CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

COMMUNITY BULLETIN

Alerts & Announcements

CISA Releases COVID-19 Election Security Resources

In response to COVID-19 consequences on election operations and administration, the Cybersecurity and Infrastructure Security Agency (CISA) is working with election officials and government and industry partners to ensure upcoming elections are accessible and secure, and that voters can safely cast their votes.

CISA supported the development of the Election Security Subsector Government Coordinating Council (GCC) and Sector Coordinating Council (SCC) resources which are on the U.S. Elections Assistance Commission website.

CISA's Protect2020 webpage provides the latest government and industry resources and up-to-date information on how to assess risk, secure election infrastructure systems, and respond to cyber-related incidents. Learn how to manage inbound/outbound ballots, prepare electronic ballot delivery and marking, ensure signature verification, and more.

Explore these resources and more at https://go.usa.gov/xw4Nd.

Introducing CISA Central: A Single Entry Point into CISA

CISA Central is CISA's hub for staying on top of threats and emerging risks to our nation's critical infrastructure, whether they're of cyber, communications, or physical origin. CISA Central is the simplest, most centralized way for a critical infrastructure partners and stakeholders to engage with CISA, and is the easiest way for all critical infrastructure stakeholders to request assistance and get the information you need to understand the constantly evolving risk landscape.

Through CISA Central, CISA coordinates situational awareness and response to national cyber, communications, and physical incidents. CISA works closely with public, private sector, and international partners, offering technical assistance, information security, and education to protect our nation's critical infrastructure from a broad range of

current cyber, communication, and physical threats. Organizations that are already working with CISA through any one of our more specialized engagements, or are signed up for alerts or bulletins, will be unaffected. For more specific work with CISA programs, such as working groups and sector partnerships, organizations should continue to engage in those relationships.

For more information, email central@cisa.gov.

CISA Insights: COVID-19 Disinformation Activity

The latest CISA Insight, "COVID-19 Disinformation Activity," provides an overview of false information and conspiracy theories related to COVID-19's origin, scale, government response, prevention, and treatment. It also provides steps individuals can take to reduce the risk of spreading false or misleading content.

Read or share this CISA Insight to increase awareness of disinformation campaigns and to reduce the risk of sharing inaccurate information: https://go.usa.gov/xw4NH.

CISA Supports State and Local Government Efforts to Counter COVID Disinformation

CISA's Countering Foreign Interference Task Force released a toolkit to help state and local officials counter COVID-19 misinformation and disinformation. The toolkit provides messaging, background information, and social media images to reinforce the importance of gathering information from trusted sources and the hazards associated with enabling the spread of false or misleading information. The toolkit is available at https://go.usa.gov/xwVR2. The materials are designed to be tailored with local government websites and logos.

The need to seek information from trusted sources is especially important during the pandemic. Our state and local officials are front and center providing this information to their communities while others, including foreign actors, undermine accurate information and access to it. This includes misinformation, which is false, but not created or shared with the intention of causing harm, and disinformation, which is deliberately created to mislead, harm, or manipulate a person, social group, organization, or country.

Please visit https://go.usa.gov/xwVRW for more information on CISA's ongoing effort to counter foreign influence and the spread of misinformation and disinformation.

CISA Releases First Cyber Essentials Toolkit

As a follow-up to the November 2019 release of Cyber Essentials, CISA released the first in a series of six Cyber Essentials Toolkits. This is a starting point for small businesses and government agencies to understand and address cybersecurity risk as they do other risks. CISA's toolkits will provide greater detail, insight, and resources on each of the Cyber Essentials' six "Essential Elements" of a Culture of Cyber Readiness.

This launch highlights the first "Essential Element: Yourself, The Leader" and will be followed each month by a new toolkit to correspond with each of the six "Essential Elements." Toolkit 1 focuses on the role of leadership in forging a culture of cyber readiness in their organization with an emphasis on strategy and investment.

Developed in collaboration with small businesses and state and local governments, Cyber Essentials aims to equip smaller organizations that historically have not been a part of the national dialogue on cybersecurity with basic steps and resources to improve their cybersecurity. Cyber Essentials includes two parts – guiding principles for leaders to develop a culture of security, and specific actions for leaders and their IT professionals to put that culture into action.

Each of the six Cyber Essentials includes a list of actionable items anyone can take to reduce cyber risks. These are:

- Drive cybersecurity strategy, investment, and culture;
- Develop heightened level of security awareness and vigilance;
- Protect critical assets and applications;
- Ensure only those who belong on your digital workplace have access;
- Make backups and avoid loss of info critical to operations; and
- Limit damage and restore normal operations quickly.

To learn more about Cyber Essentials, visit https://go.usa.gov/xwbEg.

CISA Releases the FY 2020 REMCDP Notice of Funding Opportunity

On May 8, 2020, CISA released the Fiscal Year (FY) 2020 Rural Emergency Medical Communications Demonstration Project (REMCDP) Notice of Funding Opportunity (NOFO). This opportunity will fund up to two demonstration projects that address the *National Emergency Communications Plan* and identify innovative solutions to improve the delivery of rural medical communications.

The REMCDP grant provides funding for recipients to work with a public health or medical facility to examine communications barriers and identify solutions that enhance existing emergency communications infrastructure. Specifically, applicants must demonstrate their ability to leverage existing technologies and engage non-medical professionals to help establish or sustain statewide medical communications systems and use existing infrastructures to improve the delivery of rural medical care. Eligible applicants may apply for up to $2,000,000 for a two-year period of performance, beginning on September 30, 2020. REMCDP funding will be awarded to a maximum of two recipients following a competitive review process.

The REMCDP NOFO is available on www.grants.gov; applications are due by Wednesday, June 24, 2020, at 11:59 PM EDT. Additional information about REMCDP, past recipients, and the new grant opportunity can be found on https://go.usa.gov/xw4Rg.

NIAC Report Now Available: *Transforming the Cyber Threat Partnership*

On Tuesday, May 5, 2020, the President's National Infrastructure Advisory Council's (NIAC) most recent study, *Transforming the Cyber Threat Partnership*, was transmitted to the White House by Acting Homeland Security Secretary Chad Wolf.

In September, the National Security Council (NSC) asked the NIAC to examine how the Federal Government and private industry can collaborate seamlessly to confront urgent cyber risks in the most critical and highly targeted private infrastructure industries and provide recommendations by the end of the year.

The study focused on the most at-risk entities and functions within the energy, financial services, and communications sectors where a successful cyber-attack could threaten public health and safety, national or regional economic stability, and the security of the Nation.

As part of this accelerated effort, a NIAC Working Group of four members received classified threat briefings and had unclassified conversations on how the status quo is not enough to respond to the growing cyber threat. The Working Group built on the foundation of prior efforts and engaged senior leaders from the NSC and CISA in three concentrated face-to-face meetings.

The result was nine recommendations that fall into four strategies:

- Make Cyber Intelligence Actionable
- Protect Highly Critical Cyber Systems by Establishing the Federal Cybersecurity Commission
- Modernize Legal Authorities to Improve Cyber Defense

- Secure the Supply Chain of Sensitive Cyber Components

The NIAC deliberated and approved the report and its recommendations at the December 2019 Quarterly Business Meeting. The final report is available here: https://go.usa.gov/xw4RB.

CISA Releases New Trust in Smart City Systems Report

More cities are investing in information technology (IT) with their existing operational technology (OT) and public service requirements. These Smart City Projects are challenging endeavors that can fail or underperform for many reasons. The expansion of IT into city functions brings benefits, but also added complexity and challenges.

The Trust in Smart Cities Systems Report is a resource meant to guide discussions between Smart City decision-makers, designers, and implementers during the initial, high-level design of a smart city project and make decisions based on a more complete understanding of the tradeoffs. The recommendations outlined in this report facilitate early, important steps in the process of developing a smart city system.

To access the full report and to share with stakeholders, please visit https://go.usa.gov/xwVRA.

Events

Webinars: Cyber Essentials and More from the National Cyber Security Alliance

On August 11, the National Cyber Security Alliance (NCSA) will host a webinar featuring CISA's first Cyber Essentials toolkit, "Yourself, the Leader."

- **Title**: Cyber Essentials Chapter 1: Yourself as the Leader. Driving Cybersecurity Strategy, Investment and Culture
- **Date**: Tuesday, August 11
- **Time**: 2:00-3:00 pm ET
- **Link**: https://staysafeonline.org/event/cyber-essentials-chapter-1/

This is just one of several upcoming NCSA webinars on a variety of cybersecurity topics. Visit the links below to learn more and to register:

- June 25, 2020: Cybersecurity Q&A Session 1: You Have Questions; These Experts Have Answers
- June 25, 2020: Psychology of Passwords: Combatting Cognitive Dissonance in Password Creation
- July 14, 2020: Business Identity Theft: What You Should Know

---

Featured Programs & Resources

CISA Publishes Guidelines for 911 Centers Regarding Pandemic

911 centers, including emergency communication centers (ECC), public safety answering points (PSAP), emergency operations centers (EOC), public safety communication centers (PSCC), and other public service command centers, are a critical component of emergency communications, and they face a unique set of challenges when planning for, and responding to, pandemics. CISA's *Guidelines for 911 Centers: Pandemic* document suite aims to assist public safety partners across all levels of government when developing plans and actions regarding governance, procedures, staffing, and cleaning and disinfecting in response to a pandemic.

Aligned to existing guidance, recommendations, and training courses, and inclusive of input from practitioners and subject matter experts from CISA, SAFECOM, the National Council of Statewide Interoperability Coordinators, and the National 911 Program, the document suite contains four sets of guidance:

- ***Guidelines for Executives: 911 Center Pandemic Recommendations*** – emphasizes the importance of communications centers, accentuates the particular risk of a pandemic to resiliency of 911 operations, communicates executive-level action, and provides a description of available guidance for 911 administrators.
- ***Guidelines for 911 Centers: Pandemic Planning*** – highlights governance, resource planning, and contingency considerations from a holistic perspective during a pandemic.
- ***Guidelines for 911 Centers: Pandemic Operating Procedures*** – provides recommendations on how to organize, train, and care for personnel while operating through a pandemic.
- ***Guidelines for 911 Centers: Cleaning and Disinfecting During a Pandemic*** – presents cleaning and disinfecting guidance specific to public safety and resources for 911 centers during a pandemic.

The document suite provides recommendations that are advisory and are not to be considered federal directives or standards. Individual centers should review and apply the guidance based on their own requirements and discretion. CISA recommends that all pandemic planning actions appropriately balance public safety, the health and safety of the workforce, and the continued delivery of essential services and functions.

For more information about the document suite, visit https://go.usa.gov/xw4RA.

CISA Offering Virtual Technical Assistance Programs and Services

During this period of heightened social distancing, CISA is now offering many of its emergency communications technical assistance programs and services virtually. These programs include but are not limited to: Statewide Communication Interoperability Plan (SCIP) workshops; Tactical Interoperable Communications Plan (TICP) development; Tactical Interoperable Communications Field Operations Guide (TIC-FOG) development; Electronic Field Operations Guide (eFOG) data collection and analysis; and initial and mid-exercise planning meetings.

To learn more about virtual CISA technical assistance, please visit https://go.usa.gov/xw4ny.

Join CISA's STOP. THINK. CONNECT.™ Campaign

In today's challenging environment, Americans are spending more and more time online, putting our infrastructure under enormous stress. There is no single agency that can manage all the threats and vulnerabilities that arise in the current threat landscape, so CISA needs the help of communities across the United States to play an active role in helping our Nation stay ahead of the curve.

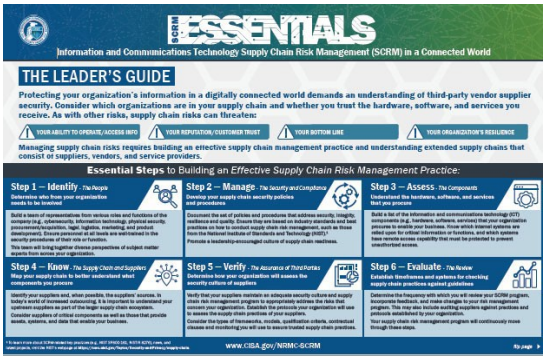
CISA's STOP. THINK. CONNECT.™ (STC) Campaign provides a great opportunity to be a vital part of this national effort. STC is a year-round public awareness campaign, led by CISA and the National Cyber Security Alliance, and aims to increase understanding of current cyber threats and empower the public to take charge of their online safety and security. STC encourages Americans to view Internet safety as a shared responsibility—at home, in the workplace, and in our communities—and provides individuals and organizations with simple, easy-to-understand resources and tools so they can make informed, smart, safe choices online.

The STC campaign creates a broad and diverse network where partners, including federal, state, local, tribal, and territorial governments, academia, industry, and non-profit organizations, discuss current cybersecurity trends,

exchange best practices, and share experiences and ideas. STC partners have front-row access to vital cybersecurity tips to share with employees and students, and advice from the Department of Homeland Security, industry speakers, and cybersecurity experts.

The STC Campaign is open to all government entities, 501c-registered non-profits, and academic institutions, both inside and outside the United States. There are no fees or financial obligations associated with membership. Those seeking to join the campaign can contact stopthinkconnect@hq.dhs.gov to become a partner.

Building Collective Resilience for the ICT Supply Chain



Last month, CISA's National Risk Management Center (NRMC) released two supply chain risk management (SCRM) resources to help businesses and organizations boost supply chain security. As organizations are increasingly using Information and Communications Technology (ICT) to keep their operations running in today's evolving risk environment, they must also stay vigilant of adversaries seeking to target critical systems and downstream suppliers.

The *ICT SCRM Essentials* is a guide for leaders and staff containing actionable steps on how to build a supply chain risk management program. The ICT SCRM Fact Sheet is a quick reference on ICT supply chain risks and how to improve overall security resilience.

Learn more about CISA's SCRM effort at https://go.usa.gov/xw4nF, or read the latest CISA blog article, *Building Collective Resilience for the ICT Supply Chain*.

Strengthening Positioning, Navigation, and Timing Services

One of CISA's top priorities is strengthening the security and resiliency of the national Positioning, Navigation, and Timing (PNT) ecosystem. Nearly all critical infrastructure sectors heavily rely on accurate PNT information. However, the ubiquitous use of the Global Positioning Navigation (GPS) makes these sectors vulnerable to risks associated with disruption or loss of GPS.

CISA's NRMC is working with federal partners and the critical infrastructure community to promote the responsible use of GPS and other PNT sources. Last month, CISA published the *Report on PNT Backup and Complementary Capabilities to the GPS*, which analyzes the GPS applications used by critical infrastructure and provides next steps to enhance PNT resilience.

For more information and resources or to read this report, visit: https://go.usa.gov/xw4Qb.

CISA's Office for Bombing Prevention Releases *TRIPwire* Annual Report

CISA's Office for Bombing Prevention (OBP) has released the *TRIPwire* 2019 Domestic Open Source Intelligence (OSINT) Improvised Explosive Device (IED) Report.

The annual report, which can be accessed by logging into TRIPwire and clicking on the report graphic in the carousel, provides an overview of open source data for each of the 10 federal regions and includes key trends in explosive and bombing-related incidents, notable tactics, techniques, and procedures. It is designed to provide key analyses for

intelligence and law enforcement communities, public safety officers and many other security and emergency services professionals across the federal, state, local, and tribal sectors of the United States.

Some of the report's key findings include:

- In 2019, there were 2,912 total bomb threat, suspicious package, and device-related incidents. There were 786 device-related incidents in 2019, marking a continuous increase over the past threeyears.
- Triacetone triperoxide remained a dominant material used by malicious actors in incidents involving homemade explosives.
- An ISIS-aligned manual reprinted in 2019 drew attention to CISA's Bomb-Making Materials Awareness Program and provided future threat actors with best practices for avoiding detection when acquiring bomb-making materials.
- Domestic ATM attacks by criminal actors continued to rise in 2019, highlighting the need for increased awareness by first responders, public safety bomb technicians, and military explosive ordnance disposal technicians, who may encounter devices or blast scenes near ATMs.

For the report, OBP derived its data from open source reporting by news outlets, social media, and other multimedia channels related to explosive activity.

Learn about evolving IED tactics, techniques, and procedures by signing up for a TRIP*wire* account at https://go.usa.gov/xw4Pq. For assistance registering for the site, please contact the TRIP*wire* Helpdesk at 866-987-9473, or email TripWireHelp@dhs.gov.

Social Media

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

- .@CISAgov published new guidelines for emergency response centers for thepandemic: https://go.usa.gov/xw35D
- Confronting urgent cyber risk: Read the NIAC advisory committee's latest report on #cyber defense, #supplychain, and more on @CISAgov: https://go.usa.gov/xw35B
- More time online = more risk online. Visit @CISAgov @STOPTHINKCONNECT for #cybersecuritysafety tools & tips: https://go.usa.gov/xw4nd
- Even remote, schools must remain safe. See @CISAgov info for parents, teachers & admins for K-12 at https://go.usa.gov/xw4m8
- The Office for Bombing Prevention at @CISAgov released its new TRIPwire Annual Report on the latest news on the topic: https://go.usa.gov/xw4Pq
- What's real vs fake? Visit @CISAgov COVID-19 Disinformation Activity for details on false information and conspiracy theories & how to avoid: https://go.usa.gov/xw4NH
- New #supplychain guidance from @CISAgov out now! Stay vigilant and safe with your tech suppliers. Read more: https://go.usa.gov/xw4nF
- #COVID-19 working group with @CISAgov & @EACgov helps election officials navigate accessible and secure elections: https://go.usa.gov/xw4Nd
- Making #GPS safer: @CISAgov and #criticalinfrastructure partners have a new report on responsible use of #GPS: https://go.usa.gov/xw4Qb

---

The CISA Community Bulletin is a monthly newsletter featuring cybersecurity and infrastructure security resources, events, and updates from CISA and its partners. Learn more at https://www.cisa.gov.

OTHER RESOURCES:
About Us | Getting Started | Cybersecurity Framework | Assessments | Events and Media | Privacy
STAY CONNECTED:

SUBSCRIBER SERVICES:
Manage Preferences | Unsubscribe | Help