CISA Community Bulletin - October 22, 2020

National Cybersecurity Awareness Month 2020 is here!

Led by the Cybersecurity and Infrastructure Security Agency (CISA) and the National Cyber Security Alliance (NCSA), and now in its 17th year, Cyber Month highlights the role individuals play in keeping us all safe online.

With more and more of our lives going virtual, this October has been the ideal time for all Americans to unite behind the 2020 Cyber Month theme—**"Do Your Part. #BeCyberSmart."** This theme encourages each of us to own our role in cybersecurity and emphasizes the necessity of keeping online devices up-to-date and secure.

This October has focused on four key areas:

- **Week 1: If You Connect It, Protect It.** The first week addressed how online devices have impacted our lives, empowering all users to take the right steps to reduce risk.
- **Week 2: Securing Devices at Home and Work.** The second week focused on steps individuals and organizations can take to protect online devices for personal and professional use.
- **Week 3: Securing Internet-Connected Devices in Health Care.** The third week examined health care device use and how consumers and industry can secure these devices.
- **Week 4: The Future of Connected Devices.** The final week will look to the future of smart devices and addresses how technology can change consumers' and business' online experiences.

With so many still working remotely, CISA has simple, straightforward tips on how you can be more safe and secure online.

Visit the Cyber Month resources page to learn how to protect yourself while working, learning, or playing at home, how to stay cybersecure while traveling, how to identify and guard against online fraud and scams, how to enable extra security measures like multi-factor identification, and how to create strong passwords.

As physical security and cybersecurity grow more linked, you can help others stay safer and more secure online.

There are many ways to spread the word this month:

- Meet virtually with your favorite non-profit, charity, or your local PTA, and volunteer to help them enhance their cybersecurity posture. Other options include blogging about cybersecurity, or hosting a webinar on how to enable multi-factor authentication, set up a VPN, and other best practices.

- You don't need any special computer knowledge to get the word out. Actions can be as simple as discussing cybersecurity with friends and family, especially with more vulnerable populations like children, teens, and seniors. Make them aware of the simple steps highlighted in CISA's cybersecurity resources.

- Are you a social media influencer, or do you just enjoy posting and chatting with friends and family on social media? You can also follow CISA on Twitter, LinkedIn, Facebook, Instagram, and YouTube, and use the hashtag ***#BeCyberSmart***, to help promote cybersecurity awareness across your networks.

These are great ways to make your voice heard and show your support for National Cybersecurity Awareness Month. Please email the CISA National Cybersecurity Awareness Month Team with any questions, and check out links to other CISA resources to learn more about good cybersecurity practices you can put to use this October and throughout the year.

Learn More About Cybersecurity Awareness Month

Alerts and Announcements

CISA Releases Resources to Fight Foreign Influence in the 2020 Election Season

"Election Day is in December this year!" Disinformation messages like this one can circulate online during the 2020 election season, with a range of bad actors trying to undermine confidence in our elections and electoral processes. Being savvy consumers of online information – whether on the internet or social media platforms – is an important factor in stopping disinformation from having an impact. Most importantly, we need to seek out trusted sources of information. For elections, that is state and local election officials via their websites and social media.

Foreign actors use a range of tactics that include crafting mis- and disinformation to provoke a response and selectively amplifying domestic information that is divisive. We also need to scrutinize the information we see on social media platforms and the internet. Consider whether the source is authentic and whether sharing that information is useful. Most research suggests

that it is better to ignore mis- and disinformation instead of calling it out. Always taking time to "Think Before You Link" is a key step in the fight against foreign influence.

CISA's Countering Foreign Influence Task Force (CFI TF) offers a range of information on their web page that provides further information to help fight foreign influence, including fact sheets and public service announcements. The newest additions include a graphic novel and a toolkit for state and local officials as well as a Rumor Control page for people with questions about the security of their vote.

Explore the Resources Here

CISA Releases New Cyber Essentials Toolkit on Data Security

CISA released its Cyber Essentials Toolkit, *Chapter 5: Your Data* – the fifth in a series of six toolkits set to be released each month. The Cyber Essentials Toolkit is a set of modules designed to break down the CISA Cyber Essentials into bite-sized actions for IT and C-suite leadership to work toward full implementation of each Cyber Essential. Each chapter focuses on recommended actions to build cyber readiness into the six interrelated aspects of an organizational culture of cyber readiness.

This toolkit chapter emphasizes protecting your information where it is stored, processed, and transmitted. Organizations that secure their data, intellectual property, and other sensitive information strengthen their cyber hygiene. Leaders must have a contingency plan to recover systems and data to avoid loss of information critical to operations.

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

- Learn what information resides on their network,
- Establish regular automated backups,
- Learn how their data is protected,
- Leverage malware protection,
- Leverage protections for backups,
- Learn what is happening on their network.

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 to download the other chapters, visit CISA.gov/Cyber-Essentials or email CISAEssentials@cisa.dhs.gov.

Explore the Five Toolkit Chapters

CISA Enables Emergency Communications During Recent Hurricanes

As hurricane season winds down, CISA reminds readers that its Priority Telecommunications Services (PTS) has been critical to ensuring continuity of emergency communications operations, especially during natural disasters.

Such programs include:

- Government Emergency Telecommunications Service (GETS): Nationwide landline telephone service that provides priority telecommunications
- Wireless Priority Service (WPS): Nationwide wireless telephone service that interoperates with GETS to provide Priority Services via selected commercial wireless service providers
- Telecommunications Service Priority (TSP): Provides priority provisioning and restoration services
- PTS Dialer App: Mobile application that provides a streamlined way of making priority calls

Learn More About Priority Telecommunications Services Here

Events

Partner Webinar: RNSBDC Cybersecurity for Small Businesses

The Rutgers-Newark Small Business Development Center has developed a Small Business Cyber Security Program to provide management teams of established small businesses with cyber security awareness.

Date: November 10, 2020

Time: 3:00 - 4:30 p.m. ET

Register Here

Virtual Chemical Security Seminars

CISA will be hosting three virtual Chemical Security Seminars in December. Agenda and registration details will be posted soon on the Chemical Security Summit webpage.

Date: December 2, 2020, December 9, 2020, and December 16, 2020

Time: 11:00 a.m. - 2:00 p.m. ET

Register Here

Webinar: 5G Impact on Emergency Communications

Join this webinar to learn about 5G capabilities and impacts on public safety communications. Topics include CISA's 5G strategy, how to prepare for emerging technologies, and how to leverage the National Emergency Communications Plan to address emerging technology challenges.

Date: December 9, 2020

Time: 1:00 p.m. ET

Learn More Here

Featured Programs and Resources

From Boots to Bots: Transitioning Veterans into Cybersecurity Careers

According to the National Institute for Standards and Technology (NIST), an estimated four million cybersecurity jobs are vacant across the globe, with an estimated half million open positions in the United States alone.

One available pipeline that often goes underutilized are Veterans transitioning from the armed forces to civilian life. Veterans are a diverse group with multiple skill sets and experiences, and often have cybersecurity related technical skills. However, a 2015 survey found that 40 percent of Veterans found their transition to civilian employment especially difficult.

To learn about and confront the challenges Veterans face during the transition, NIST and the National Initiative for Cybersecurity Education (NICE) held a working group of approximately 40 representatives from government, military, academia, industry, and workforce development organizations.

According to the working group report, cybersecurity is not well known or understood as a career field where military experience can qualify someone for future civilian career opportunities. Participants noted the need for more awareness building efforts to introduce cybersecurity in the early stages of military careers, as well as the need for continual guidance to on how their skills and education map to the NICE Cybersecurity Workforce Framework (NICE Framework).

With approximately 200,000 Veterans transitioning to civilian life each year, there is great opportunity to create clear pathways to cybersecurity careers and fill workforce vacancies. CISA

offers many valuable resources to help Veterans transition out of the military and begin a career in cybersecurity that allows them to make the best use of their skills. These resources include:

- Federal Virtual Training Environment (FedVTE) with over 800 hours of training on dozens of cybersecurity topics, FedVTE provides free online cybersecurity training. Veterans can easily register for an account here.
- Cyber Career Pathways Tool a new and interactive way to explore work roles within the NICE Framework.
- National Initiative for Cybersecurity Careers and Studies (NICCS) a nationwide resource for cybersecurity awareness, education, training, and career opportunities.
- NICCS Education and Training Catalog a comprehensive catalog with over 5,000 cybersecurity related courses.

Now more than ever, the United States needs qualified cybersecurity professionals. To find out more about how to enter this exciting field, Veterans can check out the NICCS Veterans' webpage and download a complete user guide on cybersecurity education and training opportunities.

Visit the NICCS Veterans Webpage

CISA's Cyber Career Pathways Tool featured on *Federal Drive*

On September 15, CISA's Cyber Career Pathways Tool was featured on *Federal Drive*, a Federal News Network podcast. This tool provides a new and interactive way for individuals to identify, build, and navigate a potential cyber career pathway.

Mapped to the NICE Cybersecurity Workforce Framework, the tool lays out the knowledges, skills, and abilities (KSAs) needed to begin, transition, or advance a cyber career. In collaboration with interagency partners, CISA designed the tool to allow users access to the framework and show how they can progress from one position to another. By presenting common and different aspects of each work role in the framework, users can quickly identify the KSAs they will need to acquire to advance their career.

The Cyber Career Pathways Tool depicts the cyber workforce according to five distinct, yet complementary, skill communities. The communities include:

- Information Technology (IT) Skills required to design, build, configure, operate, and maintain IT, networks, and capabilities.
- Cybersecurity Skills required to secure, defend, and preserve data, networks, net centric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place, and taking internal defense actions.
- Cyber Effects Skills required to plan, support, and execute cyber capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace.

- Cyber Intel Skills required to collect, process, analyze, and disseminate information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, and operational activities.

- Cross Functional Roles that are not hands on keyboards, but support and enable effective cyber operations, such as legal, planning, development, and acquisition.

Additionally, the Cyber Career Pathways Tool presents pathways between both the technology and management sides of cybersecurity. The tool visually depicts different skill communities and work roles to see how a person could move from a technical position to a managerial position and vice versa.

The Cyber Career Pathways Tool is accessible to anyone, anywhere, on any device. Get started today at niccs.us cert.gov/workforce development/cyber career pathways. Questions about the tool? Contact education@cisa.dhs.gov.

To hear the interview on *Federal Drive*, visit: www.podcastone.com/federal drive with tom temin.

Explore the New Cyber Career Pathways Tool

Suite of National Risk Management Center Resources

In the past several months, CISA's National Risk Management Center (NRMC) the planning, analysis, and collaboration center that leads the Nation's strategic risk reduction efforts released an array of resources on 5G resilience, electromagnetic pulses, national critical functions, pipeline cybersecurity, and more.

Download and share these new and updated resources to help strengthen the Nation's critical infrastructure security and resilience.

- 5G Basics Infographic: Visually outlines how 5G networks work and the challenges and risks that need to be addressed to help ensure the U.S. can fully benefit from the advantages of 5G connectivity.

- CISA 5G Strategy: Seeks to advance the development and deployment of a secure and resilient 5G infrastructure, one that promotes national security, data integrity, technological innovation, and economic opportunity for the U.S. and its allied partners.

- Electromagnetic Pulse (EMP) Program Status Report: An update on how DHS, through CISA's NRMC and in coordination with interagency partners, is taking key actions including vulnerability assessments and testing and pilot programs to address EMP related vulnerabilities to critical infrastructure.

- National Risk Management Center Fact Sheet: Updated overview of NRMC's mission and vision, it's two divisions, the National Critical Functions (NCF) Framework, and NRMC's priority risk management initiatives.

- National Critical Functions Fact Sheet: An overview of the NCFs, how the NRMC has leveraged the NCF's Framework in response to emerging threats, and the ongoing effort to deepen the understanding of how NCFs operate.

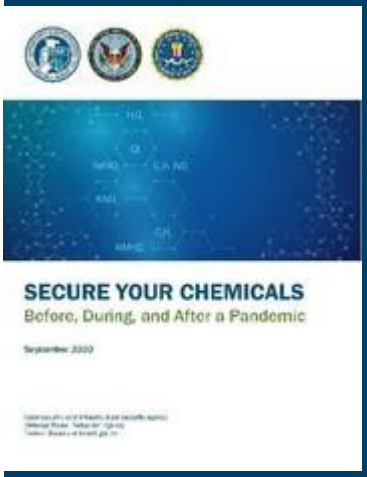
- NCF: Status Update to the Critical Infrastructure Community: A summary of how the NRMC is working to deepen the understanding of critical infrastructure risk and how to add resilience and harden systems in a more targeted, prioritized, and strategic manner.

- Pipeline Cybersecurity Initiative (PCI) Fact Sheet: An overview of the PCI, how the NRMC is working to understand risks to the pipeline systems and operations, and the ongoing effort to build long term resilience.

- Pipeline Cyber Risk Mitigation Infographic: Outlines activities that pipeline owners/operators can undertake to improve their ability to prepare for, respond to, and mitigate against malicious cyber threats.

- Time Guidance for Network Operators, Chief Information Officers, and Chief Information Security Officers: Provides practical information, use cases, and recommendations on how to enhance positioning, navigation, and timing resilience and security practices in enterprise networks and systems.

Explore More NRMC Resources



Global Congress on Chemical Security

CISA recently conducted a webinar on government priorities during a pandemic during which government and industry experts discussed tactical considerations for how to address regulatory inspections and enforcement, delineate and manage essential and critical workers, and identify and respond to emerging criminal activity. The webinar was part of the inaugural webinar series organized by the co implementing partners of the Global Congress on Chemical Security and Emerging Threats.

The Global Congress is an annual conference that convenes a community of international experts that work to counter the threat of chemical and explosive terrorism by non state actors. It is organized and implemented by CISA, INTERPOL, the United States Federal Bureau of Investigation (FBI), and the Defense Threat Reduction Agency (DTRA), in cooperation with the G7 Global Partnership Against the Spread of Weapons and Materials of Mass Destruction.

In conjunction with the webinar series, CISA also released the *Secure Your Chemicals: Before, During, and After a Pandemic* guide. This guidance document a collaborative effort between CISA, FBI, and DTRA provides a set of special considerations so that chemical companies and facilities can maintain critical operations safely and securely before, during, and after a pandemic event.

If you are interested in learning more or becoming a part of the Global Congress network, please contact chemcongress@interpol.int.

Read the Full Chemical Security Guide

Hydrogen Peroxide at Warehouses

Hydrogen peroxide which is used in more than 100 different industries for a variety of purposes is one of the most common chemicals of interest reported by warehouse, storage,

and distribution facilities to CISA under the Chemical Facility Anti Terrorism Standards (CFATS) program.

Given past use and threat intelligence on the continued use of peroxides as explosive precursor chemicals, CISA is reminding law enforcement and industries that manufacture, use, store, or transport hydrogen peroxide of the vital need to keep hydrogen peroxide out of the hands of terrorists.

Learn more about what kind of hydrogen peroxide must be reported under the CFATS program in the Hydrogen Peroxide Flyer.

To learn more on how CFATS applies to warehouse, storage, and distribution facilities and how they can play a role in preventing hazardous chemicals from falling into the hands of potential terrorists, CISA Chemical Security has published a new warehouse industry fact sheet, which can be found on the CFATS Industry Resources webpage.

Learn More About CFATS Industry Resources Here

Active Shooter Preparedness Resources

CISA provides valuable active shooter preparedness resources designed to support risk mitigation activities. Amid the current COVID 19 crisis, CISA adapted new practices by transforming its day long in person workshop format to a condensed two hour virtual webinar to provide stakeholders with insightful active shooter preparedness and planning information.

Specifically, the webinar offers stakeholders options and actions that may be taken before, during, and after an incident to mitigate potential impacts and allow for a quick recovery. Through this virtual training, participants are provided with the fundamentals of developing an emergency action plan for their organizations.

Additionally, CISA offers a variety of instructional videos and resources to include:

- Posters, pocket guides, booklets, fact sheets, and training videos.
- Translated materials in nine different languages identified as the most commonly spoken in the United States.
- Independent Study Course: *IS 907 Active Shooter: What You Can Do*

For more information on how to attend an Active Shooter Preparedness Webinar, contact the CISA Active Shooter Preparedness Program: ASWorkshop@cisa.dhs.gov.

Explore CISA's Active Shooter Resources

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!

- Hurricane season is over – but priority commuications is always important. Check out how @CISAgov keeps you informed during emergencies https://www.cisa.gov/pts

- #BeCyberSmart during National Cybersecurity Awareness Month 2020! Follow @CISAgov & @StaySafeOnline to get the latest updates https://www.cisa.gov/national-cyber-security-awareness-month

- Learn about National Cybersecurity Awareness Month 2020 by following @StaySafeOnline & @CISAgov or visiting https://staysafeonline.org/ & https://www.cisa.gov/national-cyber-security-awareness-month #BeCyberSmart

- #Smallbusiness #cybersecurity: Join a @CISAgov webinar with #Rutgers on Nov 10 to learn about protecting your #SMB https://www.rnsbdc.com/events/cybersecurity-for-small-businesses-webinar-2/

- Veterans: interested in a career in #cybersecurity? @CISAgov & @NIST offer resources, training & more https://niccs.us-cert.gov/training/veterans

- What is @CISAgov National Risk Management Center working on? Everything from #5G to #criticalinfrastructure. Learn more https://www.cisa.gov/nrmc-resources