May 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

Cybersecurity Awareness Month is Fast-Approaching

Since 2004, the President of the United States and the U.S. Congress have declared October to be Cybersecurity Awareness Month, highlighting how individuals and businesses can protect themselves and others from online threats to technology and personal data and reduce the risks to the products that we use every day. Cybersecurity Awareness Month is truly a collaborative effort between government, industry, and the public to raise cybersecurity awareness nationally and internationally.

Our Cybersecurity Awareness Month partners are critical to its success. We look forward to working with you and our many new partners to encourage federal and state governments, businesses of all sizes, and non-profit organizations to work together to protect each other from malicious actors looking to do us all harm.

Cybersecurity Awareness Month is fast-approaching. For your planning purposes, the four key behaviors we will be highlighting throughout October will be consistent with last year. They are:

- Enable multi-factor authentication
- Use a strong password
- Recognize and report phishing
- Update your software

Please join us again in becoming a Cybersecurity Awareness Month partner because every little bit helps—from amplifying messages in your community about the steps we can all take to make our devices more secure to industry actions that make technology products secure by design and secure by default right out of the box—your participation matters!

To receive updates as more information becomes available, email us at AwarenessCampaigns@cisa.dhs.gov. CISA will also be sharing this year's messaging and resources on the Cybersecurity Awareness Month page as we get closer to October.

Learn More Here

Cybersecurity Best Practices for Smart Cities

Around the world, communities (such as university campuses, cities and towns, and military installations) are increasingly integrating information and communications technologies (ICT) into their day-to-day operations to improve the quality of services for their residents. However, communities considering becoming smart cities should thoroughly assess and mitigate the cybersecurity risk that comes with this integration. Criminals and cyber threat actors can exploit vulnerable systems to steal critical infrastructure data and proprietary information, conduct ransomware operations, or launch destructive cyberattacks.

CISA, the National Security Agency (NSA), the Federal Bureau of Investigation (FBI), the United Kingdom National Cyber Security Centre (NCSC-UK), the Australian Cybersecurity Centre (ACSC), the Canadian Centre for Cyber Security (CCCS), and the New Zealand National Cyber Security Centre (NCSC-NZ) developed a joint guidance to help communities considering becoming “smart cities” thoroughly assess and mitigate the cybersecurity risk that comes with this integration.

The Cybersecurity Best Practices for Smart Cities provides recommendations to balance efficiency and innovation with cybersecurity, privacy protections, and national security. Organizations should implement these best practices in alignment with their specific cybersecurity requirements to ensure the safe and secure operation of infrastructure systems, protection of citizen’s private data, and security of sensitive government and business data.

Please note that “smart cities” is an umbrella term that refers to communities implementing smart city technologies to optimize their operations. Other terms include “connected places,” “connected communities,” and “smart places.” CISA specifically refers to this as “Connected Communities”.

Download/share the Cybersecurity Best Practices for Smart Cities.

For more on CISA’s work to help cities and communities mitigate the cybersecurity risk, visit Connected Communities.

Learn More Here

CISA Leads Inaugural Cyber Workforce Development Workshop in the Philippines

CISA's International Affairs Team led a week-long workshop, co-organized by U.S. Embassy Manila (ECON) and USAID, supporting the Philippines' efforts to train, upskill, and reskill cyber officials. The workshop was CISA International's inaugural workforce development class, which was attended by more than 45 government officials from four departments. The CISA International delegation consisted of Danny E. Davis, Madison Harnett, Nancy Limauro, and Danielle Santos with the National Institute of Standards and Technology (U.S. Department of Commerce).

According to Danny, who led the delegation on behalf of CISA, "Workforce Development is a pillar of the Philippines' National Cyber Strategy, so the attendees eagerly received this training and responded well to their capstone exercise on how to implement cyber work-force strategies across their government." The entire delegation received an overwhelming response of appreciation from the class participants, U.S. Embassy Manila, and USAID.

GET Connected and STAY Connected with CISA's Free Priority Services

CISA celebrated April as the second annual Emergency Communications Month by prioritizing the people who support the systems on which we rely and highlighting the role of emergency communications as a vital function. CISA celebrated National Public Safety Telecommunicators Week (NPSTW), which is held annually during

the second week of April to honor telecommunications personnel for their commitment, service, and sacrifice.

As part of this year's efforts, CISA empowered all emergency communications partners to "Get Connected and Stay Connected" by enrolling in the agency's free Priority Telecommunications Services. CISA's Priority Services allow for communication with priority capability when networks are degraded or congested. No matter what industry you represent, it is imperative to have the means to communicate during times of importance. Priority Services include:

- Government Emergency Telecommunications Service (GETS) – covering wireline communications
- Wireless Priority Service (WPS)– covering wireless communications
- Telecommunications Service Priority (TSP)– covering repair and installation of critical voice and data circuits or IP-based services

Visit Priority Telecommunications Services to learn more about CISA's free priority services.

CISA Webinar on Interoperable Backup Communications Systems

On April 26, CISA's Emergency Communications Division hosted the webinar, "Is This Thing On? Using Backup Communications Systems to Ensure Mission Readiness," which highlighted the importance of maintaining resilient communications. During the webinar, participants explored collaborative planning approaches for establishing and testing interoperable backup communications capabilities and discussed National Emergency Communications Plan resources that can assist with backup communications readiness.

Learn More Here

CISA Office For Bombing Prevention Leaders Sit Down with *Homeland Security Today* Following Recognition for Outstanding Service in Security Community

Three members of CISA's Office For Bombing Prevention (OBP) recently sat down with *Homeland Security Today* to discuss their recent accomplishments, emerging threats, and how this work prevents, protects against, and mitigates the malicious use of explosives.

OBP's Training Branch Chief Curt Tilley accepts awards on behalf of OBP.

The *Homeland Security Today* Homeland Hero Award winners and their respective interviews are as follows:

- Associate Director Sean Haglund received the Mission Award
- Strategy Branch Chief Doug DeLancey received the Most Innovative Campaign to Increase Security Award
- Training Branch Chief Curt Tilley received the Excellence in Outreach Award

For over a decade, the Government Technology & Services Coalition (GTSC) has been serving DHS and other federal agencies with the mission of protecting citizens, assets, and way of life. The *Homeland Security Today* awards are the only national program awards devoted to recognizing heroes from across the many disciplines within homeland security. From individual citizens to mayors to first responders, the nomination process helps GTSC find incredibly special people working diligently to ensure the safety of this nation.

To learn more about the award winners, visit Homeland Stars Burning Bright: 2022 Mission Awards - *HS Today*.

Learn More Here

New Free Open-Source Hunt and Incident Response Tool

CISA, in coordination with Sandia National Laboratories, released a free, open-source hunt and incident response tool, known as Untitled Goose to the CISA GitHub Repository in March. Untitled Goose Tool adds novel authentication and data gathering methods to help network defenders analyze Microsoft cloud services and detect potentially malicious activity in Microsoft Azure, Active Directory (AAD), and Microsoft 365 (M365) environments. Users can run Untitled Goose Tool once,

as a snapshot in time, or routinely. For certain log types, the tool will pick up from the last time it was executed.

CISA advises users to employ Untitled Goose Tool to:

- Export and review AAD sign-in and audit logs, M365 unified audit log (UAL), Azure activity logs, Microsoft Defender for IoT (internet of things) alerts, and Microsoft Defender for Endpoint (MDE) data for suspicious activity.
- Query, export, and investigate AAD, M365, and Azure configurations.

The repository has already garnered over 23,000 unique visitors and received 668 stars from the community. CISA welcomes user contributions to add new features or further build out the tool via the Untitled Goose Tool GitHub Repository.

Learn More Here

Final Version of TIC Use Cases Covering Cloud Services

Highlighting unique considerations for Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), Software-as-a-Service (SaaS), and Email-as-a-Service (EaaS), CISA published the Trusted Internet Connections (TIC) 3.0 Cloud Use Case that provides common network and multi-boundary security guidance for agencies that operate in cloud environments on April 17.

The Cloud Use Case outlines security patterns, applicable security capabilities, and telemetry requirements specific to this particular use case. This guidance also incorporates cloud-specific considerations, such as the shared services model and cloud security posture management principles outlined in the Cloud Security Technical Reference Architecture. This use case is written from the vantage point of cloud-hosted services, as opposed to from the vantage point of the client accessing these services.

CISA also published updates of the TIC Branch Office Use Case and the Remote User Use Case. These updates were based on new security capabilities updates in the Security Capabilities Catalog v3.0.

The final Cloud Use Case satisfies the use case requirements prescribed under the Office of Management and Budget's (OMB) Memorandum M-19-26 for the modernized TIC 3.0 initiative.

All of these new documents and other helpful reference materials, like frequently asked questions (FAQs) and trainings, can be found on the TIC homepage.

Learn MoreHere

ChemLock Program

The ChemLock program provides voluntary, no-cost, tailored services and tools to any facilities with dangerous chemicals to help improve their overall chemical security posture in a way that works for their business model.

On-Site Assessments and Assistance – CISA's ChemLock program offers chemical security assessments to facilities that possess dangerous chemicals. These assessments are structured in a three-level approach, starting with a security awareness consultation that serves as an initial conversation with the facility to help them better understand the risks associated with their specific chemical holdings.

- From there, facilities can choose to move to the next level by having a Chemical Security Inspector (CSI) conduct a voluntary security posture assessment.
- During this visit, the CSI will walk through the facility and develop options for consideration to help the facility improve their chemical security posture.
- The final level of the assessment is the security planning visit, where the CSI will help the facility integrate options for consideration into their security plan.
- Participation in ChemLock On-Site Assessments and Assistance come at no cost to the facility.

To learn more or submit a ChemLock service request please visit our webpage.

Quarterly ChemLock Trainings

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

ChemLock: Introduction to Chemical Security

This course provides an introduction to identifying, assessing, evaluating, and mitigating chemical security risks. This easy-to-understand overview identifies key

components and best practices of chemical security awareness and planning to help kickstart chemical security discussions at your facility.

Save the Date! This course runs one to two hours in length and is appropriate for all personnel regardless of their level of involvement with dangerous chemicals.

- Register for July 13, 2023 – 1-3 pm ET
- Register for October 17, 2023 – 10 am-noon 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.

Save the Date! 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 10, 2023– 1-4 pm ET
- Register for November 14, 2023 – 10 am-1 pm ET

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

Learn More Here

CISA Hosts Chemical Security Summit 2023

August 29-31, 2023

Save the Date! CISA will host the 2023 Chemical Security Summit virtually and in-person from August 29-31, 2023, in Northern Virginia.

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

- When: August 29-31, 2023
- Where: Northern Virginia and Microsoft Teams
    - Venue will be announced with registration in the coming weeks
    - Links for virtual attendees will be sent out closer to the Summit date

- Who should attend:

    - Chemical and related industry stakeholders
    - Corporate and facility security officers
    - Environment, health, and safety professionals

The Summit is free to attend and open to the public. Registration, provisional agenda, and further information will be available in the coming weeks on the 2023 Chemical Security Summit webpage. For more information, please email chemicalsector@cisa.dhs.gov and/or ChemicalSummitReg@hq.dhs.gov.

We look forward to seeing you in person or virtually at the 2023 Chemical Security Summit.

Learn More Here

Save the Date! Regional Webinars

Enhance Awareness of and Response to an Active Shooter Incident

CISA Region 9 (Arizona, California, Hawaii, Nevada, Guam, American Samoa, Commonwealth of the Northern Mariana Islands) invites partners from the Food and Agriculture Sector to join a two-hour security webinar to enhance awareness of and response to an active shooter incident.

- Tuesday, May 23, 2023
- 12:00 p.m. PDT (3:00 p.m. EDT)
- Register Here

Cyber Defense Education and Training (CDET) Offerings for May – June 2023

Highlights: What You Want to Know

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.

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. Additionally, we are in the process of changing the registration period from opening one month before the course date to opening two months before the course date.

IR Training Events through June 2023

Date	Course Code	Registration Opens	Course	Hours
06/06/2023	IR108	05/05/2023	**Indicators of Compromise**	1
06/15/2023	IR208	05/15/2023	**Understanding Indicators of Compromise**	4
06/21/2023	IR104	05/19/2023	**Defending Internet Accessible Systems**	1
06/22/2023	IR210	05/22/2023	**Introduction to Log Management**	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. MDT (10:00 a.m. – 7:00 p.m. EDT). 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 June 2023

Date	Course Code	Course	Location
05/23/2023-05/25/2023	401L	**Industrial Control Systems Evaluation Training – In-Person 3 Days**	IN-PERSON TRAINING (3 days)
06/05/2023-06/23/2023	401v	**Industrial Control Systems Evaluation (401v)**	Scheduled Online Training
06/05/2023-06/23/2023	301v	**Industrial Control Systems Cybersecurity (301v)**	Scheduled Online Training
06/05/2023-06/08/2023	301L	**Industrial Control Systems Cybersecurity Training – In-Person 4 Days**	IN-PERSON TRAINING (4 days)
06/27/2023-06/29/2023	401L	**Industrial Control Systems Evaluation Training – In-Person 3 Days**	IN-PERSON TRAINING (3 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.*

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
05/18/2023	General Public	**May Master Class – Ransomware** May Master Class | CyberWarrior.com
06/15/2023	General Public	**June Master Class – Social Engineering** June Master Class | CyberWarrior.com
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.

Skilling Academy Cohorts 2023

Date	Audience	Event
05/22/2023	DHS Employees	Second May 2023 Program Begins

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

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 June 2023

Date	Audience	Course

06/20/2023-06/22/2023	K-12 Educators	**CYBER.ORG EdCon:** CYBER.ORG's national conference designed to inspire and empower novice and expert cybersecurity K-12 educators alike. EdCon | CYBER.org
06/26/2023-06/30/2023	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

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 June 2023

Date	Course Code	Registration Opens	Course	Hours
05/24/2023	CDM210	04/24/2023	**Introduction to CDM Enabled Threat Hunting (CETH)**	4
06/01/2023	CDM220	05/01/2023	**CDM and Federal Directives**	4
06/07/2023	CDM111	05/08/2023	**Analyzing Cyber Risk (In-Person)**	7
06/08/2023	CDM111	05/08/2023	**Analyzing Cyber Risk (In-Person)**	7
06/13/2023	CDM142	05/12/2023	**Asset Management with the CDM Agency Dashboard**	4

06/27/2023CDM201	05/26/2023	**Identity and Access Management with the CDM Dashboard**	4

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

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*

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*