Announcements

CISA Releases Telework Guidance for Schools and Organizations

As the Nation's risk advisor, the Cybersecurity and Infrastructure Security Agency (CISA) brings together its partners in industry and the full power of the federal government to improve American cyber and infrastructure security. To help secure schools and organizations during the unprecedented surge in telework and video conferencing, CISA recently released new telework guidance and resources.

The resources below are provided to assist organizations and teleworkers to be secure when working remotely.

- Guidance and Tips for Schools, Staff, and Students to Help Secure Video Teleconferencing
- General Guidance for Securing Video Conferencing
- Cybersecurity Recommendations for Federal Agencies Using Video Conferencing
- Cybersecurity Recommendations for Critical Infrastructure Using Video Conferencing
- National Security Agency (NSA) & DHS Telework Best Practices
- Video Conferencing Tips

Learn more on the CISA website.

#Protect2020: CISA's Savvy Steps to Election Security

In the United States, voting is a right, and free and fair elections are the backbone of our democracy. As the lead federal agency responsible for election security, CISA has started #Protect2020, a national call to action to enhance the security and resilience of the Nation's critical election infrastructure.

American elections have been a target of foreign adversaries. These threats are constantly evolving, so defending our elections needs vigilance and innovation. CISA works with election officials, responsible for approximately 8,800

voting districts across the country, to find security gaps ahead of and during elections. #Protect2020 also includes engaging with the electorate and political parties, campaigns, and committees at the national level.

To help guard against cyberattacks, CISA encourages election officials to take some basic steps:

- Patch applications and operating systems with the latest update. This can reduce the number of entry points for hackers.
- Only allow access to approved personnel and applications. This can prevent malicious software from running and limit its spread through a network.
- Use firewalls. Easy network access means a network is more open to attack. Firewalls can be configured to block data from certain locations or apps and allow necessary data through.
- Report an intrusion or request technical assistance. If you believe your network has been compromised, contact CISA (cisaservicedesk@cisa.dhs.gov) or the Federal Bureau of Investigation (FBI) through a local field office or the FBI's Cyber Division (CyWatch@ic.fbi.gov).

Taking these steps can play a huge part in stopping adversaries seeking to access or manipulate voter registration data and interfere with election websites and databases through ransomware attacks and phishing emails and texts.

But election security is about more than just good cybersecurity. CISA deploys Protective Security Advisors (PSAs) across the country to conduct physical security assessments of election infrastructure facilities and provide advice on physical risks.

As state and local election officials grapple with how to conduct elections safely and securely in the face of COVID-19, CISA has partnered with the U.S. Election Assistance Commission and the Election Infrastructure Subsector Government Coordinating Council and Subsector Coordinating Council to develop a series of voluntary informational resources to assist them. They offer considerations on topics related to expanded implementation of absentee and mail voting, modifying in-person voting to maximize voter and election worker safety, and communicating with the public about what to expect around their voting experience. As always, CISA recommends that voters consult trusted sources like their state or local election official for accurate information on how to vote.

#Protect2020 also offers useful information for voters on how they can be resilient against disinformation. These resources include how to spot and help stop disinformation, and how the debate about pineapple pizza can be used to illustrate the way disinformation campaigns attempt to influence voter opinions and behavior (no, really).

Visit CISA's Election Security page to learn more about our services and our work with those on the front lines of elections to make sure all votes are counted—and counted correctly.

New Value Analysis Guide and Brochure Help Agencies Evaluate Emergency Communications Cost Effectiveness

CISA, in partnership with SAFECOM and the National Council of Statewide Interoperability Coordinators (NCSWIC), published the *Emergency Communications Systems Value Analysis Guide and Understanding the Value of Public Safety Communications Systems: A Brochure for Elected Officials and Decision-Makers.*

Throughout 2019, SAFECOM and NCSWIC recognized the growing competition for public safety funding and the need to analyze various features of communications systems and equipment. This new guide aims to help agencies determine right-sized solutions that strike the balance between cost and value.

The guide contains recommendations, best practices, and considerations for public safety agencies to evaluate cost effectiveness, including:

- Descriptions, costs, and expected lifespans of common emergency communications systems;
- Key features of emergency communication systems and equipment based on user position and responsibility; and

- Value Analysis Checklist, which summarizes analysis questions across common system components and serves as a tool to identify public safety user requirements.

The accompanying brochure, *Understanding the Value of Public Safety Communications Systems: A Brochure for Elected Officials and Decision-Makers*, provides key considerations and trade-offs between cost and value of communications systems components. The brochure serves as a leave-behind for decision-makers to better understand public safety requirements and solutions aligned with their strategic goals, while allowing agencies to save costs where possible.

For more information, please visit the CISA SAFECOM website.

Featured Programs & Resources

Trust in Smart City Systems Report

CISA and the Homeland Security Systems Engineering and Development Institute, a DHS-owned Federally Funded Research and Development Center, published a paper examining smart city projects through the lens of homeland security priorities.

Smart City Projects are those that integrate information technology with the management and operation of civic functions and include operational technology and public service requirements. The systems upon which Smart City Projects are built can impact virtually every aspect of modern life, including communications, utilities such as water and power, transportation, and government services due to the wide-ranging scope and the amount invested.

Smart City Projects are challenging endeavors and can fail or underperform for many reasons, so it is necessary to implement an integrated solution that addresses the broad scope of Smart City Projects.

This report is intended as a resource to guide discussions between Smart City decision-makers, designers, and implementers during the initial high-level design of a Smart City Project to make decisions based on a more complete understanding of the tradeoffs. The recommendations outlined in this report facilitate an early, important step in the process of developing a smart city system.

Read the full report on the CISA Publications page.

COVID-19 Disinformation Toolkit

CISA designed a toolkit to help state, local, tribal and territorial officials bring awareness to misinformation, disinformation, and conspiracy theories appearing online related to COVID-19's origin, scale, government response, prevention, and treatment. The toolkit also includes communication strategies to help regional offices share verified information with constituents.

Download the toolkit along with talking points, FAQS, and posters to help spread awareness at www.cisa.gov/covid-19-disinformation-toolkit.

New COVID-19 Resources for Returning to the Workplace

The Communications Sector Coordinating Council has released a "Return to Normal" Guidance and Resources document. The council created this document to provide guidance to online resources available to assist Communications providers to establish and implement a plan as they consider returning to the workplace following COVID-19 closures.

The resources provided in this document include:

- State and federal government recommendations;
- Industry best practices, articles, and questionnaires that may be useful with efforts to create a safe work environment and mitigating the spread of COVID-19.

To learn more and download the full document, visit the U.S. Telecom website: https://www.ustelecom.org/wp-content/uploads/2020/07/CSCC-Return-to-Normal-Guidance-and-Resources.pdf.

CISA Releases New Cyber Essentials Toolkit on Organization-Wide Cybersecurity

CISA released its Cyber Essentials Toolkit, *Chapter 2: Your Staff, The Users*. This toolkit is the second in a series of six toolkits set to be released each month. This chapter follows the release of *Chapter 1: Yourself, The Leader* – Drive Cybersecurity Strategy Investment and Culture and CISA Cyber Essentials in November 2019.

Chapter 2 emphasizes the importance of the organization as a whole in cybersecurity, requiring a shift toward a culture of cyber readiness and greater cyber awareness among staff by providing cyber education, training, and other resources. Focus areas include, leveraging basic cybersecurity training; developing a culture of cyber awareness that incentivizes making good choices online; teaching employees about risks such as phishing and ransomware; and identifying available training resources from partner organizations.

To learn more about the Cyber Essentials Toolkits, visit https://go.usa.gov/xfbFN.

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!

- Amid the COVID-19 pandemic, @CISAgov is leading the way in #electionsecurity. Whether voter or official, check out CISA's new #Protect2020 campaign to protect our elections https://go.usa.gov/xfb6W
- Create a culture of cyber readiness in your org: Read up on @CISAgov's new Cyber Essentials Toolkits. The first two are out now! https://go.usa.gov/xfbFN

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.

This product is provided subject to this Notification and this Privacy & Use policy.

STAY CONNECTED:

SUBSCRIBER SERVICES:
Manage Preferences | Unsubscribe | Help
