TLP:CLEAR

CISA

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

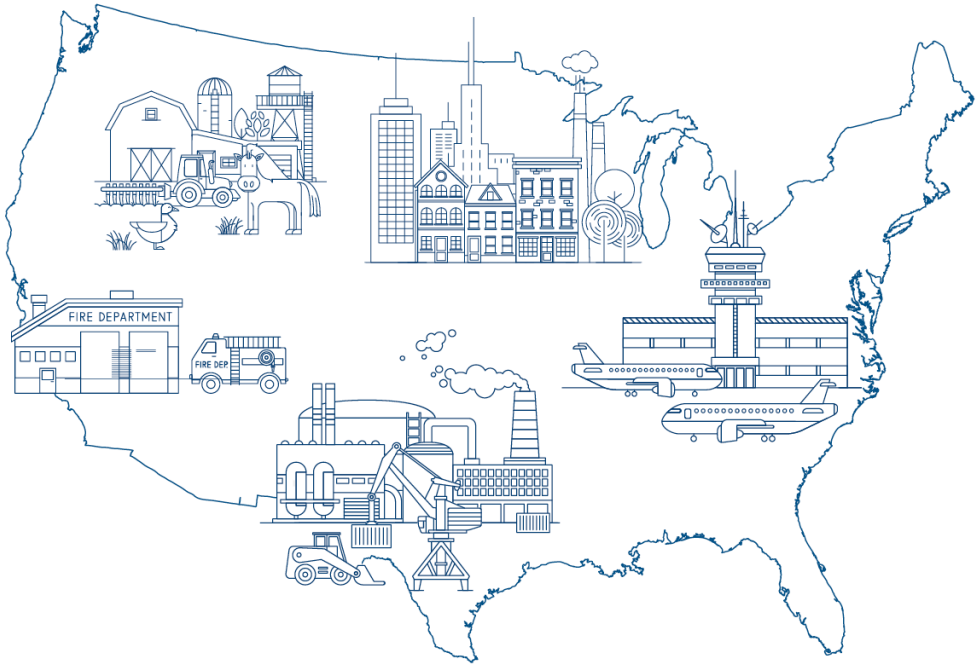
TLP:CLEAR

Cybersecurity and Infrastructure Security Agency (CISA)

As America's Cyber Defense Agency and the National Coordinator for critical infrastructure resiliency and security, CISA leads the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day.

TLP:CLEAR

Integrated Operations



CISA enhances the resilience of our nation's critical infrastructure by taking an integrated approach to delivering services and sharing information. By meeting our stakeholders where they are, we help critical infrastructure owners and operators mitigate risk.

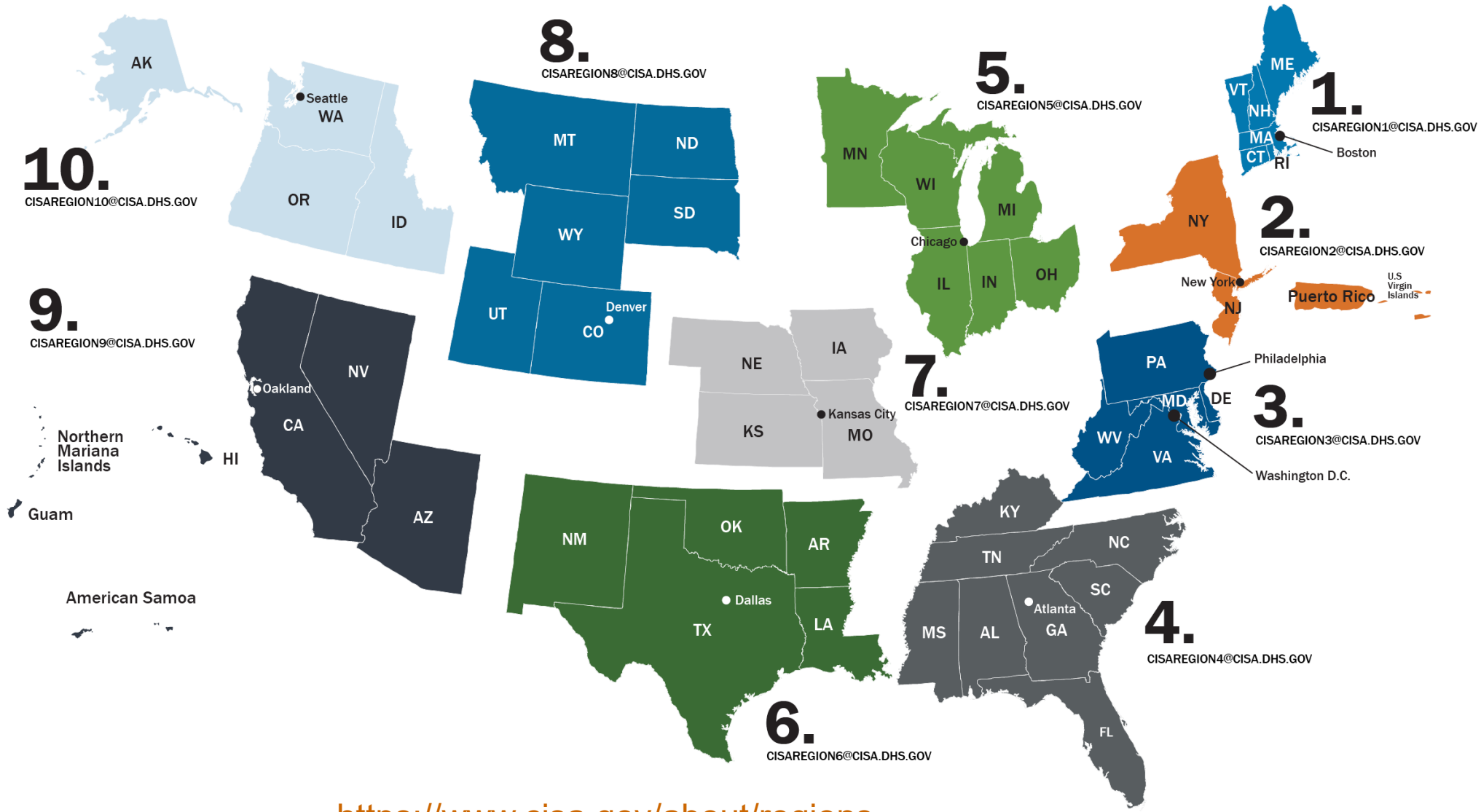
HOW CISA IS CARRYING OUT ITS INTEGRATED OPERATIONS MISSION:

- Provide Operational Visibility to Understand, Manage, and Reduce Risk to the Nation
- Offer a Unified Regional Approach to Sharing Information and Delivering CISA Services

TLP:CLEAR

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



https://www.cisa.gov/about/regions

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

TODAY'S CYBER THREAT LANDSCAPE

Cyber Threats of Today*

* Not an exhaustive list!

TLP:CLEAR

Ransomware

- Double/Multi-extortion (Lockbit Conti, Hive, Vice Society, etc.)

Malware

- IT and OT specific malware

Denial of Service

- Cyber criminals, Hacktivists (KillNet / Aviation Sector)

Threats to External Dependencies

- 3rd party vendors, service providers, infrastructure providers
- Supply chain compromise

Advanced Persistent Threats (APTs)

- Highly sophisticated with substantial financial backing
- Various motivations (political, economic, etc.)

CISA SERVICES & RESOURCES

Cybersecurity Services

CISA Cybersecurity Services & Assessments

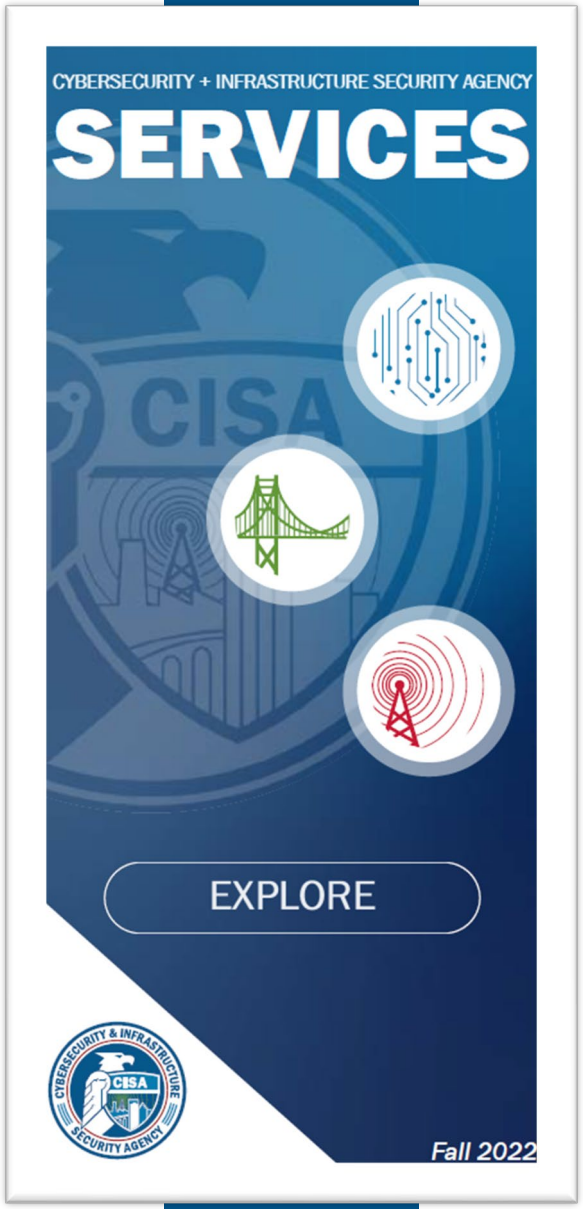
- Cyber Hygiene Vulnerability Scanning
- Cybersecurity Performance Goals (CPG)
- Cybersecurity Assessments
- Tabletop Exercises (TTX)
- Training
- & more

For more information on these services and more, please visit

https://www.cisa.gov/topics/cyber-threats-and-advisories

or

https://www.cisa.gov/cyber-resource-hub



TLP:CLEAR

Cyber Hygiene Vulnerability Scanning

GOAL:
Reduce exposure to threats by taking a proactive approach to identifying and mitigating attack vectors

- Hosts with no vulnerabilities detected are rescanned every 7 days
- Hosts with low-severity vulnerabilities are rescanned every 6 days
- Hosts with medium-severity vulnerabilities are rescanned every 4 days
- Hosts with high-severity vulnerabilities are rescanned every 24 hours
- Hosts with critical-severity vulnerabilities are rescanned every 12 hours

Email us at **vulnerability@cisa.dhs.gov** with the subject line “Requesting Cyber Hygiene Services” to get started.

Cybersecurity Performance Goals (CPGs)

- What are the 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).
- How should organizations use the CPGs?
  - Inform strategy decisions and resource investment.

The CPG's Address:

- Account Security
- Device Security
- Data Security
- Governance and Training,
- Vulnerability Management,
- Supply Chain/Third Party,
- Response and Recovery
- Other (network segmentation, email, etc,)

The most current version of the CPGs is located at:
https://www.cisa.gov/cpg

Where to Find Them

- The most current version of the CPGs is located at: https://www.cisa.gov/cpg
  - Here you can find:

The core list of CPGs

CPG Checklist

Spreadsheet of all text content

Link to our GitHub discussion page

Cybersecurity Performance Goals

Approximate Cost/Impact/Complexity ratings to inform investment planning.

Mapping to NIST CSF Subcategory

8.1 Network Segmentation	PR.AC-5, PR.PT-4, DE.CM-1	CURRENT ASSESSMENT	YEAR 1 ASSESSMENT	NOTES
COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** HIGH **TTP OR RISK ADDRESSED:** Network Service Discovery (T1046) Trusted Relationship (T1199) Network Connection Enumeration (ICS T0840) Network Sniffing (T1040, ICS T0842) **RECOMMENDED ACTION:** All connections to the OT network are denied by default unless explicitly allowed (e.g. by IP address and port) for specific system functionality. Necessary communications paths between the IT and OT networks must pass through an intermediary, such as a properly configured firewall, bastion host, "jump box," or a demilitarized zone (DMZ), which is closely monitored, captures network logs, and only allows connections from approved assets.		DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	DATE: ☐ IMPLEMENTED ☐ IN PROGRESS ☐ SCOPED ☐ NOT STARTED	

MITRE ATT&CK TTPs addressed by the Goal

How organizations can demonstrate the effective implementation the security practice, based on input from CISA's collaborative stakeholder process. These Actions will be updated regularly as new threats and defenses arise.

TLP:CLEAR

Cyber Information Sharing

Information sharing is the key to preventing a wide-spread cyber-attack. CISA develops partnerships to rapidly share critical information about cyber incidents.

Cybersecurity Alerts & Advisories

- Offers the latest cybersecurity news, advisories, alerts, tools, and resources.
- Found at:

  https://www.cisa.gov/news-events/cybersecurity-advisories


CYBERSECURITY ADVISORY

People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection

Release Date: May 24, 2023 **Alert Code:** AA23-144a

Reducing Risk of Known Exploited Vulnerabilities

CISA's Known Exploited Vulnerabilities Catalog

The following sections detail the criteria behind each of the three thresholds for KEV catalog updates, which are:

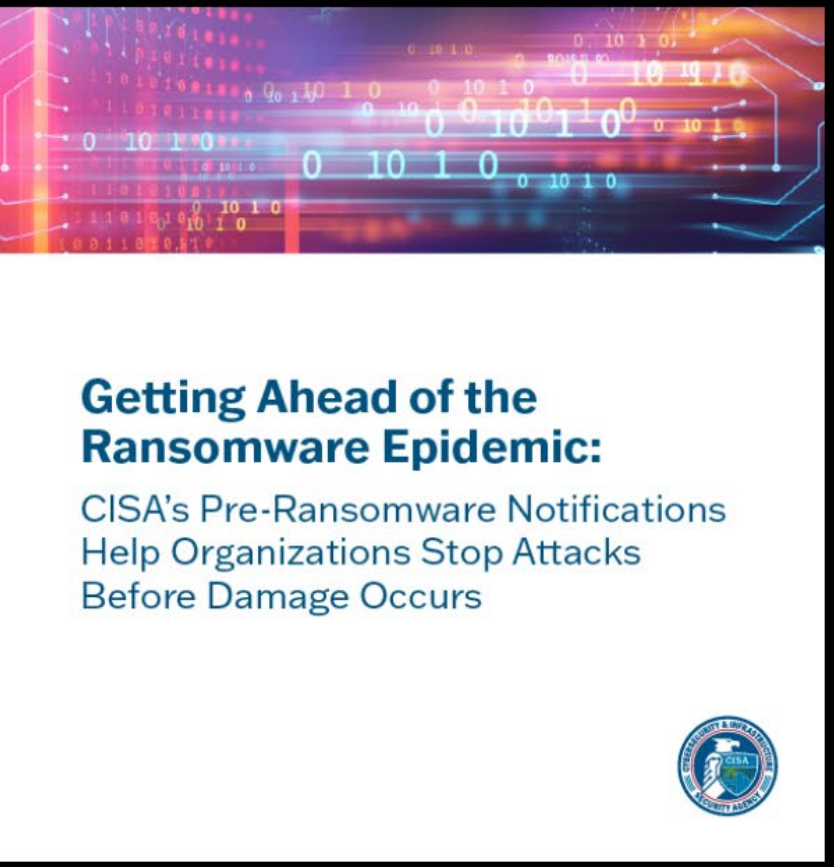
- The vulnerability has an assigned Common Vulnerabilities and Exposures (CVE) ID.
- There is reliable evidence that the vulnerability has been actively exploited in the wild.
- There is a clear remediation action for the vulnerability, such as a vendor-provided update.

https://www.cisa.gov/known-exploited-vulnerabilities-catalog

TLP:CLEAR

https://www.cisa.gov/stopransomware

RESOURCES NEWSROOM ALERTS REPORT RANSOMWARE CISA.GOV



Protection and Response | Services | Public Safety | Preparation

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 is the U.S. Government's official one-stop location for resources to tackle ransomware more effectively.

Ransomware Vulnerability Warning Pilot (RVWP)

- The Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), signed into law in March 2022, required CISA to establish the RVWP
- CISA accomplishes this work by leveraging its existing services, data sources, technologies, and authorities, including
  - CISA's Cyber Hygiene Vulnerability Scanning service
  - Administrative Subpoena Authority
- CISA Regional staff members, located throughout the country, make notifications and may provide resources to mitigate the vulnerability.

Ransomware Vulnerability Warning Pilot (RVWP)

- In 2023, CISA conducted more than 1,700 notifications to various organizations about open vulnerabilities on their networks that are specifically exploited by ransomware actors
- If you receive a notification, you can verify the identity of the CISA personnel through CISA Central: Central@cisa.gov or (888) 282-0870.

TLP:CLEAR

2023 Pre-Ransomware Notifications

In 2023, CISA conducted more than 1200 pre-ransomware notifications to include:

7
U.S. Water and Wastewater Sector Entities

37
U.S. Transportation System Sector and Energy Sector Entities

39
U.S. Emergency Services Sector Entities

274
U.S. and Int'l K-12 School Districts & Institutes of Higher Education

154
U.S. Healthcare Organizations

94
U.S. State, Local, Tribal, and Territorial Governments

Driven by the cybersecurity research community, infrastructure providers, and cyber threat intelligence companies about potential early-stage ransomware activity.

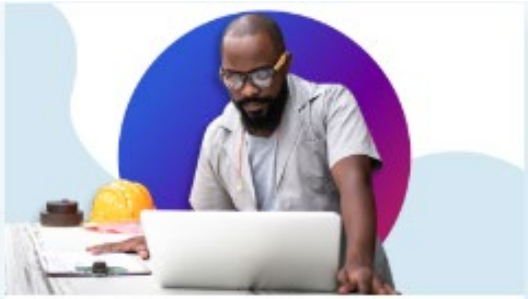
https://www.cisa.gov/about/2023YIR

https://www.cisa.gov/secure-our-world

- CISA's cybersecurity awareness program to provide small businesses, communities and individuals with the guidance and tools they need to protect themselves online. The program emphasizes four simple steps:
  - Use strong passwords and a password manager.
  - Turn on multifactor authentication.
  - Recognize and report phishing.
  - Update software.

Secure Yourself & Your Family

Quick steps we can all take to greatly increase our safety and protect our money, identity, data and more.



Secure Your Business

Prevent malicious threats that could cause hassle, financial losses or even business closure. Protect your business, employees and customers!

Secure Your Products

Adopt Secure by Design practices for your products that reasonably protect against malicious actors and put customer safety first.

TLP:CLEAR

Cyber Incident Reporting

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

REPORTING CYBER ATTACKS

- Contact CISA at central@cisa.gov or 888-282-0870
- FBI Field Office: http://www.fbi.gov/contact-us/field or the FBI's 24-7 Cyber Watch at 855-292-3937 or by e-mail at cywatch@fbi.gov
- State reporting laws & requirements
- Regulatory Authorities

“If You See Something, Say Something”

TLP:CLEAR

"If You See Something, Say Something®" is a national campaign that raises public awareness of the signs of terrorism and terrorism-related crime, and how to report suspicious activity to state and local law enforcement.

To become a partner, send an email to:
seesay@hq.dhs.gov

For more information visit:
www.dhs.gov/see-something-say-something

J.D. Henry
January 29, 2024

TLP:CLEAR

Questions?

Central@CISA.GOV
888-282-0870

Or

https://www.cisa.gov/about/regions

Or

Joseph "JD" Henry
Cybersecurity Advisor
Joseph.Henry@cisa.dhs.gov

All CISA services and resources can be found by visiting
www.CISA.gov

TLP:CLEAR

For more information, visit **CISA.gov** or contact **central@cisa.dhs.gov**