DEFEND TODAY, SECURE TOMORROW

CISA Community Bulletin - April 27, 2021

April is National Supply Chain Integrity Month

In partnership with the Office of the Director of National Intelligence (ODNI), the Department of Defense, and other government and industry partners, the Cybersecurity and Infrastructure Security Agency is promoting a call to action for a unified effort by organizations across the country to strengthen global supply chains.

Information and communications technology (ICT) products and services ensure the continued operation and functionality of U.S. critical infrastructure. However, recent software compromises and other events have shown the far-reaching consequences of these threats. When a supply chain incident occurs, everyone suffers: buyers, suppliers, and users.

As the Nation's risk advisor, CISA's top priorities include securing the global ICT supply chain from the evolving risks of tomorrow. Every week, CISA is promoting resources, tools, and information, including those developed by the public-private ICT SCRM Task Force.

CISA themes for each week include:

- Week 1: Building Collective Supply Chain Resilience
- Week 2: Assessing ICT Trustworthiness
- Week 3: Understanding Supply Chain Threat
- Week 4: Knowing the Essentials

Learn more on CISA's National Supply Chain Integrity Month webpage.

Learn More Here

Alerts & Announcements

CISA Issues Emergency Directive on Pulse Connect Secure

CISA has issued Emergency Directive (ED) 21-03, as well as Alert AA21-110A, to address the exploitation of vulnerabilities affecting Pulse Connect Secure (PCS) software. An attacker could exploit these vulnerabilities to gain persistent system access and take control of the enterprise network operating the vulnerable PCS device. These vulnerabilities are being exploited in the wild.

Specifically, ED 21-03 directs federal departments and agencies to run the Pulse Connect Secure Integrity Tool on all instances of PCS virtual and hardware appliances to determine whether any PCS files have been maliciously modified or added.

Although ED 21-03 applies to Federal Civilian Executive Branch departments and agencies, CISA strongly recommends state and local governments, the private sector, and others to run the Pulse Connect Secure Integrity Tool and review ED 21-03: Mitigate Pulse Connect Secure Product Vulnerabilities for additional mitigation recommendations.

Learn More Here

Joint Report Finds No Evidence that a Foreign Government Manipulated Any Election Results

On March 16, CISA issued a joint report with the Department of Homeland Security (DHS), Department of Justice, and Federal Bureau of Investigation on the impact of foreign governments and their agents on the security and integrity of the 2020 U.S. federal elections. The report includes unclassified findings and recommendations derived from a classified report submitted to the President in February.

Among its key findings, the report states, "we […] have no evidence that any foreign government-affiliated actor prevented voting, changed votes, or disrupted the ability to tally votes or to transmit election results in a timely manner; altered any technical aspect of the voting process; or otherwise compromised the integrity of voter registration information of any ballots cast during 2020 federal elections."

However, the agencies did identify "several incidents when Russian, Chinese, and Iranian government-affiliated actors materially impacted the security of networks associated with or pertaining to U.S. political organizations, candidates, and campaigns." The joint report was issued alongside a declassified Intelligence Community Assessment on foreign threats to the 2020 U.S. federal elections. The assessment documents election influence

campaigns orchestrated by Russia, Iran, and other countries, but finds “no indications that any foreign actor attempted to alter any technical aspect of the voting process in the 2020 U.S. elections.”

The reports demonstrate clearly that sophisticated, state-sponsored threat actors continue to engage in cyber and influence activity that can impact U.S. election infrastructure. The rationale behind the 2017 designation of election infrastructure as critical infrastructure – that state and local election officials should not be expected to combat sophisticated, state-sponsored threat actors alone – remains as true today as it did in the aftermath of Russian interference in 2016. CISA remains committed to advancing its vital mission to assist election officials and their private sector partners in securing and building resilience in U.S. election infrastructure.

Learn More Here

SAFECOM Publishes Updated Fact Sheet for Stakeholder Use

SAFECOM is a key CISA partner in driving advancements to emergency communications capabilities. It recently released an updated stakeholder resource to support organizations in navigating the evolving emergency communications ecosystem.

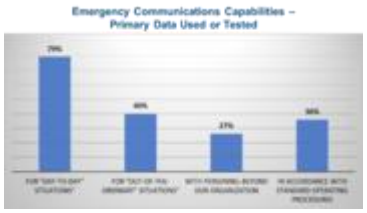
The new SAFECOM Fact Sheet emphasizes how SAFECOM is simultaneously addressing emerging issues, such as information sharing and cybersecurity, and continuing to support legacy public safety operations.

Learn More Here

CISA Supports Public Safety Concerns with Partner Webinar

On March 17, CISA partnered with the National Emergency Number Association (NENA) and National Association of State 911 Administrators (NASNA) to conduct its first Implementing the National Emergency Communications Plan (NECP) webinar of 2021. Nearly 300 participants attended to learn about the negative impacts of human factors on the public safety professional and what can be done to prevent them with training and exercises.

Participants joined from across all levels of government and varying public safety disciplines and included representatives from the Sam Manuel Band of Mission Indians; Alaska State Troopers; La Salle County, Illinois; Lowes Corporation; and the United States Department of Justice, to name a few.



The SAFECOM Nationwide Survey (SNS) found that 79 percent of the public safety community uses data. New technologies illustrate threats and hazard to public safety professionals through photos, videos, and live streaming. As a result, many of these critical employees suffer from information overload, additional stress, and trauma.

To obtain a copy of the slide deck, which includes a comprehensive list of resources, please send a request to necp@cisa.dhs.gov.

Learn More Here

Events

Webinar: Getting Smarter About K-12 Cybersecurity

CISA is co-hosting a webinar with the Regional Consortium Coordinating Council (RC3) and State, Local, Tribal, and Territorial Government Coordinating Council (SLTTGCC). Cybersecurity experts from industry and government will discuss how to protect school systems from DDoS attacks, ransomware, and cyber threats.

Date: April 28, 2021

Time: 2:00 p.m. ET

Learn More Here

Webinar: Federal Computer Week (FCW) Cloud Summit

CISA Chief Technology Officer Brian Gattoni is speaking at the 2021 FCW Cloud Summit. His panel will highlight how agencies can manage cloud migrations more effectively.

Date: April 28, 2021

Time: 9:00 a.m. ET

Learn More Here

Partner Webinar: Managing Cybersecurity Threats with the Data Assured Program

This webinar will equip your small businesses with foundational cybersecurity knowledge, based on the 5 central concepts of the National Institute of Standards and Technology (NIST) Cybersecurity Framework: Identify, Protect, Detect, Respond and Recover.

Date: May 6, 2021

Time: 1:00 p.m. ET

Learn More Here

Featured Programs and Resources

Combating Online Influence and Manipulation Webinar Recording Available Now

On February 25, 2021, CISA hosted the webinar Combating Online Influence and Manipulation as part of a series co-hosted by the RC3 and the SLTTGCC. This webinar explored methods for combating online interference, such as source checking online networks and link analysis. Experts joined from across government and industry to discuss deep source checking, use cases, and promoting awareness and truth-based narratives.

The webinar is published and available to view on CISA's Youtube channel. To see recordings from this and other past webinars, explore CISA's Past Events page.

CISA Provides Cyber Essentials Resources

The success of a business depends on cyber readiness but where to start?

CISA's Cyber Essentials is a leadership-driven starting point toward achieving the basics of organizational cyber readiness. The Cyber Essentials are a set of easy-to-adopt and easy-to-understand, community-endorsed cybersecurity practices. They are designed specifically to be used by leaders of small businesses without any cybersecurity expertise or technical background.

The Cyber Essentials use a holistic approach to tackling cybersecurity and address everything from employee behavior to systems configuration and the role of leaders. Moreover, they can be adapted to a wide range of business types and industries. Leaders shouldn't wait to start making their people, property and profits more secure online.

Download the Cyber Essentials Starter Kit today by visiting https://www.cisa.gov/publication/cyber-essentials-toolkits.

CISA CETAP Grant Highlights Importance of K-12 Cybersecurity Education

CISA's commitment to Defend Today, Secure Tomorrow begins by reaching students at a very young age. Through the Cybersecurity Education Training Assistance Program (CETAP) grant, CISA provides funds to CYBER.ORG, a nonprofit organization that develops and distributes free cybersecurity, STEM, and computer science curricula to K-12 educators across the United States.

Last summer, CYBER.ORG released a study outlining the results from a survey of over 900 U.S. educators that indicates there is uneven access to cybersecurity education, with lower levels in public schools, particularly in high poverty areas and communities that lack cybersecurity industry or universities that offer coursework on the subject (also known as cybersecurity deserts).

The study includes recommendations for K-12 educators to help develop the basic level of understanding they need to protect their own data privacy and security, and to improve the odds that students pursue cybersecurity careers. These recommendations include ensuring access to cybersecurity education in cybersecurity deserts, raising basic levels of knowledge about cybersecurity education, increasing the number of schools offering

cybersecurity education, enhancing educational offerings, and informing students about cybersecurity careers.

Read the full study on CYBER.org.

CISA Publishes FY21 Emergency Communications TA Planning Guide

CISA published the FY2021 Emergency Communications Technical Assistance (TA) Planning Guide (TA/SCIP Guide) to help public safety partners enhance their interoperable communications capabilities. CISA provides no-cost support to state, local, and tribal emergency responders and government officials through the delivery of training, tools, and onsite assistance to advance public safety interoperability. This year's TA/SCIP Guide includes several offerings designed to help public safety and government officials meet the challenges of the rapidly changing emergency communications ecosystem.

The TA/SCIP Guide follows the structure of the 2019 update to the National Emergency Communications Plan (NECP). The NECP establishes a vision for strengthening and enhancing emergency communications capabilities nationwide and shares a strategic plan for driving towards interoperability. The NECP establishes six strategic goals focused on the following: Governance and Leadership; Planning and Procedures; Training, Exercises, and Evaluation; Communications Coordination, Technology and Infrastructure; and Cybersecurity.

During FY2021, CISA will continue to expand and customize service offerings with a focus on supporting states and territories in the following areas:

- Alerts and warnings
- Communications unit planning and procedure
- Coordinated statewide governance (e.g. State Mapping Tool, Interoperability Communications Reference Guides, etc.)
- Cybersecurity education and awareness
- Encryption Planning and Usage
- Grant Funding for Emergency Communications
- Standard Operating Procedure (SOP) Review and Development
- Statewide Communication Interoperability Plan (SCIP) Workshop

To view the FY2021 TA/SCIP Guide please visit: https://www.cisa.gov/safecom/ictapscip-resources.

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!

- @CISAgov releases Joint Report Finding No Evidence that a Foreign Government Manipulated Any Election Results: https://www.cisa.gov/publication/cisa-2020-year-review

- Don't miss next week's K-12 Cybersecurity webinar. Sign up here: https://k12cybersecurity.eventbrite.com/

- April is National Supply Chain Integrity Month. Learn more here: https://www.cisa.gov/supply-chain-integrity-month #supplychain