DEFEND TODAY, SECURE TOMORROW

CISA Community Bulletin August 20, 2020

Get Ready for the 2020 President’s Cup Cybersecurity Competition!

The deadline to register for the second annual President’s Cup Cybersecurity Competition is fast approaching. Sign up today, spots fill up fast!

What is the President's Cup?

The President’s Cup is one of our Nation’s top cybersecurity competitions, challenging participants in three exciting rounds of tasks mapped to the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. The competition aims to find and reward top cyber talent in the Federal government and is open to all members of the Federal workforce and U.S. military.

How Can You Compete?

Participants will apply their skills to real-world scenarios to complete a task or solve a problem. This year, contestants can compete individually or as part of a five-member team. The Individuals Competition will be split into two tracks – Forensics Analysis and Incident Response Work Roles and Exploitation Analysis and Vulnerability Assessment Analysis Work Roles. The Teams Competition will focus on eight in-demand roles.

The top 10 individual finishers and the top five teams will move on to the championship round. Team registration closed August 14; individuals have until August 28 to register.

This year, the President’s Cup will be in a cloud environment, with minimal system requirements for competitors. All you need for the first two qualifying rounds is a supported web browser (Chrome, Firefox, or Edge).

President's Cup 2019 Success!

Started by Executive Order 13870, the first President’s Cup was in 2019, with more than 1,000 registrants and over 200 active teams. Participants engaged in 6,000 combined hours of active challenge participation across 3,300 challenge attempts. An Air Force Academy cadet and a U.S. Army team won last year’s President’s Cup, which Vice President Mike Pence presented to the winners at the White House Eisenhower Executive Office Building.

What Makes a Great Team?

Teams that excelled last year had well-rounded and complementary skill sets. Successful teams also took a divide-and-conquer approach in the qualifying rounds, allowing those with more expertise in certain areas to work on challenges best suited to their talents. Before this year’s competition begins, CISA will release last year’s challenges on GitHub and Docker Hub.

If you’re looking to show off your cyber skills and gain some recognition from your peers and colleagues, mark your calendars and sign up for the President’s Cup Cybersecurity Competition 2020. Visit the 2020 President’s Cup website for more information.

Learn More

Alerts and Announcements

COVID-19 Recovery CISA Tabletop Exercise Package

The Cybersecurity and Infrastructure Security Agency (CISA) is pleased to release the COVID-19 Recovery CISA Tabletop Exercise Package (CTEP). This exercise package was developed in coordination with interagency partners and has been approved by the White House COVID-19 Task Force. This CTEP was developed to assist private sector stakeholders and critical infrastructure owners and operators across all sectors in assessing short-term, intermediate, and long-term recovery and business continuity plans and addressing key questions related to organizational recovery from the COVID-19 pandemic. The CTEP also provides organizations the opportunity to discuss how ongoing recovery efforts are impacted by concurrent response operations to a potential “second wave” of global pandemic infections.

The purpose of this CTEP is to provide critical infrastructure stakeholders and their public safety partners a customizable resource to internally identify and address areas for improvement, threats, issues, and concerns affecting their organization. Within the CTEP is also a compiled list of Federal COVID-19 resources that can assist organizations and their efforts.

If you have questions about the CTEP or supporting documentation, recommendations for improvement, information on available CTEP products, or are interested in tailored exercises for your specific program please contact: CISA.Exercises@cisa.dhs.gov or you can review the fact sheet.

Learn More Here

Progress Report in the Fight Against Botnet Attacks

The Trump administration has made substantial progress in improving the resilience of the Internet ecosystem and reducing the threat of botnets. In a report released in July, the Department of Commerce and the Department of Homeland Security (DHS) documented more than 50 success stories in the drive to counter botnet threats, building upon work started two years ago with the Botnet Report and Road Map. Government and industry are working hard to put a stop to these dangerous attacks.

Here are a few of the milestone achievements:

- The National Institute of Standards and Technology (NIST) published draft guidance for Internet of Things (IoT) device manufacturers, which defines a core baseline of cybersecurity capabilities that manufacturers can voluntarily adopt for IoT devices they produce.

- The National Telecommunications and Information Administration (NTIA) published its first set of community-drafted documents to offer guidance around the practice of a software bill of materials.

- DHS hosted the first annual President's Cup Cybersecurity Competition—an interagency effort to identify, challenge, and reward the government's best personnel supporting cybersecurity and cyber excellence.

- The Council to Secure the Digital Economy, representing the information and communications technology industry, published an international anti-botnet guide and expert guidance to industry and government on securing new IoT devices.

- The Global Cyber Alliance published cybersecurity toolkits for small businesses and election security, and continued adding to its suite of free cybersecurity tools.

Stopping botnet threats is an ecosystem-wide challenge that will take significant cooperation over time to accomplish. The Botnet Report and Road Map emphasized that the U.S. government cannot and should not attack the botnet problem alone. This report demonstrates the commitment across government and industry to continue to build increased security and resilience to protect U.S. networks.

View the Full Report Here

CFATS Extended for Three Years

On July 22, 2020, President Trump signed S. 4148 to extend the Chemical Facility Anti-Terrorism Standards (CFATS) statute to July 27, 2023.

This three-year extension provides much-needed stability, not only for CISA as we continue to make programmatic enhancements and strategic planning decisions for the CFATS program, but also for our chemical security stakeholders. The extension provides stakeholders with the certainty needed to continue to plan for and invest in CFATS-related security measures at high-risk chemical facilities.

CISA looks forward to the next steps in the CFATS journey as we continue to enhance the security of our Nation's highest-risk chemical infrastructure and make our communities more secure.

Learn More Here

Events

Partner Webinar: Cybersecurity and Business Resilience

This workshop, hosted by the U.S. Small Business Association, will talk about cybersecurity and assessing risk, how to protect against cyber attacks, natural disasters and assessing risk, and how to protect against natural disasters for business resiliency.

Date: August 27, 2020

Time: 4:30 p.m. ET

Register Here

Partner Webinar: Assembling Your Data Security Toolbox

The National Cybersecurity Alliance is hosting a webinar on key tools for data security. It will cover some essential elements business owners can leverage, including specific tools to help improve efficiency and secure sensitive data.

Date: September 8, 2020

Time: 2:00 p.m. ET

Register Here

Webinar: How to Turn Evaluations into Real-world Communications Improvements

CISA is hosting a webinar on implementing the National Emergency Communications Plan (NECP), convening approximately 200 CISA stakeholders.

Date: September 17, 2020

Time: 1:00 p.m. ET

Learn More Here

Featured Programs and Resources

Introducing the New CISA Services Catalog

CISA is excited to announce a fantastic new tool: The CISA Services Catalog!

The CISA Services Catalog is as much an invitation to partner with CISA as it is a library of services. The Catalog is a single touch point for anyone interested in CISA services, and its interactive elements allow users to quickly and intuitively filter down to those services that best fit their capabilities and challenges.

CISA thinks of partnership as a bi directional service, and stakeholder partnership allows CISA to better tailor products, services, and engagements to meet stakeholders' most immediate priorities and capabilities. It gives partners a seat at the table to join CISA in better understanding stakeholders' unique risk environments, and to identify and implement solutions. Partnership is the essence of collective defense, and this approach continues to yield results.

Some key features of the CISA Services Catalog:

- Maximized convenience and seamless user experience;
- Directs users to the appropriate contact for each service;
- Assigns maturity levels to CISA services, part of CISA's ongoing efforts to create stakeholder roadmaps to guide users toward higher tiers of resilience

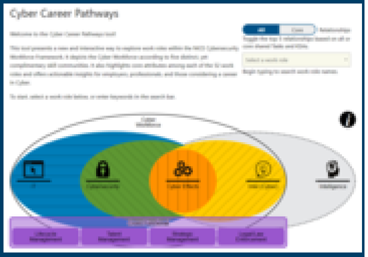
Navigating the CISA Services Catalog gives users a sense of how cybersecurity, infrastructure security and emergency communications intersect to form a holistic approach to risk management and resilience.

This Catalog is the first edition of many to come. As always, CISA welcomes feedback.

For questions about the services featured in the CISA Services Catalog or for questions about the Catalog itself, please email Central@cisa.gov.

Download the Full Catalog

CISA Releases New Career Pathways Tool



On August 5, CISA released the Cyber Career Pathways Tool! Please share this tool with individuals looking to start a career in cybersecurity, considering a change within the cyber field, college students, managers, and workforce development specialists interested in the cyber ecosystem.

This tool will help individuals identify, build, and navigate a potential cyber career pathway by increasing understanding of the knowledge, skills, and abilities needed to begin, transition, or advance a cyber career.

The Cyber Career Pathways Tool presents a new and interactive way to explore work roles within the NICE Cybersecurity Workforce Framework. It depicts the cyber workforce as five distinct, yet complimentary skill communities. It also highlights core attributes among each of the 52 work roles and offers actionable insights for employers, professionals, and individuals considering a career in cyber.

You can find this tool on CISA's National Initiative for Cybersecurity Careers and Studies (NICCS) website in addition to other tools and resources for current and future cybersecurity professionals. The Cyber Careers Pathway Tool was created and is maintained in partnership with the Interagency Federal Cyber Career Pathways Working Group, led by CISA, the Department of Defense, and the Department of Veterans Affairs.

Explore the New Tool

CISA Develops PSAP Ransomware Poster for Stakeholders

CISA recently released a poster that provides comprehensive information to stakeholders on how to protect public safety answering points (PSAPs) and emergency communications centers (ECCs) from ransomware. The poster contains space to fill in agency specific resources, providing stakeholders with a customized product.

The poster defines ransomware and provides information on:

- Why PSAPs and ECCs may be targeted,
- Specific recommendations on how to protect PSAPs and ECCs, and
- Contact information for agency specific resources and federal partners.

The customized posters will be distributed via Statewide Interoperability Coordinators (SWIC) to state 9 1 1 Administrators, PSAPs, and 9 1 1 dispatch operators. To receive an agency specific customized PSAP Ransomware Poster, SWICs can contact their CISA Emergency Communications Coordinator or email ecd@cisa.dhs.gov.

Download the PSAP Ransomware Poster

CISA and Partners Release Encryption Key Management Fact Sheet

Public safety voice communications are continually at risk of being intercepted by unauthorized personnel. Vulnerability to radio transmissions can jeopardize tactical operations, put law enforcement officers and other responders at risk, and compromise personal identifiable information. When public safety agencies make the decision to encrypt any or all transmissions, effective encryption key management is paramount.

To help agencies understand and effectively manage encryption keys, CISA, in collaboration with SAFECOM, National Council of Statewide Interoperability Coordinators, and the Federal Partnership for Interoperable Communications, developed the Encryption Key Management Fact Sheet.

Public safety organizations can leverage the Fact Sheet's information to familiarize themselves with the many aspects of encryption key management. Specifically, the document:

- Provides an overview of some of the different types of encryption and how to obtain encryption keys,
- Guides public safety organizations on whether to encrypt their land mobile radio systems, and
- Offers information on how public safety organizations can best manage encryption keys.

Learn More About SAFECOM Here

Pipeline Cyber Risk Mitigation Infographic

CISA is pleased to announce the publication of the Pipeline Cyber Risk Mitigation Infographic.

Developed in coordination with the Transportation Security Administration, this infographic outlines activities that pipeline owners/operators can undertake to improve their ability to prepare for, respond to, and mitigate against malicious cyber threats.

Download and share this resource on the importance of pipeline infrastructure resilience and check out CISA’s blog article, Working Together to Strengthen Pipeline Systems, for more information.

Download the Pipeline Cyber Risk Mitigration Infographic

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

New Tools, Capabilities, and Resources Launched on SchoolSafety.gov

In June, the Federal School Safety Clearinghouse launched the State Information Sharing Tool on SchoolSafety.gov to better address the needs of the K 12 academic community at the state level.

The tool is state focused and designed to provide the academic community access to state specific school safety information, including programs, points of contact, resources, grant and funding opportunities, and key engagement opportunities. It also aims to enhance collaboration between state school safety leaders and the Federal School Safety Clearinghouse by establishing sustained engagement platform.

The School Safety Task Force also collaborated with CISA in developing two cybersecurity guidance documents for members of the K 12 academic community in a COVID 19 environment:

- Cybersecurity Recommendations for K 12 Schools Using Video Conferencing Tools and Online Platforms designed for K 12 district administrators and IT team members from a network protection perspective.
- CISA Cybersecurity Tip Sheet for Schools Using Video Conferencing designed for K 12 parents and teachers around best practices and guidance for distance based learning.

In addition, the Federal School Safety Clearinghouse created a webpage, recently revamped and released at the end of July, COVID 19 Resources for Schools, on the SchoolSafety.gov website to provide one stop access to key COVID 19 guidelines and other resources for the K 12 academic community from across the Federal School Safety Commission interagency partners (Departments of Homeland Security, Education, Health & Human Services, and Justice).

Explore the State Information Sharing Tool

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!

- Learn all about the new National Emergency Communications Plan (NECP) on an upcoming @CISAgov webinar https://go.usa.gov/xfuF6

- Registration is open for the 2nd annual President's Cup Cybersecurity Competition to reward the best cyber talent in the Federal government! To compete, visit https://go.usa.gov/xfuFF

- Countering Botnets: read the new @CISAgov & @CommerceGov report on stopping these dangerous attacks https://go.usa.gov/xfuFM

- Introducing the new CISA Services Catalog – all of @CISAgov, all in one place, all the resources you need. https://go.usa.gov/xfuFt

- CISA is now on Instagram! Follow @CISAgov for updates on #CyberSecurity programs, priorities, and threats: instagram.com/cisagov