CISA COMMUNITY BULLETIN

April 2024 Issue

SECURE OUR WORLD

In this edition:

- Information Exchange
  - Secure Our World Resources
  - New Election Security Fact Sheet
  - Find Resources to Create a Safer School
  - CISA Shares Video on Violence Prevention Through De-escalation
  - Change Healthcare Cyber Incident Information
  - CISA OBP Launches Comprehensive Bomb Threat Guide
  - New ChemLock Resources
- Education and Training and Workshops
  - Upcoming Interagency Security Committee Risk Management Process & Facility Security Committee Trainings
  - Quarterly ChemLock Trainings
  - Join the Federal Cyber Defense Skilling Academy

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**

Learn More Here

ANNOUNCEMENTS

U.S. and International Partners Publish Cybersecurity Advisories on People's Republic of China State-Sponsored Hacking of U.S. Critical Infrastructure

JOINT CYBERSECURITY ADVISORY:
PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure

CISA in partnership with U.S. and international government agencies published a Joint Cybersecurity Advisory (CSA) on malicious activity by the People's Republic of China (PRC) state-sponsored cyber actor, known as Volt Typhoon, to compromise critical infrastructure and associated actions that should be urgently undertaken by all organizations.

CISA and its U.S. Government partners have confirmed that PRC state-sponsored cyber actors have compromised entities across critical infrastructure sectors, including communications, energy, transportation, and water, in the United States and its territories. The data, gathered by CISA and its U.S. Government partners, suggests the PRC is preparing for destructive cyber-attacks, posing a threat to American's safety and military readiness in the event of a major crisis or conflict with the United States.

In addition to the joint Cybersecurity Advisory, CISA and our partners also released complementary Joint Guidance to assist all organizations in effectively detecting and hunting for sophisticated techniques used by actors such as Volt Typhoon, known as "living off the land." In recent years, there has been a strategic shift in PRC cyber threats activity from espionage to preparing for disruptive cyber-attacks against U.S. critical infrastructure. PRC cyber actors employ "living off the land" techniques to blend in with normal system and network activities, evade detection by network defenses, and minimize activity captured in common logging configurations.

The joint CSA is based primarily on technical insights gleaned from CISA and industry response activities at victim organizations within the United States, primarily in communications, energy, transportation, and water and wastewater sectors. Our complementary Joint Guidance is derived from those insights as well as previously published products, red team assessments, and industry partners.

For more information, visit People's Republic of China Cyber Threat.

Learn More Here

Homeland Security Grant Program (HSGP) Supports Homeland Security Information Network (HSIN)

HSIN HOMELAND SECURITY INFORMATION NETWORK LOG IN

The Homeland Security Grant Program (HSGP) uses monies received through FEMA-funded awards towards the organization and support of HSIN user communities and information sharing activities. The list below includes a description of funding types and how these funds can be used to support participation in HSIN:

- HSIN Community Development
- Information Sharing and Operational Coordination Enhancement
- Training
- Limited Travel

HSIN is the Department of Homeland Security's official system for trusted information sharing of Sensitive But Unclassified information between federal, state, local, tribal, territorial, international and private sector partners. Organizations also use HSIN to plan for and communicate in real-time during major events, exercises and incidents. HSIN supports information sharing across multiple mission areas including, but not limited to, law enforcement, emergency management and emergency services, infrastructure protection, intelligence, and cybersecurity. tps://www.dhs.gov/homeland-security-information-network-hsinhttps://www.dhs.gov/homeland-security-information-network-hsin.

HSIN provides valuable services for secure and trusted information sharing among homeland security user communities to collaborate on issues and operations. HSIN is a distribution channel for homeland security reports and information, as well as the conduit for information for the National Operations Center. HSIN serves as a central access point for homeland security data, and is the virtual hub for the National Network of Fusion Centers

To learn how the HSGP uses monies received through FEMA-funded awards, please see the information available at Homeland Security Grant Program.

For more information about HSIN and HSGP guidance for HSIN, visit: HSIN HSGP Guidance | Homeland Security (dhs.gov)

Learn More Here

CISA Releases Industrial Control Systems Advisory

CISA released an Industrial Control Systems (ICS) advisory on February 22, 2024. These advisories provide timely information about current security issues, vulnerabilities, and exploits surrounding ICS.

- ICSA-24-053-01 Delta Electronics CNCSoft-B DOPSoft

CISA encourages users and administrators to review the newly released ICS advisory for technical details and mitigations.

This product is provided subject to this Notification and this Privacy & Use policy.

Learn More Here

CISA Launches New National Security Memorandum (NSM) Implementation Program Management Office (PMO)

The CISA Act of 2018 established the CISA Director as responsible for “coordinat[ing] a national effort to secure and protect against critical infrastructure risks.” In this role, the CISA Director leads, organizes, and coordinates cybersecurity and infrastructure security actions across Sector Risk Management Agencies (SRMAs) and the federal government, collaborating between government and industry, and convening and sharing information with State, Local, Tribal, and Territorial (SLTT) private-sector entities.

In addition, the Fiscal Year 2021 National Defense Authorization Act (FY21 NDAA) codified the roles of SRMAs and directed them to work with CISA to fulfill statutory requirements. Resultingly, CISA established the NSM Implementation PMO to organize internally, fulfill these requirements, and for coordinating SRMA activities. Housed in the Stakeholder Engagement Division (SED), the NSM Implementation PMO brings together CISA’s capabilities to support collaboration across Federal departments and agencies and meet the National Coordinator requirements in supporting SRMA responsibilities. Through the NSM Implementation PMO, CISA will leverage its statutory responsibility by working across the interagency to support SRMAs in carrying out their responsibilities outlined in FY21 NDAA.

The NSM Implementation PMO held its kick-off meeting on January 17, 2024.

Learn More Here

The Secure Cloud Business Applications (SCuBA) has a New Update

In case you missed it, on February 1, the Secure Cloud Business Applications (SCuBA) team released a new update for ScubaGear, and we are excited to have you check out all the new features available for download!

Developed by CISA, ScubaGear is an assessment tool that verifies a Microsoft 365 (M365) tenant's configuration conforms to the policies described in the Secure Cloud Business Applications (SCuBA) Security Configuration Baseline documents.

Learn More Here

PARTNERSHIPS

CISA, FBI, EAC and USPIS Release Election Mail Handling Procedures to Protect Against Hazardous Materials

CISA, Federal Bureau of Investigation (FBI), the U.S. Election Assistance Commission (EAC), and the United States Postal Inspection Service (USPIS) published *Election Mail Handling Procedures to Protect Against Hazardous Materials*. This resource helps officials understand safe mail handling procedures and provides guidance on responding to potential hazardous materials exposure.

Over the past two decades, U.S. government offices and employees have been the target of multiple incidents using letters containing hazardous materials, including suspicious letters mailed to election offices in California, Georgia, Nevada, Oregon, and Washington in 2023. Since mail is a key component of both standard office operations and mail balloting across the country, this guidance document provides information for election offices on how to identify and handle potentially suspicious mail and respond to potential hazardous materials exposure while handling suspicious mail. The guide also provides specific information on how to protect against the three hazardous powders of greatest concern, fentanyl, anthrax, and ricin, in addition to more routine mail hazards.

“CISA is proud to stand shoulder to shoulder with state and local election officials who face a complex threat environment,” **said CISA Director Jen Easterly**. “Today’s guidance on safe mail handling procedures will help election officials and others on the frontlines of our democracy take steps to protect themselves and their personnel from hazards sent through the mail. We will continue to work with our partners to ensure election officials have the information and resources they need to run a safe, secure and resilient election.”

To learn more, visit *Election Mail Handling Procedures to Protect Against Hazardous Materials* on CISA.gov.

To read the full news release article, visit CISA, FBI, EAC and USPIS Release Election Mail Handling Procedures to Protect Against Hazardous Materials | CISA

Learn More Here

CISA Meets with City Officials at the National League of Cities

CISA's staff met with a number of mayors and city officials as they participated in the National League of Cities Congressional Cities Conference the week of March 10. Partnerships Branch Chief Bob Nadeau spoke with the IT & Communications Committee about Secure Our World, and CISA priorities election security, AI, Secure by Design, threats posed by nation state actors, and how cities can engage with regional offices for products and services to better prepare them for cyber threats.

The Partnerships team also hosted a federal office hours table for city officials to connect with the team about information on HQ and regional resources. CISA Emergency Communications Division staff was also in attendance to share information on our communications products and resources available in the regions.

Learn More Here

CISA Region 10 Discusses Partnership Opportunities for Big City Emergency Managers

CISA Region 10 Regional Director Pat Massey spoke recently at the Big City Emergency Managers Winter meeting and engaged with emergency managers in important discussions on the current threat environment, CISA regional resources available to emergency managers, how CISA is engaging on Secure by Design principles with the IT industry and efforts to ensure election security, and protection of other critical infrastructure.

Emergency managers expressed concern to RD Massey and Strategic Relations Partnerships Branch Chief Bob Nadeau, about the growing use of AI, how cyber threats could impact critical infrastructure in their communities, escalation of global conflicts and how more threats are being sent to emergency management to deal with. RD Massey provided timely information on how BCEM and their members can work with regions to prepare for incidents and increase awareness and capabilities through training, products and resources.

Learn More Here

CISA to Speak at ICMA on Artificial Intelligence Opportunities and Risks

ICMA | conference

Local Government
REIMAGINED
CONFERENCES

As new and emerging technologies continue to grow, so do the opportunities for local governments to enhance services to their communities. Artificial Intelligence (AI) is one of those new technologies that offers new opportunities for innovation but also carries potential risks. The International City/County Management Association (ICMA) is a leading association of local government professionals dedicated to creating and supporting thriving communities and seeks to identify and speed the adoption of government practices to improve the lives of residents. ICMA invited CISA Strategic Technology Branch Chief Martin Stanley to speak to its members on April 10 at its Local Government Reimagined Conference, on how to leverage AI and discuss approaches to governing, mapping, measuring, and managing benefits and risks of AI to cities, towns and counties. Through this discussion local officials will learn to identify opportunities for AI adoption; make benefit-risk determinations for AI systems; and identify, measure, and manage AI risks. This is another way that CISA is supporting efforts by local governments to improve services while balancing the risks and challenges of new technologies.

Learn More Here

CISA Releases New Open-Source Resource: Principles for Package Repository Security

CISA partnered with the Open Source Security Foundation (OpenSSF) Securing Software Repositories Working Group to publish the Principles for Package Repository Security framework. Open source software is part of the foundation of the digital infrastructure we all rely upon and is widely used across the federal government and every critical infrastructure sector. As America's Cyber Defense Agency, CISA works to understand and reduce cyber threats to the federal government and critical infrastructure. Ensuring secure open source software is a critical part of this effort.

CISA's Open Source Software Security Roadmap establishes CISA's role in helping to secure open source software by aligning it with CISA's mission to identify and reduce risks to the federal government and critical infrastructure. In turn, CISA's efforts will contribute to the improved security of the broader open source ecosystem.

CISA has several ongoing initiatives around open source security, including our community-driven work around software bill of materials (SBOM). We also actively contribute by open sourcing much of our code via our "open-by-default" software development policy.

Learn More Here

CISA and FBI issue the Cybersecurity Guidance: Chinese-Manufactured UAS

CISA and the Federal Bureau of Investigation (FBI) released a joint Cybersecurity Guidance: Chinese-Manufactured UAS highlighting the significant threats of Chinese-manufactured UAS to critical infrastructure and U.S. national security.

This guidance serves as an update from CISA's Chinese Manufactured UAS Industry Alert released on May 20, 2019. CISA and the FBI encourage critical infrastructure organizations and federal, state, local, tribal, and territorial (FSLTT) partners to adopt the recommended cybersecurity guidance to enhance UAS cybersecurity posture.

Learn More Here

INFORMATION EXCHANGE

Secure Our World Resources

CISA's new enduring cybersecurity program, Secure Our World, encourages individuals and families; small and medium-sized businesses; and technology manufacturers, among others, to take simple steps to stay safe and secure online:

- Use strong passwords and a password manager
- Turn on multifactor authentication
- Recognize and report phishing
- Update software

To make it easy to get the word out, we released the first ever CISA Public Service Announcement and created a host of other easy to use resources, including animated videos about the four ways to stay safe online, tip sheets translated into various languages, and more!

Learn More Here

New Election Security Fact Sheet

CISA along with DHS, the Department of Justice, the Federal Bureau of Investigation, the United States Postal Inspection Service, and the Office of the Director of National Intelligence, released a new fact sheet to help state and local officials mitigate election security challenges as part of #Protect2024. This fact sheet provides state and local officials with vital information and resources to securely conduct election functions.

To report instances of voting rights violations, visit https://civilrights.justice.gov/

To report instances in which voting discrimination is taking place, visit www.ada.gov/file-a-complaint/

To search for an FBI office near you, visit www.fbi.gov/contact-us/field-offices/

To contact the FBI regarding threats or violence to voter personnel, call 1-800-CALL-FBI (225-5324) or visit tips.fbi.gov

Visit www.vote.gov and www.eac.gov for more information on the efforts being made for election security.

Learn More Here

Find Resources to Create a Safer School

Ensuring the safety of our schools lies at the heart of our CISA mission, and one of our most impactful endeavors in this regard is SchoolSafety.gov. This platform serves as a comprehensive repository of federal and state resources, programs, tools, and actionable recommendations on a range of school safety topics. CISA works alongside the U.S. Department of Education, U.S. Department of Health and Human Services, U.S. Department of Homeland Security, and U.S. Department of Justice to carry out the work of SchoolSafety.gov and make our schools safer and more supportive for students and educators.

Learn More Here

CISA Shares Video on Violence Prevention Through De-escalation

Violence Prevention through De-escalation Video
Share
Aggressive Personal Space Violation
Tightened Jaw
Clenched Fists
Watch on YouTube

CISA developed the **Violence Prevention Through De-escalation video** to help the critical infrastructure community and public gathering locations identify concerning behaviors and mitigate the risk from incidents of targeted violence. The video provides both security and non-security professionals with principles and techniques that can augment traditional security protocols. This conflict prevention approach can help individuals who observe activities and behaviors that may be considered suspicious, or indicative of potentially violent activity, reduce the risk of a potentially volatile situation.

Learn More Here

Change Healthcare Cyber Incident Information

The Health Information Sharing and Analysis Center (H-ISAC) Report was released following the Change Healthcare Cyber Incident:

https://h-isac.org/change-healthcare-optum-network-connectivity-and-additional-recommendations/

The URL provides background information on the incident and details about the Indicators of Compromise (IOCs) involved.

Leran More Here

CISA OBP Launches Comprehensive Bomb Threat Guide

BOMB THREAT GUIDE

CISA OBP's new Bomb Threat Guide

As the threat landscape evolves, security measures must respond in kind to address it. The recently published CISA Office for Bombing Prevention (OBP) Bomb Threat Guide was developed to help decision makers respond to bomb threats in an orderly and controlled manner.

When it comes to bomb threats, having a clear, specific and well-developed plan can save lives, protect critical infrastructure, and reduce the financial impact. Each bomb threat is unique and requires rapid evaluation to mitigate the immediate impact and manage in accordance with site needs. CISA OBP recommends owners and operators periodically review bomb threat guidance (including this product) and collaborate with first responders to establish and rehearse a bomb threat management plan that addresses each risk level appropriate for their specific site location.

Highlights from the Bomb Threat Guide include:

- Planning and preparation information
- Threat assessments
- Response options
- Suspicious items recognition

- Additional resources and training opportunities

Learn More Here

New ChemLock Resources

CISA's ChemLock program recently released several new products: three customizable templates that facilities and organizations can use as part of developing and implementing a facility security plan and two new resource flyers.

CHEM LOCK

cisa.gov/chemlock

- ChemLock: Chemical Inventory Template – This document serves as a template for maintaining an accurate inventory of the location, quantities, and physical states of chemicals at your facility.
- ChemLock: Personnel Background Checks Policy Template – This document includes background checks that facilities can consider conducting for personnel and serves as a template for a personnel background checks policy.
- ChemLock: Security Organization Roles and Responsibilities Template – This document includes a listing of security roles and responsibilities. It serves as a template to assist your facility in developing and maintaining a security organization.
- ChemLock On-Site Assessments and Assistance Flyer – This flyer advises facilities on the various levels of the ChemLock On-Site Assessment and Assistance services and how those levels can help to enhance a facility's security posture in a way that works for their business model.
- ChemLock Exercises Flyer – This flyer details how both the ChemLock customized, tailored chemical security exercises and CISA facilitated exercises can help facilities test their response and security plans in a wide range of scenarios.

For more information on how to develop a facility security plan, see the ChemLock Security Plan webpage or contact the ChemLock team at ChemLock@cisa.dhs.gov.

Learn More Here

EDUCATION, TRAINING, AND WORKSHOPS

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

The Interagency Security Committee (ISC) invites you to participate in its award winning Risk Management Process (RMP) and Facility Security Committee (FSC) Training. This training provides an understanding of the ISC, the ISC Risk Management Process Standard (RMP Standard), and the roles and responsibilities of Facility Security Committees (FSC). The course fulfills the necessary training requirements for FSC membership and is valuable for executives; managers; and personnel involved in making facility funding, leasing, security, or other risk management decisions. Participants will receive continuing education units through the International Association for Continuing Education and Training upon completion of the course. The ISC offers the training at no cost to participants.

The schedule for upcoming in-person and virtual trainings is below.

In-Person Trainings:

- April 2, 2024 – Arlington, Virginia at 8 a.m. ET
- April 23, 2024 – Beaufort, North Carolina at 8 a.m. ET
- May 2, 2024 – Tampa, Florida at 8 a.m. ET
- June 25, 2024 – Charleston, South Carolina at 8 a.m. ET
- August 15, 2024 – Atlanta, Georgia at 8 a.m. ET

Virtual, Instructor-Led Trainings:

- April 9-10, 2024 – 9 a.m. PT, Code 24NV-0165
- May 7-8 – 9 a.m. MT, Code 24NV-0166
- June 4-5 – 9 a.m. CT, Code 24NV-0167
- July 16-17 – 9 a.m. ET, Code 24NV-0168
- September 10-11 – 9 a.m. CT, Code 24NV-0169

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

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.

This course runs 1-2 hours in length and is appropriate for all personnel regardless of their level of involvement with dangerous chemicals.

- Register for April 8, 2024 – Noon-2 pm ET
- Register for July 11, 2024 – 1-3 pm ET
- Register for October 7, 2024 – 11 am-1 pm ET

ChemLock: Secure Your Chemicals Security Planning

This course walks through how to create a tailored, scalable security plan that meets the business model and unique circumstances of a facility. Participants will learn the key elements of a chemical security plan and benefit from examples, lessons learned, and best practices.

This course runs 2-3 hours in length and is designed to help leadership, facility security personnel, and other applicable personnel understand, develop, and implement a facility security plan.

- Register for May 6, 2024 – Noon-3 pm ET
- Register for August 7, 2024 – 11 am-2 pm ET
- Register for November 7, 2024 – 1-4 pm ET

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

Learn More Here

Join the Federal Cyber Defense Skilling Academy

Join the Federal Cyber Defense Skilling Academy

CISA’s Federal Cyber Defense Skilling Academy was launched on January 31 and provides students an opportunity to focus on professional growth through an intense, full-time, three-month accelerated training program. Those looking to join the cybersecurity community or learn cybersecurity skills are encouraged to apply for the Skilling Academy.

Applications will be accepted for Cohorts 11 & 12 until 4/9, so don’t miss out on your chance to learn the skills of a Cyber Defense Analyst! The Skilling Academy is open to federal employees only. Apply now here.

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.*

SECURE OUR WORLD