CISA Community Bulletin - August 16, 2021

CISA Launches New Joint Cyber Defense Collaborative

CISA announced the standup of the Joint Cyber Defense Collaborative (JCDC) on August 5th with the goal of driving down risk before an incident happens and unifying defensive actions should an incident occur. The JCDC is a new agency effort to lead the development of cyber defense operations plans, and facilitate execution of those plans in coordination with partners from the federal interagency, private sector, and state, local, tribal, and territorial (SLTT) government stakeholders.

Specifically, the JCDC will:

- Design and implement comprehensive, whole-of-nation cyber defense plans to address risks and facilitate coordinated action;
- Share insight to shape joint understanding of challenges and opportunities for cyber defense;
- Implement coordinated defensive cyber operations to prevent and reduce impacts of cyber intrusions; and
- Support joint exercises to improve cyber defense operations.

The initial industry partners that are participating in the JCDC include Amazon Web Services, AT&T, CrowdStrike, FireEye Mandiant, Google Cloud, Lumen, Microsoft, Palo Alto Networks, and Verizon. Government partners include the Department of Defense, U.S. Cyber Command, the National Security Agency, the Department of Justice, the Federal Bureau of Investigation and the Office of the Director of National Intelligence, with Sector Risk Management Agencies joining the effort moving forward.

With these extraordinarily capable partners, CISA's initial focus will be on efforts to combat ransomware and developing a planning framework to coordinate incidents affecting cloud service providers.

The JCDC will strive to include private sector and SLTT partners from across sectors as focus areas expand.

Learn More About JCDC Here

Alerts & Announcements

This October is National Cybersecurity Awareness Month

This October, individuals and organizations alike can #BeCyberSmart by using CISA and NCSA Cybersecurity Awareness Month products to create their own cybersecurity awareness campaigns. To help interested parties create effective campaigns, CISA and NCSA have created four weekly themes to focus on during Cybersecurity Awareness Month:

Week 1: Be Cyber Smart. The first week will explore cybersecurity fundamentals: how simple actions can help secure the digital lives of Americans and improve the security of smart and internet-connected devices, and how other fundamentals can help reduce cyber risks.

Week 2: Fight the Phish! The second week will focus on how individuals can spot potential phishing attempts—which often lead to ransomware vulnerabilities. This week will focus on how to help reduce the chances of falling victim to phishing attacks.

Week 3: Explore. Experience. Share. During week three, CISA and NCSA will join the National Initiative for Cybersecurity Education (NICE) to celebrate Cybersecurity Career Awareness Week. This week will illustrate how cybersecurity professionals play a vital role in global security and call attention to their contributions and innovations. It will also showcase how building a global cybersecurity workforce enhances each nation's security and promotes economic prosperity.

Week 4: Cybersecurity First. The final week will examine how what is done today can affect the future of personal, consumer, and business cybersecurity. Cybersecurity is increasingly becoming a consideration in how Americans work, learn, and play. This week emphasizes how cybersecurity is a year-round effort and should be a top consideration in the creation or purchase of new devices and connected services.
Cybersecurity and physical security have never been more closely linked to the Nation's security.

To learn how to help your communities and companies protect themselves, visit cisa.gov/cybersecurity-awareness-month.

Learn More About CSAM Here

CISA Announces Renewal of the Information and Communications Technology Supply Chain Risk Management Task Force

On August 2, CISA announced the two-year extension of the Information and Communications Technology (ICT) Supply Chain Risk Management (SCRM) Task Force to July 31, 2023. The Task Force, chaired by CISA and the IT and Communications Sector Coordinating Councils, is the premier public-private partnership for managing risks to the global ICT supply chain.

Under the newly signed Charter, the Task Force will continue and conclude ongoing efforts such as the release of two products. This includes a report focused on liability protections for the private sector when sharing supply chain risk information, and a guide that will help small and medium-sized businesses better understand and manage their ICT SCRM needs to mitigate the effects in the event of a cyber incident. The Task Force will also continue to build partnerships, develop new resources, and collectively enhance ICT supply chain resilience.

Learn More About ICT SCRM Here

CISA Hosts Virtual Industry Day

The U.S. Department of Homeland Security (DHS) and CISA hosted a virtual Industry Day on August 05, 2021.

CISA is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future. The threats the Nation faces—digital and physical, man-made, technological, and natural—are more complex, and the threat actors more diverse, than at any point in history.

CISA is at the heart of mobilizing a collective defense as it leads the Nation's efforts to understand and manage risk to our critical infrastructure. CISA's partners in this mission span the public and private sectors. The agency provides programs and services driven by its comprehensive understanding of the risk environment and the corresponding needs identified by its stakeholders.

CISA seeks to help organizations better manage risk and increase resilience using all available resources, whether provided by the Federal Government, commercial vendors, or their own capabilities.

In its ongoing efforts to engage closely with industry, CISA's Industry Day provided insight into CISA's current and future challenges, including presentations regarding:

- Software vulnerability collaboration

- Next Generation Network Priority Services
- Risk architecture and cyber risk reduction
- Supply Chain
- Public/private partnership efforts on 5G Security and Resilience
- Building long-term analytic capability
- Machine learning and large-scale analytics
- Zero-Trust Architecture (ZTA)
- Digital Twin

Learn More About New Director Here

CISA and Partners Hold Successful Tabletop the Vote Exercise

Last month, CISA in coordination with the National Association of Secretaries of State (NASS) and the National Association of State Election Directors (NASED), kicked off the fourth annual Tabletop the Vote. This is the Nation's largest election security exercise.

Over the course of three days, from July 13-15, more than 1,000 participants attended virtually to discuss lessons learned, share best practices, and identify ways to strengthen and secure voting processes.

Following the event, CISA Director Jen Easterly and members of the Election Infrastructure Government Coordinating Council (including CISA Assistant Director for the National Risk Management Center Bob Kolasky) issued a joint statement about the importance of this event in helping the election community strengthen their resilience.

Learn More About Tabletop the Vote Here

CISA Introduces New Funding Opportunity: Cybersecurity Workforce Development and Training Pilot for Underserved Communities

CISA is dedicated to filling the cybersecurity workforce gap of more than 400,000 vacancies across the Nation, and understands that equal access to professional development opportunities is an essential step to educate and train cyber professionals. CISA has announced funding of up to $2 million to organizations in underserved communities that create or enhance entry-level cybersecurity training and apprenticeship programs.

Applications for this funding opportunity must be submitted by Wednesday, August 25, 2021.

Learn More About the Pilot Here

Register Today for the 2021 Chemical Security Seminars

Register today for the virtual 2021 Chemical Security Seminars on December 1, 8, and 15, 2021, from 11 am to 3 pm ET (8 am to noon PT).

These seminars will feature important chemical security information for industry organizations, facility owners and operators, government officials, first responders, and law enforcement. Sessions will discuss and share the latest in chemical security best practices, including:

- The state of chemical security—updates for the program and ongoing voluntary chemical security efforts
- CISA leadership's priorities and vision
- Case studies from industry representatives
- A discussion on ransomware incidents and best practices
- A deep-dive into the topic, including best practices
- Chemical threat and economic espionage briefings
- Challenges encountered with chemical security during the COVID-19 pandemic
- The convergence of cyber and physical security

Please visit the Chemical Security Summit webpage for more information. There is no cost to attend this event. Registrants will receive the links to join virtually through Microsoft Teams closer to the date of the 2021 Seminars. For questions, please email the Chemical Security Seminars Team at ChemicalSummitReg@hq.dhs.gov.

Learn More About Chemical Security Here

Events

Partner Webinar: Detection and Response for Inside Threats

Partner Webinar:

A Blueprint for Small Business Cybersecurity

Partner Webinar: Cybersecurity Labeling Programs for Consumers

Join the National Institute of Standards and

Join the National Cybersecurity Alliance (NCSA) for a webinar that will focus on the detection and response strategies for insider threats.

Date: August 19, 2021

Time: 2:00 p.m. ET

Learn More Here

Join the Small Business Administration for a webinar on small businesses managing cybersecurity risks.

Date: August 19, 2021

Time: 12:00 p.m. ET

Learn More Here

Technology (NIST) for a webinar on challenges and practical approaches to initiating cybersecurity labeling efforts for Internet of Things devices and consumer software.

Date: September 14-15, 2021

Learn More Here

Featured Programs and Resources

Improving Emergency Communications Resiliency Through Redundancies

Redundancies in emergency communications allow public safety agencies to more effectively respond to emergency situations when problems arise, such as those caused by software or hardware issues, small incidents, natural and man made disasters, and other events. It is critical that public safety organizations have redundant systems and back up plans in place to ensure continuity of service to their communities.

The National Emergency Communications Plan (NECP) advocates that public safety organizations incorporate risk management strategies into their plans to maintain the continuity and recovery of critical communications.

This NECP spotlight looks at how three public safety agencies in Colorado, Maryland, and Ohio have implemented redundancies to prepare for potential failures of their primary emergency communications. To read more and stay current on the latest NECP Spotlights, please visit: cisa.gov/necp.

CISA Releases New Cyber Training Guide

CISA released a new downloadable Cybersecurity Workforce Training Guide on August 6 to assist future and current cybersecurity and IT professionals chart a successful career path. This guide is a one stop shop for information and resources to help professionals start and/or advance their careers in cybersecurity through training.

By using this guide, the cybersecurity professional will understand the applicable work roles, tasks, and knowledge, skills, and abilities that are the keys to success; and discover training and professional development opportunities to build skills and maximize potential. Also, they will find:

- Entry, Intermediate, and Advanced Level Cybersecurity Certifications
- Professional Development Trainings and Certification Prep Courses
- Experience and Hands On Opportunities
- Additional Cyber/IT Resources from across the federal government

The Cybersecurity Workforce Training Guide is a first step to help professionals chart a path to future success in the federal and SLTT cybersecurity communities.

To download and view the guide, please visit cisa.gov.

New ICT Supply Chain Resource and Library

CISA and the ICT SCRM Task Force released two new resources to enhance ICT supply chain resilience.

The **Threat Scenarios Report** provides practical, example based guidance on SCRM threat analysis that can be applied by acquisitions professionals to assess supply chain risks. To read/download the report, visit: CISA.gov/publication/ict scrm task force threat scenarios report

The **ICT Supply Chain Resource Library** is a non exhaustive list of free, voluntary resources and information (e.g., reports, papers, Executive Orders, etc.) on supply chain programs, rulemakings, and other activities from across the federal government. To explore the Library, visit: cisa.gov/ict supply chain library.

In Case You Missed It

Executive Order on Improving the Nation's Cybersecurity

On May 12, 2021, President Biden signed an Executive Order to improve the Nation's cybersecurity and protect federal government networks. CISA recently published a webpage on the Executive Order that includes resources like fact sheets, key points, and information about CISA's role in the Executive Order.

National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems

On July 28, 2021, President Biden signed a National Security Memorandum formally establishing an Industrial Control Systems Cybersecurity Initiative and directing the Secretary of Homeland Security and the Secretary of Commerce, acting through the Director of NIST, in collaboration with other agencies, to develop and issue cybersecurity performance goals for critical infrastructure.

Social Media

Help CISA spread the word about upcoming events and new resources by sharing the following posts via your social media channels. Thank you for your support!

- Check out the new cybersecurity workforce training guide from @CISAgov: https://www.cisa.gov/publication/cybersecurity-workforce-training-guide
- Want to learn more about supply chain risks? @CISAgov has the resources you need: https://www.cisa.gov/ict-supply-chain-library
- @CISAgov is dedicated to closing the cybersecurity workforce gap. Learn more about the new funding opportunity here: https://www.grants.gov/web/grants/view-opportunity.html?oppId=334707?