CISA Updates Supporting SLTT Governments - January 2025

John Harrison
Cybersecurity State Coordinator, Virginia, Region 3
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

TLP: GREEN

Cybersecurity State Coordinators and Cybersecurity Advisors

Established in Section 2215 of the 2021 National Defense Authorization Act, **Cybersecurity State Coordinators** are highly qualified CISA employees appointed to **serve in each state as the principal point of contact** with CISA on preparing, managing, and responding to cybersecurity risks and incidents.

Cybersecurity State Coordinators (CSCs) and Cybersecurity Advisors (CSAs):

- **Build** strategic public and private sector relationships,
- **Support** preparation, response, and remediation efforts relating to cybersecurity risks and incidents
- **Facilitate** cyber threat information sharing to improve understanding of ,cybersecurity risks and situational awareness
- **Raise** awareness of the financial, technical, and operational cybersecurity resources available to SLTT governments
- **Support** cybersecurity training and exercises
- **Assist** in developing and coordinating vulnerability disclosure programs consistent with Federal and information security industry standards
- **Assist** SLTT governments in developing and coordinating cybersecurity plans
- **Coordinate** and perform other duties as necessary to achieve the goal of managing cybersecurity risks in the United States

Notifications From "US" To You

CIRCIA

Cyber Incident Reporting For Critical Infrastructure Act of 2022 (CIRCIA)

- Regulatory Requirement: Requires CISA to establish a new regulatory program requiring reporting of certain cybersecurity related information:
  - **Covered entities** must report to CISA **covered cyber incidents within 72 hours** after the entity reasonably believes that a covered cyber incident occurred
  - **Covered entities** must report to CISA any ransomware payments **within 24 hours of making the payment**
- Requires CISA to coordinate with Federal SRMA partners on various cyber incident reporting and ransomware related activities
- CIRCIA Reports may receive information protections listed under 6 U.SC. 681e.
- **Sec. 105 requires CISA to stand up a Ransomware Vulnerability Warning Pilot (RVWP)**
- CIRCIA reporting requirements is not required until after the final rule issued and effective *(~Q4, 2025)*

CISA Regional Operations & Entity Notifications

Entity Notifications via CISA Regional Operations

- Administrative Subpoena notifications
- General vulnerability notifications
- Critical Vulnerability/KEVs notifications
- Ransomware Vulnerability Warning Program (RVWP), and Ransomware tippers
- Targeted Notifications

Special event support (on-site, or virtual/remote)

Ransomware Vulnerability Warning Pilot Program

Key Points from Legislation

- Research and identify common vulnerabilities associated with ransomware attacks.
- Identify vulnerable systems and alert owners of their ransomware associated vulnerabilities.
- Use existing authorities such as the subpoena authority to assist in the identification of system owners.
- Prioritize CIRCIA covered entity identification and notifications.
- CISA cannot compel entities to mitigate the vulnerabilities.

Implementation

Identify and prioritize vulnerabilities using CIRCIA data, commercial intelligence, JRTF intelligence, and KEV Catalog.

Develop a common ransomware vulnerability list on StopRansomware.gov.

Leverage existing subpoena vulnerability hunt model; CSD will identify vulnerabilities and push to IOD regions for notification and information passing to organizations.

Cultivate a hunting strategy on known ransomware vulnerabilities, while maintaining flexibility to react to current campaigns.

Notifications From You to "US"

Incident Coordination & Response

Public Entities in Commonwealth of Virginia:

Report cybersecurity incidents and vulnerabilities to the Virginia Fusion Center (VFC)

804-674-2196

vfc@vfc.vsp.virginia.gov

When to Report

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

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

Why to Report

- ➢ For additional assistance
- ➢ To aid in understanding risks and the threat
- ➢ You are required to report by law (e.g. CIRCIA2022)

UNCLASSIFIED

CISA Regional Operations & Entity Notifications

WWW.CISA.GOV

Sign-in

Choose your preferred Login

Sign-In

Report Unregistered

Or

Create an Account

Don't have an account? Create One!

Once you have an account, you'll have more options when you're reporting an incident.

Save Your Progress: Started your report but don't have time to complete it? You can save it to finish later.

Continue Your Progress: Pick your report right up again where you left off.

Track Your Issue: Once you've submitted an issue, you'll be able to come back to track its progress with CISA.

Want to Continue Anonymously?

If you don't wish to share your identity, you're free to submit your issue anonymously for CISA's review

Why Worry? Critical Infrastructure & the Threat Landscape

SHIELDS UP

Current Geopolitical Cyber Threats

2011-2013, Chinese Gas Pipeline Intrusion Campaign

- Chinese-sponsored actors conducted spear-phishing and intrusion campaign to U.S. Pipelines

2017, WannaCry /WannaCry 2.0 campaign and ransomware

- Widespread ransomware campaign affected various organizations with reports of tens of thousands of infections in over 150 countries, including the United States, United Kingdom, Spain, Russia, Taiwan, France, and Japan.

2014-2018, CLOUD HOPPER Campaign

- Chinese APT actors have used various Tactics, Techniques, and Procedures (TTPs) to attempt to infiltrate the networks of global Managed Service Providers (MSPs) for the purposes of cyber espionage and intellectual property theft targeting of critical infrastructure in IT, Energy, Healthcare and Public Health, Communications, and Critical Manufacturing

SHIELDS UP

Geopolitical Cyber Threats Over Time

2020, Iran-Based Threat Actor Exploits VPN Vulnerabilities

- Iranian threat actor observed exploiting several publicly known Common Vulnerabilities and Exposures (CVEs)
- Mainly targeted U.S. information technology, government, healthcare, financial, insurance, and media sectors

2020, Iranian APT Actors Threaten Election-Related Systems

- Created fictitious media sites & spoofed legitimate sites to spread anti-American propaganda & misinformation

2019-2021, PRC-affiliated cyber actors target COVID-19 related healthcare & support

2021, Iranian Islamic Revolutionary Guard (IRGC) Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations

- Actively targeted a broad range of entities, including entities across multiple U.S. critical infrastructure sectors along with Australian, Canadian, and United Kingdom organizations

Geopolitical Cyber Threats Over Time

2022, North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector

2023, IRGC-Affiliated CyberAv3ngers Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities

- Using the persona “CyberAv3ngers”, APT actor was actively targeting and compromising **Israeli-made** Unitronics Vision Series PLCs that are publicly exposed to the internet, through the use of default passwords.

2017-2023; **Lazarus Group (Aka Hidden Cobra)**

- Internet Protocol (IP) addresses associated with a malware variant, known as DeltaCharlie, used to manage North Korea’s distributed denial-of-service (DDoS) botnet infrastructure (TA17-164A).
- A number of malware strains affiliated to Hidden Cobra over the years including DeltaCharlie, Volgmer trojan, FALLCHILL remote access trojan (RAT), BANKSHOT RAT, HARDRAIN, SHARPKNOT wiperware, Joanap trojan, Brambul SMB worm, COPPERHEDGE, FASTCASH/FASTCash 2.0, and others

Current Geopolitical Cyber Threats

2021-2024: Volt Typhoon

- PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure.
- PRC-based Cyber Threat Actors using Living Off the Land (LOTL) techniques to pre-position themselves inside of U.S. Based critical infrastructure for disruptive or destructive cyber attacks in the event of a major crisis or conflict with the U.S.
- LOTL techniques to include deploying Fast Reverse Proxy (RFP) clients with hard-coded C2 callback, malware with fileless techniques via malware stored in system's registry and in memory, and targeting Small Office/Home Office (SOHO) routers with malicious firmware/hard-coded malware

2024-2025: Salt Typhoon

- In early October 2024, it was reported that PRC state-sponsored hackers infiltrated United States telecommunications companies (including internet service providers).
- They conducted counterintelligence operations, seeking information on PRC targets that the United States may be surveilling.

16 Critical Service Sectors

as defined by Presidential Policy Directive 21 (PPD-21)

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Defense Industrial Base
- Emergency Services
- Energy
- Financial Services
- Food & Agriculture
- Government Services & Facilities
- Healthcare & Public Health
- Information Technology
- Nuclear
- Transportation Systems
- Water & Wastewater

Potential Impact for Critical Infrastructure

Sector and Risk Types	Reputational Damage	Health and Safety	Regulatory Fines and Compliance Actions	Third Party Legal Exposures	Decreased Revenue
Healthcare	✓	✓	✓	✓	✓
Energy		✓	✓		
Critical Manufacturing		✓		✓	✓
Chemical		✓	✓	✓	
Financial	✓		✓	✓	✓
Emergency Services		✓			
Water and Wastewater		✓		✓	

Threat Landscape – Election Security

Potential Adversaries

- Nation-State Actors
- Black Hat Hackers
- Criminals
- Politically Motivated Groups
- Insider Threats
- Terrorists
- Domestic Violent Extremists
- Natural Threats

Possible Motivations

- Undermine Trust in Democracy and/or Election Results
- Foreign Policy Goals
- Sow Social Division
- Financial Gain
- Subvert Political Opposition
- Fame and Reputation
- Foment Chaos/Anarchy
- Retribution for Perceived Grievances

Potential Targets

- Voter Registration Databases
- Voting Systems
- Election Reporting Systems
- Public Information Websites
- Election Facilities
- Polling Places
- Election Offices
- People: Election Officials, Vendors, Voters, Political Candidates, etc.

What Do You Need To Do?

Protective Measures in the "New Normal"

Organizational Leaders

- **Know** business risks and treat cyber attacks as a risk area, to operations and to supply chains
- **Foster** a culture of operational resilience and cyber readiness
- **Incorporate** cybersecurity as a part of business strategy, including all external relationships
- **Build** and expand a network of trusted relationships with sector partners and government agencies for access to timely cyber threat information, incident reporting, and response coordination

All End Users

- Participate in security awareness training and a general awareness in cyber threats
- Be aware of your digital footprint and know the end-user security features available to you
- Practice good operational security when participating in web conferencing
- Know the data backup options available and ensure locally stored data is backed up
- Be vigilant, accountable, and report incidents and suspicious activity immediately

Protective Measures in the "New Normal"

What your IT, and IT Security shops need to have in place (i.e., *the basics*)

Today

- Inventory all people, processes, technology and information
- Document critical systems and the services they support
- **Have a plan for responding to cyber incidents**
- **Maintain offline, encrypted backups of critical data**
- **Backup all data and test backed-up data regularly**
- Deploy and update endpoint detection on all servers and workstations
- Turn on logging for all network appliances, servers and services
- **Develop and Implement comprehensive patch management process**
- Know and understand any available cyber insurance policies

Tomorrow

- **Implement strong identity and authentication management (IAM) practices (i.e., MFA)**
- **Plans to decommission End of Life systems**
- Know supply chain and external dependencies risks, security measures and gaps
- Develop and strengthen situational awareness
- Implement innovative security awareness training
- Implement a secure network architecture (i.e. zero trust)
- Conduct internal audits and periodic cyber assessments
- Utilize cyber attack frameworks when responding to cyber incidents

CISA SERVICES

JOINT CYBER DEFENSE COLLABORATIVE

Mission

- To **unite** the global cyber community in the **collective defense** of cyberspace.

Vision

- **Fuse** JCDC members' insight, expertise, and capabilities to enable **synchronized cyber defense** planning and collective response to promote **national resilience** and **reduce risk** to U.S. critical infrastructure.

Value

- To **create a proactive capability** for government and private sector to work together closely before an incident occurs **to strengthen the connective tissue** and ensure a common understanding of processes.

TLP: GREEN

JOINT CYBER DEFENSE COLLABORATIVE

JCDC works with **Alliance Partners**, industry partners who are fully integrated into JCDC's cyber defense planning and operations and have committed personnel, tools, or other resources on an ongoing basis and regularly collaborate with all JCDC entities.

JCDC Alliance Partners include:

- Akamai Technologies, Inc
- AT&T Services, Inc
- Broadcom, Inc (formerly, Symantec Corporation
- CISCO Systems, Inc
- CloudFlare, Inc
- CrowdStrike, Inc
- Google Cloud
- International Business Machines Corporation (IMB)
- Juniper Networks (US), Inc
- Lumen Technologies, Inc
- Mandiant
- Microsoft
- Oracle America, Inc
- Palo Alto Networks, Inc
- SecureWorks, Inc
- Splunk, Inc
- Tenable Public Sector LLC
- Trelix
- Verizon Communications, Inc
- Vmware. Inc

CISA Offers No-Cost Cybersecurity Services

- **Preparedness Activities**
  - Cybersecurity Assessments
  - Cybersecurity Training and Awareness
  - Cyber Exercises and "Playbooks"
  - Cybersecurity Advisories and Alerts
  - Operational Products and Threat Indicator Sharing
  - Known Exploited Vulnerabilities (KEV) Catalog
  - Cybersecurity Performance Goals (CPGs)
  - Free Cybersecurity Tools and Services Catalog
  - Information Products and Recommended Practices

- **Response Assistance –** 24/7/365
  - Incident Coordination
  - Remote Assistance
  - Threat Intelligence Reporting and Information sharing
  - Malware Analysis

- **Cybersecurity State Coordinators and Cybersecurity Advisors**
  - Advisory Assistance
  - Cybersecurity Assessments
  - Incident Response Coordination
  - Working group collaboration
  - Public Private Partnership Development

Contact CISA to report a cyber incident

Call 1-888-282-0870 | email report@cisa.dhs.gov | visit https://www.cisa.gov

CISA Cyber Services: Right Organization. Right Service. Right time.

Regional Services

- Cyber Protective Visits
- Cyber Resilience Review
- External Dependencies Management Assessment
- Cyber Infrastructure Survey
- Workshops
  - Incident Management Workshop
  - Cyber Resilience Workshop
  - SLTT/ Cybersecurity Essentials Workshop
- Cyber Security Evaluations Tool (CPGs, RRA, CSF, etc.)

Enterprise Services

- Cyber Hygiene (Technical)
  - Vulnerability Scanning
  - Web Application Scanning
  - Continuous Phishing Campaign Assessment

National Services

- Remote Penetration Test
- Risk and Vulnerability Assessment
- Validated Architecture Design Review
- Red Team Assessment

STRATEGIC
(Management/C-Suite Level)

CSC/CSA Nominated

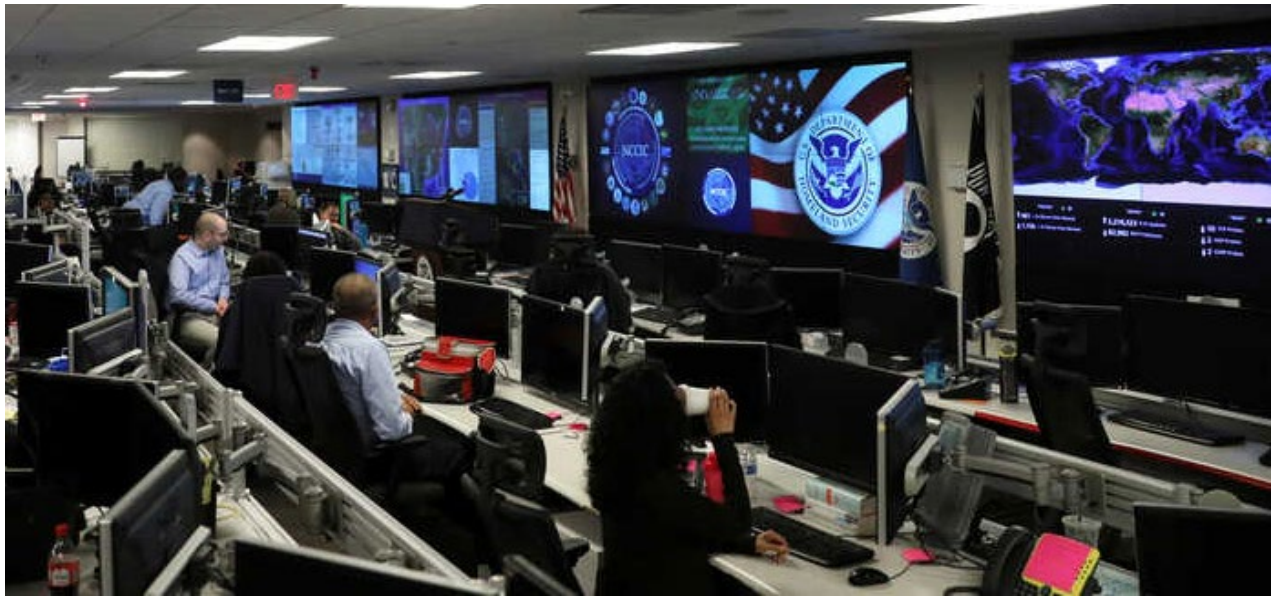
TECHNICAL
(Network-Administrator Level)

Cyber Exercise & Planning Program

CISA designs, develops, conducts, and evaluates cyber exercises ranging from small-scale, limited scope, discussion-based exercises to large-scale, internationally-scoped, operations-based exercises.

CISA offers the following services at no-cost on an as-needed and as-available basis:

- Cyber Storm Exercise (CISA's flagship national level cyber exercise)
- End-to-End Cyber Exercise Planning
- Cyber Exercise Consulting
- Cyber Planning Support
- **CISA Tabletop Exercise Packages (CTEPs)**



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

CISA CPGs

Cybersecurity Performance Goals (CPGs)

- A core set of cybersecurity practices with known risk-reduction value broadly applicable across sectors.
- A combination of recommended practices for IT and OT owners, including a prioritized set of security practices.
- Unique from other control frameworks
  - Clear, actionable, easily definable
  - Significantly and directly reduce the risk or impact caused by commonly observed, cross-sector threats and adversary TTPs
- **38 Performance Goals across 8 Categories:**
  - Account Security
  - Device Security
  - Data Security
  - Governance and Training
  - Vulnerability Management
  - Supply Chain/ Third Party
  - Response and Recovery
  - Other

Additional CISA Resources for SLTT

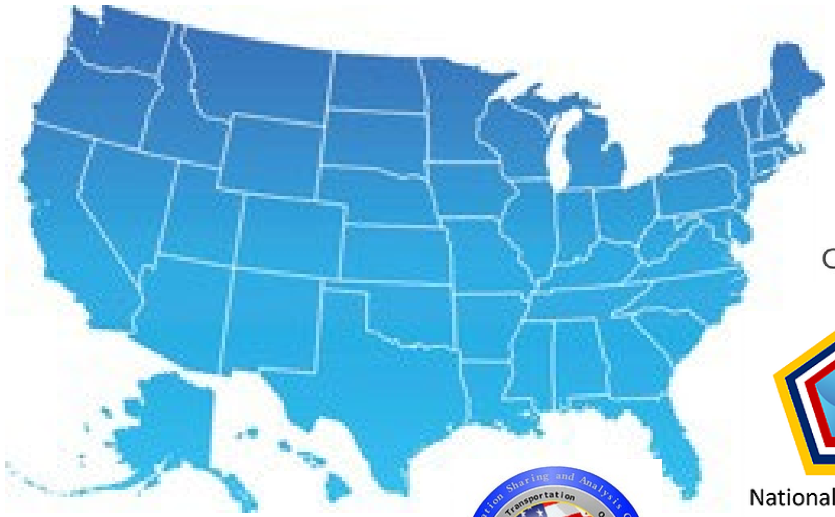
- **DotGov Program**
  - https://home.dotgov.gov/
- **Known Exploited Vulnerabilities (KEV) Catalog**
  - https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- **STOPRANSOMWARE.gov and #StopRansomware Guide**
  - https://www.cisa.gov/stopransomware
- **Catalog of FREE Cybersecurity Services and Tools**
  - https://www.cisa.gov/free-cybersecurity-services-and-tools

Additional Information Sharing Opportunities

- **Multi-State Information Sharing and Analysis Center:**
  - Focal point for cyber threat prevention, protection, response and recovery for state, local, tribal, and territorial governments.
  - Operates 24 x7 cyber security operations center, providing real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response. For more information, visit www.cisecurity.org/ms-isac or email info@msisac.org

MS-ISAC®
Multi-State Information Sharing & Analysis Center®

Elections Infrastructure ISAC™



- **ISACs and ISAOs:**
  - **Information Sharing and Analysis Centers** (ISACs) or **Organizations** (ISAOs) are communities of interest sharing cybersecurity risk, threat information, and incident management to members. For more information on ISACs, visit www.nationalisacs.org. For more on ISAOs visit www.isao.org/about.

ONG-ISAC

National Defense ISAC

FS-ISAC

RETAIL & HOSPITALITY ISAC

Real Estate ISAC Information Sharing and Analysis Center
Serving the Commercial Facilities Sector

WATER ISAC

SPACE ISAC

CISA Cybersecurity & Infrastructure Security Agency

Maritime Transportation System Information Sharing and Analysis Center

MEISAC Media + Entertainment Information Sharing Analysis Center

REN-ISAC

IT ISAC

DNG-ISAC

H-ISAC Health - ISAC

AVIATION ISAC

E-ISAC Electricity Information Sharing and Analysis Center

AUTO-ISAC Automotive Information Sharing and Analysis Center

TLP: GREEN

SHIELDS UP

To Wrap Up: Key Takeaways

1. Become familiar with CISA webpage and Subscribe to CISA Advisories
   - www.cisa.gov
2. Engage with your local CISA region and get in contact with your CSC/CSA
   - https://www.cisa.gov/cisa-regions
3. Sign-up for CISA's cyber hygiene services and other resilience services
   - Engage your local CSC or CSA
4. Sign up to be MS-ISAC member
   - https://www.cisecurity.org/ms-isac
5. Encourage lowering cyber incident reporting thresholds

No-Cost CISA Cybersecurity Services Available

- **Preparedness Resources**
  - Cybersecurity Assessments
  - Cybersecurity Training and Awareness
  - Cyber Exercises and "Playbooks"
  - Cybersecurity Advisories and Alerts
  - Operational Products / Threat Indicator Sharing
  - Known Exploited Vulnerabilities (KEV) Catalog
  - Cybersecurity Performance Goals (CPGs)
  - Free Cybersecurity Tools and Services Catalog
  - Information Products and Recommended Practices

- **Response Assistance**
  - 24/7 Response assistance and malware analysis
  - Incident Coordination
  - Threat intelligence and information sharing
- **Cybersecurity Advisors & Cybersecurity State Coordinators**
  - Advisory Assistance & Cyber Protective Visits
  - Cybersecurity Assessments and Workshops
  - Incident Response Coordination
  - Public Private Partnership Development

CISA Contact Information

John Harrison, CSC, VA – Region 3 **General CISA Inquiries**	John.Harrison@cisa.dhs.gov CISARegion3@cisa.dhs.gov
CISA URL	https://www.cisa.gov
To Report a Cyber Incident to CISA	***Call 1-888-282-0870*** ***Email*** *report@cisa.gov* ***visit*** *https://www.cisa.gov*

QUESTIONS?


CYBERSECURITY & INFRASTRUCTURE
SECURITY AGENCY
CISA