**CISA Community Bulletin** - November 16, 2021

# November is Infrastructure Security Month


On November 1, the Cybersecurity and Infrastructure Security Agency (CISA) kicked off Infrastructure Security Month! This year's theme is "*Critical Infrastructure Security and Resilience: Build it In*"

All month, CISA is encouraging stakeholders to "Build it In" to emphasize the need to consider infrastructure security and resilience from design concept through development and implementation. CISA is spotlighting a different way to think about this theme each week.

- **Week 1 (November 1-7)**: Interconnected and interdependent critical infrastructure: Shared risk means building in shared responsibility.
- **Week 2 (November 8-14)**: Secure Public Gatherings: Build in security for mass gatherings starting with your planning.
- **Week 3 (November 15-21)**: Build security and resilience into critical Infrastructure.

- **Week 4 (November 22-30)**: Secure Elections: Build resilience into our democratic processes.

The Nation's infrastructure relies on a highly interdependent environment and interacts with everyday lives in many ways. Now is the time to act, whether by participating in exercises, learning about your organization's interdependencies and planning accordingly, or promoting smart and secure investments.

For more information about Infrastructure Security Month and to access this year's toolkit, please visit CISA.gov/ismonth or see the Social Media section below.

**Learn More Here**

---

# Alerts & Announcements

## CISA Hosts Supply Chain Risk Management Strategies for State & Local Government Webinar

CISA will host the Cyber Supply Chain: Risk Management for State, Local, Tribal, and Territorial Governments webinar on November 17, 2021, at 12:00 p.m. ET. Hear from government and industry experts on cyber supply chain risk reduction strategies, lessons learned from recent cyber supply chain events, and best practices for organizations of any size – including state, local, tribal and territorial governments.

**Learn More Here**

## CISA's Office for Bombing Prevention (OBP) Marks 15th Year Anniversary

The Office for Bombing Prevention plays a leading role in protecting the United States against bombing incidents by enhancing security and resilience at all levels of government, across the private sector, and among the public.

On October 4, 2006, Congress formally recognized "the need for an enhanced and coordinated national bombing prevention effort," which established OBP, now part of CISA. CISA OBP has since developed many resources to counter improvised explosive device (IED) threats, including:

- Tripwire, DHS's information sharing website

- National Counter-IED Capabilities Analysis Database
- Multi-Jurisdiction IED Security Planning
- Counter-IED Training and Awareness-
- Bomb-Making Materials Awareness Program

CISA OBP is committed to sharing resources and encouraging active participation and partnership in the national effort to enhance security and resilience for IED incidents.

**Learn More Here**

## Advisory Council Study on Workforce and Talent Management Delivered to President Biden

On September 22, the President's National Infrastructure Advisory Council approved its Workforce and Talent Management Report. This report provides recommendations for addressing the skilled worker shortage among the critical infrastructure workforce. The complete report and fact sheet can be found on CISA.gov.

**Learn More Here**

# CISA Releases Updated Interoperability Field Operations Guide

CISA released the 14th version of its National Interoperability Field Operations Guide**,** a technical reference designed to support incident communications. The NIFOG is a compilation of communication references and information recommended by public safety practitioners across the country.

CISA updates the guide regularly to keep pace with the technical and regulatory nature of incident communications and technology. New content includes references on information technology, emergency wireless carrier services, interference management, encryption, and cybersecurity.

**Learn More Here**

## CISA Hosts Asian American Pacific Islander (AAPI) Hometown Security Webinar

Join representatives from CISA, the DHS Center for Prevention Programs and Partnerships, the Federal Bureau of Investigation, and the Georgia Bureau of Investigation on Tuesday, November 16, 2021, 9 a.m.-12 p.m., for a webinar to explore AAPI community concerns regarding violence towards its members and gaps in hate crimes reporting. Participants will learn about mitigation methods for protecting shared community spaces and how to respond to an active shooter situation.

Learn More Here

## Register Today for the 2021 Chemical Security Seminars

The 2021 Chemical Security Seminars will be held virtually on December 1, 8, and 15, 2021, from 11 a.m. to 3 p.m. ET. To register and view the preliminary agenda, visit the Chemical Security Summit webpage.

Learn More Here

# Events

### Partner Webinar:

### Keeping your Family Safe Online: Securing your Home and Devices

Join the National Cyber Security Alliance and Palo Alto Networks for a webinar on keeping families safe online.

**Date**: November 17, 2021

**Time**: 2:00 p.m. ET

Learn More Here

### Partner Webinar: What CISA is Doing to Help SMBs Tackle Remote/Hybrid Workforces

Join Nodeware and CISA for a webinar on remote work and how it is here to stay.

**Date**: November 18, 2021

**Time**: 2:00 p.m. ET

Learn More Here

### Partner Webinar: Cybersecurity: Basics for Business

Join the Small Business Administration webinar to learn the best practices for identifying risks and securing information.

**Date**: November 18, 2021

**Time**: 12:30 p.m. ET

Learn More Here

# Featured Programs and Resources

### CISA Releases Joint Cybersecurity Advisory on Water Supply and Wastewater Management

On October 14, CISA and its partners released a Joint Cybersecurity Advisory. The advisory highlights ongoing malicious cyber activity — by both known and unknown actors — targeting the information technology and operational technology networks (IT/OT), systems, and devices of U.S. Water and Wastewater Systems Sector facilities.

The advisory includes two new infographics — Cyber Risks & Resources for the Supply Water National Critical Function and Cyber Risks & Resources for the Manage Wastewater National Critical Function. Developed by CISA's National Risk Management Center, these infographics identify cyber risks under three categories: IT, OT, and information technology/operational technology convergence.

Please share these resources to help spread the importance of cybersecurity to U.S. water and wastewater systems. To learn more, visit: CISA.gov/ncf-water.

## CISA Releases .gov Domain Fact Sheet


CISA released a fact sheet, Sign Up for a .gov Domain: Information for Election Officials, on the importance of registering for a .gov domain for election officials to combat false and misleading election information.

As the government agency that oversees the .gov top-level domain, CISA provides .gov domains for election offices to help the public quickly identify election websites and election communications as trusted Government sources.

To learn more about mis-, dis-, and mal-information, visit: CISA.gov/mdm.

## CISA Releases New Public Safety Standard Video

CISA released "The Funding and the Future of Project 25 (P25)" video to showcase P25's proven value to public safety operations. The video provides recommendations on funding P25 systems.

For agencies considering the transition to P25, the video offers insights and advice from public safety officials with firsthand experience. The video can be found here: cisa.gov/safecom/technology.

## CISA Releases Infrastructure Resilience Planning Framework

CISA released the Infrastructure Resilience Planning Framework (IRPF) to help stakeholders identify critical infrastructure, assess related risks, and develop and implement resilience solutions. The framework is targeted to government, infrastructure owners and operators, manufacturing clusters, and planning commissions.

Consisting of five key steps, the IRPF can be incorporated into existing planning processes to enhance resilience. The IRPF consists of guidance, tools, resources, a facilitation guide, and mechanisms to fund resilience solutions. The IRPF will help users:

- Understand critical infrastructure risk and opportunities to increase resilience,
- Collaborate with diverse stakeholders, and
- Identify funding sources and improve competitiveness for grant and loan requests.

To learn more, visit: cisa.gov/idr-program.

### CISA Releases Supply Chain Resources

CISA published two products by industry members of the Information and Communications Technology Supply Chain Risk Management Task Force.

- The Preliminary Considerations of Paths to Enable Improved Multi-Directional Sharing of Supply Chain Risk Information offers information to address liability limitations to improve supply chain risk information sharing between the Federal Government and industry.
- The Operationalizing the Vendor SCRM Template for Small and Medium-sized Businesses (which includes an easy-to-use spreadsheet) applies the previously released enterprise Vendor Template to be used by small and medium-sized businesses. The product provides guidance on applying industry standards and best practices for reporting and vetting processes when purchasing information and communications technology hardware, software, and services.

To learn more, please visit, Sharing Information to Get Ahead of Supply Chain Risks.

---

## In Case You Missed It

- ***New Guidance: Security Guidance for 5G Cloud Infrastructure***

  CISA partnered with the National Security Agency to publish the "Security Guidance for 5G Cloud Infrastructures: Prevent and Detect Lateral Movement." As the first installment in a four-part series, this document provides detection and mitigation guidance on securely building and configuring cloud infrastructures in support of 5G.

- ***4th Annual National Cybersecurity Summit Review***

  The month of October marked CISA's 4th Annual National Cybersecurity Summit! Throughout the month of October, cybersecurity and critical infrastructure leaders from government, industry, and academia participated in powerful forums about protecting our Nation's physical and cyber infrastructure. Topics covered during the #CISACyberSummit included: the vulnerability management ecosystem,

collective defense collaboration, the cyber workforce, the power of partnerships, and much more. Take a look at the events page to watch all the recordings.

## 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!

- Tune into the @CISAgov's Supply Chain Risk Management Strategies for State & Local Government webinar on November 17. Register here: https://www.eventbrite.com/e/4th-annual-national-cybersecurity-summit-tickets-169672754777
- Want to learn more about mitigating supply chain risks? Check out @CISAgov's blog article: https://www.cisa.gov/blog/2021/09/21/sharing-information-get-ahead-supply-chain-risks
- @CISAgov will use social media to share news and updates about Infrastructure Security Month. Follow on Twitter @CISAgov and @CISAInfraSec, like us at facebook.com/CISA, and follow on Instagram @cisagov and share messages about Infrastructure Security Month. Also, be sure to check out updates at CISA.gov/infrastructure-security-month.

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