CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

COMMUNITY BULLETIN

Announcements

CISA Releases New Resources in Response to Increasing Geopolitical Tensions

Earlier this month, the Cybersecurity and Infrastructure Security Agency (CISA) published several products in response to an increase in geopolitical tensions and threats, including potential malicious cyber and physical activity from Iran and its proxies.

The new resources include:

- An Increased Geopolitical Tensions and Threats CISA Insights Bulletin strongly urging organizations to assess and take action to strengthen their basic cyber and physical defenses and protect against this potential threat.
- An Enhanced Chemical Security CISA Insights bulletin urging facilities with chemicals of interest — whether tiered or untiered under the Chemical Facility Anti-Terrorism Standards (CFATS) program — to consider enhanced security measures to decrease the likelihood of a successful attack. Read the both bulletins on the CISA Insights webpage.
- An Activity Alert (AA20-006A) reminding members of the critical infrastructure community of malicious cyber and physical activities that could be directed at United States industries and government agencies. Focused on potential Iranian offensive cyber activity, the Activity Alert provides details of potential threats, historical accounts of their malicious activity, and recommended mitigation actions and resources to assist in the defense of our Nation's critical infrastructure.

CISA continues to work closely with interagency and private sector partners to assess threats, mitigate risk, and increase the cost to malicious actors.

CISA Releases Emergency Directive and Activity Alert on Critical Microsoft Vulnerabilities

CISA has released an Emergency Directive and Activity Alert addressing critical vulnerabilities affecting Windows CryptoAPI and Windows Remote Desktop Protocol server and client. A remote attacker could exploit these vulnerabilities to decrypt, modify, or inject data on user connections.

Although Emergency Directive 20-02 applies only to certain Executive Branch departments and agencies, CISA strongly recommends state and local governments, the private sector, and others also patch these critical vulnerabilities as soon as possible.

Review the following resources for more information:

- Activity Alert AA20-014A: Critical Vulnerabilities in Microsoft Windows Operating Systems
- Emergency Directive 20-02: Mitigate Windows Vulnerabilities from January 2020 Patch Tuesday
- CISA Blog: Windows Vulnerabilities That Require Immediate Attention
- National Security Agency Cybersecurity Advisory

National 911 Program Launches New Next Generation 911 Self-Assessment Tool

The National 911 Program released a new self-assessment tool for administrators in emergency communication centers and public safety answering points. The tool helps administrators evaluate a system's Next Generation 911 (NG911) maturity state.

NG911 is an update to the existing 911 service infrastructure to improve public emergency communications services. As state offices, 911 authorities, emergency communication centers, and public safety answering points work toward implementing NG911 networks, assessing progress can pose challenges.

Now available online at 911.gov, the new self-assessment tool is built on feedback received from government, industry, and academia stakeholders. It compiles respondents' answers and categorizes their 911 system into one of five maturity states for NG911 implementation.

The results are intended to help agency leadership to: (1) document their 911 system's current functions and capabilities; (2) strengthen their understanding of NG911 elements; and (3) help outline next steps to transition their system into a fully integrated NG911 network.

About the National 911 Program

The National 911 Program was created by Congress to provide information to improve the 911 system and to coordinate information sharing and activities among federal agencies and the 911 community. The program fulfills its mission by developing and distributing a variety of tools and resources for the Nation's 911 stakeholders. The National 911 Program is housed within the Office of Emergency Medical Services at the U.S. Department of Transportation's National Highway Traffic Safety Administration.

For any questions about the NG911 Self-Assessment Tool, please contact ng911wg@hq.dhs.gov, or access the website: https://www.cisa.gov/news/2019/12/06/new-self-assessment-tool-helps-identify-next-generation-911-readiness.

CISA Releases New Products to Help Communities Recognize Suspicious Items

CISA has released two new products to assist individuals in identifying suspicious items with the goal of reducing improvised explosive device (IED) attacks. Criminals or terrorists sometimes conceal IEDs in backpacks, suitcases, packages, and other common items.

CISA's outreach comes at a time when the nation faces numerous threats, including a heightened fear of attacks on U.S. assets from Iran. Everyone has a role to play in security by being acutely aware of an unattended item that may seem out of the ordinary and thus pose a possible threat.

The outreach products, a poster and postcard that are easily accessible online, use easy-to-remember acronyms to highlight important lessons. These lessons teach individuals how to quickly recognize and respond to suspicious items.

Additional details can be found in the poster and postcard and at the Office for Bombing Prevention's webpage focused on recognizing bomb threats. Take a free, online training to learn how to respond to suspicious behavior or items, guard against bomb threats, and safeguard precursor chemicals to IEDs at https://cdp.dhs.gov/obp.

Events

Webinar: Smart Cities

The city of the future is the city that's connected. Municipalities across the United States are utilizing "smart" IT systems to improve the daily lives of residents. For city leaders and constituents, these increasingly complex technologies present benefits, but also risks.

Join this webinar, co-hosted by the Regional Consortium Coordinating Council and the State, Local, Tribal, and Territorial Government Coordinating Council, to hear directly from city government and industry leaders about the opportunities and vulnerabilities related to Smart Cities technologies – and how everyone can participate in cities of the future.

- **Date**: Thursday, January 30, 2020
- **Time**: 1:00-2:00 p.m. ET
- **Registration**: https://cisadhs.zoomgov.com/webinar/register/WN_3O3zDYkpTNWNvqXitMd3cA

NICE Webinar: Learning Principles for Cybersecurity Practice

What are the "cybersecurity principles" that all students and workers should learn? The National Institute of Standards and Technology (NIST) is holding a webinar as part of its National Initiative for Cybersecurity Education (NICE) that explores this question.

The webinar will begin a dialogue about reaching consensus for a common set of cybersecurity principles to be communicated, acquired, and practiced by learners of all ages – from children and youth to adults – and workers at every stage of their career – from entry- to advanced-levels.

Learn more and register on the NIST events page.

- **Date**: Wednesday, January 29, 2020

- **Time**: 2:00-3:00 p.m. ET
- **Registration**: https://www.nist.gov/news-events/events/2020/01/nice-webinar-learning-principles-cybersecurity-practice

---

Featured Resource

The CISA Government Emergency Telecommunications Service

Supporting CISA National Security and Emergency Preparedness Users

The Department of Defense's National Communications System established the Government Emergency Telecommunications Service (GETS) in 1994 to meet White House requirements for a survivable, interoperable, nationwide voice band service for authorized users engaged in national security and emergency preparedness (NS/EP) missions.

With specialized processing in local and long-distance public telephone networks, GETS provides NS/EP users a high rate of call completion during network congestion or outages arising from natural or manmade disasters. GETS is complemented by the Wireless Priority Service (WPS), which provides priority for cellular calls, and by Telecommunications Service Priority (TSP), which provides priority restoration and expedited installation for vital voice and data circuits. WPS and TSP are provided in accordance with the Federal Communications Commission (FCC) Report and Orders.

Following three years of groundbreaking design and implementation, the first GETS call was completed one minute after midnight on September 30, 1994, between Richmond, Va., and Potomac, Md. This successful call marked GETS' limited priority capability implementation in the long-distance networks. One year later, Lieutenant General Albert J. Edmonds, Director of the Defense Information Systems Agency and National Communications System Manager, placed the first GETS call to the White House. This was the first GETS call made to achieve initial operational capability (IOC) — in accordance with White House tasking. In September 2001, GETS achieved full operational capability (FOC), providing a nationwide end-to-end priority service including the Local Exchange Carriers.

Since its inception, first responders have relied on GETS during emergencies. The 1995 earthquake in Kobe, Japan was the first natural disaster where GETS assisted in emergency response efforts. Since then, GETS has been used for domestic and international priority calling during a variety of natural and manmade disasters.

During the terrorist attacks on September 11, 2001, more than 18,000 GETS calls were made at a 95% call completion rate, allowing response teams to communicate on decisions, support needs, and recovery efforts. GETS users also distributed information and coordinated activities among government officials and emergency personnel during the destructive Hurricanes Katrina, Rita, and Wilma that hit the Gulf Coast states in 2005.

GETS is also available for priority communications involving national level events. The 2002 Salt Lake City Winter Olympics; the 2013 Boston Marathon bombing; the 2009, 2013, and 2017 presidential inaugurations; along with the 2018 California Wildfires and Hurricane Dorian in 2019 are just a few of many occasions where GETS was available for emergency communications to overcome network congestion.

GETS continues to support officials from federal, state, tribal, and local governments, U.S. territories, and other qualified NS/EP industry and non-profit organizations. GETS subscribers are in all U.S. states and territories, military installations, and U.S. embassies worldwide.

Now, more than ever, GETS subscribers are ready for any situation, big or small, when they need to complete their critical calls.

To access this document on the web, please visit: https://www.dhs.gov/safecom/blog/2020/01/06/gets-supports-cisa-national-security-and-emergency-preparedness-users.

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!

- As geopolitical tensions increase, what's your organization doing to prepare? @CISAgov has resources on how to protect against potential threats from Iran and its proxies. https://www.cisa.gov/insights #cyber #Iran
- @CISAgov just released an activity alert on critical Microsoft vulnerabilities. Check out https://www.us-cert.gov/ncas/alerts/aa20-014a for more info. #cybersecurity #MicrosoftUpdates
- Can you ID a suspicious package? @CISAgov has a guide to show you how. https://www.cisa.gov/publication/unattended-vs-suspicious-item-postcard-and-poster #safetyawareness #bombthreats
- Cities are increasingly utilizing "smart" IT systems – but what are the risks? Join @CISAgov on Jan. 30 for a webinar on Smart Cities: https://cisadhs.zoomgov.com/webinar/register/WN_3O3zDYkpTNWNvqXitMd3cA #smartcities #cyber
- What are the cybersecurity principles that all students and workers should learn? @usnistgov is holding a webinar on Jan 29 about just that. Register at https://www.nist.gov/news-events/events/2020/01/nice-webinar-learning-principles-cybersecurity-practice #cybersecurity

---

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.
