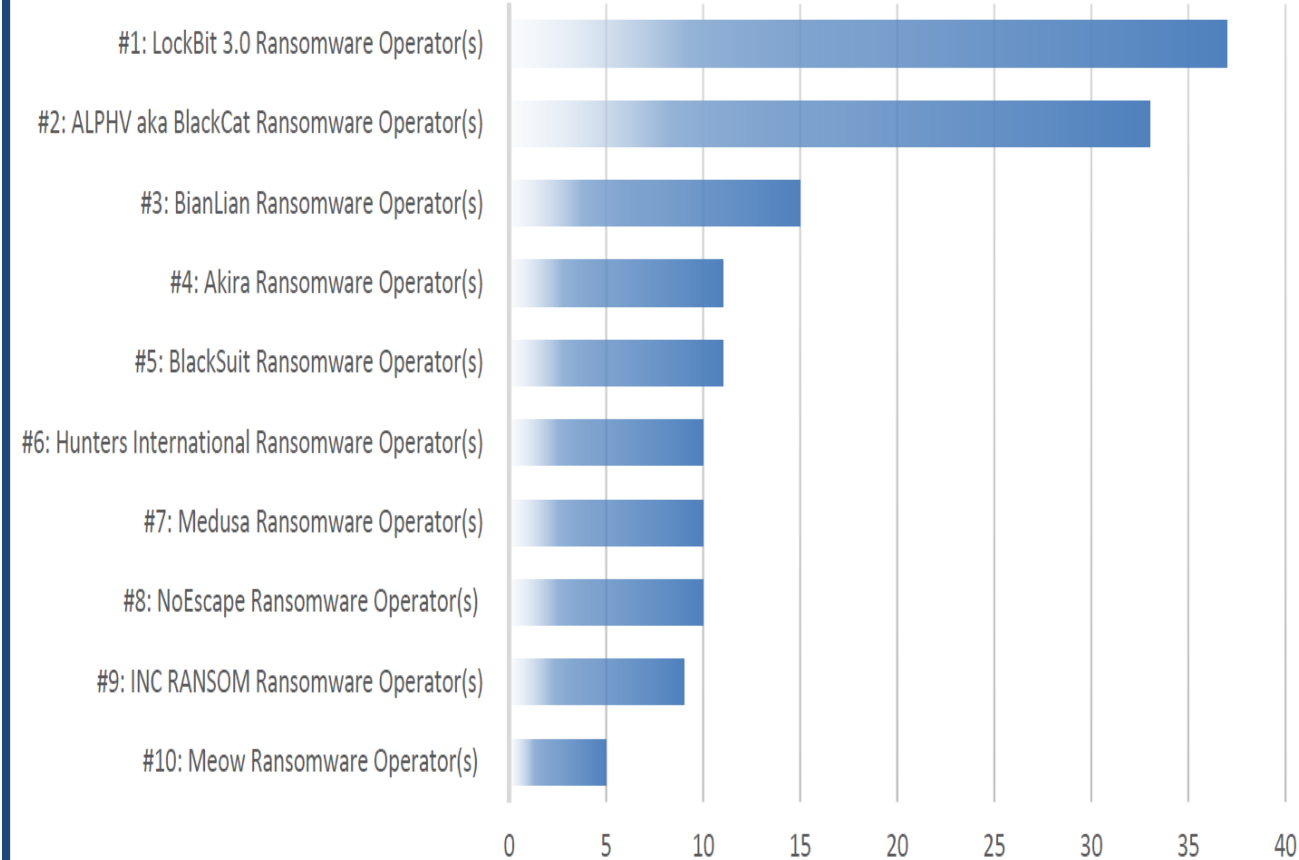
# The Threat is Real

The Record.  
Recorded Future News

Reported Ransomware Attacks on Healthcare Providers



## HC3'S TOP 10 MOST ACTIVE RANSOMWARE GROUPS (LAST SIX MONTHS)





# The Threat is Real – Here in Montana

## Montana State University Ransomware Attack, Hackers Steal Over 100GB Data

The cyberattack has disrupted MSU's services, and the University Information Technology (UIT) team is working to restore the services.



by Ashish Khaitan — May 2, 2023 in Data Breach News, Firewall Daily



## Montana health record hackers compromise 1.3 million people

By Laura Zuckerman


3 MIN READ




(Reuters) - A data security breach of Montana's state health records has compromised the Social Security numbers and other personal information of some 1.3 million people, but the full extent of damage from the intrusion is unclear, state officials said on Tuesday.

[Montana State University Ransomware Attack | The Cyber Express](#)

[Hackers Compromise 1.3 Montanans Health Records | Reuters](#)



Office of Information Security  
Securing One HHS




Health Sector Cybersecurity  
Coordination Center

### HC3: Analyst Note


January 30, 2023 TLP:CLEAR Report: 202301301200

**Pro-Russian Hacktivist Group 'KillNet' Threat to HPH Sector**





YOU HAVE BEEN HACKED  
DOWN WITH ISRAEL الموت لإسرائيل  
EVERY EQUIPMENT "MADE IN ISRAEL" IS CYBER AVENGERS LEGAL TARGET



UnitedHealthcare

The corporate logo of the UnitedHealth Group appears on the side of one of their office buildings in Santa Ana, California, U.S., April 13, 2020. REUTERS/Mike Blake/Purchase/Corbis/Bettmann

Joe Frohlich  
June 10, 2024

# CISA/HHS Cybersecurity Toolkit

- Released Oct 25<sup>th</sup> 2023
- Consolidates CISA and HHS resources such as:
  - [CISA Cyber Hygiene](#)
  - HHS [Health Industry Cybersecurity Practices](#) (HICP)
  - HPH Sector [Cybersecurity Framework Implementation Guide](#)



[Link to CISA/HHS Toolkit](#)

Joe Frohlich  
June 10, 2024

# CISA/HHS Toolkit Homepage



## Healthcare and Public Health Sector: Know the Risks, Use Cyber Hygiene

Cybersecurity isn't one size fits all. Different healthcare entities have distinct strengths and weaknesses and a wide range of needs. Regardless of where an organization fits into the picture, these resources can help build a cybersecure foundation.



## Healthcare and Public Health Sector: Strengthen your Defenses and Mature your Cybersecurity Efforts

CISA offers industry best practices and resources on training and exercises, incident response planning, priority telecoms services, cyber resilience, tackling ransomware and much more to help healthcare organizations strengthen their defenses.



## Healthcare and Public Health Sector: Address Resource Constraints

Recognizing that the nation's healthcare systems and providers have been under severe resource constraints—especially since the start of COVID-19—members of the HPH sector should actively take steps to address their constraints.



[Link to CISA/HHS Toolkit](#)

# CISA/HHS Toolkit: Cyber Hygiene

## Hospital Cyber Resiliency Landscape Analysis

This joint product developed by HHS and industry includes a deeper investigative study into the methods that cyber adversaries are using to compromise US hospitals, disrupt operations, and extort for financial gain.

## HPH Sector Cybersecurity Framework Implementation Guide, Version 2

This product was developed jointly by HHS and the HSCC Cybersecurity Working Group, in consultation with the Sector Coordinating Council and Government Coordinating Council to help HPH sector organizations.

## Health Industry Cybersecurity Practices (HICP): Managing Threat and Protecting Patients

This product developed jointly by HHS and the HSCC Cybersecurity Working Group outlines the top threats facing the HPH sector and provides recommendations and best practices to prepare and fight against cybersecurity threats.

## Healthcare and Public Health Sector Risk Identification and Site Criticality (RISC) Toolkit

The RISC Toolkit is an objective, data-driven, all-hazards risk assessment that can be used by public and private organizations within the HPH Sector to inform emergency preparedness planning, risk management activities, and resource investments.

## Security Risk Assessment (SRA) Tool

HHS ONC and OCR developed this risk assessment tool designed to assist small and medium-sized organizations operating in the health care sector to identify and assess security risks within their organization.

## Cyber Hygiene Services

Reduce the risk of a successful cyberattack with vulnerability scanning. CISA's Cyber Hygiene Services help secure internet-facing systems from weak configurations and known vulnerabilities and encourages the adoption of best practices.

## Known Exploited Vulnerabilities Catalog

This catalog is the authoritative source of cyber vulnerabilities that have been exploited in the wild. By prioritizing known exploited vulnerabilities, healthcare organizations can significantly reduce their likelihood of compromise.

## Secure Our World

CISA has just launched Secure Our World, a new cybersecurity awareness program aimed at educating individuals and businesses on four easy ways to stay safe online.



[Link to CISA/HHS Toolkit](#)

Joe Frohlich  
June 10, 2024

# CISA/HHS: Resiliency Landscape Analysis



<b>Executive Summary</b>	<b>9</b>
Key Observations.....	9
HICP Practice Adoption.....	15
Data Sources .....	15
<b>Threat Analysis</b>	<b>17</b>
Evolving Threat of Ransomware .....	18
Link Between Threats and Potential Mitigation .....	20
<b>Capabilities and Performance Assessment</b>	<b>26</b>
Staffing Analysis.....	28
Cyber Expense to Revenue Analysis.....	28
Industry Coverage to NIST CSF.....	30
Industry Coverage to HICP .....	32
<b>Adoption of HICP Practices</b>	<b>33</b>
<b>HICP Components with Significant Progress</b> .....	<b>33</b>
HICP Practice: Email Protection Systems .....	33
<b>HICP Components with Urgent Need for Improvement</b> .....	<b>35</b>
HICP Practice: Endpoint Protection Systems.....	35
HICP Practice: Identity and Access Management .....	36
HICP Practice: Network Management.....	37
HICP Practice: Vulnerability Management.....	38
HICP Practice: Security Operations Center and Incident Response .....	39
<b>HICP Components in Need of Additional Research/Follow-up</b> .....	<b>42</b>
HICP Practice: IT Asset Management .....	42
HICP Practice: Cybersecurity Oversight and Governance .....	43
HICP Practice: Network Connected Medical Devices.....	46
<b>HICP Components Where Further Attention is Recommended (Not Urgent)</b> .....	<b>49</b>
HICP Practice: Data Protection and Loss Prevention .....	49

[Link to CISA/HHS Toolkit](#)

# CISA/HHS: Resiliency Landscape Analysis

## Key Findings

- 1) Growing threat of ransomware
- 2) Variable adoption of critical security features
  - 1) MFA
  - 2) Vulnerability Assessments
  - 3) Training & Outreach
  - 4) Hospital-at-Home
- 3) Email protections are way up! ✓
- 4) Supply chain risk is pervasive
- 5) Medical devices generally aren't targeted

No Action Required— Significant Progress Made	Urgent Improvement Needed	Additional Research Required	Further Attention Required (Not Urgent)
<ul style="list-style-type: none"><li>E-mail protection systems</li></ul>	<ul style="list-style-type: none"><li>Endpoint Protection Systems</li><li>Identity and Access Management</li><li>Network Management</li><li>Vulnerability Management</li><li>Security Operation Center and Incident Response</li></ul>	<ul style="list-style-type: none"><li>IT Asset Management</li><li>Network Connected Medical Device Security</li><li>Cybersecurity Oversight and Governance</li></ul>	<ul style="list-style-type: none"><li>Data Protection and Loss Prevention</li></ul>

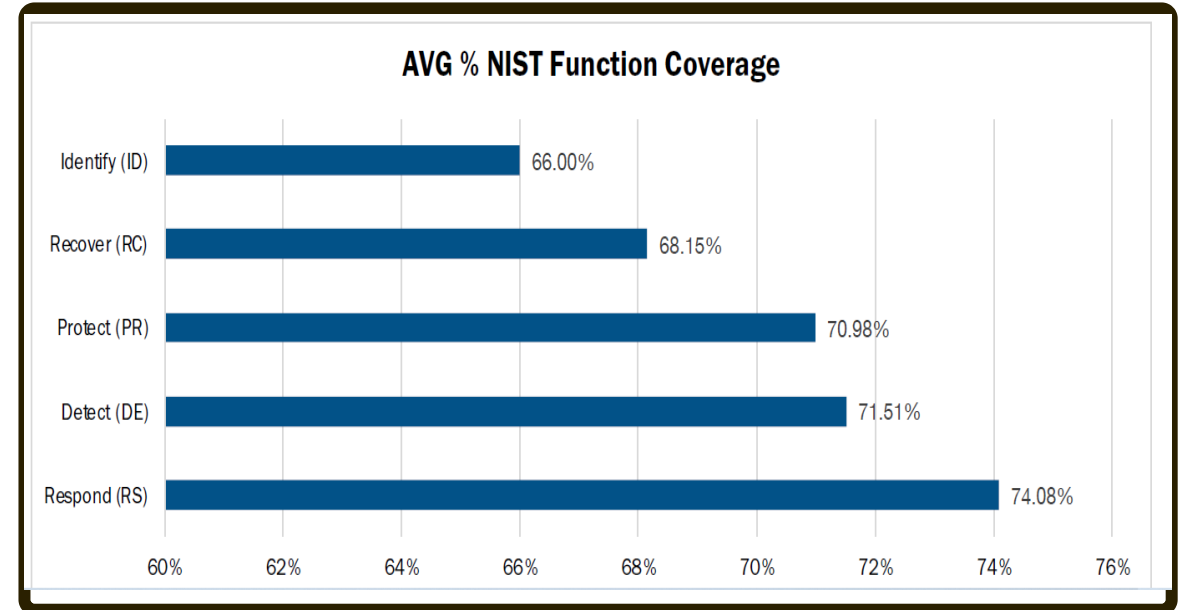


[Link to CISA/HHS Toolkit](#)

# CISA/HHS: Resiliency Landscape Analysis

## Key Findings

- 6) Inconsistency across health orgs
- 7) Use of antiquated hardware, software, and systems
- 8) Insurance premiums continue to rise
- 9) Recruiting and retaining cyber talent is a challenge
- 10) **Adopting Health Industry Cybersecurity Practices works!!** ✓



[Link to CISA/HHS Toolkit](#)

# CISA/HHS Toolkit: Cyber Hygiene

## Hospital Cyber Resiliency Landscape Analysis

This joint product developed by HHS and industry includes a deeper investigative study into the methods that cyber adversaries are using to compromise US hospitals, disrupt operations, and extort for financial gain.

## HPH Sector Cybersecurity Framework Implementation Guide, Version 2

This product was developed jointly by HHS and the HSCC Cybersecurity Working Group, in consultation with the Sector Coordinating Council and Government Coordinating Council to help HPH sector organizations.

## Health Industry Cybersecurity Practices (HICP): Managing Threat and Protecting Patients

This product developed jointly by HHS and the HSCC Cybersecurity Working Group outlines the top threats facing the HPH sector and provides recommendations and best practices to prepare and fight against cybersecurity threats.

## Healthcare and Public Health Sector Risk Identification and Site Criticality (RISC) Toolkit

The RISC Toolkit is an objective, data-driven, all-hazards risk assessment that can be used by public and private organizations within the HPH Sector to inform emergency preparedness planning, risk management activities, and resource investments.

## Security Risk Assessment (SRA) Tool

HHS ONC and OCR developed this risk assessment tool designed to assist small and medium-sized organizations operating in the health care sector to identify and assess security risks within their organization.

## Cyber Hygiene Services

Reduce the risk of a successful cyberattack with vulnerability scanning. CISA's Cyber Hygiene Services help secure internet-facing systems from weak configurations and known vulnerabilities and encourages the adoption of best practices.

## Known Exploited Vulnerabilities Catalog

This catalog is the authoritative source of cyber vulnerabilities that have been exploited in the wild. By prioritizing known exploited vulnerabilities, healthcare organizations can significantly reduce their likelihood of compromise.

## Secure Our World

CISA has just launched Secure Our World, a new cybersecurity awareness program aimed at educating individuals and businesses on four easy ways to stay safe online.



[Link to CISA/HHS Toolkit](#)

Joe Frohlich  
June 10, 2024



# CISA/HHS: HICP Guide on Managing Threat



Letter from the HHS Deputy Secretary	2
<b>Executive Summary</b>	<b>3</b>
Call to Action: Cybersecurity, a Priority for Patient Safety	3
Why Cyber Safety is Patient Safety	3
In The News	5
Can It Happen to Me?	6
<b>Cybersecurity in the Workplace</b>	<b>7</b>
Effective Cybersecurity is a Shared Responsibility	7
The Human Element	8
Be Proactive: Hand Hygiene for Cybersecurity	9
<b>How to Use this Publication</b>	<b>10</b>
The Publication: Health Industry Cybersecurity Practices (HICP)	10
Audience and Publication Components	10
Cybersecurity Threats and Mitigation Practices	11
How Does this Publication Help Me?	12
Where Do I Fit?	12
HICP & Cybersecurity Strategy Approaches	14
The Zero Trust Strategy	14
Defense-in-Depth	15
<b>Current Threat Scenarios Facing the HPH Sector</b>	<b>16</b>
Explaining Threats and Vulnerabilities	16
A Translation: Threats, Vulnerabilities, Impact, and Practices	16
Introducing Current Threats to the HPH Sector	17
<b>Threat: Social Engineering</b>	<b>18</b>
<b>Threat: Ransomware Attack</b>	<b>21</b>
<b>Threat: Loss or Theft of Equipment or Data</b>	<b>24</b>
<b>Threat: Insider, Accidental or Malicious Data Loss</b>	<b>27</b>
<b>Threat: Attacks Against Network Connected Medical Devices</b>	<b>29</b>
<b>Looking Ahead</b>	<b>32</b>



Healthcare & Public Health  
Sector Coordinating Council  
PUBLIC PRIVATE PARTNERSHIP

[Link to CISA/HHS Toolkit](#)

Joe Frohlich  
June 10, 2024

# Health Industry Cyber Practices



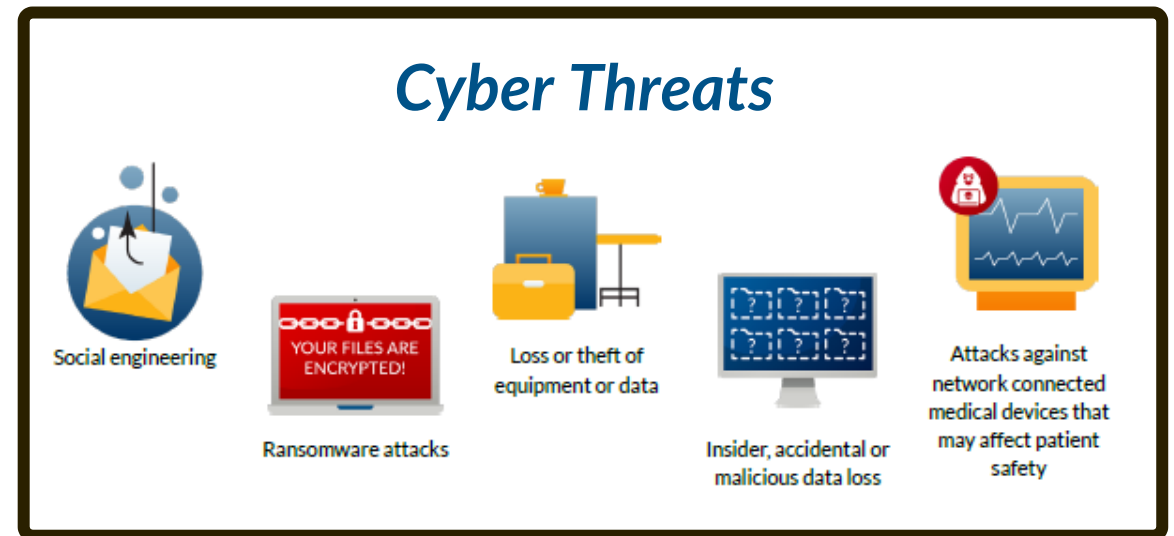
- The **Main Document** discusses the current cybersecurity threats facing the HPH sector. It sets forth a call to action for the HPH sector, especially executive decision makers, with the goal of raising general awareness.
- **Technical Volume 1** outlines the ten HICPs for small healthcare organizations. It is intended for use by IT and/or cybersecurity professionals, it also serves to guide organizations on what to ask their IT and/or cybersecurity teams or vendors.
- **Technical Volume 2** outlines the ten HICPs for medium-sized and large healthcare organizations. It is intended for IT and/or cybersecurity professionals.



# HICP Main Guide on Managing Threat

## Health Industry Cyber Practices

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



[Link to CISA/HHS Toolkit](#)

Joe Frohlich  
June 10, 2024

# CISA/HHS Toolkit Homepage



## [Healthcare and Public Health Sector: Know the Risks, Use Cyber Hygiene](#)

Cybersecurity isn't one size fits all. Different healthcare entities have distinct strengths and weaknesses and a wide range of needs.

Regardless of where an organization fits into the picture, these resources can help build a cybersecurity foundation.



## [Healthcare and Public Health Sector: Strengthen your Defenses and Mature your Cybersecurity Efforts](#)

CISA offers industry best practices and resources on training and exercises, incident response planning, priority telecoms services, cyber resilience, tackling ransomware and much more to help healthcare organizations strengthen their defenses.



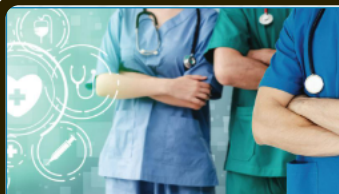
## [Healthcare and Public Health Sector: Address Resource Constraints](#)

Recognizing that the nation's healthcare systems and providers have been under severe resource constraints—especially since the start of COVID-19—members of the HPH sector should actively take steps to address their constraints.



[Link to CISA/HHS Toolkit](#)

# CISA/HHS Toolkit: Strengthen Your Defenses



## [Healthcare Sector Council Publications](#)

Learn from what has worked well for others in the HPH sector. This site offers resources developed specifically for organizations across healthcare subsectors as best practices prepared by the most sophisticated health industry cyber practitioners.

## STOP RANSOMWARE

### [StopRansomware.gov](#)

CISA hosts the federal government's official one-stop location for resources to tackle ransomware more effectively. This website includes information, guidance, and other tools to help organizations protect, prepare for and respond to ransomware.



### [Cyber Resource Hub](#)

The Cyber Resource Hub includes information on how to "[Get your stuff off search](#)" as well as more complex, non-scalable services such as Cyber Hygiene Vulnerability Scanning, Web Application Scanning (WAS), Phishing Campaign Assessments (PCAs), etc.



### [Cybersecurity Training and Exercises](#)

Healthcare and public health staff need to know what to do in a cyber incident. CISA helps build a cyber-ready workforce by offering training and education for different groups, including healthcare and public health.



### [Cyber Incident Response Plan Basics](#)

Every healthcare organization should have an Incident Response Plan that spells out what the organization needs to do before, during, and after an actual or potential security incident.



### [Free Cybersecurity Services and Tools](#)

This web page offers free services from CISA and our industry partners, starting with basic steps to take immediately and building up to more complex actions and resources.



### [Priority Telecommunications Services](#)

To ensure reliable communications when circuits are congested, CISA offers GETS for priority access to local and long distance calls on landline networks and WPS for prioritized wireless calling on nationwide and several regional cellular networks.



### [Communications and Cyber Resiliency Toolkit](#)

CISA developed an interactive graphic for those who are responsible for communications networks to help evaluate current resiliency capabilities, identify ways to improve resiliency, and develop plans for mitigating the effects of potential threats.



# CISA/HHS Toolkit Homepage



## [Healthcare and Public Health Sector: Know the Risks, Use Cyber Hygiene](#)

Cybersecurity isn't one size fits all. Different healthcare entities have distinct strengths and weaknesses and a wide range of needs.

Regardless of where an organization fits into the picture, these resources can help build a cybersecure foundation.



## [Healthcare and Public Health Sector: Strengthen your Defenses and Mature your Cybersecurity Efforts](#)

CISA offers industry best practices and resources on training and exercises, incident response planning, priority telecoms services, cyber resilience, tackling ransomware and much more to help healthcare organizations strengthen their defenses.



## [Healthcare and Public Health Sector: Address Resource Constraints](#)

Recognizing that the nation's healthcare systems and providers have been under severe resource constraints—especially since the start of COVID-19—members of the HPH sector should actively take steps to address their constraints.



[Link to CISA/HHS Toolkit](#)

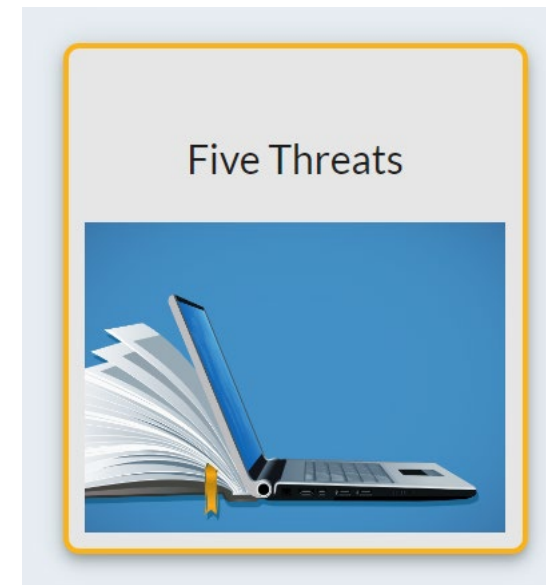
# CISA/HHS Toolkit: Address Resource Constraints

## Healthcare and Public Health Sector: Address Resource Constraints

Recognizing that the nation's healthcare systems and providers have been under severe resource constraints—especially since the start of COVID-19—members of the Healthcare and Public Health (HPH) sector should actively take steps to address their constraints.

Use free or low-cost services to make near-term improvements when resources are scarce

The tools and resources offered by CISA in this toolkit are available at no cost. In addition, HHS hosts [Knowledge on Demand \(KOD\)](#), a free cybersecurity education platform that includes multiple delivery methodologies to reach health care facilities of all sizes across the country.



[Link to CISA/HHS Toolkit](#)

Joe Frohlich  
June 10, 2024

# CISA/HHS Toolkit: Knowledge On Demand

## Knowledge on Demand

Knowledge on Demand (KOD) is a cybersecurity education platform that includes multiple delivery methodologies to reach the varied size health care facilities across the country. Five cybersecurity trainings that align with the top five cybersecurity threats outlined in HICP are featured for training your healthcare staff, security team, and any other department that is on the front lines for protecting patient safety. The best part about this resource? It's FREE!

Test your knowledge of all 5 KOD Threat Videos. Click to begin →

Download LMS Version



Each training contains:

### Job Aid

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.

### Interactive Video

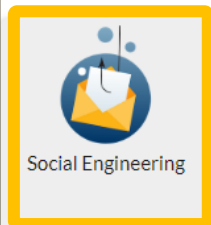
These videos are launched from the 405(d) KOD webpage. They include recorded audio to take the trainee through the video along with interactive content to include knowledge checks and animations.

### PowerPoint with Presenter Notes

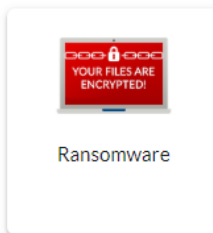
These can be leveraged for in person or on-site presentations. These will include facilitator notes with slide specific content and knowledge checks to reinforce learning. Such presentations can be delivered in presentation mode or in a "Lunch n Learn" format at your location.

### Learning Management System

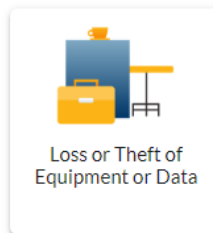
Content intended for a Learning Management System (LMS) will be similar in look and experience as the previously discussed Interactive Training video. Content will be exported and saved to a file type compatible for import to an organization's LMS platform.



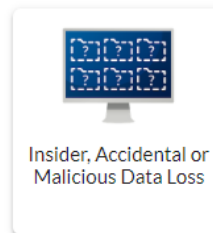
Social Engineering



Ransomware



Loss or Theft of Equipment or Data



Insider, Accidental or Malicious Data Loss



Attacks Against Network Connected Medical Devices



[Link to CISA/HHS Toolkit](#)

Joe Frohlich  
June 10, 2024



# CISA/HHS Toolkit: Knowledge On Demand

KNOWLEDGE ON DEMAND

## Social Engineering

A graphic for 'Launch Training' featuring an open laptop with a yellow envelope icon and various social media icons (Facebook, Twitter, LinkedIn) floating around it. The text 'Launch Training' is overlaid on the laptop screen.

NOTE: The training will launch in a new window.

Social Engineering is an attempt to trick you into giving out personal information or infecting your device by clicking on a link to give hackers access to patient data. This training includes statistics and resources to help spot social engineering and what to do when you encounter it.

[Job Aid](#) [PowerPoint with presenter notes](#) [LMS Version](#)

A speech bubble icon containing the text 'WE WANT YOUR FEEDBACK' with a megaphone icon below it.

[Link to CISA/HHS Toolkit](#)

Joe Frohlich  
June 10, 2024

# Sampling of Voluntary & No-Cost Cybersecurity Offerings

## • Assessments & Evaluations

### • Strategic

- Healthcare Cybersecurity Performance Goals (CPGs)
- Cyber Resilience Review (CRR™)
- Cyber Resilience Essentials (CRE)
- Cyber Infrastructure Survey (CIS)
- External Dependencies Management (EDM)
- [Cyber Security Evaluation Tool](#) (CSET™)

### • Technical

- Vulnerability Scanning (CyHy)
- Remote Penetration Test (RPT)
- Risk and Vulnerability Assessment (RVA)

## Preparedness Activities

- Tabletop Exercises
- Security Alerts, Tips and other updates (US-Cert)
  - National Cyber Awareness System
  - ICS-Cert
  - Known Exploited Vulnerabilities (KEV)
- Informational Products and Recommended Practices
- Outreach, Work group collaboration
- Cyber Exercises and Workshops
- Cybersecurity Training and Webinars
- Guides and “Playbooks”
- National Cybersecurity Workforce Framework
- October Cybersecurity Awareness Month

## Incident Response Assistance

- Incident Coordination
- Malware Next Gen Analysis

Joe Frohlich  
June 10, 2024



<https://hphcyber.hhs.gov/performance-goals.html>

# 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.
- To learn more, visit [www.dhs.gov/pcii](https://www.dhs.gov/pcii)



# Cyber Performance Goals - Healthcare

## Cyber Performance Goals (CPGs) Assessment:

- Voluntary guidelines tailored to Healthcare organizations



**10 Essential Goals** establish a floor of safeguards that will better protect from cyber attacks, improve response when events occur, and minimize residual risk



**10 Enhanced Goals** provide a path to reach the next level of defense needed to protect against additional attack vectors



<https://hphcyber.hhs.gov/performance-goals.html>

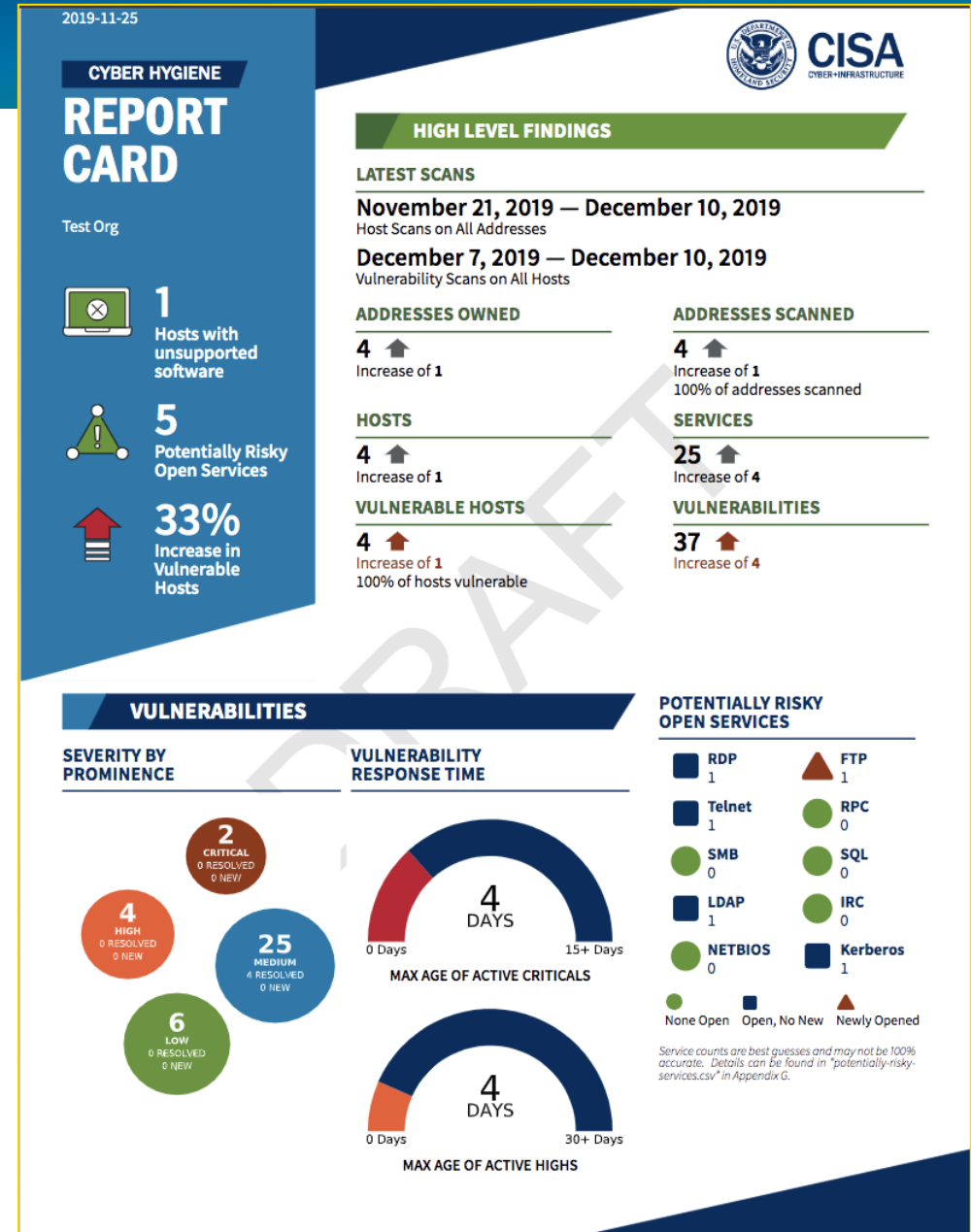


# Vulnerability Scanning

- Automated scanning of **External-facing, Internet accessible** systems (Top 1000 Ports, can include cloud sites)
- **Weekly report** card that includes current scan results, historic trends, Known Exploited Vulnerabilities, and comparisons to the national average
- Helps you understand your unique exposure
- **Know what the Internet already knows about your environment!**



Sign up by emailing  
[vulnerability@cisa.dhs.gov](mailto:vulnerability@cisa.dhs.gov)  
with subject line  
“Requesting Cyber Hygiene Services”



# #StopRansomware

RESOURCES

NEWSROOM

ALERTS

REPORT RANSOMWARE

CISA.GOV



Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. [StopRansomware.gov](https://www.stopransomware.gov) is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively.



# Cyber Tabletop Exercises (CTTX)

- Use CISA Tabletop Exercise Packages (CTEP) to help develop your own
  - [Healthcare & Public Health Sector Cyber CTEP Situation Manual](#)
  - [Industrial Controls CTEP Situation Manual](#)
  - [Ransomware CTEP Situation Manual](#)
  - [Ransomware Third Party Vendor CTEP Situation Manual](#)
  - [Vendor Phishing CTEP Situation Manual](#)
  - [Healthcare and Public Health Suicide Bomber CTEP Situation Manual](#)
- October 25, 2023 – Statewide Healthcare Cyber Incident Response TTX in Missoula – over 40 organizations joined!



<https://www.cisa.gov/cisa-tabletop-exercises-packages>

# Protective Security Advisor (PSA)



- **INFRASTRUCTURE SURVEY TOOL** - Identifying facilities' physical security, security forces, security management, information sharing, protective measures, and dependencies related to preparedness, mitigation, response, resilience, and recovery;
- **Assist Visit** – Identifies and recommends protective measures at facilities, provide comparison across like assets, and track implementation of new protective measures.
- **Infrastructure Visualization Platform (IVP)** – brings a facility's digital floorplans to life by placing on it 360° panoramic photographs, immersive video, geospatial information, and hypermedia data of critical facilities, surrounding areas, and transportation routes that assist with security planning, protection, and response efforts.
- **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



## CISA Protective Security Advisors



# Information Sharing Opportunities



[Join H-ISAC: Health Information Sharing and Analysis Center](#)

[About H-ISAC](#)



[Health Sector Cybersecurity Coordination Center \(HC3\) | HHS.gov](#)



**Health Sector Coordinating Council  
Cybersecurity Working Group**

[Healthcare Sector Coordinating Council Cybersecurity Working Group - Health Sector Council](#)





*Cyber406 strives to improve Montana's cybersecurity defensive posture across private and public sectors by increasing the state's ability to prevent, identify, and eradicate cyber threat vulnerabilities through a systematic approach of Collaboration, Operations, Education, and Research.*



<https://www.cyber406.org/>



Joe Frohlich  
June 10, 2024

# Incident Reporting

Montana Analysis and Technical Information  
Center (MATIC):  
**406-444-1318**

CISA Central 24x7 contact number:  
**888-282-0870**

[Report an Incident: www.cisa.gov/forms/report](https://www.cisa.gov/forms/report)



# The need to Work Together

*To secure the entire network (IT and OT), we need to work together. Realize the importance of each network and strive for safety, security and reliability*



- Schedule a Monthly/Quarterly Senior leadership brief on cyber risk and potential impacts to your organization.



# CISA – MT Contacts

## **TRAVIS LIGHT**

Cybersecurity Advisor

Helena, MT

(406) 894-8374

[travis.light@cisa.dhs.gov](mailto:travis.light@cisa.dhs.gov)

## **JOE FROHLICH**

Cybersecurity State Coordinator

Helena, MT

(406) 461-2651

[joseph.frohlich@cisa.dhs.gov](mailto:joseph.frohlich@cisa.dhs.gov)

## **RANDY MIDDLEBROOK**

Protective Security Advisor

Helena, MT

(406) 839-1165

[randy.middlebrook@cisa.dhs.gov](mailto:randy.middlebrook@cisa.dhs.gov)

## **ALBERT MENDOZA**

Protective Security Advisor

Billings, MT

(406) 371-3585

[albert.mendoza@cisa.dhs.gov](mailto:albert.mendoza@cisa.dhs.gov)





For more information, visit [CISA.gov](https://www.cisa.gov) or contact [central@cisa.dhs.gov](mailto:central@cisa.dhs.gov)