CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA
DEFEND TODAY, SECURE TOMORROW

CISA Community Bulletin - September 29, 2020

CISA Hosts Third Annual National Cybersecurity Summit

The Cybersecurity and Infrastructure Security Agency's (CISA) 3rd Annual National Cybersecurity Summit is underway! The Summit, which began September 16 and runs every Wednesday until October 7, has brought together stakeholders from around the country to a forum with presentations focused on emerging technologies, vulnerability management, incident response, risk mitigation, and other current cybersecurity topics. Attendees will have the opportunity to hear from Federal, state, and local agencies, as well as private sector organizations, as they highlight successes and opportunities for collective action.

The Summit is intended to be an inclusive event and will be particularly valuable for senior leaders, CISOs, general counsels, and policy experts at public and private sector organizations who have shown a commitment to advancing cybersecurity and infrastructure protection risk management discussions.

Each series has a different theme that focuses on CISA's mission to "Defend Today, Secure Tomorrow," with presentations from targeted leaders across government, academia, and industry.

This Year's Themes

- Sept 16: Key Cyber Insights
- Sept 23: Leading the Digital Transformation

- Sept 30: Diversity in Cybersecurity
- Oct 7: Defending our Democracy

Register and Watch Online

Learn more about how to register for this no-cost event and watch the sessions at https://www.CISA.gov/cybersummit2020.

Events

Partner Event: Cybersecurity Symposium for Smart Cities 2020

This annual cybersecurity symposium is an inclusive, virtual open forum to discuss the most pressing issues concerning Smart Cities with thought leaders in governments, industry, small businesses, academia, and nonprofits. The event is free.

Date: October 14-16, 2020

Time: 8:00 a.m. – 1 p.m. PT

Register Here

Partner Event: 2020 Small Business Cybersecurity Summit

Join this flash-talk format workshop for small- and medium-sized businesses. Each presentation is just 5 minutes, and the event kicks off with a live fireside chat on the state of small business cybersecurity.

Date: October 15, 2020

Time: 2:00 – 5:00 p.m. ET

Register Here

Webinar: Funding Your Emergency Communications Capabilities

CISA is hosting a National Emergency Communications Plan webinar to assist participants in identifying funding mechanisms to support emergency communications projects.

Date: October 21, 2020

Time: 1:00 p.m. ET

Learn More Here

Featured Programs and Resources

Webinar Recording Available: Disinformation in 2020

This month CISA co-hosted the webinar "Disinformation in 2020: Implications and Tools for Election Officials and the Critical Infrastructure Community" with the Regional Consortium Coordinating Council and the State, Local, Tribal, and Territorial Government Coordinating Council.

In preparation for the 2020 election season, experts across government, industry, and academia have been working diligently to develop a vibrant election security community and strengthen our Nation's cybersecurity and resilience posture.

Watch this webinar to learn more about the threat that disinformation poses, as well as tools to help election security and critical infrastructure stakeholders combat that threat -- including the Election Influence Operation Playbook for State and Local Election Officials, from Harvard's Defending Digital Democracy Project (D3P).

Watch the "Disinformation in 2020" Webinar

Cyber Career Pathways Tool Now Live

CISA is excited to announce the release of the Cyber Career Pathways Tool (CCPT). Please share this tool with individuals looking to start a career in cybersecurity or considering a change within the cyber field, as well as college students, managers, and workforce development specialists interested in the cyber ecosystem. This tool will help individuals identify, build, and navigate a potential cyber career pathway by increasing understanding of the knowledge, skills, and abilities needed to begin, transition, or advance a cyber career.

The CCPT presents a new and interactive way to explore work roles within the NICE Cybersecurity Workforce Framework. It depicts the cyber workforce as five distinct—yet complementary—skill communities. It also highlights core attributes among each of the 52 work roles and offers actionable insights for employers, professionals, and individuals considering a career in cyber.

Find this tool on the CISA National Initiative for Cybersecurity Careers and Studies website, as well as other tools and resources for current and future cybersecurity professionals. The CCPT was created and is maintained in partnership with the Interagency Federal Cyber Career Pathways Working Group, which is led by CISA, the Department of Defense, and the Department of Veterans Affairs.

Explore the Cyber Career Pathways Tool

CISA Launches Emergency Communications Tribal Website

CISA launched a webpage to promote the new Tribal Emergency Communications Program, which supports the sovereignty of federally recognized tribes and Alaska Native communities through strengthened public safety communications. CISA assists tribes with public safety operable/interoperable communications through consultative engagement, outreach, advocacy, technical assistance, access to information and resources, and inter- and intra-agency coordination.

Each tribe has unique cultures, capabilities, needs, and challenges, and CISA works individually with tribal communities to develop a cultural and technical understanding of each community and its emergency communications framework. CISA provides governance support by assessing and documenting current tribal emergency communications operations, resources, and challenges to tailor support directly to the tribal community. CISA also uses this information to develop resources and tools to support public safety communications at all levels of government and to advocate on behalf of tribal communities.

CISA's communications governance support helps tribal communities to:

- Establish and develop collaborative relationships across all levels of government.
- Identify opportunities to utilize CISA services, resources, and tools to enhance emergency communications capabilities through technical assistance, priority telecommunications services, and grant guidance.
- Communicate their current emergency management capabilities and challenges to tribal leadership, as well as to public safety partners at all levels of government.
- Plan and implement holistic communications operability and interoperability to expand and strengthen public safety services for their tribal community and neighboring jurisdictions.

For more information on CISA's communications operability and interoperability support within tribal communities, please contact Jessica.Kaputa@cisa.dhs.gov.

Learn More About the Tribal Emergency Communications Program Here

Emergency Communications Division Releases Interactive Graphic for Public Safety Communications and Cyber Resiliency Toolkit

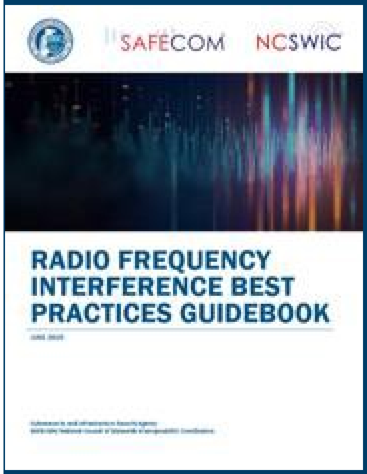
This July, CISA released an interactive graphic for the *Public Safety Communications and Cyber Resiliency Toolkit*.

CISA developed the *Public Safety Communications and Cyber Resiliency Toolkit* as a collection of resources to assist public safety agencies and others responsible for communications networks in evaluating current resiliency capabilities, identifying ways to improve resiliency, and developing plans for mitigating the effects of potential resiliency threats.

To view the graphic, and for more information, please visit the SAFECOM blog on Communications and Cyber Resiliency Toolkit.

View the Public Safety Communications and Cyber Resiliency Toolkit Graphic

CISA Releases Radio Frequency Interference Best Practices Guidebook



SAFECOM NCSWIC

RADIO FREQUENCY INTERFERENCE BEST PRACTICES GUIDEBOOK

CISA, in partnership with SAFECOM and the National Council of Statewide Interoperability Coordinators, developed and released the *Radio Frequency (RF) Interference Best Practices Guidebook.* This publication helps to educate public safety organizations on RF interference threats.

RF interference is defined as “the effect of unwanted energy due to one or a combination of emissions, radiations, or inductions upon reception in a radio communication system, manifested by any performance degradation, misinterpretation, or loss of information which could be extracted in the absence of such unwanted energy.” RF interference can impact a variety of commonly used wireless technologies, such as land mobile radio, Long-Term Evolution, Bluetooth, Wi-Fi, and Global Positioning Systems.

Public safety organizations can leverage the *Guidebook* and familiarize themselves with recognizing, reporting, and mitigating RF interference. Specifically, the *Guidebook*:

- Provides an overview of the different types of RF interference and the implications they pose to public safety communications.
- Summarizes ongoing efforts related to awareness, preparation, mitigation, and current legislation pertaining to RF interference.
- Offers information on how public safety organizations can best recognize, respond to, report, and resolve RF interference incidents.

Learn More About the Best Practices Guidebook

New CISA Products Help Identify Suspicious Unmanned Aircraft Systems

CISA has released new informational resources aimed at identifying suspicious unmanned aircraft systems (UAS).

The poster and postcard indicate how individuals can recognize the difference between a recreational UAS and a UAS that may be turned into, or carry, improvised explosive devices capable of causing serious harm to individuals and infrastructure. These products join CISA's collection of outreach materials designed to raise national awareness about suspicious activity related to the use of explosives.

Since UAS use in the United States has increased as a cost-effective, versatile business and national security tool, as well as a popular recreational hobby, the Federal Aviation Administration estimates combined hobbyist and commercial UAS sales will rise from 2.5 million in 2016 to 7 million by the end of 2020. Because of their physical and operational characteristics, UAS can often evade detection. As a result, potential threats associated with UAS will continue to expand in nature and increase in volume in the coming years.

Download the Suspicious UAS Poster and Postcard

Webinar Recording Available: COVID-19 Response

In July, CISA co-hosted the webinar "COVID-19 Response: Lessons on Cybersecurity & Resilience in a Pandemic" with the Regional Consortium Coordinating Council and the State, Local, Tribal, and Territorial Government Coordinating Council.

COVID-19 has forced state and local governments to rapidly change how they operate and adapt to a volatile new environment. Now, state and local officials are teaming up to discuss lessons learned thus far about securing our communities during a pandemic.

Watch this webinar to learn the latest on everything from cybersecurity for a remote workforce to COVID-related phishing and malware campaigns.

Watch the "COVID-19 Response" Webinar

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!

- Protect, learn, discuss: participate in the National #Cybersecurity Summit by @CISAgov every Weds through Oct 7! Take part at cisa.gov/live #CISASummit
- Looking to start or advance in a career in cybersecurity? Visit the new cyber careers pathway tool from @CISAgov in partnership with #NIST https://niccs.us-cert.gov/workforce-development/cyber-career-pathways

- New public safety & resiliency tool now out from @CISAgov in partnership with #SAFECOM https://www.cisa.gov/blog/2020/07/23/cisa-releases-toolkit-promote-public-safety-communications-and-cyber-resiliency-0

- Learn more about #smarticities at the upcoming Cybersecurity Symposium for Smart Cities, supported by @IEEESmartCities, @CISAgov & more