October 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**
    - Recognizing Cybersecurity Awareness Month
    - Public Service Announcement on Election Security
- **Partnerships**
    - Director Easterly Visits New Hampshire for Election Security
    - Water Pro Conference
    - Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure
- **Information Exchange**
    - Infrastructure Resilience Planning Framework Playbook
    - Bombing Prevention Assistance for K-12 Schools
- **Education and Training and Workshops**
    - Quarterly ChemLock Trainings - ChemLock: Introduction to Chemical Security
    - Quarterly ChemLock Trainings - ChemLock: Secure Your Chemicals Security Planning
    - Quarterly ChemLock Trainings - Upcoming Interagency Security Committee Risk Management Process & Facility Security Committee Trainings
    - Region 8 Securing Public Gatherings Webinar
    - 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

Recognizing Cybersecurity Awareness Month

This October marks the 21st annual Cybersecurity Awareness Month! CISA, in partnership with the National Cybersecurity Alliance (NCA), is amplifying cybersecurity awareness on a national and global scale. Our goal is to educate both individuals and organizations about emerging cyber threats and promote the adoption of best practices for online safety. Secure Our World, the enduring theme for Cybersecurity Awareness Month, highlights four key behaviors that we can all implement to build a safer, more trusted, digital world.

Want to get involved?

- Download this year's free Cybersecurity Awareness Month 2024 Toolkit, which includes new resources like tip sheets on how to stay safe online when using AI, reporting cybercrime, and raising digital citizens, as well as puzzles and posters.
- Join NCA and CISA as we kick-off the 21st Cybersecurity Awareness Month on October 2, 2024, at 2pm ET. To register for this virtual event, click here.
- Participate in Cybersecurity Career Week from October 14-19, 2024.
- Learn more about CISA's talent development initiatives aimed at filling the cyber workforce gap on October 16, 2024, at 2pm ET. To register, click here.

- Partner with CISA's Secure Our World Program. To learn more about ways to work with us, check out the Secure Our World Opportunities Guide.
- Follow CISA on X, LinkedIn, Facebook, Instagram, and YouTube. Don't forget to use #SecureOurWorld and #CybersecurityAwarenessMonth when posting!

Learn More Here

Public Service Announcement on Election Security

CISA and the Federal Bureau of Investigation (FBI) issued a public service announcement recently to raise awareness of potential attempts to undermine public confidence in the security of U.S. election infrastructure through the spread of disinformation falsely claiming successful cyberattacks on U.S. voter registration databases.

Key points:

- Do not accept claims of intrusion at face value. These claims may be meant to influence public opinion and undermine the American people's confidence in our democratic process.
- Visit your state and local elections offices websites for reliable elections information.
- Be wary of social media posts, emails, or calls from unknown sources making suspicious claims about elections or cyber incidents.

Learn More Here

PARTNERSHIPS

Director Easterly Visits New Hampshire, Idaho for Election Security

CISA Director Easterly recently joined New Hampshire Secretary of State Dave Scanlan to visit polling locations both large and small throughout the state during the primary election and saw firsthand the measures in place to protect the vote. The next week she visited Idaho, to meet with Secretary of State Phil McGrane to discuss election security and resilience and hold a press conference with the Secretary highlighting why voters should have confidence in the resilience of the 2024 elections.

Securing election infrastructure and polling locations is a year-round effort, and CISA is proud to work with Election Officials in support of this mission.

We are grateful for the state and local election workers across the country who are on the front lines ensuring the security of our democratic process and that every vote is counted as cast.

For the full story by In Depth New Hampshire, visit InDeptNH.org

Learn More Here

Water Pro Conference in Savannah, GA

CISA Deputy Director Nitin Natarajan and Dr. Jennifer McClain, Director of the EPA Office of Ground Water and Drinking Water, shared their insights on the intersection of cybersecurity and the water sector.

They emphasized the importance of cybersecurity and outlined steps small water and wastewater systems can take to enhance their security.

Learn More Here

Russian Military Cyber Actors Target U.S. and Global Critical Infrastructure

Our latest joint Cybersecurity Advisory with the FBI, & NSACyber, and other US and international partners provides Tactics, Techniques, and Procedures (TTPs) associated with Russian General Staff Main Intelligence Directorate (GRU) Unit 29155 cyber actors. This group is linked to the WhisperGate attacks on Ukraine and extensive cyber operations against NATO and other global entities. Their objectives span from espionage to systemic sabotage, posing serious risks to global security. Stay informed and vigilant against these evolving threats.

Learn More Here

INFORMATION EXCHANGE

Infrastructure Resilience Planning Framework Playbook

If you are looking for resources to help your community plan for better resilience, we encourage you to check out our Infrastructure Resilience Planning Framework (IRPF) and IRPF Playbook.

These resources provide instructions and templates for executing key actions to plan for resilience and can help you understand your risk picture and how to plan for it.

Learn More Here

Bombing Prevention Assistance for K-12 Schools

CISA's Office for Bombing Prevention (OBP) develops and delivers a diverse curriculum of training, awareness products, and technical assistance. These resources provide K-12 schools and districts with products, tools, and Counter-Improvised Explosive Device (C-IED) strategies to protect, prevent, mitigate, and respond to bombing threats. TRAINING Recommended for All School Employees.

- Bomb Threat Preparedness and Response (AWR-903) One-hour online independent study training to familiarize participants with the steps necessary to prepare for and respond to a bomb threat.
- Response to Suspicious Behaviors and Items (AWR-335) One-hour Virtual Instructor-Led Training (VILT) introduces participants to recognizing and responding to suspicious behaviors, activities, and items related to terrorist or criminal activities.
- Recommended for School Administrators and Security Bomb Threat Assessment for Decision Makers (AWR-945) One-hour VILT introduces the participant to types of threats, the threat assessment process, and the implementation of a bomb threat management (BTM) plan.
- Bomb Threat Management (BTM) Planning (MGT-451) One-day Instructor-Led Training (ILT) provides participants with an overview of the Department of Homeland Security's risk management process and BTM planning.

- Improvised Explosive Device (IED) Search Procedures (PER-339) One-day ILT introduces participants to basic, low-risk search protocols. It provides participants with the information required to create a search plan for their facility or special event. It provides them guidance on how to perform IED searches of a route, area, and a facility.
- VIDEOS What to Do: Bomb Threat Demonstrates procedures to follow when a bomb threat is received. This video will help individuals prepare and react appropriately. What to Do: Suspicious or Unattended Item Demonstrates the criteria used to identify a suspicious item (potential bomb) and differentiate it from an unattended item. This video will help individuals prepare and react appropriately.

The Technical Resource for Incident Prevention, TRIPwire, is a collaborative, online information-sharing and resource portal. TRIPwire's home page is publicly accessible and features valuable preparedness information for the whole community. Account registration is available to all school employees and gives members additional access to a surplus of information and resources on IED threats and corresponding prevention, protection, and response measures. Information and resources on TRIPwire increase awareness of evolving IED tactics, techniques, and procedures (TTPs), as well as incident lessons learned and counter-IED preparedness. It combines expert analyses and reports with relevant documents, images, and videos to help users anticipate, identify, and prevent IED incidents.

CONTACT US

To request training or for more information, visit us at cisa.gov/obp or email us at OBPTraining@cisa.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

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 1-2 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
- Register for January 15, 2025 - 1 pm-3 pm ET
- Register for April 15, 2025 - 11 am-1 pm ET
- Register for July 17, 2025 - 2 pm-4 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 2-3 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
- Register for February 18, 2025 - 12 pm-3 pm ET
- Register for May 21, 2025 - 10am-1pm ET
- Register for August 21, 2025 - 1 pm-4 pm ET

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

Learn More Here

Quarterly ChemLock 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:

- October 16, 2024 – Little Rock, AR at 8:30 a.m. CT
- October 23, 2024 – Boston, MA at 8:30 a.m. ET
- October 29, 2024 - Indianapolis, IN at 8:30 a.m. ET
- December 3, 2024 – Arlington, VA at 9:00 a.m. ET
- January 9, 2025 – Grand Rapids, MI at 8:30 a.m. ET

Virtual, Instructor-Led Trainings:

- October 1- 2, 2024 9 a.m. MT
- October 8- 9, 2024 9 a.m. ET
- November 5-6, 2024 9 a.m. CT

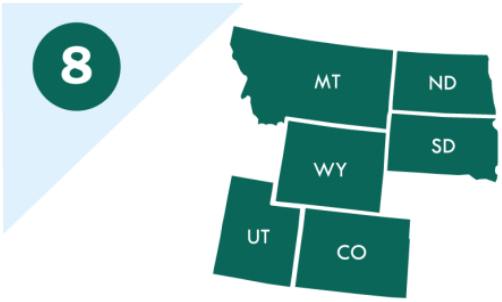
- December 10-11, 2024 9 a.m. PT
- January 28-29, 2025 9 a.m. ET
- February 4-5, 2025 9 a.m. CT
- March 4-5, 2025 9 a.m. MT
- April 8-9, 2025 9 a.m. PT
- May 13-14, 2025 9 a.m. MT
- June 24-25, 2025 9 a.m. CT
- July 15-16, 2025 9 a.m. ET
- September 9-10, 2025 9 a.m. CT

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

Region 8 Securing Public Gatherings Webinar



Have you prepared for the security of events you are organizing this winter? CISA is hosting a 2-hour webinar on November 14th, 2024, to provide tools and resources to assist with the protection of public areas from a variety of threats. Join us for one of our preparedness events during Critical Infrastructure Security and Resilience Month.

Public gatherings and crowded places are increasingly vulnerable to terrorist attacks and other extremist actors because of their relative accessibility and large number of potential targets. Organizations of all types and sizes, including businesses, critical infrastructure owners and operators, schools, and houses of worship face a variety of security risks.

The topics will include information on security concerns, vulnerabilities, mitigation options and resources available to support the protection of public venues.

For more information about securing public gatherings visit https://www.cisa.gov/topics/physical-security/securing-public-gatherings or email CISARegion8trainingexercise@cisa.dhs.gov.

Learn More Here

Cyber Education & Training Updates

Highlights: What You Want to Know

- **New Incident Response (IR) Triage Series:** It's a six-part training series that focuses on the fundamental skill development of recognizing an IR event and the steps needed to triage the incident. These courses are available for government employees and contractors across federal, state, local, tribal and territorial government, as well as educational and critical infrastructure partners.
- CISA has recently announced two new collaborative efforts: theCyberSkills2Work 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 ***Managing High Value Assets (HVAs) Using the CDM Agency Dashboard,*** focusing on HVA tracking is scheduled for another delivery October 8, 2024. This course presents foundational concepts associated with the High Value Asset (HVA) 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
- CISA is thrilled to announce that **Federal Cyber Defense Skilling Academy** courses will be returning in FY25! While all application periods for FY24 courses are now closed, please continue to check the Skilling Academy website for updates and more information.
- **The National Initiative for Cybersecurity Careers and Studies (NICCS)** **NICE FRAMEWORK UPDATE!** The tools and resources on the NICCS website are 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.

Instructor-Led Cyber Trainings

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.

Upcoming Events for the IR Triage six-part series:

IR Training Events

Date	Course Code	Registration Opens	Course	Hours
10/07/2024	IR117	09/03/2024	**Threat Intelligence Development (Awareness Webinar)**	1
10/08/2024	IR217	09/03/2024	**Threat Intelligence Development (Skills Development Cyber Range)**	4
10/09/2024	IR217	09/03/2024	**Threat Intelligence Development (Skills Development Cyber Range)**	4
10/10/2024	IR217	09/03/2024	**Threat Intelligence Development (Skills Development Cyber Range)**	4
10/22/2024	IR107	09/23/2024	**Introduction to Network Diagramming**	1
10/31/2024	IR209	09/30/2024	**Defend Against Ransomware Attacks Cyber Range Training**	4
11/04/2024	IR118	10/04/2024	**Incident Response Triage Series: Mitigation**	1
11/06/2024	IR218	10/04/2024	**Incident Response Triage Series Lab Class: Mitigation**	4
11/06/2024	IR211	10/07/2024	**Using the CISA Incident Response Playbook at Your Organization**	4
11/07/2024	IR218	10/04/2024	**Incident Response Triage Series Lab Class: Mitigation**	4
11/07/2024	IR211	10/07/2024	**Using the CISA Incident Response Playbook at Your Organization**	4

11/08/2024	IR218	10/04/2024	**Incident Response Triage Series Lab Class: Mitigation**	4
11/13/2024	IR113	10/14/2024	**Implementing SaaS Security Guidelines**	1
11/21/2024	IR210	10/21/2024	**Introduction to Log Management Cyber Range Training**	4

To learn more or register visit: **IR Training|CISA**

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.

CDM Training Events

Date	Course Code	Registration Opens	Course	Hours
10/03/2024	CDM141	08/31/2024	**Introduction to the CDM Agency Dashboard**	4
10/08/2024	CDM330	09/04/2024	**Managing High Value Assets (HVAs) Using the CDM Agency Dashboard**	4
10/17/2024	CDM142	09/05/2024	**Asset Management with the CDM Agency Dashboard**	4

10/23/2024-10/24/2024	CDM111	09/09/2024	**Analyzing Cyber Risks with the CDM Dashboard**	14
10/29/2024	CDM143	09/16/2024	**Vulnerability Management using the CDM Dashboard**	4
11/14/2024	CDM202	10/14/2024	**Configuration Settings Using the CDM Agency Dashboard**	4
11/19/2024	CDM203	10/21/2024	**CDM Agency Dashboard Role-Based Training – System Security Analyst**	4

To learn more or register visit: **CDM Training|CISA**

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			
Date	**Course Code**	**Course**	**Location**
10/07/2024-10/25/2024	401	**Industrial Control Systems Cybersecurity Evaluation (401)**	Scheduled Online Training
10/07/2024-10/25/2024	300	**Industrial Control Systems Cybersecurity (300)**	Scheduled Online Training
10/14/2024-10/17/2024	301	**Industrial Control Systems Cybersecurity & RED-BLUE Exercise (301)**	**IN-PERSON TRAINING –** **4 Days**
11/03/2024-11/21/2024	401	**Industrial Control Systems Cybersecurity Evaluation (401)**	Scheduled Online Training
11/03/2024-11/21/2024	300	**Industrial Control Systems Cybersecurity (300)**	Scheduled Online Training

11/12/2024-11/14/2024	401	**Industrial Control Systems Cybersecurity Evaluation (401)**	**IN-PERSON TRAINING –** **3 Days**
11/18/2024-11/21/2024	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: **ICS Training Calendar|CISA**

**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.*

CDET Mission	CDET Vision
Address today's cyber workforce challenges through innovative education and training opportunities.	*Lead and influence national cyber training and education to promote and enable the cyber-ready workforce of tomorrow.*

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

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.*


SECURE
OUR WORLD