CISA Community Bulletin - November 23, 2020

November is Infrastructure Security Month 2020

What is Infrastructure Security Month?

As the Nation's chief risk advisor, the Cybersecurity and Infrastructure Security Agency (CISA) works every day to improve and protect infrastructure security and essential operations throughout the United States. CISA highlights this mission each November with Infrastructure Security Month, raising infrastructure security awareness and setting a theme for the coming year.

This year's Infrastructure Security Month comes at a time of transformation for our Nation and the pillars it relies upon. As the Nation has undergone a transformative mass move to remote work, distance learning, and telemedicine, the importance of cybersecurity and infrastructure security has increased dramatically. We also experienced a historic Presidential election, the first ever in which election infrastructure has been recognized as critical infrastructure.

This Year's Themes

In recognition of this moment in history, Infrastructure Security Month 2020 focuses on two important themes:

- The Security and Response during a Global Pandemic, and
- The Future of Securing Critical Infrastructure.

As the Nation responds to COVID-19, it is vital that as new or evolving challenges emerge, we are looking at what kind of access, personal protective equipment, and other resources workers need to continue performing essential duties in a safe and healthy way.

While accomplishing that goal, we must look to the future, and see how securing infrastructure will change as a result of the virus and of rapidly evolving technology. But this will not be the work of government alone.

Get Involved

More than ever, CISA recognizes the role private organizations and individuals play in infrastructure security.

As such, during this year's Infrastructure Security Month, we ask every organization to:

- Identify and prioritize the ability of essential workers to work safely while supporting ongoing infrastructure operations across the Nation.
- Bring awareness to misinformation, disinformation, and conspiracies appearing online related to COVID-19, 5G, election security, or other infrastructure, functions, or threats to critical infrastructure.
- Recognize the societal transformation of securing infrastructure and responding to disasters during a global pandemic.
- Understand the modernization of securing critical infrastructure as we defend today and secure tomorrow.

Join us this November and take action to ensure our critical infrastructure is safe, secure, and resilient. Download your Infrastructure Security Month toolkit to get started, and visit https://www.cisa.gov/ismonth for more ways to get involved.

Learn More About Infrastructure Security Month

Alerts and Announcements

Secure the Internet of Medical Things this Infrastructure Security Month

How often do you think about the electric plants and pipelines that supply us with reliable energy and clean water? everything from medicine to our smartphones? It's easy to take this infrastructure for granted, but as more of it goe

As our online and offline lives become more intertwined, the list of IoT devices – those that send and receive online monitor our health and wellbeing.

November is Infrastructure Security Month and the themes focus on this time of transformation reflecting the rapid more people turn to telemedicine, now is a great opportunity to focus on our Nation's healthcare infrastructure and much of our medical data—the Internet of Medical Things (IoMT).

Healthcare systems all over the world are facing new and deadly threats from cybercriminals, and good security starts at the ground level, with the individual. It's vital to secure your medical devices with the same care you secure your computer or smartphone.

To help secure your medical devices and records:

- **Check and update your security settings.** Examine your devices' settings and select options that meet your needs without putting you at risk. Also, be sure to install updates as soon as they become available. These updates often patch security vulnerabilities.
- **Use strong passwords.** Passwords can be the only thing between hackers and your personal information. Choose long passwords with numbers and symbols, that are difficult to guess. Also, employ multi-factor authentication (MFA)—a code sent via text or email before you log in.

By employing these simple best practices this Infrastructure Security Month—and throughout the year—we can easily safeguard our medical data and prevent it from falling into the wrong hands.

To learn more about the IoMT and how to secure it, check out CISA's tips on securing the IoT and the National Institute of Standards and Technology's (NIST) recommendations on managing IoT risk.

Events

Webinar: Telework Essentials to Secure the Hybrid Workplace

Join experts from CISA, Global Cyber Alliance (GCA), and Cyber Readiness Institute (CRI) for a discussion covering practical tips and recommendations to help organizations strengthen their cybersecurity as they transition to long-term or permanent workplace solutions.

Date: December 3, 2020

Time: 12:00 p.m. ET

Register Here

Partner Webinar: Securing Your Data in the Cloud

The National Cyber Security Alliance is hosting a webinar on data security. William Malik, VP of Infrastructure Strategies at Trend Micro, will spend the hour breaking down steps you can take to secure the data you store in the cloud.

Date: December 8, 2020

Time: 2:00 p.m. ET

Register Here

Event: 2020 Chemical Security Seminars

Join the virtual 2020 Chemical Security Seminars, to feature important chemical security information on everything from critical infrastructure owners to health and emergency management. Registration is now open; please register by December 1, 2020.

Date: December 2, 9, and 16, 2020

Time: 11:00 a.m. ET

Register Here

Featured Programs and Resources

CISA Concludes Another Successful National Cybersecurity Awareness Month!

CISA's National Cybersecurity Awareness Month (Cyber Month) 2020 has come and gone, and we are pleased to report a successful 17th year. Though Cyber Month has officially ended, it's important to remember that cybersecurity is a year round effort.

This October, people across this Nation united behind the 2020 Cyber Month theme "Do Your Part. #BeCyberSmart." This theme encourages everyone to own their role in cybersecurity and do their part in protecting cyberspace. As always, Cyber Month emphasized the vulnerability of all online devices and the necessity of keeping them up to date and secure.

Each week of Cyber Month 2020 had a unique focus:

Week 1 of Cyber Month addressed how online devices impact our lives, empowering users to take the right steps to reduce risk by emphasizing "If You Connect It, Protect It." Week 1 featured engagements across the United States, with diverse organizations as the National Credit Union Administration, the Air Traffic Controllers Association, and Reynolds Consumer Products.

Cyber Month's second week, which focused on securing devices at home and work, emphasized the steps individuals and organizations can take to protect online devices for personal and professional use. Week 2 saw a dramatic 41 percent increase in traffic to the Cyber Month website, as well as events like the 4th Annual Auto ISAC Cybersecurity Summit, the Wireless Leadership Summit, and the Cybersecurity Symposium for Smart Cities '20.

Interest in Cyber Month maintained its high level into Week 3, with a focus on securing healthcare related devices, and featuring more events like the Oregon Cybersecurity Summit and the National Association of Counties Fall Virtual CIO Forum.

As October ended, the final week of Cyber Month looked to the future of smart devices, addressing how technology can change consumers' and businesses' online experiences. Overall, Cyber Month 2020 was a huge success, featuring a dynamic and active social media campaign on CISA's Facebook, Twitter, and LinkedIn accounts, which brought new visibility to Cyber Month efforts and initiatives, as well as to CISA as a whole.

As physical security and cybersecurity grow more linked, you can continue to help others stay safe and more secure online by sharing the Cyber Month message with friends and family, or any group or community you belong to, to teach basic steps and share best practices to improve online safety.

Explore Cyber Month Resources Here

FBI and DHS Host Faith Leaders and Security Professionals for Security and Safety Symposium

DHS, the Federal Bureau of Investigation, and InfraGard National Capital Region held the Faith Based Security and Safety Symposium webinar on October 27, 2020 to discuss best practices and risk mitigation strategies for protecting houses of worship amid the COVID 19 crisis.

The symposium brought together more than 1,400 faith based and community leaders, security professionals, and emergency managers to discuss the security of houses of worship and how the Government can support the faith community to help keep their practitioners safe and secure.

CISA provides a variety of training, products, and resources designed to enhance risk mitigation capabilities. For more information, please visit: cisa.gov/active shooter preparedness.

CISA Releases New Cyber Essentials Toolkit on Preparing for Cyber Incidents

CISA released its *Cyber Essentials Toolkit, Chapter 6: Your Actions Under Stress* the final toolkit in a series of six that have been released monthly. This toolkit chapter emphasizes planning and preparing for cyber incidents. Organizations that establish procedures to respond to and recover from an attack strengthen their cyber hygiene. In addition, leaders must train staff to know how to communicate during a crisis.

This chapter contains recommended action oriented approaches for leaders, such as:

- Develop and test incident response and disaster recovery plans,
- Leverage business impact assessments to prioritize resources,

- Learn who to call for help,
- Develop and internal reporting structure for cyber attacks, and
- Leverage in house containment measures.

The Toolkit Chapters are targeted toward all leadership (C suite and IT) roles in the state, local, tribal, and territorial community as well as small and medium sized businesses. Essentials is a whole of community approach intended to assist in continuously improving the basic cyber hygiene and resilience of the Nation.

To learn more about the Cyber Essentials guide or the chapters, visit CISA.gov/Cyber Essentials or email CISAEssentials@cisa.dhs.gov.

CISA Reminder: Know Your Chemicals Hydrogen Peroxide Flyer

Hydrogen peroxide is a critical chemical used in many industries as a disinfectant, bleaching agent, or oxidizer, among others. However, in the wrong hands, it can also be weaponized as an explosive precursor chemical, as seen in the attacks in Colombo, Sri Lanka; Brussels, Belgium; and Paris, France.

Given past use and current threat intelligence on the continued use of peroxides as explosive precursor chemicals, CISA reminds law enforcement and any industries that manufacture, use, distribute, or store hydrogen peroxide of the vital need to keep this chemical out of the hands of terrorists.

Chemical mixtures containing at least 35% hydrogen peroxide are regulated under the CFATS program. Learn more in the new Hydrogen Peroxide flyer.

Regardless of regulatory status, all facilities and personnel play an important role in enhancing security measures and restricting access to hydrogen peroxide. Security measures can include:

- Never allow any unauthorized person(s) to purchase, receive, and/or store hydrogen peroxide.
- Review your inventory controls, physical controls, and procedural measures.
- Know your customers.
- Be sure that all hydrogen peroxide is stored in a secure location.
- Notify local authorities if, despite your best efforts, hydrogen peroxide goes missing.

CISA's Bomb Making Materials Awareness Program includes additional resources and awareness tools on identifying and reporting suspicious activity or theft of hydrogen peroxide and other explosive precursor chemicals.

Download the CFATS Hydrogen Peroxide Flyer

CISA Releases New Cyber Essentials Toolkit on Preparing for Cyber Incidents

CISA released its *Cyber Essentials Toolkit, Chapter 6: Your Actions Under Stress* the final

toolkit in a series of six that have been released monthly. This toolkit chapter emphasizes planning and preparing for cyber incidents. Organizations that establish procedures to respond to and recover from an attack strengthen their cyber hygiene. In addition, leaders must train staff to know how to communicate during a crisis.

This chapter contains recommended action oriented approaches for leaders, such as:

- Develop and test incident response and disaster recovery plans,
- Leverage business impact assessments to prioritize resources,
- Learn who to call for help,
- Develop and internal reporting structure for cyber attacks, and
- Leverage in house containment measures.

The Toolkit Chapters are available to all leadership (C suite and IT) roles in the state, local, tribal, and territorial community as well as small and medium sized businesses. Cyber Essentials is a whole of community approach intended to assist in continuously improving the basic cyber hygiene and resilience of the nation.

To learn more about the Cyber Essentials guide or the chapters, visit CISA.gov/Cyber Essentials or email CISAEssentials@cisa.dhs.gov.

Explore the Cyber Essentials Toolkits

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!

- October was #cyber awareness month but #cybersecurity doesn't stop there. See how @CISAgov and @StaySafeOnline protects year-round: cisa.gov/ncsam #BeCyberSmart
- November is #Infrastructure Security Month with @CISAgov! This year's theme is "Time of Transformation" recognizing the changes due to the COVID-19 pandemic. Learn more at https://www.cisa.gov/ismonth
- You know IoT, but do you know #IoMT – the Internet of Medical Things? @CISAgov talks security of the medical world as part of Infrastructure Security Month. https://www.cisa.gov/ismonth
- Read up the new #cyber essentials toolkit from @CISAgov on preparing for #cybersecurity incidents: https://www.cisa.gov/cyber-essentials