September 2024 Issue

The CISA Community Bulletin is a monthly publication that shares cybersecurity webinars and workshops, new publications and best practices. In this month's edition:

- **Announcements**
  - Partnering with CISA to Secure Our World
  - National Emergency Communications Plan Webinar Recap
  - Security Programs: National Insider Threat Awareness Month
- **Partnerships**
  - Security Programs: Risk Management Process & Facility Security Committee Trainings
- **Information Exchange**
  - C-IED Federal Resources Catalog Now Available
  - 2024 Chemical Security Seminars
- **Education and Training and Workshops**
  - Attend CISA’s 2024 National Summit on K-12 School Safety and Security (Sept. 25 & 26)
  - Quarterly ChemLock Trainings - ChemLock: Introduction to Chemical Security
  - Quarterly ChemLock Trainings - ChemLock: Secure Your Chemicals Security Planning
  - Cyber Education and Training Updates

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 1-844-Say-CISA.

- 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

How to Report Online Child Sexual Exploitation and Abuse (CSEA)

Online child sexual exploitation and abuse (CSEA) is a serious crime that is never the victim's fault. Stopping exploitation usually requires a victim to come forward to someone they trust — a parent, teacher, caregiver, law enforcement official or another trusted adult. This requires a lot of vulnerability from the victim. It is important to help them gather information to report the crime, choose an option with which they are comfortable and support them through this process.

To submit a report, you can do so through one of the following ways:

- **Contact your local, state, or tribal law enforcement officials directly**. Call 911 in an emergency.

- Call the **Know2Protect Tipline at 833-591-KNOW (5669)**. All information received via the Tipline will be reviewed by appropriate personnel and referred to Homeland Security Investigations field offices for potential investigation.
- Submit a report with the National Center for Missing and Exploited Children.

Learn More Here

ANNOUNCEMENTS

Partnering with CISA to Secure Our World

CISA has launched a Secure Our World Partner Resources web page! CISA's Secure Our World program is an enduring effort to bring awareness to actionable steps we can each take to stay safe online. Secure Our World partners help amplify this messaging and drive behavior change. The web page includes a downloadable Secure Our World Opportunities Guide, which provides an overview on ways to work with CISA to help Secure Our World! A list of official Secure Our World Partners will also be featured.

Also don't forget – October is Cybersecurity Awareness Month! To download this year's free toolkit materials and resources, visit cisa.gov/cybersecurity-awareness-month.

Want to learn more about how your organization can partner with CISA's Secure Our World program and get involved in Cybersecurity Awareness Month? Email us at AwarenessCampaigns@cisa.dhs.gov.

Learn More Here

National Emergency Communications Plan Webinar Recap

CISA recently hosted a National Emergency Communications Plan webinar entitled, “Leveraging Survey Data for Collaborative Initiatives and National Planning.” The webinar introduced participants to the SAFECOM Nationwide Survey (SNS), a valuable tool for shaping national emergency communications planning. Leveraging insights from large national surveys like SNS enables public safety and emergency communications entities to better understand the ever-changing dynamics of emergency communications and the opportunity to align their strategies with broader national goals. Additionally, the webinar explored how the SNS was designed and how its findings inform national planning and support evidence-based decision-making for public safety leaders across the nation. For more information about the NECP webinar series visit the NECP webpage.

Learn More Here

Security Programs: National Insider Threat Awareness Month

September is National Insider Threat Awareness Month (NITAM). Insider threat is the potential for an insider to use their authorized access or knowledge to harm an organization. This harm can include intentional or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities. In recent years, the average cost of an insider threat incident has continued to increase and acts of

workplace violence have become more common. To mitigate potential insider threats and their impact, CISA provides information, resources and tools to help our critical infrastructure stakeholders create or improve existing insider threat mitigation programs. CISA encourages all our partners across the critical infrastructure community to consult the resources on: Insider Threat Mitigation | Cybersecurity and Infrastructure Security Agency CISA Together, we can help protect our most valuable assets from insider threats.

URL: Insider Threat Mitigation | Cybersecurity and Infrastructure Security Agency CISA

Learn More Here

PARTNERSHIPS

Security Programs: Risk Management Process & Facility Security Committee Trainings

Upcoming Interagency Security Committee Risk Management Process & Facility Security Committee Trainings

The Interagency Security Committee (ISC) invites you to participate in its award winning Risk Management Process (RMP) and Facility Security Committee (FSC) Training. This training provides an understanding of the ISC, the ISC Risk Management Process Standard (RMP Standard), and the roles and responsibilities of Facility Security Committees (FSC). The course fulfills the necessary training requirements for FSC membership and is valuable for executives; managers; and personnel involved in making facility funding, leasing, security, or other risk management decisions. Participants will receive **continuing education units** through the International Association for Continuing Education and Training upon completion of the course. The ISC offers the training at **no cost** to participants.

The schedule for upcoming in-person and virtual trainings is below.

In-Person Trainings:

- September 10, 2024 – Tucson, AZ at 8:30 a.m. MT
- September 12, 2024 – San Diego, CA at 8:30 a.m. PT

Virtual, Instructor-Led Trainings:

- September 10-11, 2024 – 9 a.m. CT

For the full list of future trainings visit the ISC website.

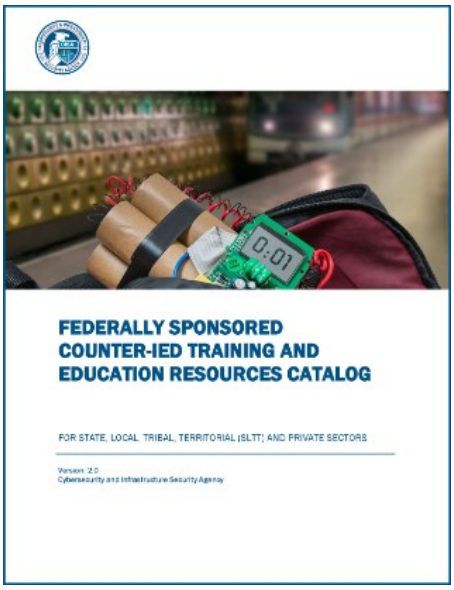
To register for any of these courses, please email the ISC Training Team at rmp_fsctrng@cisa.dhs.gov or visit our website. We look forward to seeing you.

Learn More Here

INFORMATION EXCHANGE

C-IED Federal Resources Catalog Now Available

In collaboration with federal interagency partners through the Joint Program Office for Countering-Improvised Explosive Devices (JPO C-IED), CISA's Office for Bombing Prevention developed the Federally Sponsored C-IED Training and Education Resources Catalog for State, Local, Tribal and Territorial (SLTT) and Private Sectors. This catalog compiles explosive and IED-related federal training and education resources for the SLTT and private sector communities.



The JPO C-IED is responsible for coordinating the implementation of the U.S. Policy for C-IEDs. The resources within the catalog support the goals and capabilities outlined by this policy and are intended to enhance the effectiveness of U.S. C-IED efforts.

To view the catalog, please visit Federally Sponsored C-IED Training and Education Resources Catalog | CISA.

Learn More Here

2024 Chemical Security Seminars

CHEMICAL SECURITY SEMINARS 2024

Thanks to everyone who joined us for the 2024 Chemical Security Seminars on July 11 and 18! Select presentations from the Seminars published on the Chemical Security Summit webpage.

For questions or comments, please email us at Chemicalsummitreg@hq.dhs.gov.

Learn More Here

EDUCATION, TRAINING, AND WORKSHOPS

CISA Education and Training

CISA offers a variety of free courses and scheduled training events. For a complete list, visit the links below:

Upcoming CISA Training Events

CISA Training Catalog

Attend CISA's 2024 National Summit on K-12 School Safety and Security (Sept. 25 & 26)

CISA will host the third annual National Summit on K-12 School Safety and Security on September 25 and 26. This virtual event brings together K-12 school leaders and practitioners to discuss and share actionable recommendations that enhance safe and supportive learning environments. Each day will feature three hours of panel discussions, sessions and keynote speakers covering topics such as school violence prevention, emergency planning, K-12 cybersecurity, youth online safety and student interventions and support.

Registration is open for the Summit and anyone with a passion for improving school safety can attend. The subject matter covered will be of particular interest to K-12 school and district administrators and leaders; school-based law enforcement; teachers and school staff; mental health practitioners; first responders; federal,

state, local, tribal and territorial government partners; and other school safety and security professionals.

Learn more about the Summit and register at 2024CISASchoolSummit.eventbrite.com.

Learn More Here

Quarterly ChemLock Trainings - ChemLock: Introduction to Chemical Security

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 to 2 hours in length and is appropriate for all personnel regardless of their level of involvement with dangerous chemicals.

- Register for October 7, 2024 – 11 am-1 pm ET

Learn More Here

Quarterly ChemLock Trainings - 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 to 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 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

Cyber Education & Training Updates

September 2024

Highlights: What You Want to Know

CISA is excited to announce its first federally focused Zero Trust (ZT) Awareness Course. This course, ***Basics of Zero Trust for Federal Agencies***, is a one-hour, self-paced online training, tailored for all federal employees/contractors who require/want a basic understanding of Zero Trust. If you know someone who is interested or could benefit from a ZT basics training, please visit FedVTE under "All Cybersecurity Courses" (requires login) or under "Public Content" (no login required)!

CISA recently announced two new collaborative efforts: the CyberSkills2Work program and new micro-challenges on Try Cyber. Both efforts were designed to help individuals launch or advance cybersecurity careers. To learn more, please visit CISA's Cybersecurity Education and Career Development Website.

A new CDM Dashboard course on HVA Tracking has been scheduled for September 12, 2024, *Managing HVAs Using the CDM Agency Dashboard*. This course presents foundational concepts associated with the High Value Asset Program and how HVAs can be managed with the CDM Agency Dashboard. The course introduces learners to key HVA guidance, the HVA Management Lifecycle and HVA tracking capabilities within the CDM Agency Dashboard. With the assistance of the dashboard, users can identify, track, and prioritize their mitigation activities as they relate to HVA assets. From an operational perspective, the increased visibility will enable quicker response and assist decision makers in determining criticality of actions.

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 September 2024

Date	Course Code	Registration Opens	Course	Hours
09/10/2024	IR211	08/12/2024	**Using the CISA Incident Response Playbook at your Organization**	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 September 2024

Date	Course Code	Course	Location
09/02/2024-09/20/2024	401	**Industrial Control Systems Cybersecurity Evaluation (401)**	Scheduled Online Training
09/02/2024-09/20/2024	300	**Industrial Control Systems Cybersecurity (300)**	Scheduled Online Training
09/16/2024-09/19/2024	301	**Industrial Control Systems Cybersecurity & RED-BLUE Exercise (301)**	**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 ICS300 online course is a prerequisite for attending the in-person ICS301 training hosted by CISA at the Idaho National Laboratory. This ICS300 course focuses on many of the hands-on skills needed to protect and secure Industrial Control Systems and Operational Technology networks. The ICS401 course is available either online (ICS401V) or in-person (ICS401L).*

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 how to use 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-6.2) within a cyber virtual training range (CVLE). The course content focuses on the current version ES-6 of the CDM Dashboard, including the latest dashboard content pack, version 6.2. The latest CDM Dashboard capabilities will be discussed, including FISMA Automation, HVA reporting and Mobile tracking. The current CDM courses fall into the 100 level (Introductory) and 200 level (Intermediate) level offerings.

CDM Training Events through September 2024

Date	Course Code	Registration Opens	Course	Hours

09/05/2024	CDM201	08/05/2024	**Identity and Access Management within the CDM Agency Dashboard**	4
09/12/2024	CDM330	08/12//2024	**Managing High Value Assets (HVAs) Using the CDM Agency Dashboard**	4
09/17/2024	CDM202	08/19/2024	**Managing Configurations Settings within the CDM Agency Dashboard**	4
09/19/2024	CDM203	08/19/2024	**CDM Agency Dashboard Role-Based Training: System Security Analyst**	4
09/25/2024-09/26/2024	CDM222	08/26/2024	**Using the CDM Dashboard to Advance Cyber Defense – IN PERSON**	14
09/30/2024	CDM301	08/30/2024	**Executive Overview of the CDM Agency Dashboard**	2

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

The National Initiative for Cybersecurity Careers and Studies (NICCS) NICE FRAMEWORK UPDATE! The tools and resources on the NICCS website are now live with the new Workforce Framework for Cybersecurity (NICE Framework) components! This data includes updated Work Role Categories, Competency Areas, Work Roles, and Task, Knowledge, and Skill (TKS) statements as well as identifies the relationships between those elements. Check out the NICE Framework, Education & Training Catalog, and Cyber Career Pathways Tool and Roadmap on niccs.cisa.gov for more information.

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**

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.*