February 2024 Issue

In this edition:

- FBI, CISA, and ASD's ACSC Release Advisory on Play Ransomware
- CISA Releases Personal Security Considerations Action Guide: Critical Infrastructure Workers
- CISA Issues Request for Information on Secure by Design Software Whitepaper by February 20, 2024
- security.txt: A Simple File with Big Value
- CISA Releases Key Risk and Vulnerability Findings for Healthcare and Public Health Sector
- Enabling Threat-Informed Cybersecurity: Evolving CISA's Approach to Cyber Threat Information Sharing
- Best Practices for Securing Election Systems
- Secure Tomorrow Series Toolkit
- Statewide Communication Interoperability Plans Workshops
- Cyber Education and Training Updates

Report a Cyber Incident

CISA provides secure means for constituents and partners to report incidents, phishing attempts, malware, and vulnerabilities.

Report a Cybersecurity Incident: Report anomalous cyber activity and/or cyber incidents 24/7 to report@cisa.gov or (888) 282-0870.

- Report an Incident
- Report Phishing
- Report a Vulnerability

Report incidents as defined by NIST Special Publication 800-61 Rev 2, to include

- Attempts to gain unauthorized access to a system or its data,

- Unwanted disruption or denial of service, or
- Abuse or misuse of a system or data in violation of policy.

Federal incident notification guidelines, including definitions and reporting timeframes can be found here.

Organizations can also report anomalous cyber activity and/or cyber incidents 24/7 to: **Central@CISA.dhs.gov**

Learn More Here

Announcements

FBI, CISA, and ASD's ACSC Release Advisory on Play Ransomware

FBI, CISA, and the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) released a joint Cybersecurity Advisory (CSA), #StopRansomware: Play Ransomware, to disseminate Play ransomware group's tactics, techniques, and procedures (TTPs) and indicators of compromise (IOCs) identified through FBI investigations as recently as October 2023.

Play ransomware actors employ a double-extortion model, encrypting systems after exfiltrating data and have impacted a wide range of businesses and critical infrastructure organizations in North America, South America, Europe, and Australia.

FBI, CISA, and the ASD's ACSC encourage organizations review and implement the recommendations provided in the joint CSA to reduce the likelihood and impact of Play and other ransomware incidents. For more information, see CISA's #StopRansomware webpage, which includes the updated #StopRansomware Guide.

Learn More Here

CISA Releases Personal Security Considerations Action Guide: Critical Infrastructure Workers

In today's current threat environment, remaining vigilant and taking responsibility for your personal security is crucial for all critical infrastructure workers—both on and off the job. Critical infrastructure workers perform a vast array of services that operate, run and maintain key systems and assets necessary for modern American life. Being mindful of any risks or threats associated with your line of work and following all safety procedures will help protect you, those close to you and the infrastructure you serve. Personal safety can be broken into three main parts—Physical Security, Situational Awareness and Online Security. This non-exhaustive action guide can help you assess your security posture and provides options to consider to mitigate threats.

On Friday, January 5, the CISA released the Personal Security Considerations Action Guide: Critical Infrastructure Workers to help critical infrastructure workers assess their security posture and provide options to consider when mitigating threats.

The Personal Security Considerations Action Guide: Critical Infrastructure Workers helps critical infrastructure workers assess their security posture and provide options to consider whether they are on or off the job. This action guide provides actionable recommendations and resources intended to prevent and mitigate threats to a critical infrastructure worker's personal safety.

For questions regarding this action guide, please email central@cisa.gov

Learn More Here

CISA Issues Request for Information on Secure by Design Software Whitepaper by February 20, 2024

CISA published a Request for Information from all interested parties on secure by design software practices, including the Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software whitepaper, as part of our ongoing, collective secure by design campaign across the globe.

To better inform CISA's Secure by Design campaign, CISA and our partners seek information on a wide range of topics, including the following:

- **Incorporating security early into the software development life cycle (SDLC)**: What changes are needed to allow software manufacturers to build and maintain software that is secure by design, including smaller software manufacturers? How do companies measure the dollar cost of defects in their SDLC?
- **Security is often relegated as an elective in education:** What are some examples of higher education incorporating foundational security knowledge into their computer science curricula; When new graduates look for jobs, do companies evaluate security skills, knowledge, and experience during the hiring stage, or are employees reskilled after being hired?
- **Recurring vulnerabilities**: What are barriers to eliminating recurring classes of vulnerability; how can we lead more companies to identify and invest in eliminating recurring vulnerabilities; how could the common vulnerabilities and exposures (CVE) and common weakness enumeration (CWE) programs help?
- **Operational technology (OT)**: What incentives would likely lead customers to increase their demand for security features; Which OT products or companies have implemented some of the core tenants of secure by design engineering?
- **Economics of secure by design:** What are the costs to implement secure by design and default principles and tactics, and how do these compare to costs responding to incidents and breaches?

Learn more about how to submit comments and Secure by Design below.

Learn More Here

security.txt: A Simple File with Big Value

A frequent question we receive is why the creation of a "security.txt" file was included as one of the priority Cybersecurity Performance Goals (CPGs). Why is it so important? Well, it's such a simple concept, but it provides great value to all of those involved in vulnerability management and disclosure.

When security researchers and bug hunters uncover vulnerabilities in an organization's ecosystem, how do they even know who to reach out to? Without clear reporting channels, researchers may be unable to quickly discern where to report vulnerabilities – meanwhile the organization remains vulnerable to attackers. However, there is an opportunity for all organizations to overcome this obstacle in line with CISA's guidance through a simple text file - the security.txt file.

Earlier this year, CISA launched the Ransomware Vulnerability Warning Pilot (RVWP) program, which proactively discovers and notifies organizations of their exposure to internet-accessible vulnerabilities used in ransomware attacks. This is a proactive program used to enable organizations to take early mitigation measures before an incident occurs. Our current notification process can be hampered by the inability to find appropriate point of contact information for organizations. According to a recent study, only about a half of a percent of the world's top one million websites publish a security.txt file. The lack of this simple file leads to multiple emails and phone calls to the organization, delaying the notification process and the organization's awareness of the critical need to mitigate their risk to ransomware.

CISA's security.txt file resides on our public-facing domain, at https://www.cisa.gov/security.txt (this will redirect, per our canonical):

Contact: mailto:ContactOCIO@cisa.dhs.gov

Learn More Here

Partnerships

CISA Releases Key Risk and Vulnerability Findings for Healthcare and Public Health Sector

CISA published a Cybersecurity Advisory (CSA), *Enhancing Cyber Resilience: Insights from the CISA Healthcare and Public Health Sector Risk and Vulnerability Assessment*, detailing the agency's key findings and activities during a Risk and Vulnerability Assessment (RVA) conducted at a healthcare and public health (HPH) organization in early 2023. The advisory also provides network defenders and software manufacturers recommendations for improving their organizations' and customers' cyber posture, which reduces the impact of follow-on activity after initial access.

The CISA assessments team identified several findings as potentially exploitable vulnerabilities that could compromise the confidentiality, integrity, and availability of the tested environment. Tailored for HPH organizations of all sizes as well as for all critical infrastructure organizations, the advisory provides several recommended mitigations mapped to 16 specific cybersecurity weaknesses identified during the RVA. Also, the advisory provides three mitigation strategies that all organizations should implement: (1) Asset management and security, (2) Identity management and device security, and (3) Vulnerability, patch, and configuration management. Each strategy has specific focus areas with details and steps on how HPH entities can implement them to strengthen their cybersecurity posture.

This advisory builds on the CISA and Health and Human Services Healthcare Cybersecurity Toolkit and CISA's Mitigation Guide for HPH Sector that were recently released. The recommended mitigations for network defenders are mapped to the Cross-Sector Cybersecurity Performance Goals (CPGs).

The recommended actions for software manufacturers are aligned to the recently updated, Principles and Approaches for Secure by Design Software, a joint guide co-sealed by 18 U.S. and international agencies. It urges software manufacturers to

take urgent steps necessary to design, develop, and deliver products that are secure by design.

For more information and resources, HPH entities can visit CISA's Healthcare and Public Health Cybersecurity Toolkit and Healthcare and Public Health Sector webpages.

Learn More Here

Information Exchange

Enabling Threat-Informed Cybersecurity: Evolving CISA's Approach to Cyber Threat Information Sharing

One of CISA's most important and enduring roles is providing timely and actionable cybersecurity information to our partners across the country. Nearly a decade ago, CISA stood up our Automated Indicator Sharing, or AIS, program to widely exchange machine-readable cyber threat information. We know that the only constant in cybersecurity is change, and we're evolving our information sharing approaches to maximize value to our partners and keep pace with a changing threat environment.

Where Are We Going?

As the cyber threat environment evolves, so must our capabilities to analyze and share cyber threat information. When AIS was first designed, the U.S. Government was focused on filling an identified gap in cyber threat intelligence for many organizations and ensuring strong privacy controls. In the early days of AIS, the priority was speed. A decade later, the cybersecurity industry has matured substantially; current products and services are addressing information requirements for most organizations and, in an era of information overload, practitioners still require speed but value context, precision, and tailored insights over volume and velocity alone.

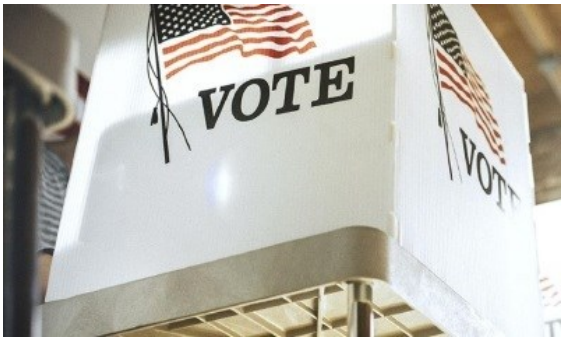
What to Expect Next?

Our goal is to facilitate collective, automated cyber defense through increased sharing and context, shaped by an acute understanding of the threat environment. While CISA implements this transition over the next two years, the AIS program will remain available, and we encourage users to continue leveraging this capability and actively share indicators back with CISA.

Our shared visibility into cyber threats is our best defense. When an organization identifies threat activity and keeps it to itself, our adversaries win. When we rapidly share actionable information across a community of partners, we take back the advantage. And, when we turn actionable information into strategic investments to drive the most important mitigations, we achieve enduring change. In this new year, we encourage every organization to make a commitment- perhaps a New Year's resolution- to cybersecurity information sharing, including incident information, indicators of compromise, or even feedback and insights that could benefit peers across the Nation. We look forward to sharing more details about Threat Intelligence Enterprise Services (TIES) and our cyber threat exchange modernization initiatives throughout the year.

Learn More Here

Best Practices for Securing Election Systems



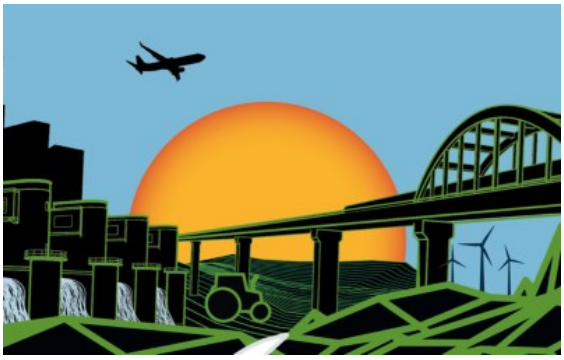
By adhering to cybersecurity best practices, election organizations—including state, local, tribal, and territorial (SLTT) governments—can improve the security of their election systems. CISA developed the best practices found in the links below from lessons learned through engagements with SLTT governments, election stakeholders, and others. Organizations can implement these best practices, which harden enterprise networks and strengthen election infrastructure, at little or no cost.

Find CISA's latest election systems best practices at

Election Security | Cybersecurity and Infrastructure Security Agency CISA

Learn More Here

Secure Tomorrow Series Toolkit



The **Secure Tomorrow Series Toolkit** is a diverse array of interactive and thought-provoking products uniquely designed to assist stakeholders across the critical infrastructure community to self-facilitate and conduct strategic foresight activities that will enable them to derive actionable insights about the future, identify emerging risks, and develop risk management strategies that, if taken today, could enhance long-term critical infrastructure security and resilience to implement now.

Central to the Secure Tomorrow Series effort is the selection of topics that are likely to have highly disruptive impact across multiple National Critical Functions. To this end, the National Risk Management Center worked with subject matter experts from academia, think tanks, the private sector, and the National Labs to help build and refine the knowledge base that underlies the Toolkit activities.

These free voluntary resources are available to stakeholders in every critical infrastructure sector. More specifically, the Toolkit will assist users in identifying and examining risk mitigation strategies, managing uncertainty and encouraging strategic foresight methods in their long-term planning.

By downloading the Toolkit, users will learn how to conduct foresight activities that will enable them to derive actionable insights about the future, identify emerging risks, and proactively develop corresponding risk management strategies they can implement now. As a starting point, please review the Scenarios Workshop Synopses about future risks, and then move on to explore the Matrix Games and Cross-Impacts depending on time and participant needs and interest.

Learn More Here

Education and Training and Workshops

Statewide Communication Interoperability Plans Workshops

Statewide Communication Interoperability Plans (SCIPs) are locally-driven, multi-jurisdictional, and multi-disciplinary statewide plans to enhance emergency communications. The SCIP creates a single resource for all stakeholders and a unified approach for enhancing interoperable communications for public safety and officials at all levels of government. SCIPs define the current and future direction for interoperable and emergency communications within a state or territory.

SCIPs are comprehensive plans which outline the:

- Current and future interoperable and emergency communications environment;
- Goals with specific steps for action (including owners and completion timeframes);
- Defined mechanisms to measure achievements; and,
- Process by which the state will record progress and challenges each year.

The SCIP structure is designed to demonstrate accomplishments and challenges and define the strategic direction and priorities in the state or territory for the next three to five years. SCIPs focus on the strategic direction and alignment of all emergency communications (voice and data) in the state, and include all forms of

related technology and a broader community of stakeholders. They are living documents that should be updated on an as needed basis.

SCIP Workshops

CISA supports states and territories in the implementation of their SCIPs by providing SCIP workshops.

During the workshops, state and local representatives gather to discuss communications gaps and ways to implement SCIP initiatives. The SCIP Implementation Workshops are participatory and hands-on and focus on the specific needs and priorities of each state and territory.

In preparation for the In-Person or Virtual SCIP workshop, CISA utilizes on-line surveys and webinars to gather input from constituents. Webinars are conducted for:

- Interoperability Governance
- Technology and Cybersecurity
- Funding

The gathered input is then crafted into the SCIP during a one- or two-day workshop.

For More Information

Further information on the SCIP process is available in the SCIP Overview Guide.

For additional information on requesting a SCIP workshop, contact TARequest@cisa.dhs.gov

Learn More Here

Cyber Education and Training Updates

Highlights: What You Want to Know

CISA has recently announced two new collaborative efforts, as it continues striving to maximize access for underrepresented communities in cyber and establish alliances that strengthen CISA's ability to reach the national cyber talent pool:

The CyberSkills2Work program, part of the University of West Florida Center for Cybersecurity, is an intensive online cybersecurity training program focused on critical infrastructure security and industrial control systems security. It is designed to help individuals launch or advance cybersecurity careers, with an emphasis on

federal, state, and local government personnel, transitioning military, veterans, women, and underrepresented minorities.

CISA offers new micro-challenges on Try Cyber that are now part of the Cyber Careers Pathway Tool, located on the National Initiative for Cybersecurity Careers and Studies (NICCS™) website. For K-12 students and individuals looking to reskill or transition from a non-cyber career, CISA's micro-challenges provide a chance to experience the knowledge, skills, and tasks enacted in the top cybersecurity workforce roles.

Industrial Control Systems (ICS): We offer free, virtual ICS trainings geared toward Critical Infrastructure owners and operators. The trainings are designed to reduce cybersecurity risks to critical infrastructure and encourage cooperation between CISA and the private sector. Trainings vary in length and run from 8:00 a.m. – 5:00 p.m. MST (10:00 a.m. – 7:00 p.m. EST). All trainings are conducted through Online Training or CISA Virtual Learning Portal (VLP), with the exception of the three- or four-day, in-person courses at Idaho National Labs (INL) in Idaho Falls, ID.

ICS Training Events through February 2024

Date	Course Code	Course	Location
02/05/2024-02/23/2024	401v	**Industrial Control Systems Evaluation (401v)**	Scheduled Online Training
02/05/2024-02/23/2024	301v	**Industrial Control Systems Cybersecurity (301v)**	Scheduled Online Training
02/06/2024-02/08/2024	401L	**Industrial Control Systems Evaluations (401L) – In-Person 3 Days**	IN-PERSON TRAINING (3 days)
02/12/2024-02/15/2024	301L	**Industrial Control Systems Cybersecurity Training (301L) – In-Person 4 Days**	IN-PERSON TRAINING (4 days)
On Demand	100W	**Operational Security (OPSEC) for Control Systems**	CISA Training Virtual Learning Portal (VLP)

On Demand	210W-1	**Differences in Deployments of ICS**	CISA Training Virtual Learning Portal (VLP)
On Demand	210W-2	**Influence of Common IT Components on ICS**	CISA Training Virtual Learning Portal (VLP)
On Demand	210W-3	**Common ICS Components**	CISA Training Virtual Learning Portal (VLP)
On Demand	210W-4	**Cybersecurity within IT & ICS Domains**	CISA Training Virtual Learning Portal (VLP)
On Demand	210W-5	**Cybersecurity Risk**	CISA Training Virtual Learning Portal (VLP)
On Demand	210W-6	**Current Trends (Threat)**	CISA Training Virtual Learning Portal (VLP)
On Demand	210W-7	**Current Trends (Vulnerabilities)**	CISA Training Virtual Learning Portal (VLP)
On Demand	210W-8	**Determining the Impacts of a Cybersecurity Incident**	CISA Training Virtual Learning Portal (VLP)
On Demand	210W-9	**Attack Methodologies in IT & ICS**	CISA Training Virtual Learning Portal (VLP)
On Demand	210W-10	**Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1**	CISA Training Virtual Learning Portal (VLP)
On Demand	210W-11	**Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2**	CISA Training Virtual Learning Portal (VLP)

On Demand	FRE2115	**Industrial Control Systems Cybersecurity Landscape for Managers**	CISA Training Virtual Learning Portal (VLP)

To learn more or sign up, visit: **https://www.cisa.gov/ics-training-calendar**

**The following virtual courses are prerequisites to attending in-person 301 and 401 trainings hosted by CISA at the Idaho National Laboratory:*

- *ICS 301v: Focuses on understanding, protecting and securing ICS from cyberattacks.*
- *ICS 401v: Focuses on analyzing and evaluating an ICS network to determine its defense status and what changes need to be made.*

CyberWarrior's Master Class: The CISA Cyber Workforce Development and Training for Underserved Communities program increases opportunity and economic mobility for people of all backgrounds through training, mentorship and technology. Our program partners at the CyberWarrior Academy, deliver hands-on, intensive, lab-driven technical training in cybersecurity methods and procedures.

CyberWarrior Training Events

Date	Audience	Course
02/08/2024	General Public	**February Master Class – Intro to Splunk** February Master Class - Intro to Splunk | CyberWarrior.com
03/21/2024	General Public	**March Master Class – Intro to Python** March Master Class – Intro to Python | CyberWarrior.com

To learn more or sign up, visit: **https://www.cyberwarrior.com/cybersecurity-events/**

CISA's K – 12 Cybersecurity Education Training Assistance Program (CETAP): Through CETAP grantee, we offer K-12 teachers with cybersecurity curricula and education tools. CYBER.ORG develops and distributes cybersecurity, STEM and computer science curricula at no cost to K-12 educators across the country. Below are upcoming training events through CYBER.ORG.

CYBER.ORG Training Events through February 2024

Date	Audience	Course
09/01/2023-08/31/2024	K-8 Educators	**K-8 Cybersecurity Teachers Cohort, 2023-2024 School Year:** Are you a K-8 educator teaching cybersecurity in a classroom this 2023-2024 school year? Come exchange ideas with other teachers across the U.S.! K-8 Cybersecurity Teachers Cohort 2023-2024 | CYBER.org
09/01/2023-08/31/2024	High School Educators	**High School Cybersecurity Teachers Cohort, 2023-2024 School Year:** Are you an educator teaching cybersecurity in a high school classroom this 2023-2024 school year? Come exchange ideas with fellow U.S. educators! High School Cybersecurity Teachers Cohort 2023-2024 | CYBER.org
09/01/2023-08/31/2024	K-12 Educators	**CYBER.ORG Range Teachers Cohort, 2023-2024 School Year:** Are you an educator using the Cyber Range during the 2023-2024 school year? Come exchange ideas with fellow U.S. educators doing the same! CYBER.ORG Range Teachers Cohort 2023-2024 | CYBER.org

To learn more or sign up, visit: **https://cyber.org/events**

Federal Cyber Defense Skilling Academy: The Federal Cyber Defense Skilling Academy helps civilian federal employees develop their cyber defense skills through training in the baseline knowledge, skills and abilities of a Cyber Defense Analyst (CDA). Students will have the opportunity to temporarily step away from their current role while they participate in the intense, full-time, three-month accelerated training program. Below are the Skilling Academy cohort dates for FY24:

Skilling Academy Program Dates through 2024

Academy	Program Start/End Date	Applications Open	Applications Close
5 and 6	02/05/24 – 05/15/24	11/27/2023	01/03/2024
7 and 8	03/04/24 – 06/12/24	12/18/2023	01/11/2024
9 and 10	04/01/24 – 07/11/24	01/22/2024	02/08/2024
11 and 12	05/06/24 – 08/14/24	02/19/2024	03/07/2024

To learn more or register, visit**:** **https://www.cisa.gov/SkillingAcademy**

Continuous Diagnostics and Mitigation (CDM): We offer instructor led, hands-on CDM Dashboard training for U.S. Executive Branch employees and contractors in our virtual cyber range training environment. These courses are intended for those at agencies participating in the CDM program who monitor, manage and/or oversee controls on their information systems (e.g., ISSOs, CDM POCs, ISSMs and those who report metrics and measures).

The CDM training goal is to provide the learner the basics of CDM and using the CDM Dashboard capabilities to help mitigate agency threats. We will also provide numerous CDM resources and external references.

All courses will be taught utilizing the latest version of the CDM Dashboard (ES-6.0.5) within a cyber virtual training range (CVLE). The course content has been updated and will focus on the current version ES-6 of the CDM Dashboard, including the latest dashboard content pack, version 6.0.5. The latest CDM Dashboard capabilities will be discussed, including FISMA Automation. The current CDM courses fall into the 100 level (Introductory) and 200 level (Intermediate) level offerings.

CDM Training Events through February 2024

Date	Course Code	Registration Opens	Course	Hours
02/06/2024	CDM142	12/29/2023	**Asset Management with the CDM Agency Dashboard**	4
02/15/2024	CDM201	01/08/2024	**Identity and Access Management within the CDM Agency Dashboard**	4

02/22/2024	CDM202	01/16/2024	**Managing Configurations Settings with the CDM Agency Dashboard**	4
02/29/2024	CDM203	01/19/2024	**CDM Dashboard Role-Based Training - System Analyst**	4

To learn more or register visit: **https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-training**

Contact Us: *Education@cisa.dhs.gov*

Want to subscribe? Sign up a co-worker or friend?

Email education@cisa.dhs.gov to receive this Cyber Training Bulletin each month!

For additional, ongoing cyber training check out the **Cybersecurity Workforce Training Guide**

Learn More Here

The CISA Community Bulletin is a monthly publication that shares cybersecurity webinars and workshops, new publications, and best practices.

***To access past editions of this CISA Community Bulletin newsletter, please visit the** CISA Community Bulletin archive.*