March 2024 Issue

In this edition:

- Secure Our World
  - Secure Our World at Super Bowl LVIII & NFL Partnership
- Announcements
  - Director Jen Easterly testified on the nation-state threat the People's Republic of China (PRC) poses to U.S. critical infrastructure.
  - CISA and FBI release Guidance to Increase Awareness of Chinese-manufactured Unmanned Aircraft Systems (UAS) Risks
  - Logging Made Easy (LME) v1.2.0 Just Dropped a Cyber Mic
- Partnerships
  - CISA and International Partners Release Guidance on Engaging with Artificial Intelligence
  - CISA and FBI Release joint Cybersecurity Advisory (CSA) Known Indicators of Compromise Associated with Androxgh0st Malware
  - CISA, FBI and EPA Release Incident Response Guide for Water and Wastewater Systems Sector
  - CISA's Stakeholder Engagement Division (SED) Sector Liaisons
- Information Exchange
  - Handling Destructive Malware
  - The Cloud Log Aggregation Warehouse (CLAW)
  - Release of the Connected Communities Procurement and Implementation Guidance
  - New ChemLock Resources
  - CISA Considers Software Developers a Key Part of the Cybersecurity Workforce
- Education and Training and Workshops
  - Quarterly ChemLock Trainings

- Region 8 Training and Exercise Resources Webinar

To see the latest CISA Cybersecurity Alerts and Advisories visit Cybersecurity Alerts & Advisories | CISA

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

Secure Our World at Super Bowl LVIII & NFL Partnership

Last month the National Football League (NFL) announced they are joining the Secure Our World cybersecurity awareness effort. Launched in September 2023 and led by CISA, Secure Our World encourages individuals, families, and small to medium-sized businesses to take simple steps, like using strong passwords, enabling multifactor authentication, recognizing and reporting phishing, and updating software, to stay safe and secure online. The cybersecurity tips were seen at the NFL Fan Experience during Super Bowl Week and during the big game. The NFL has also committed to working with their teams to advance cybersecurity awareness throughout the 2024-2025 season. Secretary of Homeland Security Alejandro N. Mayorkas traveled to Las Vegas for the announcement and was joined by CISA's Assistant Director for Stakeholder Engagement, Alaina Clark, and Associate Director for Strategic Relations, Kevin Dillon.

For more information, see CISA's Secure Our World webpage, which includes the Secure Our World: Super Bowl LVIII Video.

Learn More Here

Announcements

Director Jen Easterly testified on the nation-state threat the People's Republic of China (PRC) poses to U.S. critical infrastructure

On January 31, the House Select Committee on the Strategic Competition Between the United States and the Chinese Communist Party (CCP) conducted a hearing on the CCP's nation-state threat to the American homeland. During the hearing, the Cybersecurity and Infrastructure Security Agency (CISA) Director Jen Easterly testified on the nation-state threat the People's Republic of China (PRC) poses to U.S. critical infrastructure. During her testimony, Director Easterly addresses CISA's concern about a strategic shift in the PRC's malicious cyber activity against U.S. critical infrastructure, and what the agency is doing to deter potential interference from the PRC.

We invite you to read Director Easterly's opening statement Opening Statement by CISA Director Jen Easterly | CISA, or read it below. We also encourage you to visit cisa.gov/China to learn more about the agency's efforts around the PRC. Our updated page on the PRC also links to the Director's submitted testimony and a full recording of the hearing which is housed on the Committee's page: Hearing Notice: The CCP Cyber Threat to the American Homeland and National Security | Select Committee on the CCP (house.gov).

Learn More Here

CISA and FBI release Guidance to Increase Awareness of Chinese-manufactured Unmanned Aircraft Systems (UAS) Risks.

The Cybersecurity and Infrastructure Security Agency (CISA), in coordination with the Federal Bureau of Investigation's (FBI) Cyber Division, released *Cybersecurity Guidance: Chinese-Manufactured UAS*. CISA and FBI developed this guidance to increase awareness on the risks associated with Chinese-manufactured Unmanned Aircraft Systems (UAS).

This product provides critical infrastructure and state, local, tribal, and territorial (SLTT) partners insight into Chinese-manufactured UAS that carry an increased risk of the Chinese Communist Party gaining unauthorized access to sensitive information. It also provides a series of cybersecurity recommendations to mitigate risk to networks and information.

The *Cybersecurity Guidance: Chinese-Manufactured UAS* product is a continuation of CISA's suite of products related to UAS cybersecurity, including *Cybersecurity Best Practices for Operating Commercial Unmanned Aircraft Systems* and *Secure Your Drone: Privacy and Data Protection Guidance*.

To access this guidance and learn more about Chinese-manufactured UAS vulnerabilities and cybersecurity recommendations, visit: https://www.cisa.gov/resources-tools/resources/cybersecurity-guidance-chinese-manufactured-uas.

Learn More Here

Logging Made Easy (LME) v1.2.0 Just Dropped a Cyber Mic

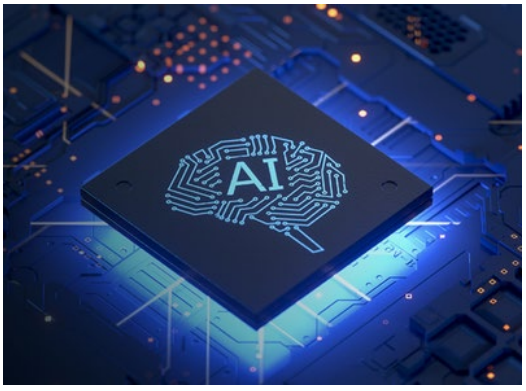
Exciting news, cyber guardians! Logging Made Easy (LME) v1.2.0 just dropped a cyber mic, taking log management to new heights! Explore LME's new sleek dashboards, bug fixes, and a fortified ELK stack at v8.11.1.Dive deeper at CISA's site and LME's GitHub.

Logging Made Easy (LME) is CISA's reimagined version of an internationally well-known log management toolset, which offers a reliable, no-cost centralized log management solution. LME is the perfect option for those organizations hampered by limited resources and currently lacking a comparable capability.

Learn More Here

Partnerships

CISA and International Partners Release Guidance on Engaging with Artificial Intelligence



Joint guidance on Engaging with Artificial Intelligence was released on January 23, 2024. CISA, along with the Canadian Centre for Cyber Security (CCCS), New Zealand National Cyber Security Centre (NCSC-NZ), United Kingdom (UK) National Cyber Security Centre (NCSC-UK), Federal Bureau of Investigation (FBI), and National Security Agency (NSA) collaborated with the Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC), who led the development of this product.

This guidance focuses on using AI systems securely rather than developing secure AI systems. For guidance on the latter, the authoring agencies encourage developers of AI systems to refer to the joint Guidelines for Secure AI System Development.

Specifically, organizations are provided with a summary of threats to AI systems, best practices for managing risk, and recommended mitigations for self-hosted and third-party hosted AI systems. The guide also offers mitigation considerations for organizations with guiding questions to help organizations assess an AI system's cybersecurity implications.

Organizations that use or are considering AI systems need to assess the system's cyber security implications and evaluate the benefits, risks and consequences of the system within the organization's context. We encourage these organizations to review this guide.

Learn More Here

CISA and FBI Release joint Cybersecurity Advisory (CSA) Known Indicators of Compromise Associated with Androxgh0st Malware

CISA and FBI released joint Cybersecurity Advisory (CSA) Known Indicators of Compromise Associated with Androxgh0st Malware to disseminate known indicators (IOCs) and tactics, techniques and procedures (TTPs) associated with threat actors using Androxgh0st malware.

Androxgh0st malware establishes a botnet to scan for websites using the Laravel web application framework. On these websites, threat actors have attempted to determine if the domain's root-level .env file is exposed and if they contain credentials for accessing additional services.

Multiple investigations are ongoing regarding Androxgh0st malware's capability to establish a botnet and further identify and compromise vulnerable networks. Threat actors exploiting Androxgh0st malware have been observed exploiting specific vulnerabilities which could lead to remote code execution; those common vulnerabilities and exposures (CVE) are CVE-2017-9841 (PHP Unit Command), CVE-2021-41773 (Apache HTTP Server versions) and CVE-2018-15133 (Laravel applications).

Recommended actions include prioritize patching known exploited vulnerabilities in internet-facing systems; review and ensure only necessary servers and services are

exposed to the Internet; and review platforms or services that have credentials listed in .env files for unauthorized access or use.

All organizations are urged to review the advisory, implement recommended mitigations, and validate your organization's security controls against the threat behaviors mapped to the MITRE ATT&CK.

Read the latest Cybersecurity Advisories and Alerts on CISA.gov

Subscribe here to receive alerts via email of Cybersecurity Advisories and other cybersecurity topics from CISA.

Learn More Here

CISA, FBI and EPA Release Incident Response Guide for Water and Wastewater Systems Sector

Cybersecurity and Infrastructure Security Agency (CISA), Environmental Protection Agency (EPA) and Federal Bureau of Investigation (FBI), published "Incident Response Guide: Water and Wastewater Systems (WWS) Sector."

Developed in collaboration with over 25 WWS Sector industry, nonprofit, and state/local government partners, this guide assists WWS owners and operators with best practices for cyber incident response and information about federal roles, resources and responsibilities for each stage of the response lifecycle.

This resource covers the four stages of the incident response lifecycle. For each stage, the guidance identifies ways to interface with the federal-level response and highlights key measures to better posture and prepare for collaboration with federal partners.

Technical expertise is not required to understand and use this guide. All WWS utilities are encouraged to use this incident response guide to augment their incident response planning and collaboration with federal partners and the WWS before, during, and following a cyber incident. Familiarity with this guide will better prepare WWS utilities to respond to—and recover from—a cyber incident.

For more information and resources, WWS utilities are encouraged to visit cisa.gov/water.

Learn More Here

CISA's Stakeholder Engagement Division (SED) Sector Liaisons

CISA’s Stakeholder Engagement Division (SED) Sector Liaisons

There are 16 critical infrastructure sectors vital to the United States, with assets, systems, and networks deemed crucial for national security, economic well-being, public health or safety. Each sector has unique characteristics, operating under the oversight of a designated Sector Risk Management Agency (SRMA). DHS/CISA serves as the SRMA for eight sectors, while for the other eight, CISA appoints Sector Liaisons to coordinate with relevant Federal departments and agencies.

Who are the Liaisons and what do they do?

CISA collaborates with other federal agencies managing critical infrastructure risks, implementing various coordination mechanisms. Sector Liaisons, acting as subject matter experts, engage with their assigned sectors to understand SRMA priorities and challenges, advancing CISA's mission. Due to sector-specific differences, Liaisons focus on enhancing risk reduction capabilities, building security capacity, and supporting CISA as the National Coordinator, functioning in discrete areas of responsibility to protect cyber and physical infrastructure.

Critical Infrastructure Sector	Designated SRMA:	CISA Sector Liaison
Defense Industrial Base	Department of Defense (DoD)	Rola Hariri, rola.hariri@cisa.dhs.gov
Energy	Department of Energy (DoE)	Justin Verbarendse, justin.verbarendse@cisa.dhs.gov

Financial Services	Department of Treasury (Treasury)	Ashley Freitas, ashley.freitas@cisa.dhs.gov
Food and Agriculture	Department of Agriculture (USDA) & Department of Health and Human Services (HHS)	Justin Louchheim, justin.louchheim@cisa.dhs.gov
Government Facilities	General Services Administration (GSA) & DHS/Federal Protective Service (FPS)	Arlene Guevara Zuleta, arlene.guevara-zulet@cisa.dhs.gov
Healthcare and Public Health	Health and Human Services (HHS)	Dr. Charles Sweat, charles.sweat@cisa.dhs.gov
Transportation Systems	DHS/Transportation Security Administration (TSA) & Department of Transportation (DoT)	Nancy Pomerleau, Nancy.Pomerleau@cisa.dhs.gov
Water and Wastewater Systems	Environmental Protection Agency (EPA)	Lauren Wisniewski, lauren.wisniewski@cisa.dhs.gov

Additionally, the SRMA Sector Liaisons are led by Section Chief Justin Rinck, who can be reached at: justin.rinck@cisa.dhs.gov. For more information on the SRMA Sector Liaisons, please reach out to: srmaliaisons@cisa.dhs.gov.

Learn More Here

Information Exchange

Handling Destructive Malware

Destructive malware can threaten an organization's access to critical assets and data, but there are steps organizations can take to protect their enterprise networks before and after a destructive malware incident.

Destructive malware is malicious code that is designed to destroy data. It impacts the availability of critical assets and data, presenting a direct threat to an organization's daily operations.

Organizations must enhance vigilance and assess their readiness, including planning, preparation, detection, and response for continuously evolving indicators and modules related to destructive malware. It is crucial to actively prepare for and respond to such events.

Destructive malware leverages common communication tools, spreading through email, instant messages, website-delivered Trojan horses, and virus-infected files from peer-to-peer connections. It aims to exploit system vulnerabilities for discreet access.

The malware can target various systems and spread across networks. Organizations should evaluate their environment for unusual channels facilitating malware delivery and propagation. This includes assessing enterprise applications like patch management, asset management, remote assistance software, antivirus software, systems of administrative personnel, centralized backup servers, and file shares.

Additionally, threat actors might compromise resources like centralized storage devices and network devices, posing risks such as direct access to data warehouses and manipulation of routing tables that could impact critical network resources.

To learn more about best practices and planning strategies to strengthen an organization's resilience against destructive malware, check out CISA's Blog on Handling Destructive Malware.

Learn More Here

The Cloud Log Aggregation Warehouse (CLAW)

The Cloud Log Aggregation Warehouse (CLAW) provides persistent cloud monitoring of FCEB cloud infrastructure and assets. It ingests logs from specific services from participating FCEB agencies, such as various components of DHS, Department of State (DoS), Department of Transportation (DoT), and Department of Energy (DOE). Service logs ingested from participating agencies vary and currently CLAW has capability to gather information from Microsoft Azure Active Directory, Microsoft M365, Azure Firewall, and authentication logs from Amazon Web Services (AWS) Cloud Trail.

CLAW is built using cloud native services, allowing FCEB agencies to take advantage of low inter-region data transfer cost. Cloud data collected from individual agencies preserves agency data isolation and each agency has a dedicated S3 data store.

CLAW has enabled analytics groups to effectively unite and actively work towards a common goal of producing better cloud analytics. Prior to the introduction of CLAW, different analytic groups were fragmented across CSD; little to no communications occurred between groups and efforts in analytics development were redundant. OTD and CFS were the major driving forces of this project. CLAW has plans for expansions for both onboarding new FCEB agency partners and expanding logs collected from more services.

Learn More Here

Release of the Connected Communities Procurement and Implementation Guidance

Connected Communities Initiative (CCI) released the *Connected Communities Procurement and Implementation Guidance*. Developed in close collaboration between CCI and the Department of Homeland Security Office of Cyber, Infrastructure, Risk, and Resilience Policy, this guidance is designed to encourage conversations at the state, local, tribal and territorial (SLTT) government levels about critical questions to ask when procuring and implementing smart and connected technologies, and to serve as a resource for SLTT governments to plan for security and resilience in their supply chains. The guidance is illustrated by two infographics. The first provides a list of questions that local leaders can utilize internally to help clarify their procurement and implementation goals. The second infographic presents a list of questions for local

leaders to ask third-party vendors. The *Connected Communities Procurement and Implementation Guidance* can be found here: Connected Communities Procurement and Implementation Guidance | CISA.

Learn More Here

New ChemLock Resources

CISA OBP Launches Comprehensive Bomb Threat Guide

As the threat landscape evolves, security measures must respond in kind to address it. The recently published CISA Office for Bombing Prevention (OBP) Bomb Threat Guide was developed to help decision makers respond to bomb threats in an orderly and controlled manner.

When it comes to bomb threats, having a clear, specific and well-developed plan can save lives, protect critical infrastructure, and reduce the financial impact. Each bomb threat is unique and requires rapid evaluation to mitigate the immediate impact and manage in accordance with site needs. CISA OBP recommends owners and operators periodically review bomb threat guidance (including this product) and collaborate with first responders to establish and rehearse a bomb threat management plan that addresses each risk level appropriate for their specific site location.

Highlights from the Bomb Threat Guide include:

- Planning and preparation information
- Threat assessments
- Response options
- Suspicious items recognition
- Additional resources and training opportunities

CISA's ChemLock program released three new customizable templates that facilities and organizations can use as part of developing and implementing a facility security plan.

- ChemLock: Chemical Inventory Template – This document serves as a template for maintaining an accurate inventory of the location, quantities, and physical states of chemicals at your facility.
- ChemLock: Personnel Background Checks Policy Template – This document includes background checks that facilities can consider conducting for personnel and serves as a template for a personnel background checks policy.
- ChemLock: Security Organization Roles and Responsibilities Template – This document includes a listing of security roles and responsibilities. It serves as a template to assist your facility in developing and maintaining a security organization.

For more information on how to develop a facility security plan, see the ChemLock Security Plan webpage or contact the ChemLock team at ChemLock@cisa.dhs.gov.

Learn More Here

CISA Considers Software Developers a Key Part of the Cybersecurity Workforce

CISA published a blog titled We Must Consider Software Developers a Key Part of the Cybersecurity Workforce. Even after seeing some of the most brazen ransomware attacks ever and increasingly bold cyberattacks on the federal government by nation-state adversaries within the past few years, cybersecurity in computer science education remains an elective. Indeed, of the top 24 American universities in computer science, 23 still don't require a cybersecurity course.

Cybersecurity is viewed as a subdiscipline, much like graphics or human-computer interaction – not essential knowledge that every future software developer should be equipped with as they enter the workforce. This oversight is unacceptable. All too often, attacks exploit simple weaknesses that any developer with basic security knowledge could have stopped.

At CISA, we're continuing to drive the mission of making software secure by design. This mission includes working across academia and industry to further establish cross-

disciplinary education for both computer science and cybersecurity professionals to better integrate security in the earliest stages of product development.

To learn more, read our full blog post and visit CISA's Secure by Design webpage.

Learn More Here

CISA Launches #Protect2024 Resources Webpage for State and Local Election Officials

Today, as part of its unwavering commitment to safeguarding the integrity of the nation's electoral processes, CISA proudly announced the launch of the #Protect2024 website.

As part of the #Protect2024 initiative, CISA developed a webpage to serve as a central point for consolidated critical resources, training lists and security service offerings to support the over 8,000 election jurisdictions for the 2024 election cycle. These efforts build upon prior years of working with elections officials to mitigate the cyber, physical, and operational risks to election infrastructure.

CISA encourages stakeholders, government officials, and the public to explore the #Protect2024 website, joining the collective effort to ensure a secure and resilient 2024 election cycle.

Learn More Here

U.S. and International Partners Publish Cybersecurity Advisories on People's Republic of China State-Sponsored Hacking of U.S. Critical Infrastructure

CISA in partnership with U.S. and international government agencies, published a Joint Cybersecurity Advisory (CSA) on malicious activity by a People's Republic of China (PRC) state-sponsored cyber actor, known as Volt Typhoon, to compromise critical infrastructure and associated actions that should be urgently undertaken by all organizations.

CISA and its U.S. government partners have confirmed that this group of PRC state-sponsored cyber actors has compromised entities across multiple critical infrastructure sectors, including communications, energy, transportation, and water and wastewater,

in the United States and its territories. The data and information CISA and its U.S. government partners have gathered strongly suggest the PRC is positioning itself to launch destructive cyberattacks that would jeopardize the physical safety of Americans and impede military readiness in the event of a major crisis or conflict with the United States.

In addition to the joint Cybersecurity Advisory, CISA and our partners also released complementary Joint Guidance to help all organizations effectively hunt for and detect the sophisticated types of techniques used by actors such as Volt Typhoon, known as "living off the land." In recent years, the U.S. has seen a strategic shift in PRC cyber threat activity from a focus on espionage to pre-positioning for possible disruptive cyberattacks against U.S. critical infrastructure. By using "living off the land" techniques, PRC cyber actors blend in with normal system and network activities, avoid identification by network defenses, and limit the amount of activity that is captured in common logging configurations.

Today's joint CSA is based primarily on technical insights gleaned from CISA and industry response activities at victim organizations within the United States, primarily in communications, energy, transportation, and water and wastewater sectors. Our complementary Joint Guidance is derived from those insights as well as previously published products, red team assessments, and industry partners.

Learn More Here

Education, Training, and Workshops

Quarterly ChemLock Trainings

CISA's ChemLock program provides the ChemLock training courses every quarter on a first-come, first-serve basis.

ChemLock: Introduction to Chemical Security

This course provides an introduction to identifying, assessing, evaluating, and

mitigating chemical security risks. This easy-to-understand overview identifies key components and best practices of chemical security awareness and planning to help kickstart chemical security discussions at your facility.

This course runs 1-2 hours in length and is appropriate for all personnel regardless of their level of involvement with dangerous chemicals.

- Register for April 8, 2024 – Noon-2 pm ET
- Register for July 11, 2024 – 1-3 pm ET
- Register for October 7, 2024 – 11 am-1 pm ET

ChemLock: Secure Your Chemicals Security Planning

This course walks through how to create a tailored, scalable security plan that meets the business model and unique circumstances of a facility. Participants will learn the key elements of a chemical security plan and benefit from examples, lessons learned, and best practices.

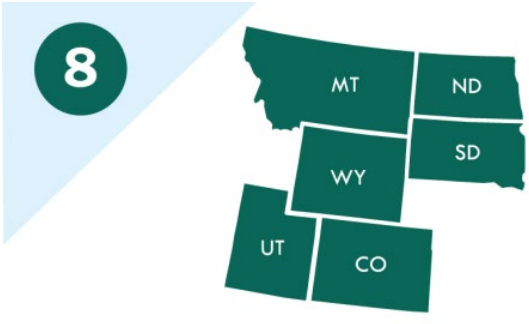
This course runs 2-3 hours in length and is designed to help leadership, facility security personnel, and other applicable personnel understand, develop, and implement a facility security plan.

- Register for May 6, 2024 – Noon-3 pm ET
- Register for August 7, 2024 – 11 am-2 pm ET
- Register for November 7, 2024 – 1-4 pm ET

For more information or to request a specific training for your facility, please visit the ChemLock Training webpage.

Learn More Here

Region 8 Training and Exercise Resources Webinar



The Cybersecurity and Infrastructure Security Agency (CISA) is hosting a 1-hour webinar on March 19th, 2024, to provide information on training & exercise resources to complement your critical infrastructure and community preparedness programs.

Whether you have a well-established program or are looking for a place to start, the webinar

will provide useful information to help navigate available training & exercise tools and materials.

The topics will include training and exercise resources to support the protection and resilience of all critical infrastructure sectors, with a focus on cybersecurity, physical infrastructure security (including soft targets and crowded places), chemical security, and emergency communications.

For more information about the CISA Region 8 Training & Exercise program email CISARegion8trainingexercise@cisa.dhs.gov or visit https://www.cisa.gov/about/regions/region-8.

Learn More Here

Cyber Education & Training Updates

March – April 2024

Highlights: What You Want to Know

The **Federal Cyber Defense Skilling Academy** is excited to share that they have added THREE new Pathways to the program! These sessions discuss the work roles of a Cyber Defense Forensics Analyst (CDFA), Cyber Defense Incident Responder (CDIR), and Vulnerability Assessment Analyst (VAA).

The Skilling Academy is a unique opportunity for federal civilian employees to learn the baseline knowledge, skills, and abilities of these work roles through an intense, full-time, three-month accelerated training program.

Additional information can be found in the Skilling Academy section below and on the Skilling Academy website. Applications for all three new Pathways are **now open** so be sure to sign up today!

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.

A new in-person, advanced level Continuous Diagnostics and Mitigation (CDM) Dashboard course will be available in March. CDM 222: Cyber Risk and Recovery Using the CDM Dashboard, will be offered March 20-21.

On June 15-17, CISA will be hosting the CYBER.org EdCon 2024 in Orlando, FL. This national conference is designed to inspire and empower novice and expert K-12 cybersecurity educators and counselors alike. Attendees will have the opportunity to learn ready-to-implement lessons from CYBER.ORG curriculum developers, explore no-cost resources from industry experts, and gain firsthand knowledge from K-12 educators who teach foundational and technical cybersecurity. To register and for additional information on conference agenda, stay, travel grants, and more, visit the EdCon website.

Incident Response (IR): This free training series includes 100-level webinars for a general audience which are cybersecurity topic overviews that provide core guidance and best practices to make your network more resilient to attacks. It also includes 200-level Cyber Range Training courses for government employees and contractors across federal, state, local, tribal, and territorial government, educational partners, and critical infrastructure partners. These Cyber Range Trainings provide guided step-action labs to learn and practice investigation, remediation, and incident response skills.

IR Training Events through April 2024

Date	Course Code	Registration Opens	Course	Hours
03/07/2024	IR111	02/07/2024	**Using the Incident Response Playbook at Your Organization**	1
03/28/2024	IR210	03/04/2024	**Introduction to Log Management Cyber Range Training**	4
04/25/2024	IR204	03/25/2024	**Defending Internet Accessible Systems Cyber Range Training**	4

To learn more or register visit**: https://www.cisa.gov/resources-tools/programs/Incident-Response-Training**

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 April 2024

Date	Course Code	Course	Location
03/04/2024-03/22/2024	401v	**Industrial Control Systems Evaluation (401v)**	Scheduled Online Training
03/04/2024-03/22/2024	301v	**Industrial Control Systems Cybersecurity (301v)**	Scheduled Online Training
03/11/2024-03/14/2024	301L	**Industrial Control Systems Cybersecurity (301L) – In-Person 4 Days**	IN-PERSON TRAINING (4 days)
03/25/2024-03/28/2024	301L	**Industrial Control Systems Cybersecurity (301L) – In-Person 4 Days**	IN-PERSON TRAINING (4 days)
04/01/2024-04/19/2024	401v	**Industrial Control Systems Evaluation (401v)**	Scheduled Online Training
04/01/2024-04/19/2024	301v	**Industrial Control Systems Cybersecurity (301v)**	Scheduled Online Training
04/01/2024-04/04/2024	301L	**Industrial Control Systems Cybersecurity (301L) – In-Person 4 Days**	IN-PERSON TRAINING (4 days)
04/23/2024-04/25/2024	401L	**Industrial Control Systems Evaluations (401L) – In-Person 3 Days**	IN-PERSON TRAINING (3 days)

04/29/2024-05/02/2024	301L	**Industrial Control Systems Cybersecurity (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
03/21/2024	General Public	**March Master Class – Intro to Python** March Master Class - Intro to Python | CyberWarrior.com
04/11/2024	General Public	**April Master Class – Overview of Five Recent Cyber Attacks and their Real-Life Impact** April Master Class - Overview of Five Recent Cyber Attacks and their Real-Life Impact | 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 April 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
12/08/2023-07/15/2024	8-12 Educators	**On Demand Workshop – Overview of Cyber Society for 8-12 Teachers:** This asynchronous workshop explores the features of CYBER.ORG's Cyber Society course! Overview of Cyber Society for 8-12 Teachers | CYBER.org
01/15/2024-07/15/2024	High School Educators	**On Demand Workshop – Overview of CYBER.ORG's Cybersecurity Course:** This asynchronous workshop is ideal for high school educators looking to implement cybersecurity and/or a cyber range! Overview of CYBER.ORG's Cybersecurity Course | CYBER.org

01/15/2024-07/15/2024	Middle School Educators	**On Demand Workshop – Overview of Cybersecurity Basics for 6-8 Teachers:** This asynchronous workshop is ideal for middle school educators looking to build cybersecurity awareness in their classrooms. Overview of Cybersecurity Basics for 6-8 Teachers | CYBER.org
06/15/2024-06/17/2024	K-12 Educators	**CISA's CYBER.ORG EdCon:** A national education conference held in Orlando, FL, designed to inspire and empower novice and expert K-12 cybersecurity educators and counselors alike. CYBER.org EdCon| CYBER.org

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

Federal Cyber Defense Skilling Academy: The Federal Cyber Defense Skilling Academy provides its students an opportunity to focus on professional growth through an intense, full-time, three-month accelerated training program. Students will have the opportunity to temporarily step away from their current role while they participate in the program. All full-time civilian federal employees in any job series, and any grade or grade equivalent for non-GS employees, are eligible to apply to the Skilling Academy.

Below are the Skilling Academy session dates for FY24:

Skilling Academy Session Dates for FY24			
Session	**Session Start/End Date**	**Applications Open**	**Applications Close**
CDA - 7 and 8	03/04/24 – 06/14/24	12/18/2023	01/11/2024
CDA - 9 and 10	04/01/24 – 07/12/24	01/22/2024	02/08/2024
CDA - 11 and 12	05/06/24 – 08/16/24	02/19/2024	03/07/2024
CDFA	04/22/24 – 07/24/24	01/31/2024	03/15/2024
CDIR	05/20/24 – 08/21/24	01/31/2024	04/19/2024

VAA	06/17/24 – 9/16/24	01/31/2024	05/10/2024
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-6.1) 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 6.1. 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.

A new in-person advanced level CDM Dashboard course: Cyber Risk and Recovery Using the CDM Dashboard will be offered March 20-21. This course will be held in Arlington, Virginia.

CDM Training Events through April 2024

Date	Course Code	Registration Opens	Course	Hours
03/05/2024	CDM210	02/05/2024	**Introduction to CDM Enabled Threat Hunting (CETH)**	4
03/14/2024	CDM220	02/14/2024	**CDM and Federal Directives**	4
03/20/2024-03/21/2024	CDM222	02/20/2024	**Cyber Risk and Recovery Using the CDM Dashboard - (NEW) – in-person**	14
03/26/2024	CDM141	02/26/2024	**Introduction to the CDM Agency Dashboard**	4

04/04/2024	CDM301	03/04/2024	**Executive Overview of the CDM Agency Dashboard**	2
04/09/2024	CDM320	03/11/2024	**Using the CDM Agency Dashboard to Respond to Federal Directives**	2
04/18/2024	CDM210	03/18/2024	**Introduction to CDM Enabled Threat Hunting (TH)**	4
04/30/2024	CDM203	03/28/2024	**Systems Security 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!

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.*