September 2023 Issue

In this Edition:

Report a Cyber Incident

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.

Contact Us: Central@CISA.dhs.gov

Announcements, Opportunities and Resources

September is National Preparedness Month

National Preparedness Month is an observance each September to raise awareness about the importance of preparing for disasters and emergencies that could happen at any time. This year's theme is "Preparing for Older Adults."

The Ready Campaign's 2023 National Preparedness Month campaign will focus on preparing older adults for disaster, specifically older adults from communities that are disproportionally impacted by the all-hazard events, which continue to threaten the nation.

We know older adults can face greater risks when it comes to the multitude of extreme weather events and emergencies we now face, especially if they are living alone, are low-income, have a disability, or live in rural areas.

Emergency managers and all those who work with and support older adult communities to access the new webpage available in English and Spanish languages at Ready.gov/older-adults and Ready.gov/es/adultos-mayores for initial messaging, graphics and resources.

The Cybersecurity and Infrastructure Security Agency (CISA) recommends users and administrators use this month as an opportunity to assess cybersecurity preparedness for cyber-related events, such as identity theft, ransomware infection, or a data breach.

Learn more about preparing for a natural disaster or general emergency at Ready.gov/September. See Ready.gov/Cybersecurity

Learn More Here

Extended! SAFECOM Nationwide Survey Open until September 29th

Calling all Public Safety agencies to take the SAFECOM Nationwide Survey (SNS)! Agencies at all levels of government have the opportunity to participate in the SNS and in turn, drive key funding, policy, and programmatic decisions that will shape the future of emergency communications. The survey takes approximately 30 minutes to complete and will remain open through September 29, 2023.

Take Survey Here

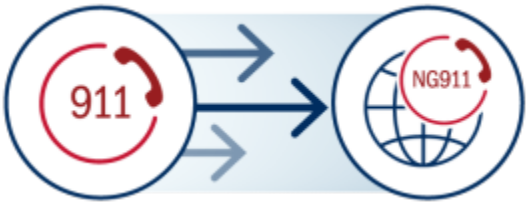
SAFECOM Releases Updated Introductory Presentation

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.

Learn More Here

CISA to Host Cyber Resilient 911 Symposiums



CISA's Cyber Resilient 911 (CR911) program is an initiative dedicated to assisting Emergency Communications Centers (ECCs) at federal, state, local, tribal, and territorial (FSLTT) levels in addressing operational cybersecurity challenges. As ECCs transition from legacy technology and systems to Next Generation 911 (NG911), they are exposed to a range of potential cybersecurity risks. Guided by the needs of 911 stakeholders, CISA is hosting four interactive regional symposiums across the United States through 2024. These symposiums inform the 911 community on cyber threats, available tools, frameworks, and solutions. Supported by the program's other legislated partners – FCC, NHTSA, and NTIA – the first symposium is scheduled for September 2023 in the Northeast Region, covering Regions 1, 2, and 3. The second symposium will be held in the Southeast Region (encompassing Regions 4 and 6) in the 2nd quarter of FY2024. The Western Region (including Regions 8, 9, and 10) and the Central Region (Regions 5 and 7) will host subsequent symposiums during the first half of CY2024. For more information, contact CR911@cisa.dhs.gov.

Learn More Here

Emergency Communications Policy and Planning

The Department of Homeland Security (DHS) Emergency Communications Division (ECD) supports the advancement of interoperable communications and the adoption of broadband technologies through the development and implementation of strategic planning and national policy and issuance of stakeholder guidance. ECD develops guidance on emergency communications grant programs, oversees the development and implementation of the National Emergency Communications Plan (NECP), establishes criteria for Statewide Communications Interoperability Plans (SCIPs), and develops policy strategies and policy recommendations for the use of land mobile radio (LMR), broadband and other emergency communications

technologies by the public safety community. ECD also conducts assessments of the national security and emergency preparedness communications capabilities of federal, state, local, tribal, and territorial public safety agencies.

Learn More Here

Cross-Sector Cybersecurity Performance Goals

A common set of protections that all critical infrastructure entities - from large to small - should implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques.

CISA's Cybersecurity Performance Goals (CPGs) are a subset of cybersecurity practices, selected through a thorough process of industry, government, and expert consultation, aimed at meaningfully reducing risks to both critical infrastructure operations and the American people. These voluntary CPGs strive to help small- and medium-sized organizations kickstart their cybersecurity efforts by prioritizing investment in a limited number of essential actions with high-impact security outcomes.

The CPGs are intended to be:

- A baseline set of cybersecurity practices broadly applicable across critical infrastructure with known risk-reduction value.
- A benchmark for critical infrastructure operators to measure and improve their cybersecurity maturity.
- A combination of recommended practices for information technology (IT) and operational technology (OT) owners, including a prioritized set of security practices.
- Unique from other control frameworks as they consider not only the practices that address risk to individual entities, but also the aggregate risk to the nation.

Now that the cross-sector CPGs have been published, CISA is working with Sector Risk Management Agencies (SRMAs) to directly engage with each critical infrastructure sector to develop Sector-Specific Goals (SSGs). In most instances,

these goals will likely consist of either new, unique additional goals with direct applicability to a given sector, or, materials to assist sector constituents with effective implementation of the existing cross-sector CPGs

To achieve its sector-specific goals development aims, CISA intends to actively engage with sector stakeholders, including holding multiple development workshops. While Sector Coordinating Councils (SCCs) will be one conduit for part of this outreach, CISA is committed to working closely with SRMAs to ensure that development of all sector-specific materials is done in an open and collaborative fashion, that includes participation from stakeholders of varying size and perspective.

More information on the sector-specific goals will be provided as efforts progress. To learn more about Cybersecurity Performance Goals (CPGs), visit CISA.gov.

Learn More Here

National Risk Management Center (NRMC)

NRMC provides critical analytical support to CISA's mission to understand, manage, and reduce risk to the cyber and physical infrastructure Americans rely on every day. Our work enables CISA and other critical infrastructure partners to apply actionable analysis to the decisions and investments they make to manage risk.

Our critical infrastructure community faces a risk environment that is complex, evolving, and interconnected. NRMC uses analytic insights to identify risk mitigation opportunities that improve national security and resiliency. We recognize that this depends on meaningful, value-driven partnerships across critical infrastructure sectors, industries, and functions. We believe that an integrated, collaborative approach to cyber and physical risk mitigation results in a stronger nation. We are excited to serve as the Nation's center for cross-sector critical infrastructure risk analysis, and we are ready for the challenges ahead.

Top NRMC initiatives include 5G, election security, electromagnetic pulses, national critical functions, pipeline cybersecurity and more.

Learn More Here

ISC's RMP and FSC Training in Oklahoma City, OK

ISD Security Programs hosted the Risk Management Process (RMP) and Facility Security Committee Training (FSC) in Oklahoma City, Oklahoma on August 17 at the Oklahoma City Memorial and Museum. This half-day, instructor-led course provided an understanding of the Interagency Security Committee (ISC), its Risk Management Process and the roles and responsibilities of Federal Security Committees. The course is valuable for executives, managers and any personnel involved in making facility funding, leasing, security, or other risk management decisions.

Office for Bombing Prevention's Empowered Trainer Program Reached Milestone

The CISA Office for Bombing Prevention (OBP) achieved a major milestone on July 26, 2023, with the delivery of its 500th bombing prevention course through the OBP Empowered Trainer Program. The Las Vegas Fire and Rescue Bomb Squad delivered the Bombing Prevention Awareness course, which provided local security personnel and stakeholders an overview of improvised explosive devices (IEDs) and explosive effects, an introduction to the terrorist attack cycle, and response to suspicious behaviors and items. The course also addressed general bombing prevention measures for mitigating the impact of a bombing incident.

OBP established the Empowered Trainer Program to enhance the counter-IED (C-IED) capabilities of public and private stakeholders by equipping local trainers with the expertise to effectively deliver this training to their jurisdictions and organizations using accredited curriculum and learning management systems. OBP leverages these pre-certified trainers to deliver OBP training courses through a train-the-trainer model. Empowered Trainers come from federal agency, law enforcement, first responder, emergency management, and private sector security communities. These trainers are dedicated professionals providing safety and security in their communities and organizations.

For more information on OBP's Empowered Trainer Program, please visit us at Bombing Prevention Training | CISA or email us at OBPTraining@cisa.dhs.gov.

Learn More Here

2023 Chemical Security Summit Presentations

Select presentations from the 2023 Chemical Security Summit hosted on August 29-31, 2023, are now posted on the Chemical Security Summit webpage.

CHEMICAL SECURITY SUMMIT 2023

Learn More Here

Critical Manufacturing Sector Risk Management Agency

The Critical Manufacturing Sector comprises manufacturing that is crucial to the economic prosperity and continuity of the United States. Manufacturers in the Sector process raw materials and primary metals; produce engines, turbines, and power transmission equipment; produce electrical equipment and components; and manufacture cars, trucks, commercial ships, aircraft, rail cars, and their supporting components. Products made by these manufacturing industries are essential to many other critical infrastructure sectors, and a failure or disruption in the Critical

Manufacturing Sector could result in cascading disruptions to other critical infrastructure sectors in multiple regions. The Cybersecurity and Infrastructure Security Agency (CISA), which serves as the Critical Manufacturing Sector Risk Management Agency (SRMA), and sector partners collaboratively develop guidance, resources, and training that support the security and resilience of our Nation's prominent manufacturers.

Learn More Here

Region 2 Critical Manufacturing Sector Security Roundtable

The Critical Manufacturing (CM) Sector Management Team (SMT), in collaboration with CISA Region 2, will execute an in-person meeting of the Region 2 CM Sector Security Roundtable on September 27th. The event will be hosted by The Manufacturers Association of Central New York in Syracuse, New York. This Security Roundtable will gather Region 2 manufacturing stakeholders to facilitate information sharing, networking, and outreach, while addressing Region 2 risks related to cybersecurity, natural hazards, the impacts of local disasters, supply chain security, and physical security. Some agenda topics include and an FBI Threat Brief, Insider Threat Program, and Regional Security Panel.

Learn More Here

Region 6 Congressional Visit

U.S. Congressman Morgan Luttrell (TX-8) hosted a CISA Critical Infrastructure Roundtable in Conroe, Texas on Aug. 23. Cybersecurity & Infrastructure Security Agency (CISA), Region 6 Regional Director Harvey Perriott participated, along with CISA Region 6 Protective Security Advisors, Cybersecurity Advisors and Chemical Security Inspectors. For more information, contact CISA Region 6 at CISARegion6@cisa.dhs.gov.

Learn More Here

Region 8 Critical Manufacturing Sector Security Roundtable

Manufacturing partners from Region 8 (Colorado, Montana, North Dakota, South Dakota, Utah, and Wyoming) are invited to join the 2023 Critical Manufacturing Sector Security Roundtable in Colorado Springs, CO on September 12th, 2023.

The roundtable will bring together manufacturing partners to address regional threats and risks related to cybersecurity, natural hazards, and supply chain security that impact manufacturing resiliency. This unique event is an opportunity for outreach, to share information, and network with other sector partners. In addition to a regional panel discussion, the event will address topics related to:

- Threats to the Critical Manufacturing Sector
- Critical Manufacturing and the importance to our Nation's security
- Critical Mineral Supply Chains

View more details and register here: Eventbrite Registration

For more information about Critical Manufacturing Sector resources email CISA Region 8 at CISARegion8Outreach@cisa.dhs.gov.

Learn More Here

Region 9 Critical Manufacturing Sector Security Roundtable

The Critical Manufacturing (CM) Sector Management Team (SMT), with CISA Region 9, executed an in-person meeting of the Region 9 CM Sector Security Roundtable on July 11th. The event was hosted by CM Sector Coordinating Council (SCC) partner Panasonic Energy of North America (PENA) at the Gigafactory, a 5.4 million square-foot manufacturing facility in Sparks, Nevada. Following a tour of the facility, the meeting opened with remarks from CISA's Region 9 Supervisory Cybersecurity Advisor and PENA's Business Continuity Lead. DHS's Office of Intelligence & Analysis Counterterrorism Center provided a threat briefing entitled Homeland Counterterrorism Threats, and the CM SMT delivered an overview of the sector, the Sector Risk Management Agency (SRMA) role, and programs and resources. The Protective Security Advisor (PSA) for northern Nevada and the Cybersecurity State Coordinator for Arizona gave an overview of both physical security and cybersecurity resources. The meeting also included two presentations, one addressing drones and their prevalent security issues, and the other exploring artificial intelligence's rapid evolution and its security impact. Attendees provided positive feedback, exchanged contact information, showed interest in joining the CM SCC, and collected meeting resources, like the Pandemic Planning Guide. The next Region 9 Roundtable is scheduled for 2024.

Learn More Here

Cyber Defense Education and Training (CDET) Offerings for September 2023

Highlights: What You Want to Know

Incident Response (IR) and Continuous Diagnostics and Mitigation (CDM) program trainings are now offered on Webex by Cisco rather than Adobe Connect, and GovDelivery will be used for all training-related announcements. In addition, the following changes have been made to improve your IR and CDM training experiences:

- Training courses will now be featured directly on the IR and CDM training web pages, rather than having to use the course catalog on the CISA website.
- Those on the current email distribution list will be copied over to the new platform, where subscriptions can be self-managed.

- Invitations to register for training events will be sent from Cyber Insights (CyberInsights@messages.cisa.gov) via GovDelivery.

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.

In August and September, 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. For awareness, this training series' meeting platform changed in mid-July. See the Cyber Training Bulletin Highlights above for more information on the platform change.

IR Training Events through September 2023

Date	Course Code	Registration Opens	Course	Hours
09/06/2023	IR105	08/07/2023	**Preventing Web and Email Server Attacks**	1
09/12/2023	IR209	08/14/2023	**Defending Against Ransomware Attacks**	4
09/21/2023	IR206	08/21/2023	**Preventing DNS Infrastructure Tampering**	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 September 2023

Date	Course Code	Course	Location
09/04/2023-09/22/2023	401v	**Industrial Control Systems Evaluation (401v)**	Scheduled Online Training
09/04/2023-09/22/2023	301v	**Industrial Control Systems Cybersecurity (301v)**	Scheduled Online Training
09/11/2023-09/14/2023	301L	**Industrial Control Systems Cybersecurity Training – In-Person 4 Days**	IN-PERSON TRAINING (4 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

09/14/2023	General Public	**September Master Class – Incident Response** September Master Class | CyberWarrior.com
10/12/2023	General Public	**October Master Class – Generative AI** October Master Class | CyberWarrior.com
11/16/2023	General Public	**November Master Class – Pentesting** November Master Class | CyberWarrior.com
12/14/2023	General Public	**December Master Class – Cloud Security** December Master Class | 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) and CYBER.ORG: 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 September 2023

Date	Audience	Course
09/01/2023-08/31/2024	K-8 Educators	**K-8 Cybersecurity Teachers Cohort, 2023-2024 School Year:** Are you a K-8 educator teaching cybersecurity in a classroom this 2023-2024 school year? Come exchange ideas with other teachers across the U.S.! K-8 Cybersecurity Teachers Cohort 2023-2024 | CYBER.org
09/01/2023-08/31/2023	High School Educators	**High School Cybersecurity Teachers Cohort, 2023-2024 School Year:** Are you an educator teaching cybersecurity in a high school classroom this 2023-2024 school year? Come exchange ideas with fellow U.S. educators!

09/01/2023-08/31/2023	K-12 Educators	High School Cybersecurity Teachers Cohort 2023-2024 | CYBER.org **CYBER.ORG Range Teachers Cohort, 2023-2024 School Year:** Are you an educator using the Cyber Range during the 2023-2024 school year? Come exchange ideas with fellow U.S. educators doing the same! CYBER.ORG Range Teachers Cohort 2023-2024 | 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 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).

All courses will be taught using the latest version of the CDM Dashboard (ES-5) using a virtual training range. Beginning in late August, the CDM Dashboard course material will be updated to reflect version ES-6 of the CDM Dashboard. The newest offering is the CDM220 and CDM320 Federal Mandates and BOD 22-01 & 23-01 Reporting courses, which will focus on the newest version ES-6 of the CDM Dashboard. For awareness, this training series' meeting platform changed to Webex Webinar in mid-July. See the Cyber Training Bulletin Highlights above for more information on the platform change.

CDM Training Events through September 2023

Date	Course Code	Registration Opens	Course	Hours
09/07/2023	CDM203	08/07/2023	**Systems Security Analyst**	4
09/13/2023	CDM111	08/14/2023	**Analyzing Cyber Risk**	8
09/14/2023	CDM111	08/14/2023	**Analyzing Cyber Risk**	8
09/19/2023	CDM220	08/21/2023	**CDM and Federal Mandates – How to use the CDM Dashboard to enable BOD 22-01 Reporting**	4

09/28/2023	CDM143	08/28/2023	**Vulnerability Management using the CDM Agency Dashboard** 4

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

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

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

Leran 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, please visit the *CISA Community Bulletin Archive.*