May 2024 Issue

In this edition:

- NPower Virtual Coaching Volunteer Opportunity
- Upcoming Interagency Security Committee Risk Management Process & Facility Security Committee Trainings
- Cyber Education & 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 (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

The President's National Security Telecommunications Advisory Committee Approves Two Products for Transmission to the President

The President's National Security Telecommunications Advisory Committee (NSTAC) provides industry-based analyses and recommendations to the Executive Office of the President on how the government can take actions to enhance national security and emergency preparedness telecommunications. On March 7, 2024, the NSTAC unanimously approved two products containing recommendations for the president's consideration.

Tasked in May 2023 to study barriers that inhibit the adoption of cybersecurity standards and best practices in both public and private sectors, the NSTAC conducted an 8-month study that resulted in the *NSTAC Report to the President on Measuring and Incentivizing the Adoption of Cybersecurity Best Practices*. This report provides 12 key findings and 30 recommendations detailing how the government can incentivize and promote the adoption of cybersecurity best practices.

In December 2023, the NSTAC was asked to provide industry perspective on dynamic spectrum sharing plans outlined in the National Cybersecurity Strategy Implementation Plan. In response, the committee produced the *NSTAC Letter to the President on Dynamic Spectrum Sharing*. In the letter, the NSTAC expressed the need to make available additional spectrum resources for commercial use but also recognized that requirements must be balanced against current uses of spectrum to protect national defense interests.

Learn More Here

CISA OBP Launches The B.O.M.B.E.R Initiative and Suite of Products

CISA's Office of Bombing Prevention (OBP) announces the development of a suite of products to recognize and report suspicious activity. These products feature the BOMBER acronym which is a tool you can use to assess your surroundings, identify suspicious activity, and help prevent a potential bombing incident.

- **Baseline:** Establish a baseline of what normal behaviors and activities look like.
- **Operational Indicators:** A bombing attack requires a planning process that may include surveillance, target selection, testing or probing security and practice runs.
- **Materials:** Terrorists and criminals acquire materials to create a homemade or improvised explosive device.
- **Bomb-Building Activity:** Potential indicators of bomb-building activity include evidence of bomb-making research, testing of mixtures or devices and chemical exposure.
- **Elicitation:** An attempt to discreetly gain information by asking questions about a place, person or operation.
- **Respond:** Report suspicious activity. Products in this collection include:

- Identify Suspicious Activity Card and Poster
- Identifying Suspicious Activity Video

Suspicious Activity Recognition for Bombing Prevention Course

Learn More Here

Threat Actors Exploit Multiple Vulnerabilities in Ivanti Connect Secure and Policy Secure Gateways

CISA, FBI, Multi-State Information Sharing & Analysis Center (MS-ISAC), and international partners in Australia, United Kingdom, Canada, and New Zealand released a joint Cybersecurity Advisory (CSA) in response to the active exploitation of multiple vulnerabilities within Ivanti Connect Secure and Ivanti Policy Secure gateways.

The authoring agencies and industry partners have observed persistent targeting of these vulnerabilities by a variety of cyber threat actors. These vulnerabilities can be used in a chain of exploits to bypass authentication, craft malicious requests, and execute arbitrary commands with elevated privileges. In turn, exploitation of these vulnerabilities may allow lateral movement, data exfiltration, web shell deployment, credential theft including domain administrators, and persistent access on a target network.

This joint advisory provides technical details on observed tactics used by these threat actors and indicators of compromise to help organizations detect malicious activity. All organizations using these devices should assume a sophisticated threat actor could achieve persistence and may lay dormant for a period of time before conducting malicious activity. Organizations are urged to exercise due caution in

making appropriate risk decisions when considering a virtual private network (VPN), to include whether to continue operating Ivanti Connect Secure and Policy Secure gateways.

All organizations and vendors are urged to review the advisory, implement recommended mitigations which align to the Cross-Sector Cybersecurity Performance Goals and Secure by Design principles, and validate your organization's security controls against the threat behaviors mapped to the MITRE ATT&CK.

Learn More Here

PARTNERSHIPS

Partner with CISA to Secure Our World

In an exciting effort to educate the public on how to stay safe online, CISA launched the enduring Secure Our World program last fall, providing resources and actions we all can take to keep our connected devices safe and secure. Secure Our World underscores how individuals, small business, and organizations of all sizes, can play a part to secure our customers, families, and businesses against cyber threats.

We ask you to join CISA in promoting Secure Our World through a strategic partnership and amplify the importance of reducing cyber risks. Your organization can collaborate with us by developing co-branded materials, sharing tips and resources, or proposing creative avenues that increase cybersecurity awareness. By educating others about the four easy ways to stay safe online, and the importance of cybersecurity in general, you will play an integral role in helping all of us Secure Our World.

Join other collaborators like Google, the NFL, NASDAQ and hundreds of small businesses and organizations that recognize the importance of Secure Our World's message. We need you to join us to help spread the message!

Please reach out to awarenesscampaigns@cisa.dhs.gov to become a Secure Our World Partner today! Feeling more empowered? Become a Cybersecurity Awareness Month partner this October, as well!

To learn more about the Secure Our World program, explore our free, comprehensive suite of cybersecurity tools, resources, and guidance available at cisa.gov/SecureOurWorld.

Learn More Here

Unity, Resilience and Election Security

CISA recently launched #Protect2024 to "help election officials and election infrastructure stakeholders protect against the cyber, physical, and operational security risks to election infrastructure during the 2024 election cycle." CISA will work to do this by providing resources and stakeholder engagement throughout the country, during not only an election year but also our agency's Year of Unity and Resilience. CISA aims to boost election infrastructure resilience and work collaboratively to support those engaged in this important work.

Election infrastructure is disparate, complex, and very much state and locally based. CISA encourages strength through unity by providing election officials with numerous resources, consistent guidance, and thorough participation in groups of election officials like the Election Infrastructure Information Sharing and Analysis Center (EI-ISAC). CISA is also unifying with organizations across the government to publish election security products.

The #Protect2024 resources and guidance encourages resiliency among election infrastructure and the officials safeguarding it. The site provides guidance to

develop an incident response plan and encourages personnel to rehearse it. It links to free cyber hygiene services that can help an organization manage vulnerabilities. Protective Security Advisors are making physical security assessments available across CISA's regions. As the year progresses, more resources, services, and information are becoming available!

Follow CISA on social media and check back on the #Protect2024 website throughout the year. Please share the information widely with CISA stakeholders.

Learn More Here

Interagency Security Committee Publishes 2023 Annual Review

The Interagency Security Committee published the 2023 Interagency Security Committee Annual Review. The Annual Review highlights the ISC's continued dedication to providing its 66 members and stakeholders with excellence in federal facility security guidance, best practices, and training opportunities.

The 2023 ISC Annual Review also highlights many of the ISC's accomplishments and activities including the signing of Executive Order 14111, the development and release of numerous publications, completion of the ISC's fifth year of compliance reporting, and a collection of entries that showcase the impactful work of member departments and agencies in the field.

Learn More Here

INFORMATION EXCHANGE

Data Protection: Safeguarding Your Information at the Right Time

CISA, Region 6 Deputy Regional Director Robert Russell participated in the panel discussion on *Data Protection: Safeguarding Your Information at the Right Time*, at the 2024 International Leadership Summit, in Dallas, Texas March 21, 2024.

The panel discussion moderated by T.D. Jakes Ministries Executive Director of Information Technology Lance Goudy, was presented by Wells Fargo. Panel members included Microsoft Chief Security Advisor Terence Jackson, Elastic Senior Director Lisa Jones-Huff, and Givelify Vice President of Technology and Compliance Hari Krishna. Cybersecurity Advisor (CSA) Michael Kingsley also attended the panel and helped answer questions from the audience. The panel discussion covered Multi Factor Authentication (MFA), CISA tools and services, Secure by Design, zero trust and more.

Learn More Here

Building Critical Infrastructure Resilience for Our Nation

Building resilience is important for everyone, but especially for our nation's critical infrastructure stakeholders. That's why CISA has Shields Ready. "As the National Coordinator for critical infrastructure security and resilience, CISA stands ready to help America prepare for and adapt to changing risk conditions and withstand and recover rapidly from potential disruptions, regardless of cause."

The Shields Ready resilience campaign helps critical infrastructure stakeholders take action to enhance security and resilience—from industry and businesses to government entities at all levels, and even individuals by providing recommendations, products, and resources to increase individual and collective resilience for different risk contexts and conditions. It's about preparing before an incident—from extreme weather and climate change, to cyber threats, to targeted violence and terrorism—to increase resilience and reduce impact during and after.

Shields Ready provides information, resources and partnership in order to improve critical infrastructure resilience though four steps.

- Identify Critical Assets and Map Dependencies
- Assess Risks
- Plan and Exercise
- Adapt and Improve

Learn More Here

CISA Celebrated its Third Emergency Communications Month Last Month

April was the third annual Emergency Communications Month to honor the nation's emergency responders and communicators, emphasizing the importance of interoperable emergency communications and the need to work together in building resilient critical infrastructure. This year's theme placed a special focus on how our nation is **Resilient Together,** highlighting the importance of secure, interoperable emergency communications and how CISA supports this effort in collaboration with its partners across the emergency communications ecosystem.

Throughout April, CISA Emergency Communication's Division encouraged organizations to significantly bolster their communications resiliency and emergency preparedness by enrolling in the agency's free priority telecommunications services. These services, which include the Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS), enable essential personnel to communicate when networks are degraded or congested due to weather events, mass gatherings, cyberattacks, or events stemming from human error.

To learn more about Emergency Communications Month and how to amplify our resources, visit cisa.gov/emergency-communications-month.

During the second week of April, CISA also recognized and celebrated National Public Safety Telecommunicators Week.

Learn More Here

Federal (PNT) Services Acquisitions Guidance

CISA released Federal Positioning, Navigation and Timing (PNT) Services Acquisitions Guidance (V1.0) on March 22, 2024. Stakeholders from both industry and government space-related initiatives provided significant input and collaboration to facilitate development of this guidance. This effort is in support of DHS's requirement under EO 13905, *Presidential Executive Order 13905, Strengthening National Resilience Through Responsible Use of Positioning, Navigation, and*

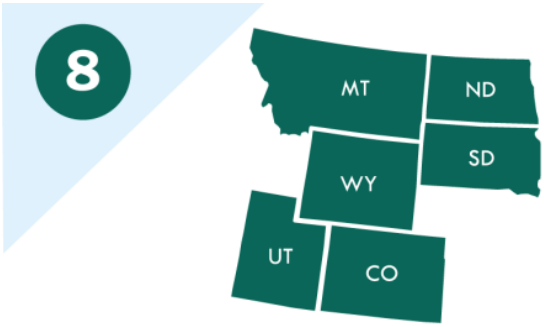
Timing Services (EO 13905). This resource incorporates interagency and cross-sector acquisition recommendations for PNT resiliency requirements. The guidance offers an overarching view of the model PNT contractual language construction process, key tenets of PNT resiliency and an associated workflow for the requisite drafting steps. CISA acknowledges and thanks all those who contributed to this guidance.

The intended audience includes federal departments and agencies, along with state, local, tribal, and territorial (SLTT) organizations, PNT program managers, acquisition professionals, and contract bidders. The primary aim is to guide users in assessing their PNT dependencies and establishing requirements for appropriate levels of resiliency based upon the operational needs of the proposed product, system, or service. The guide provides workflows, steps, and recommended structures for requirements for federal contracts for products, systems, and services that integrate or utilize PNT services, with the goal of encouraging the private sector to use additional PNT services and develop new robust and secure PNT services.

This guidance is voluntary and does not: constitute regulations, define mandatory practices, provide a checklist for compliance, or carry statutory authority. It is intended to be a set of guidelines, which will then be sent for consideration to the Federal Acquisition Regulation (FAR) Council.

Learn More Here

Region 8 Securing Public Gatherings Webinar



Are you prepared for events you are organizing for the summer? The CISA is hosting a 2-hour webinar on May 7, 2024, to provide tools and resources to assist with protection of public areas from a variety of threats.

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

CISA Hosts Second Cyber Resilient 911 Symposium

CISA's Emergency Communications Division (ECD) led the Cyber Resilient 911 (CR911) Program's second regional symposium in the Southeast, which included CISA regions 4 and 6 as well as Delaware, Puerto Rico, West Virginia, and the U.S. Virgin Islands. Attendees included 911 administrators, representatives from local centers and IT/cyber communities, and Statewide Interoperability Coordinators (SWICs) from each state and territory.

CISA's collaboration history with SWICs is crucial for enhancing nationwide interoperability and strengthening stakeholder relationships, especially in emergency communication systems like 911. The Federal Communications Commission (FCC), the National Highway Traffic Safety Administration (NHTSA) and the National Telecommunications & Information Administration (NTIA) partnered with CISA to engage stakeholders to determine cybersecurity priorities for the CR911 Program.

At the symposium, speakers and panelists presented an overview of the current cyber threat landscape and shared resources to help enhance the cybersecurity posture of Emergency Communication Centers (ECCs). Symposium topics included the current state of cyber resilience in the 911 ecosystem, best practices for responding to a cyberattack and the available program resources for each region. CISA facilitators utilized interactive live polling, breakout sessions and group discussions to gather stakeholders' current needs, concerns and capability gaps with regards to cybersecurity. Attendees also participated in a tabletop discussion focused on a simulated cyberattack scenario.

Learn More Here

CISA Updates Toolkit to Promote Public Safety Communications and Cyber Resiliency

To keep America safe, secure, and resilient, CISA collaborates with public safety, national security, and emergency preparedness communities to enhance seamless communications. An interruption in communications impacts a public safety agency's ability to deliver critical lifesaving services to the community. It is imperative that public safety agencies carefully plan, implement, and review communications capabilities to maintain daily communications abilities and prepare for future emergency events.

To assist public safety agencies in navigating the wealth of information available regarding communications resiliency, CISA created the *Public Safety Communications and Cyber Resiliency Toolkit* to identify and address emergent trends and issues, consolidate resources, educate stakeholders at all levels of government, and propose mitigations to enable resilient public safety communications. It is designed to assist those responsible for communications networks by providing the tools that evaluate current resiliency capabilities, identify ways to improve resiliency, and develop plans for mitigating the effects of potential resiliency threats.

Using an interactive graphic, Toolkit users can easily navigate through several topics and access applicable resources. Current topics include:

- Alerts, Warnings, and Notifications
- Cyber Incidents
- Cybersecurity
- Electromagnetic Pulse (EMP)
- Healthcare
- Jamming
- Land Mobile Radio (LMR)
- Local Access Networks (LAN)
- Next Generation 911 (NG911)
- Positioning, Navigation, and Timing (PNT) Disruptions
- Power
- Priority Services
- Ransomware
- Resiliency Introduction
- Site Hardening
- Unmanned Aircraft Systems (UAS)

Since its last update in August 2023, the Toolkit has been updated with seven new resources across the existing sections. Users are encouraged to revisit the Toolkit regularly and take advantage of new information and resources. Check out the updates at https://www.cisa.gov/communications-resiliency today!

For more information and additional guidance regarding communications resiliency, visit cisa.gov/safecom/technology.

Learn More Here

Publication Release: SCuBA Hybrid Identity Solutions Guidance

CISA, as part of its Secure Cloud Business Applications (SCuBA) Project, just finalized and published its Hybrid Identity Solutions Guidance to help organizations better understand identity management capabilities, the tradeoffs that exist in various implementation options, and factors that should be considered when making implementation decisions. This guidance supports the SCuBA Project's goal of helping agencies effectively implement cybersecurity capabilities as they migrate from traditional on-premises infrastructure to the cloud.

Although primarily intended for FCEB agencies, this guidance is broadly applicable for state, local, tribal, and territorial government and critical infrastructure entities, as well as private industry, academia, and more. Learn more about options for identity management between cloud and on-premises systems here Secure Cloud Business Applications: Hybrid Identity Solutions Guidance | CISA

Leran More Here

ICT SCRM Conference

Connected Communities and ICT SCRM efforts: On **June 12, 2024**, CISA will host the Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force's first annual conference, **Innovations in Supply Chain Risk Management**. The conference will be a one-day event held at the **MITRE Corporation** in **McLean, Virginia**.

The conference panel topics include supply chain transparency, the impact of cyber incidents on supply chains, the role of technology in supply chain risk management, supply chain impacts to small and medium-sized businesses, and the influence of new and emerging technologies on supply chains.

Speakers and panelists will include senior officials from CISA and the homeland security and cyber community as well as Task Force members, CEOs, senior executives, SCRM SMEs, and policy experts. During the panel discussions panelists will also highlight various ICT SCRM Task Force products, tools, and templates publicly available on the ICT SCRM Task Force webpage. Additional details and registration information are forthcoming.

Learn More Here

Save the Date! Pre-Register Now!

NCIRP 2024 Listening Session - Wednesday, May 8, 2024 1:00 PM - 2:00 PM Eastern Time (US & Canada) (UTC-04:00)

CISA is leading an effort to update the National Cyber Incident Response Plan (NCIRP) by the end of 2024, as directed in the 2023 National Cybersecurity Strategy, ". . . to ensure that the breadth of our nation's capacity is effectively coordinated and leveraged in reducing the impact of cyber incidents." CISA is working hand in hand with our public and private sector partners including interagency partners, sector risk management agencies (SRMAs), and regulators to build upon the successes of the first inaugural plan and incorporate valuable lessons learned during the last seven years.

The NCIRP was first published in 2016 and serves as the nation's framework for coordinated response to significant cyber incidents. Since that time, the

cybersecurity threat landscape and national response ecosystem have changed dramatically, resulting in a growing need to update this foundational document.

Pre-register for the listening session if you want to attend, register now. When your registration is approved, you'll receive an invitation to join the webinar.

For more information on the NCIRP, visit the https://www.cisa.gov/resources-tools/resources/national-cyber-incident-response-plan-ncirp

Learn More Here

EDUCATION, TRAINING, AND WORKSHOPS

NPower Virtual Coaching Volunteer Opportunity

Interested in sharing your tech experience with those just starting their career journey? One of CISA's Cybersecurity Workforce Development and Training for Underserved Communities (CWD) cooperative agreement recipients, NPower, has developed a Coaching Session program for their trainees, where IT and tech career professionals volunteer to share how they have successfully navigated the tech landscape.

The program speaks to NPower's ultimate goal of empowering young adults from underserved communities to pursue careers in tech.

This volunteer coaching opportunity is available to CISA employees who are IT/Tech professionals and wish to share their experiences in alignment with CISA's goal to educate and train the future cybersecurity workforce. Coaching sessions are held via Zoom with 3 to 6 trainees, to offer them a comfortable environment to set goals and ask questions about their intended career path. Multiple, two-hour coaching sessions will be offered throughout April and May, meeting with students

in cohorts across the nation, from California to New York. There are many dates and times to choose from, including multiple evening sessions!

Learn More Here

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

The Interagency Security Committee (ISC) invites you to participate in its 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. The ISC invites you to participate in the following upcoming **Risk Management Process (RMP) and Facility Security Committee (FSC) Trainings** and **In-Person Trainings:**

- May 2, 2024 – Tampa, Florida
- May 14, 2024 – Oklahoma City National Memorial Museum, Oklahoma
- June 25, 2024 -- Charleston, South Carolina

Virtual, Instructor-Led Trainings:

- May 7-8, 2024 – 9 a.m. MT, Code 24NV-0166
- June 4-5, 2024 – 9 a.m. CT, Code 24NV-0167

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

May – 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)!

The **Federal Cyber Defense Skilling Academy** is excited to share that they have added THREE new Pathways to the program! These sessions discuss the work roles of a Cyber Defense Forensics Analyst (CDFA), Cyber Defense Incident Responder (CDIR), and Vulnerability Assessment Analyst (VAA). Additional information can be found in the Skilling Academy section below and on the Skilling Academy website. Applications for all three new Pathways are now open so be sure to sign up today!

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.

On June 15-17, CISA will host the **CYBER.ORG EdCon 2024** in Orlando, FL. This national conference is designed to inspire and empower novice and expert K-12 cybersecurity educators and counselors alike. Attendees will have the opportunity to learn ready-to-implement lessons from CYBER.ORG curriculum developers, explore no-cost resources from industry experts, and gain firsthand knowledge from K-12 educators who teach foundational and technical cybersecurity. To register and for additional information on conference agenda, stay, travel grants, and more, visit the EdCon website.

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 June 2024

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

Date	Course Code	Course	Location
05/06/2024-05/24/2024	401	**Industrial Control Systems Evaluation (401)**	Scheduled Online Training
05/06/2024-05/24/2024	300	**Industrial Control Systems Cybersecurity (300)**	Scheduled Online Training
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**
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
05/09/2024	General Public	**May Master Class – Introduction to Firewalls** May Master Class - Introduction to Firewalls | CyberWarrior.com
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 June 2024

Date	Time	Audience	Course	Location	Hours
On Demand	On Demand	8-12 Educators	**On Demand Workshop – Overview of Cyber Society for 8-12 Teachers:** This asynchronous workshop explores the features of CYBER.ORG's Cyber Society course! 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. Overview of Cyber Society for 8-12 Teachers | CYBER.org	Virtual	1.5 Hours
On Demand	On Demand	High School Educators	**On Demand Workshop – Overview of CYBER.ORG's Cybersecurity Course:** This asynchronous workshop is ideal for high school educators looking to implement cybersecurity and/or a cyber range! Overview of CYBER.ORG's Cybersecurity Course | CYBER.org	Virtual	1.5 Hours
On Demand	On Demand	Middle School Educators	**On Demand Workshop – Overview of Cybersecurity Basics for 6-8 Teachers:** This asynchronous workshop is ideal for middle school educators looking to build cybersecurity awareness in their classrooms.	Virtual	1.5 Hours

06/15/2024-06/17/2024	On Demand	K-12 Educators	Overview of Cybersecurity Basics for 6-8 Teachers | CYBER.org **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. CYBER.org EdCon| CYBER.org To learn more or sign up, visit: **https://cyber.org/events**	Orlando, FL	2 ½ Days

Federal Cyber Defense Skilling Academy: The Federal Cyber Defense Skilling Academy provides its students an opportunity to focus on professional growth through an intense, full-time, three-month accelerated training program. Students will have the opportunity to temporarily step away from their current role while they participate in the program. All full-time federal employees, in any job series and any grade or grade equivalent for non-General Schedule (GS) employees, are eligible to apply to CISA's Federal Cyber Defense Skilling Academy. Government contractors are not permitted to participate.

Below are the Skilling Academy session dates for FY24:

Skilling Academy Session Dates for FY24

Session	Session Start/End Date	Applications Open	Applications Close
Cyber Defense Analyst (CDA) - 13 and 14	06/03/2024 – 09/17/2024	03/25/2024	05/08/2024
Vulnerability Assessment Analyst (VAA)	06/17/2024 – 9/16/2024	01/31/2024	05/10/2024

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

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 June 2024

Date	Course Code	Registration Opens	Course	Hours
05/07/2024	CDM142	04/08/2024	**Asset Management with the CDM Agency Dashboard**	4
05/16/2024	CDM143	04/16/2024	**Vulnerability Management with the CDM Agency Dashboard**	4
05/21/2024-05/22/2024	CDM111	04/22/2024	**Analyzing Cyber Risk with the CDM Agency Dashboard (in person)**	14
05/30/2024	CDM201	04/30/2024	**Identity and Access Management within the CDM Agency Dashboard**	4
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

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.

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.*