CISA COMMUNITY BULLETIN

June 2024 Issue

In this edition:

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**

To report an incident, you can call the Know2Protect Tipline at 1-833-591-KNOW (5669) or visit the NCMEC CyberTypline at https://report.cybertip.org.

Learn More Here

ANNOUNCEMENTS

Launch of CISA's Second Secure Our World PSA

Last month at RSA Conference 2024, CISA launched *We Can Secure Our World*, the second PSA in our Secure Our World cybersecurity public awareness program. The PSA will be promoted widely across the U.S. on television, radio, digital ads, retail centers, social media platforms, and billboards throughout 2024. *We Can Secure*

Our World builds on the success of CISA's first ever public service announcement (PSA) which launched in September 2023.

A Pew Research Center survey conducted last year shows that 95% of American adults use the internet, 90% have a smartphone and 80% subscribe to high-speed internet at home. Additionally, the survey also reported nearly 70% of children and adolescents have been exposed to at least one cyber risk in the past year. With cyber threats increasing among Americans of all ages, CISA is working to empower all Americans to protect themselves from hackers getting into their devices through easy steps that anyone can do anywhere and anytime.

The Secure Our World cybersecurity public awareness program, launched in September 2023, with its first PSA receiving nearly 20,000 views on YouTube, and educational materials including "How to" videos and tip sheets, were downloaded approximately 50,000 times. CISA also had a video air at the NFL Experience in the week leading up to the Super Bowl. CISA had a Super Bowl-related social media campaign that garnered more than 200,000 views and reached audiences spanning America's diverse population.

The Secure Our World program is designed to educate and empower individuals to take proactive steps in safeguarding their digital lives. Tapping into the nostalgia of beloved musical cartoon series from the 1970s and 1980s, the new PSA features lovable character Max from the first PSA and introduces "Joan the Phone" who teaches us how to stay safe online. Through engaging messaging encouraging simple steps to protect ourselves online, the program aims to raise awareness about the importance of cybersecurity and empower individuals to adopt best practices to mitigate online risks.

To watch CISA's newest PSA and learn more about Secure Our World, visit cisa.gov/SecureOurWorld. Help CISA spread the word about how we can all make meaningful changes to boost online safety, and together, we can Secure Our World.

Learn More Here

CISA Announces Secure by Design Commitments from Leading Technology Providers

In April 2023, CISA kicked off our Secure by Design initiative, the agency's effort to shift the responsibility of security from end users to technology manufacturers, in line with the National Cybersecurity Strategy.

Just over a year later, on May 8, 2024, CISA was pleased to announce voluntary commitments by 68 of the world's leading software manufacturers to CISA's Secure by Design pledge to design products with greater security built in.

"More secure software is our best hope to protect against the seemingly never-ending scourge of cyberattacks facing our nation. I am glad to see leading software manufacturers recognize this by joining us at CISA to build a future that is more secure by design," CISA Director Jen Easterly said. "I applaud the companies who have already signed our pledge for their leadership and call on all software manufacturers to take the pledge and join us in creating a world where technology is safe and secure right out of the box."

A list of the 68 companies, including leading software manufacturers, participating in the pledge can be found at the Secure by Design Pledge page, and statements of support for the pledge can be read here.

By catalyzing action by some of the largest technology manufacturers, the Secure by Design pledge marks a major milestone in CISA's Secure by Design initiative. Participating software manufacturers are pledging to work over the next year to demonstrate measurable progress towards seven concrete goals. Collectively, these commitments will help protect Americans by securing the technology that our critical infrastructure relies on.

Learn More Here

The Cyber Intelligence Network and CISA Region 7 Win 2023 Best of HSIN Gold Award

Last November, the Cyber Intelligence Network and CISA Region 7 facilitated a virtual, functional exercise for more than 45 agencies from nearly all 50 states. The team won the 2023 Best of HSIN Gold Award for Greatest Impact to the Information Sharing Environment. Among the nominations the Homeland Security Information Network team received, this was voted the best for exemplary performance using HSIN to leverage information sharing that contributes to saving lives across public safety and homeland security operations.

The exercise was designed to triage efforts to isolate and recover from a multi-layer cyber event, utilize communications, defend data and protect brand integrity. In the scenario, the ransomware group Rhysida targeted various state county courthouse networks. The participants utilized the HSIN for information sharing, and the CISA Region 7 team used the FEMA Preparedness Toolkit for multimedia injects.

“The Cyber Intelligence Network appreciates the CISA Region 7 exercise team for all the time and hard work they put into our national exercise,” said Angela Robinson, cybersecurity specialist at the Missouri Department of Public Safety and CIN Central Region coordinator. “The exercise was executed with the utmost in professionalism and creativity, and we felt it was a huge success.”

Learn More Here

Cyber Safety Review Board Report

DHS released the Cyber Safety Review Board’s (CSRB) findings and recommendations following the Review of the Summer 2023 Microsoft Exchange Online Intrusion. The review finds that a threat actor—known as Storm-0558 and assessed to be affiliated with the People’s Republic of China in pursuit of espionage objectives—was able to compromise the Microsoft Exchange Online mailboxes of 22 organizations, including those of senior United States government representatives working on national security matters. The Board points to a cascade of security failures at Microsoft and issues recommendations to all cloud service providers (CSPs) to improve the identity and access infrastructure that safeguards the information they are entrusted to maintain.

Learn More Here

PARTNERSHIPS

CISA Supports Maui Following Recent Wildfires

CISA Region 9 Strategic Outreach Planner, Justin Greenfield has been actively involved in supporting recovery efforts in Maui following the recent wildfires. Working with a mission-assigned HQ Planner on Infrastructure Resilience Planning Framework (IRPF) efforts in Hawaii, Greenfield focused on integrating an infrastructure resiliency planning framework to bolster Maui's recovery and future preparedness.

This initiative aims to fortify Maui's ability to withstand and recover from disasters by identifying vulnerabilities and implementing mitigation measures. Such proactive planning can minimize damage and disruption to essential services during future crises.

Collaboration is key to success, and Greenfield's work promotes partnerships among government agencies, local communities, and businesses. By pooling resources and expertise, a more robust and interconnected infrastructure network can be built, capable of withstanding diverse challenges.

Furthermore, the integration of sustainable practices and innovative technologies, such as renewable energy and smart infrastructure, allows Maui to reduce its environmental impact and enhance adaptability.

The project involved collaboration with external participants from various agencies, including the Army Corps of Engineers, EPA, DOT, and FEMA, as well as internal participants like Spencer Whitaker from the Resilience Services Branch.

This strategic effort highlights the importance of resilience planning for safeguarding Maui's future and preserving its natural beauty. Through continued collaboration, Maui can build a stronger, more sustainable, and inclusive community resilient to future disasters.

Learn More Here

The Secure-By-Design Imperative: A One-Year Retrospective with the Atlantic Council

Persistent insecurity poses a threat to US national security and personal privacy alike, with businesses and end users continuing to face risks from insecure software. CISA's Secure by Design (SBD) initiative seeks to move security earlier in the product lifecycle for organizations that produce and sell software, reducing vulnerability and increasing the resilience of software to make it safer for its many users.

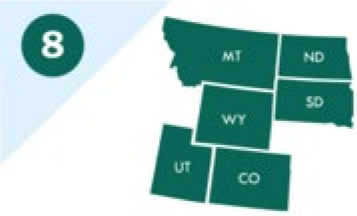
In light of the initiative's one-year anniversary, The Atlantic Council's Cyber Statecraft Initiative, gathered experts in April for a discussion on SBD's progress so far and the work yet to come. Which organizations have adopted SBD principles, and what is in the way of organizations that have not? What is industry's perspective on the most impactful and efficient principles and practices within the SBD framework with respect to security outcomes? How can CISA advance the adoption of these principles in cooperation with software developers large and small, as well as other influential ecosystem actors like cyber insurers?

This discussion included Lauren Zabierek, Senior Advisor, CISA; Jack Cable, Senior Technical Advisor, CISA; Dan Lorenc, CEO and Co-Founder, Chainguard; and Sarah Novotny, Founder, Klever Consulting. The event featured pre-recorded remarks from Jen Easterly, Director, CISA.

Learn More Here

INFORMATION EXCHANGE

Region 8 Water & Wastewater Sector Cyber Incident Response Webinar



The Water and Wastewater Sector has been impacted by various cyber events, including unauthorized access, and ransomware. Continued compromises or failures could cause cascading impacts across critical infrastructure.

CISA Region 8 invites you to the Region 8 Water & Wastewater Sector Cyber Incident Response Webinar on June 18th, 2024 at 10 am MDT to learn more.

The webinar will review the Water and Wastewater Sector Cybersecurity Toolkit, including the Incident Response Guide which outlines how water utility owners and operators can expect to work with federal partners as they prepare for, respond to, and mitigate the impact of a cyber incident.

The toolkit consolidates key resources at every level of cybersecurity maturity and provides incident response best practices and information on federal resources to enhance the security and resilience of the Water and Wastewater Sector.

For more information about Water and Wastewater Security, email CISA Region 8 at CISARegion8Outreach@cisa.dhs.gov, visit https://www.cisa.gov/water, or access the Water and Wastewater Sector - Incident Response Guide at https://www.cisa.gov/resources-tools/resources/water-and-wastewater-sector-incident-response-guide-0.

Learn More Here

CISA Live! Presents: Secure by Design

CISA invited stakeholders to join a special presentation on Wednesday, April 24 to mark the one-year anniversary of Secure by Design and debunk some misconceptions. CISA Senior Advisor Lauren Zabierek and Senior Technical Advisors Bob Lord and Jack Cable were the featured presenters at the event. The event offered participants an opportunity to learn about CISA's work to create a future where technology products are safe for customers out of the box.

Learn More Here

Preventing Ransomware Attacks at Scale

While the United States has started to make progress in responding to cyberattacks, it's clear that there is still significant work to be done to curb the ransomware epidemic. Software manufacturers must take action to prevent compromises in the first place, and businesses that use their products should push them to do so. Business leaders of software manufacturers can build products that are resilient against the most common classes of cyberattacks by ransomware gangs. Systemic classes of defect like SQL injection or insecure default configurations enable most ransomware attacks and are preventable at scale. To combat inaction in this space, CISA launched its global Secure by Design campaign last year to issue specific, actionable guidance that business leaders at software manufacturers should review and act on. Leaders of software manufacturers should urgently undertake an assessment of systemic classes of vulnerabilities present in their products. Companies that buy software can also play a role by demanding better security from their vendors. A future where ransomware attacks are significantly harder to pull off is possible. It's time for software companies to make this future a reality and protect Americans by building security into their products from the start.

Learn More Here

WPS & GETS: Helpful Tips/Best Practices

Wireless Priority Service (WPS) and Government Emergency Telecommunication Service (GETS) help make a connection when you need it most! It is essential to **be confident** with how and when to use the services **before** an emergency occurs. Empower yourself and others in your organization to improve confidence using WPS and GETS by remembering a few important tips.

WPS:

WPS calls must be made with a WPS-enabled cellular phone. Make sure to test WPS after changing phones or phone services. Simply dial *272 in front of the desired cell phone number using your cell phone with WPS capability.

GETS:

GETS calls are made using your pin + destination number. Because GETS calls can be made from any phone with your assigned pin, you should always keep your GETS card on your person. Don’t be discouraged if you experience a few seconds of silence after dialing your destination. If you must re-route the call, additional access numbers can be found on the back of your GETS card.

Dialer App:

For even easier calling with WPS and GETS, download the PTS Dialer App. Make regular calls using WPS, GETS, and the Dialer App, to familiarize yourself with using the services in an emergency. WPS and GETS can be used to communicate between all levels of personnel in an organization and should never be used to call 911. Ensure you have access to the cellular network (bars) when using the services.

For the ultimate resilience, use WPS + GETS together!

Learn More Here

EDUCATION, TRAINING, AND WORKSHOPS

Learn More Here

Register for 2024 Chemical Security Seminars

CHEMICAL SECURITY SEMINARS 2024

CISA invites you to attend the virtual 2024 Chemical Security Seminars on July 11 and 18, 2024, from 10 am-3 pm ET (7 am-noon PT). The 2024 Seminars—to be held in lieu of the 2024 Chemical Security Summit—are the signature U.S. event focused on chemical security collaboration across the public and private sectors that work with potentially dangerous chemicals.

Register today for the 2024 Chemical Security Seminars!

Join participants from across the spectrum of sectors—including chemical, energy, communications, transportation, and water—to hear the latest program updates, share perspectives and lessons learned, and engage in dialogue regarding chemical security.

- When: July 11 and 18, 2024, 10 am-3 pm ET (7 am-noon PT)
- Where: Virtual via Microsoft Teams
- Who should attend:
  - Chemical and related industry stakeholders
  - Corporate and facility security officers
  - Environment, health, and safety professionals

- What: the latest in chemical security best practices, including:
  - Case studies of real-world scenarios, including drones and cyber attacks
  - Transnational threats to the chemical industry
  - “Wicked Problems”
  - Updates on CISA’s ChemLock Program
  - Artificial intelligence
  - And more!

The Seminars are free to attend and open to the public.

For more information, visit the 2024 Chemical Security Seminars webpage. For questions or comments, please email us at Chemicalsummitreg@hq.dhs.gov.

We look forward to seeing you virtually at the 2024 Chemical Security Seminars.

Learn More Here

Quarterly ChemLock Trainings

CHEM LOCK

Know your **chemicals.**

Lock in your security posture.

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 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 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

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

CISA invites you to participate in the Interagency Security Committee (ISC) 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:

- June 25, 2024 – Charleston, SC at 8 a.m. ET
- July 2, 2024 – Arlington, VA at 9 a.m. ET
- July 23, 2024 – Boise, ID at 8 a.m. MT
- July 25, 2024 – Seattle, WA at 8 a.m. PT
- August 15, 2024 – Atlanta, GA at 8 a.m. ET

Virtual, Instructor-Led Trainings:

- June 4-5, 2024 – 9 a.m. CT
- July 16-17, 2024 – 9 a.m. ET,
- 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

Cyber Education & Training Updates

June 2024

Highlights: What You Want to Know

CISA is excited to announce that it has published the 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 has 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.

For the first time, there is an opportunity to attend both of the **CDM Dashboard** in-person courses in succession, which focus on eight CDM Dashboard courses within a four-day period July 23-26! This is an excellent opportunity to attend in-person and receive a full week of training covering all the current CDM Dashboard capabilities. To learn more and to register, visit the CDM training page!

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.

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 July 2024

Date	Course Code	Registration Opens	Course	Hours
06/13/2024	IR211	05/13/2024	**Using the CISA Incident Response Playbook**	4

06/27/2024	IR214	05/28/2024	**Incident Response Triage: Instrumentation and Environmental Preparation**	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 July 2024

Date	Course Code	Course	Location
06/03/2024-06/27/2024	401	**Industrial Control Systems Cybersecurity Evaluation (401)**	Scheduled Online Training
06/03/2024-06/27/2024	300	**Industrial Control Systems Cybersecurity (300)**	Scheduled Online Training
06/18/2024-06/20/2024	401	**Industrial Control Systems Cybersecurity Evaluation (401)**	**IN-PERSON TRAINING –** **3 Days**
07/08/2024-07/26/2024	401	**Industrial Control Systems Cybersecurity Evaluation (401)**	Scheduled Online Training
07/08/2024-07/26/2024	300	**Industrial Control Systems Cybersecurity (300)**	Scheduled Online Training
07/15/2024-07/18/2024	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 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
06/13/2024	General Public	**June Master Class – Introduction to Identity Management** June Master Class - Introduction to Identity Management | 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 July 2024

Date	Time	Audience	Course	Location	Hours
06/15/2024-06/17/2024	On Demand	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**.** **(REGISTRATION CLOSED)** CYBER.org EdCon| CYBER.org	Orlando, FL	2 ½ Days
07/30/2024	11:00 AM-12:30 PM CST	Elementary School Educators	**Implementing the Cybersecurity Basics Course for Grades K-8!:** Join us for an overview of our Cybersecurity Basics course that includes topics like digital citizenship and online safety! Implementing the Cybersecurity Basics Course for Grades K-8 | CYBER.org	Virtual	1.5 Hours

07/30/2024	1:00 PM-2:30 PM CST	Middle School Educators	**Implementing Range Activities with Middle School Students!:** Join us for an overview of Range Activities for middle school students! Implementing Range Activities with Middle School Students | CYBER.org	Virtual	1.5 Hours
07/30/2024	3:00 PM-4:30 PM CST	8-12 Educators	**Implementing the Cyber Society Course for Grades 8-12!:** The Cyber Society course is designed to introduce students to how the world of cyber affects their everyday lives, with topics ranging from law and politics to artificial intelligence and media literacy. Implementing the Cyber Society Course for Grades 8-12 | CYBER.org	Virtual	1.5 Hours
07/30/2024	3:00 PM-4:30 PM CST	8-12 Educators	**Implementing the Intro to Cybersecurity Course for Grades 8-12!:** Join us for an overview of our Intro to Cybersecurity course! The goal of this course is to introduce students to basic cybersecurity concepts and inspire interest in cybersecurity careers. Implementing the Intro to Cybersecurity Course for Grades 8-12 | CYBER.org	Virtual	1.5 Hours
	To learn more or sign up, visit: **https://cyber.org/events**				

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-6.2) 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 July 2024

Date	**Course Code**	**Registration Opens**	**Course**	**Hours**
06/06/2024	CDM202	05/06/2024	**Managing Configurations Settings with the CDM Agency Dashboard**	4
06/11/2024	CDM203	05/13/2024	**Systems Security Analyst**	4
06/20/2024	CDM220	05/20/2024	**CDM and Federal Mandates (BOD 22-01)**	4
06/25/2024	CDM301	05/27/2024	**Executive Overview of the CDM Agency Dashboard**	2
07/11/2024	CDM142	06/11/2024	**Asset Management with the CDM Agency Dashboard**	4
07/16/2024	CDM141	06/17/2024	**Introduction to the CDM Agency Dashboard**	4
07/23/2024-07/24/2024	CDM111	06/24/2024	**Analyzing Cyber Risk with the CDM Agency Dashboard – IN PERSON**	14
07/25/2024-07/26/2024	CDM222	06/25/2024	**Using the CDM Dashboard to Advance Cyber Defense – IN PERSON**	14

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

NICCS Education & Training Catalog: The NICCS website recently surpassed 13,000 total courses in our Education and Training Catalog. The Catalog is a repository of courses to help individuals of all skill levels find virtual and in-person cybersecurity-related courses across the nation. Use the interactive search functions and filters to find courses that can help you earn a cybersecurity certification or even assist you in transitioning to a new career! Visit NICCS to learn more.

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