June 2023 - CISA Community Bulletin

In this Edition:

Sign up for CISA Alerts

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

Contact Us: https://www.cisa.gov/about/contact-us

Announcements, Opportunities and Resources

CISA and Secret Service Release New K-12 School Safety Toolkit

School safety reporting programs are a key component of school violence prevention. They provide a trusted avenue for students and school personnel to seek help and report concerns on issues involving student wellness or safety. To support the kindergarten through grade 12 (K-12) community in strengthening these reporting programs and encouraging bystander reporting among students, CISA's School Safety Task Force teamed up with the U.S. Secret Service National Threat Assessment Center to develop the K-12 Bystander Reporting Toolkit.

The new toolkit offers simple strategies and guidance that K-12 schools and school districts can use to implement and enhance safety reporting programs. It helps create a school environment where students are more willing and able to report concerns for the wellness and safety of themselves or others. It is designed to help school leaders create tailored, customized approaches that meet the needs of their unique communities. In addition to best practices and strategies, the toolkit includes self-assessment worksheets and checklists and a list of related school safety resources and tools.

To learn more and download the toolkit, visit K-12 Bystander Reporting Toolkit.

Learn More Here

Register Now for the 12th Annual Building Resilience Conference

Join us on July 26-27 for the 12th Annual Building Resilience Conference, hosted in partnership with the U.S. Chamber of Commerce Foundation, in Washington, D.C.

From panel discussions to hands-on workshops, this event will bring together hundreds of cross-sector leaders to discuss key strategies for building partnerships and bolstering systems we rely on every day—moving from the theoretical to the actionable. Now is the time to ensure our communities are resilient and ready to adapt when it's needed most. Check out the agenda to view the full list of sessions.

This is an event you won't want to miss. Register now!

Learn More Here

Are You Subscribed to the Homeland Security Information Network for Critical Infrastructure Security?

HSIN HOMELAND SECURITY INFORMATION NETWORK LOG IN

The Homeland Security Information Network (HSIN) is the trusted network for homeland security mission operations to share Sensitive But Unclassified (SBU) information. The Critical Infrastructure community on HSIN (HSIN-CI) is the primary system through which private sector owners and operators, DHS, and other federal, state, and local government agencies collaborate to protect the nation's critical infrastructure. HSIN-CI provides real-time collaboration tools including a virtual meeting space, document sharing, alerts, and instant messaging at no charge.

Learn More Here

Interactive Tools on the National Initiative for Cybersecurity Careers and Studies (NICCS) Website

Did you know CISA's NICCS website hosts the interactive versions of the NICE Framework, Cyber Career Pathways Tool, and Cybersecurity Careers Map? The National Initiative for Cybersecurity Careers and Studies (NICCS) website has a plethora of resources and information for federal and state, local, tribal and territorial (SLTT) government employees, industry, academia, students, and prospective/current cybersecurity professionals. The NICCS website has cybersecurity education, training, workforce development, and career information for everyone.

Learn More Here

Congratulations 2023 Graduates! Welcome to the Cybersecurity Workforce

Congratulations recent college graduates and welcome to the workforce! While cybersecurity may not have been your specific designated choice of study throughout college, CISA is always looking for qualified, capable young professionals to join the cyber workforce.

With over 3.4 million open cybersecurity positions worldwide and over 750,000 open positions in the U.S. alone, now is the time to explore different career path options and apply the knowledge and skills you learned in college and jump into this next phase of life. Let's review some tips and tools to help you get started.

- Take time to update your resume before interviewing so recruiters and hiring managers can find the best career fit for you.
- Explore cybersecurity work roles and learn how to advance from one work role to another using the Cyber Career Pathways Tool to plan your next career move.

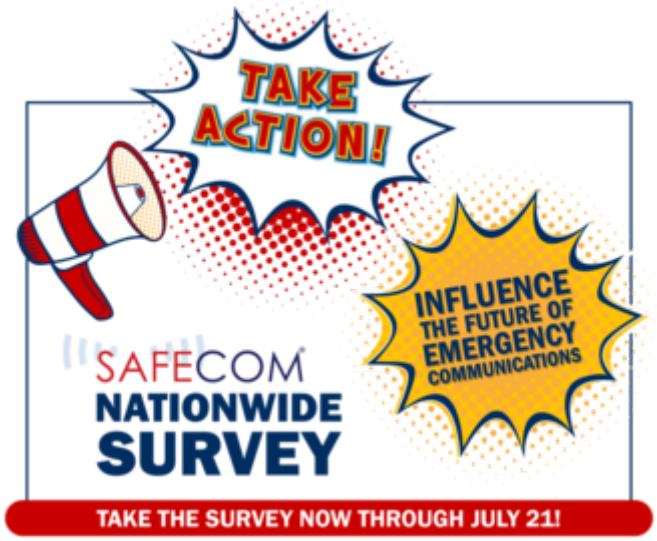
- If you are ready to enter the workforce and find a job, check out the Interactive Cybersecurity Career Map displaying thousands of federal job opportunities across the U.S. and around the world.

If you're interested in learning more about cybersecurity, check out all the tools and resources NICCS offers including the NICCS Education & Training Catalog with over 6,000 cybersecurity-related training and certification prep courses from hundreds of providers across the country. With in-person and virtual options for beginner, intermediate, and advanced users, the NICCS Education & Training Catalog has something for everyone.

For more information about cybersecurity career opportunities, visit cisa.gov/careers or email us at NICCS@hq.dhs.gov.

Learn More Here

Spread the Word: Launch of National Survey on Emergency Communications



CISA, in partnership with SAFECOM, is excited to launch the SAFECOM Nationwide Survey (SNS) and **we need your help**! The SNS provides critical data on federal, state, local, tribal and territorial emergency communications capabilities and gaps. Results from the survey will impact the future of emergency communications at all levels of government. For the data to be reliable, we need widespread participation across the public safety community. All law enforcement, 911, EMS, fire, and emergency management agencies should take the survey. The survey takes approximately 30 minutes to complete and is open through July 21, 2023.

The more public safety organizations that participate, the stronger the data will be! For information about completing the SNS, visit cisa.gov/sns or if you would like outreach materials to distribute, email us at sns@cisa.dhs.gov. We appreciate your help!

Learn More Here

SAFECOM Releases Updated Introductory Presentation for Stakeholder Use

SAFECOM is constantly adapting to the evolutions of the emergency communications ecosystem. As such, SAFECOM updated the *Introduction to SAFECOM* presentation, which provides stakeholders with information on SAFECOM's history, goals, and structure. The presentation can be used by SAFECOM members as a promotional tool to market the SAFECOM brand to the broader public safety community or other interested groups. The updated presentation includes logos for SAFECOM member organizations. The presentation also includes an updated list of recent resources and publications developed by each of SAFECOM's committees. SAFECOM members and the public safety community at-large are encouraged to leverage this presentation to assist in the promotion of SAFECOM's value to the public safety community. The updated *Introduction to SAFECOM* presentation can be found on CISA.gov at cisa.gov/safecom/about-safecom.

Learn More Here

CISA and Partners Release Joint Guide to Securing Remote Access Software

CISA, Federal Bureau of Investigation (FBI), the National Security Agency (NSA), Multi-State Information Sharing and Analysis Center (MS-ISAC), and the Israel National Cyber Directorate (INCD) released the Guide to Securing Remote Access Software on June 6, 2023. This new joint guide is the result of a collaborative effort to provide an overview of legitimate uses of remote access software, as well as common exploitations and associated tactics, techniques, and procedures (TTPs), and how to detect and defend against malicious actors abusing this software.

Remote access software provides organizations with a broad array of capabilities to maintain and improve information technology (IT), operational technology (OT), and industrial control system (ICS) services; however, malicious actors often exploit this software for easy and broad access to victim systems.

CISA encourages organizations to review this joint guide for recommendations and best practices to implement in alignment with their specific cybersecurity requirements to better detect and defend against exploitation. Additionally, please

refer to the additional information below on guidance for MSPs and small- and mid-sized businesses and on malicious use of remote monitoring and management software in using remote software and implementing mitigations.

Learn More Here

Secure by Design, Secure by Default

As America's Cyber Defense Agency, CISA is charged with defending our nation against ever-evolving cyber threats and to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day. But, as we introduce more unsafe technology to our lives, this has become increasingly difficult.

As a nation, we have allowed a system where the cybersecurity burden is placed disproportionately on the shoulders of consumers and small organizations and away from the producers of the technology and those developing the products that increasingly run our digital lives. Americans need a new model to address the gaps in cybersecurity—a model where consumers can trust the safety and integrity of the technology that they use every day.

Government cannot solve this problem alone. Technology manufacturers must increasingly embrace their role in putting consumer safety first. Technology providers and software developers must take the first step to shift this burden by claiming ownership of their customers' security outcomes.

Learn More Here

2023 Chemical Security Summit

The Chemical Security Summit is the signature U.S. event focused on chemical security collaboration across the public and private sectors that work with potentially dangerous chemicals.

SAVE THE DATE: The 2023 Chemical Security Summit will be held on August 29-31, 2023, in Northern Virginia, with an online attendance option available for many sessions. **Registration and venue information will be released as soon as possible.**

The Summit will feature important chemical security information for industry organizations, facility owners and operators, government officials, first responders, and law enforcement. Sessions will include:

- Updates on CISA's Chemical Facility Anti-Terrorism Standards (CFATS)and ChemLock programs
- Emerging threats to the chemical industry
- Demonstrations from federal partners
- Approaches to supply chain disruptions
- Case studies of real-world scenarios
- Cascading effects of cyberattacks
- International chemical security initiatives
- And more!

A preliminary agenda will be released later this summer. Not all sessions will be available to virtual attendees due to content and resource constraints.

Contact Information

For questions, please email ChemicalSummitReg@hq.dhs.gov.

Learn More Here

Cyber Defense Education and Training

Offerings for June – July 2023

Highlights: What You Want to Know

The **Cybersecurity Education and Training Assistance Program (CETAP)** is awarding $6.8 million to non-profits that seek to implement cybersecurity education and training into K-12 classrooms in all 50 states and U.S. territories. This funding seeks to bring awareness to students about cybersecurity at an early age so that they have the skills, knowledge and excitement needed to pursue a career in cybersecurity. Applications are being accepted through July 25, 2023. Learn more here.

In May and June, U.S. Executive Branch employees and contractors can participate in eleven CDM Dashboard courses, including the new **CDM and Federal Mandates-*Featuring how to use the CDM Dashboard to enable automated BOD-22-01 Reporting*** course. This course presents information regarding current federal cybersecurity directives, mandates and policies, and how they can be supported by the CDM Agency Dashboard. Featured prominently will be details on how to use the CDM Dashboard to enable automated BOD-22-01 Reporting.

CISA recently added a **new** set of training modules on **ransomware prevention** hosted in the Federal Virtual Training Environment (FedVTE). The modules provide an overview on ransomware and six preventative controls to help prevent ransomware attacks.

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 2023

Date	Course Code	Registration Opens	Course	Hours
07/07/2023	IR110	06/07/2023	**Introduction to Log Management**	1
07/11/2023	IR107	06/12/2023	**Introduction to Network Diagramming**	1
07/20/2023	IR205	06/20/2023	**Preventing Web and Email Server Attacks**	4

To learn more or register visit**: https://www.cisa.gov/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 2023

Date	Course Code	Course	Location
07/10/2023-07/28/2023	401v	**Industrial Control Systems Evaluation (401v)**	Scheduled Online Training
07/10/2023-07/28/2023	301v	**Industrial Control Systems Cybersecurity (301v)**	Scheduled Online Training
07/10/2023-07/13/2023	301L	**Industrial Control Systems Cybersecurity Training – In-Person 4 Days**	IN-PERSON TRAINING (4 days)
07/24/2023-07/27/2023	101, 201, 202	**Industrial Control Systems (101, 201, 202)**	IN-PERSON TRAINING – LOUISIANA (3 days)

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.*

CISA's Cybersecurity Workforce Training for Underserved Communities and CyberWarrior: CISA's non-traditional training program grantee, CyberWarrior, increases opportunity and economic mobility for people of all backgrounds through training, mentorship and technology. Through its CyberWarrior Academy, it delivers hands-on, intensive, lab-driven technical training in cybersecurity methods and procedures.

CyberWarrior Training Events

Date	Audience	Course
07/13/2023	General Public	**July Master Class – DeepFakes** July Master Class | CyberWarrior.com
08/17/2023	General Public	**August Master Class – Open Source Intelligence** August Master Class | CyberWarrior.com
09/14/2023	General Public	**September Master Class – Incident Response** September Master Class | CyberWarrior.com

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

Federal Cyber Defense Skilling Academy: The Federal Cyber Defense Skilling Academy helps civilian federal employees develop their cyber defense skills through training in the baseline knowledge, skills and abilities of a Cyber Defense Analyst (CDA). Students will have the opportunity to temporarily step away from their current role while they participate in the intense, full-time, three-month accelerated training program. The course provides valuable opportunities to practice new CDA skills in a lab environment. As an added incentive, students will receive CompTIA Security+ training during the last two weeks of the Skilling Academy and a voucher to take the certification exam. Please note, applications for each cohort are due approximately one month before the program begins. Visit our website for details on how to apply.

CISA's K – 12 Cybersecurity Education Training Assistance Program (CETAP): Through CISA's CETAP grantee, CYBER.ORG, we offer K-12 teachers with cybersecurity curricula and education tools. CYBER.ORG develops and distributes free cybersecurity, STEM and computer science curricula to K-12 educators across the country. Below are upcoming training events through CYBER.ORG.

CYBER.ORG Training Events through July 2023

Date	Audience	Course
07/17/2023-07/21/2023	High School Teachers	**Intro to Cybersecurity Bootcamp for 9-12 Teachers:** This bootcamp is a weeklong event that prepares teachers to teach CYBER.ORG's new Intro to Cybersecurity course.

		Intro to Cybersecurity Bootcamp | CYBER.org
07/24/2023-07/28/2023	High School Teachers	**Cybersecurity Bootcamp for 9-12 Teachers:** This bootcamp is a weeklong event that prepares teachers to teach CYBER.ORG's High School Cybersecurity course. Cybersecurity Bootcamp | CYBER.org
07/25/2023	K-5 Educators	**Non-Technical Cybersecurity Basics Bootcamp for K-5 Educators:** This bootcamp is a daylong event that prepares K-5 educators to successfully teach CYBER.ORG's Cybersecurity Basics course. Non-Technical Cybersecurity Basics Bootcamp K-5 | CYBER.org
07/26/2023	6-8 Educators	**Non-Technical Cybersecurity Basics Bootcamp for 6-8 Educators:** This bootcamp is a daylong event that prepares 6-8 educators to successfully teach CYBER.ORG's Cybersecurity Basics course. Non-Technical Cybersecurity Basics Bootcamp 6-8 | CYBER.org
07/27/2023	K-12 Educators	**Cyber Society Workshop:** Sharpen critical thinking skills and explore humanities concepts as you prepare students to live in a cyber society. Cyber Society Workshop | CYBER.org

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

Continuous Diagnostics and Mitigation (CDM): We offer instructor led, hands-on CDM Agency Dashboard training for U.S. Executive Branch employees and contractors in our cyber range virtual 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).

All courses will be taught using the latest version of the CDM Dashboard (ES-5) using a virtual training range. The newest offering is the CDM220 Federal Mandates and BOD 22-01 & 23-01 Reporting course, which will focus on the newest version ES-6 of the CDM Dashboard.

CDM Training Events through July 2023

Date	Course Code	Registration Opens	Course	Hours
07/06/2023	CDM203	05/26/2023	**CDM Dashboard Role-Based Training - System Analyst**	4
07/12/2023	CDM210	05/26/2023	**Introduction to CDM Enabled Threat Hunting (CETH)**	4
07/21/2023	CDM301	06/21/2023	**Executive Overview of the CDM Agency Dashboard**	2
07/26/2023	CDM202	06/26/2023	**Configuration Settings Using the CDM Agency Dashboard**	4

To learn more or register visit: **https://www.cisa.gov/cdm-training**

CDET Mission

Address today's cyber workforce challenges through innovative education and training opportunities

CDET Vision

Lead and influence national cyber training and education to promote and enable the cyber-ready workforce of tomorrow

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

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

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

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

Learn More Here

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

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