CISA Community Bulletin - December 15, 2021

Best Cybersecurity Practices for the Holiday Season

The Cybersecurity and Infrastructure Security Agency (CISA) is urging everyone to stay cyber safe this holiday season. CISA and the Federal Bureau of Investigation issued a cybersecurity reminder for public and private sector organizations to remain vigilant and take appropriate precautions to reduce their risk of ransomware and other cyberattacks. Malicious cyber actors have often taken advantage of holidays and weekends to disrupt networks and systems belonging to organizations, businesses, and critical infrastructure.

Best practice recommendations in the alert include:

- Identify information technology security employees available during weekends and holidays.
- Implement multi-factor authentication for remote access and administrative accounts.
- Mandate strong passwords and ensure they are not reused across multiple accounts.

- Ensure the security of remote desktop protocol if they are used.
- Remind employees not to click on suspicious links.
- Review and update ransomware incident response and communication plans.

During this time of year, it is especially important to take proactive cybersecurity measures. Simple steps include:

- Check devices: Use strong passwords, update software, and turn on multi-factor authentication.
- Shop only through trusted sources: Think about how and where to make purchases online.
- Recognize phishing scams: Don't click unknown links or download attachments. Never provide password, personal or financial information in response to an unsolicited email.
- Use safe methods for purchases: Never provide financial information when using public Wi-Fi. Use a credit card instead of a debit card and check account statements frequently.

Learn More Here

Alerts & Announcements

CISA Releases Apache Log4j Vulnerability Guidance

Through the Joint Cyber Defense Collaborative, CISA and its partners are responding to active, widespread exploitation of a critical remote code execution vulnerability (CVE-2021-44228) in Apache's Log4j software library. Consumer and enterprise services and applications, as well as operational technology products, use Log4j. The specific versions affected are versions 2.0-beta9 to 2.14.1, known as "Log4Shell" and "Logjam." While Apache has released a security update, managers must actively implement the update.

CISA urges vendors and users to take the following actions:

- Identify internet-facing endpoints that use Log4j
- Ensure security operations center is actioning alerts on these devices
- Install a web application firewall with rules that automatically update

Learn More Here

CISA Webinar: DHS Blue Campaign

Every year, millions of men, women, and children are trafficked worldwide, including right here in the United States. Traffickers might use violence, manipulation, or false promises of well-paying jobs or romantic relationships to lure victims into trafficking situations. Hear the Blue Campaign team discuss tools and resources to combat trafficking in a webinar on Thursday, December 16, 2021, 1:00 – 2:30 p.m. ET. Registration is required. The event will be recorded and posted to HSIN for future viewing. For more information, contact CISA Region 8: CISARegion8@hq.dhs.gov.

Learn More Here

CISA Releases Updated CISA Services Catalog

CISA's Services Catalog "Catalog 2.0" is a centralized resource of information on services from all CISA mission areas. Catalog 2.0 provides information for federal, state, local, tribal and territorial governments; private industry; academia; non-governmental and non-profit organizations; as well as the public.

Catalog 2.0's interactive features enable users to request, share, and tag favorite capabilities, allowing them to quickly and seamlessly access information on services tailored to their needs. Catalog 2.0 is also mobile-friendly, allowing users to access the library while "on the go."

Learn More Here

CISA Launches New ChemLock Program

CISA has launched a new, voluntary chemical security initiative: ChemLock.

ChemLock offers facilities a series of scalable, tailored options for enhancing their chemical security posture. Facilities can apply the most effective combination of services and tools that meet their unique circumstances and business models.

CISA services and tools include:

- On-site assessments and assistance;
- Fact sheets, best practices, and guidance documents;
- Exercises and drills;
- Training courses;
- Cyber Security Evaluation Tool; and
- Active shooter resources.

To sign up for any of these ChemLock services and tools, visit the ChemLock webpage.

Learn More Here

2021 President's Cup Cybersecurity Competition Winners

CISA extends its congratulations to the winners of the just-concluded 2021 President's Cup Cybersecurity Competition. Established in 2019, the competition is a national cyber event that identifies, challenges, and rewards the best cybersecurity talent in the federal workforce. Take a look at the final round livestream on CISA's YouTube Channel, featuring commentary on the competitors' progress, remarks from government officials, a look at making the competition, and interviews from across the federal workforce.

More information about the 2022 President's Cup Cybersecurity Competition will be released in Spring 2022.

Learn More Here

2021 Chemical Security Seminars

CISA has concluded the 2021 Chemical Security Seminars, the signature industry event for chemical sector representatives. Hosted on December 1, 8, and 15, this year's seminars featured three days of events covering chemical and cybersecurity threats and countermeasures, and chemical security planning and preparedness.

Select presentations from the 2021 Chemical Security Seminars will be posted in the coming weeks on the Chemical Security Summit webpage. CISA thanks those who have contributed to and participated in the ongoing, collaborative efforts to enhance our Nation's chemical security.

Learn More Here

CISA Releases Request for Information (RFI) on Federal Network Protection

CISA and its partners released this RFI to help protect federal networks and the ".gov" domain enterprise from threats while strengthening cyber defenses. CISA requests information on email security capabilities and tools, including input from entities that have delivered similar solutions to the government or private sector. This information will assist in refining solution design, use cases, and functional requirements. Responses are due December 15, 2021.

Learn More Here

CISA Hosts Strategic Assessment Interviews

CISA’s Emergency Communications Preparedness Center (ECPC) will host interviews and events in preparation for its annual strategic assessment. The assessment, submitted to Congress, relates emergency responders' capability and coordination efforts to advance interoperable emergency communications. The ECPC will conduct department and agency interviews from now through January. The center will host a workshop to prepare its findings in March. ECPC encourages all public safety communications management experts to get involved.

Learn More Here

CISA Hosts Webinar on the Ransomware Threat to Emergency Communications

On October 26, CISA held a webinar entitled, “Addressing the Ransomware Threat to Emergency Communications” as part of its effort to implement the National Emergency Communications Plan (NECP). The NECP focuses on helping public safety organizations establish proactive measures to manage cybersecurity risks, including against the increasing threat of ransomware. The webinar offered case studies, resources, and guidance. For a copy of the slides, email necp@cisa.dhs.gov.

Learn More Here

Events

Partner Webinar: The NICE Framework and Building a Better Cybersecurity Workforce

Join the National Initiative for Cybersecurity Education (NICE) for a webinar on how using the NICE Framework can

Partner Webinar: Cybersecurity Basics for Remote Work

Join this Small Business Administration webinar to learn about best practices for cyber safety when working remotely.

Date: January 20, 2021

Partner Webinar: Data Privacy Day 2022

Join the National Cybersecurity Alliance and LinkedIn for a Data Privacy Day 2022 event. Experts from industry, government, academia and non-profit entities will help build an effective cybersecurity workforce.

Date: December 15, 2021

Time: 2:00 p.m. ET

Learn More Here

Time: 11:00 a.m. ET

Learn More Here

discuss the latest topics in data privacy.

Date: January 26, 2021

Time: 12:00 p.m. ET

Learn More Here

Featured Programs and Resources

CISA Releases Guidance for Public Safety Organizations

THE NECP
NECP SPOTLIGHT
Ensuring Interoperable Encrypted Communications
For more information, visit cisa.gov/necp

In support of National Emergency Communications Plan (NECP)'s guidance on risk management, the National Capital Region (NCR) created the "NCR Public Safety – Land Mobile Radio Strategic Interoperable Encryption Plan" to help public safety organizations balance the need for communications encryption while maintaining regional interoperability. The plan is part of the NECP Spotlights series of articles that demonstrate how the NECP guidance applies to real-world events.

To read this Spotlight and to stay updated on others, visit cisa.gov/publication/necp-spotlights

CISA Releases Guidance on 5G Cloud Cybersecurity

CISA published two fifth-generation (5G) cloud cybersecurity guides to help cloud providers and mobile network operators secure network resources in the 5G cloud.

Part I: Prevent and Detect Lateral Movement - Focuses on detecting malicious cyber actor activity in 5G clouds and preventing actors from leveraging the compromise of a single cloud resource to compromise the entire network.

Part II: Securely Isolate Network Resources - Ensures secure isolation among customer resources with an emphasis on securing the container stack that supports the running of virtual network functions.

For additional 5G resources, visit CISA.gov/5G.

CISA Releases 5G Educational Videos

INNOVATION & TRANSFORMATION
The Promise and the Reality of 5G Implementation

On November 30, CISA released a set of four educational videos to highlight the benefits and risks of 5G implementation. These videos are part of CISA’s plan to build national resilience through public awareness and engagement.

Topics covered include:

- CISA’s role in enhancing 5G security and implementation;
- Vulnerabilities and risks associated with 5G;
- Unique characteristics of 5G low band, mid band, and high band networks; and
- Use cases for how 5G transforms the user experience.

To view these videos and additional resources, visit www.cisa.gov/5g-library

CISA Holiday Shopping Webinar

The holiday season is a prime time for cyber threats. This webinar offers several awareness tips and defensive strategies, including using best practices for shopping online safely and securely, ways to avoid fraudulent credit card charges, how to protect your devices when shopping online, and best ways to outsmart scammers. Learn how to best protect yourself, your system, and others by accessing the Holiday Shopping webinar through the Homeland Security Information Network (HSIN): https://share.dhs.gov/r8-holiday-shopping/

CISA Releases White Paper on P25 Technologies

The Federal Partnership for Interoperable Communications (FPIC) has released the Emergency Alarm: Project 25 (P25) Inter-RF Subsystem Interface (ISSI) and Console Subsystem Interface (CSSI) Features and Functions paper.

This is the first in a new P25 series focused on specific ISSI/CSSI features and functions that provide life-saving communications capabilities to public safety. P25 system planners and administrators can advance their understanding of the technology and potential roadblocks using this paper. To learn more about P25, ISSI and CSSI, and the FPIC, visit cisa.gov/safecom/fpic or contact FPIC@cisa.dhs.gov

CISA & SAFECOM Release Interoperable Information Sharing Framework Report

The public safety community continues to integrate new technology into its processes. Yet the growing market of new platforms and solutions does not always address operational requirements, forcing trade-offs among interoperability, flexibility, security, and sustainability.

To alleviate these challenges, CISA, SAFECOM, and the National Council of Statewide Interoperability Coordinators delivered the Approach for Developing an Interoperable Information Sharing Framework (ISF) report. This report explains how to develop an ISF to guide the transition toward a common information exchange approach. Organizations can ensure their technology and communications ecosystem are more interoperable, enhancing first responder access to timely and relevant information. CISA continues to address challenges presented by rapid technology advancements through efforts such as the ISF to achieve real-time situational awareness.

For information about such programs, visit: cisa.gov/emergencycommunications, cisa.gov/safecom or cisa.gov/safecom/ncswic.

In Case You Missed It

- Federal Government Cybersecurity Incident and Vulnerability Response Playbooks
- NSA and CISA Publish Third Installment of 5G Cybersecurity Guidance

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!

- The @CISAgov Cybersecurity Advisory Committee has announced its first members. Find out more here: https://www.cisa.gov/csac-members
- Want to learn more about CISA Services? Check out @CISAgov's updated CISA Services Catalog: https://www.cisa.gov/publication/cisa-services-catalog
- @CISAgov encourages stakeholders to remain vigilant to ransomware and cyber threats during this holiday season. For more information, go to https://www.cisa.gov/news/2021/11/22/cisa-and-fbi-urge-organizations-remain-vigilant-ransomware-and-cyber-threats

To access past editions of this CISA Community Bulletin newsletter, please visit the *CISA Community Bulletin archive*