CISA Community Bulletin - March 23, 2021

CISA Releases First International Strategy, CISA Global

The Cybersecurity and Infrastructure Security Agency (CISA) is proud to release its first-ever international strategy, entitled CISA Global. Today's globally interconnected world presents a wide array of serious risks and threats to critical infrastructure, systems, assets, functions, and citizens.

Working with foreign partners builds CISA's capacity and ability to defend against cyber incidents, enhance the security and resilience of critical infrastructure, identify and address the most significant risks to the national critical functions, and provide seamless and secure emergency communications.

CISA will leverage its global network to strengthen partner capacity and build a better, collective practice posture and response to urgent threats that are critical to U.S. national security interests.

As such, CISA Global describes CISA's international vision and commits the agency to four goals:

1. Advancing operational cooperation;

2. Building partner capacity;

3. Strengthening collaboration through stakeholder engagement and outreach; and

4. Shaping the global policy ecosystem.

CISA is committed to promoting an open, interoperable, reliable and secure interconnected world within a global, operational, and policy environment where network defenders and risk managers can collectively prevent and mitigate threats to critical

infrastructure. We invite our global partners to join us in defending today and to securing tomorrow.

Alerts & Announcements

CISA Partners Awarded for Excellence in Information Sharing

The “Best of HISN” Awards included three Department of Homeland Security (DHS) community partners for 2020: Transportation Security Administration Intelligence (TSA-Intel), The Aviation Domain Intelligence and Integration Cell (ADIAC), and the U.S. National Response Team (NRT).

CISA’s annual Best of HISN Awards commemorate teams for their outstanding work completed within the information sharing realm. With all the challenges in 2020, CISA is proud to both congratulate this year’s winners and to have witnessed the hard work and ingenuity that these partners employed in order to address important and challenging threats.

Learn More About HSIN Here

CISA Releases Third NECP Spotlight: Making the Most of Next Generation 9-1-1

CISA has released its support of the National Emergency Communications Plan (NECP), the Nation’s strategic plan for strengthening and enhancing emergency communications. The public safety community has been given an array of new capabilities thanks to the influx of rapidly evolving technologies. One of these critical technologies is Next Generation 9-1-1 (NG911), a multifaceted upgrade to the traditional 911 analog systems where emergency communication centers are updated to a digital or Internet-Protocol based 911 system.

The NECP advocates that public safety organizations continually evaluate and implement programs to keep pace with technological advancements. This spotlight looks at the NG911 implementation in North Carolina, Tennessee, and Virginia, and shows how the NECP recommendations promote the adoption of new technologies to meet mission-critical needs.

Learn More About NECP Here

Explore CISA’s Chemical Sector Security Awareness Training Course

CISA is pleased to announce the successful launch of the Chemical Sector Security Awareness Training (CSSAT) course. The CSSAT course is a voluntary foundational course for private sector stakeholders that provides knowledge of security awareness at a chemical facility. Participants will be able to identify their roles and responsibilities

regarding their facility's security posture. This will help to identify possible activities and behaviors that could potentially pose a security threat to them and their facility.

Owners and operators are encouraged to include the CSSAT into their facility training plans and implement the security practices appropriate for the facility's risk profile, operational processes, and business environments.

The web-based course is available through the FEMA Center for Domestic Preparedness (CDP) learning management system. Users will need to obtain a FEMA Student Identification Number (SID) to be able to access the course.

Learn More About CDP Training Here

Events

Webinar: K-12 Education Leaders' Guide to Ransomware

CISA is co-hosting a webinar with the National Cybersecurity Alliance on ransomware. Cybersecurity experts from industry and government will discuss the steps K-12 schools can take to prevent, respond to and recover from ransomware attacks.

Date: March 24, 2021

Time: 2:00 p.m. ET

Learn More Here

Partner Webinar: IT Infrastructure Series

This workshop, hosted by Government CIO Magazine, will consider new security blueprints and the mindset shifts required to boost federal IT infrastructure security.

Date: March 31, 2021

Time: 11:00 a.m. ET

Learn More Here

Partner Webinar: Secure Your Business with Proper Identity Management

In honor of Identity Management Day, join NCSA for a webinar on proper identity management and a look at why it is essential to maintaining your organization's Security Triangle.

Date: April 13, 2021

Time: 2:00 p.m. ET

Learn More Here

Featured Programs and Resources

CISA Provides Resources for K-12 Partners

CISA has seen a marked increase in ransomware attacks on vulnerable school systems. In a joint security alert published on December 10, CISA, the FBI, and the Multi State Information Sharing and Analysis Center (MS ISAC) detailed an increasing amount of cyberattacks targeting K 12 schools. These attacks have led to ransomware infections, data theft, and the disruption of remote learning services.

In May 2019, Baltimore City Government made national news when it was infected by the RobbinHood ransomware attack that took offline nearly 10,000 city computers for weeks. Then on November 25, 2020, not more than a year a half later, Baltimore City's closest neighbor, Baltimore County, Public Schools system suffered a ransomware attack. This incident shows that even with a national spotlight on cyber threats to critical systems, K 12 partners are still vulnerable to ransomware.

CISA has seen a marked increase in ransomware attacks on vulnerable school systems. In a joint security alert published on December 10, CISA, the FBI, and the Multi State Information Sharing and Analysis Center (MS ISAC) detailed an increasing amount of cyberattacks targeting K 12 schools. These attacks have led to ransomware infections, data theft, and the disruption of remote learning services.

According to the alert, "as of December 2020, the FBI, CISA, and MS ISAC continue to receive reports from K 12 educational institutions about the disruption of distance learning efforts by cyber actors… Cyber actors likely view schools as targets of opportunity and these types of attacks are expected to continue through the 2020/2021 academic year." Education leaders are uniquely positioned to help their schools learn how to prevent, respond to, and recover from ransomware attacks, and CISA is here to assist. Beyond basic cyber hygiene tips, CISA offers a wide variety of resources designed to help K 12 partners improve their cybersecurity posture.

To start, check out these new CISA tools:

- Ransomware Reference Materials for K 12 School IT Staff Best practices for schools and school district cybersecurity managers, system administrators, and other technical staff to enhance their school and district's security posture during distance and hybrid learning.
- Ransomware Reference Materials for Parents, Teachers, and K 12 School Administrators Best practices for non technical staff and parents and teachers to enhance a school's security poster during distance and hybrid learning conditions.
- Ransomware Reference Materials for K 12 Students Cybersecurity tips to help students stay safe and do their part in keeping their school's network secure while learning remotely.

CISA's STOP.THINK.CONNECT.™ Toolkit provides valuable information, tailored to parents and educators, on how to talk to kids about online security and privacy. CISA has

other useful tools for students in grades K 8 and 9 12 on simple best practices for safeguarding their data. CISA also has tools for K 12 teachers, focusing on how to integrate good cybersecurity practices into the classroom.

For more information on CISA's ransomware efforts and how you can participate, please visit www.cisa.gov/ransomware.

CISA Releases New Courses

- Sign up for Incident Response Training: Identify, Mitigate, Recover (IMR) series. CISA has developed no cost cybersecurity incident response training for government employees and contractors across Federal, State, Local, Tribal, and Territorial government, and is open to educational and critical infrastructure partners.
- Sign up for Continuous Diagnostics and Mitigation (CDM). This training intended for anyone who monitors, manages, and oversees controls on their information systems, such as ISSOs, CDM POCs, ISSMs, and others who report measurements and/or metrics.
- Sign up for Industrial Control Systems (ICS). CISA is offering free training with a focus on Critical Infrastructure owners/operators designed to reduce cybersecurity risks to critical infrastructure and encourage cooperation between CISA and the private sector.
- CISA's Cybersecurity Education Training Assistance Program (CETAP) equips K 12 teachers with cybersecurity curricula and education tools.

CISA's STOP.THINK.CONNECT.™ Toolkit provides valuable information, tailored to parents and educators, on how to talk to kids about online security and privacy. CISA has other useful tools for students in grades K 8 and 9 12 on simple best practices for safeguarding their data. CISA also has tools for K 12 teachers, focusing on how to integrate good cybersecurity practices into the classroom.

For more information on CISA's ransomware efforts and how you can participate, please visit www.cisa.gov/ransomware.

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!

- @CISAgov awards UT San Antonio grant to develop pilot program for SLTT governments #criticalinfrastructure cisa.gov/news/2021/03/08/university-texas-san-antonio-receives-cisa-grant-develop-pilot-program-state-local

- Check out the new ransomware resources for K-12 remote learning education. Visit cisa.gov/ransomware-reference-materials-k-12

- Introducing CISA Global – the first ever @CISAgov international strategy cisa.gov/global