DEFEND TODAY, SECURE TOMORROW

CISA Community Bulletin - July 15, 2021

StopRansomware.gov Launches Today

StopRansomware.gov is a collaborative initiative by the federal government to make it easier for stakeholders across the private and public sectors to find free, authoritative information, resources, and tools that can help prevent and mitigate ransomware attacks in the United States.

StopRansomware.gov brings together resources from across the federal government into one location, to give organizations, the general public, federal, state, local, tribal and territorial (SLTT) governments, and critical infrastructure organizations a one-stop-shop to learn how to reduce their ransomware risk. The content is sourced from agencies including the Department of Health and Human Services, the Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), National Institute of Standards and Technology (NIST), U.S. Secret Service (USSS) and other governmental partners. The site is a whole-of-government resource hub.

Learn More About Ransomware Here

Alerts & Announcements

Statement from New CISA Director, Jen Easterly

CISA Director Jen Easterly released the following statement after being sworn in on July 13:

“I am incredibly honored and humbled to join the team at CISA. I have admired the agency from afar as the organization has grown over the past several years, and seen firsthand how its guidance, insight and resources can benefit public and private sector partners as part of our collective defense to build a more resilient nation."

“I thank President Biden for putting his faith in me to lead this organization, and the Senate for confirming me for this role. I'm also very grateful for Acting Director Brandon Wales and all of CISA’s leadership for so effectively shepherding CISA through an incredibly challenging and dynamic eight months. I look forward to building on their excellent work to continue evolving the strategy, workforce, and culture of CISA to be the world’s premier cyber and infrastructure defense agency and achieve our vision of secure and resilient infrastructure for the American people.”

Director Easterly was confirmed by the Senate by unanimous consent on July 12, 2021. Prior to coming to CISA, she was the head of Firm Resilience and the Fusion Resilience Center at Morgan Stanley, responsible for ensuring preparedness and response to business-disrupting operational incidents and risks. Director Easterly served as Special Assistant to the President and Senior Director for Counterterrorism in the Obama Administration, and earlier as the Executive Assistant to National Security Advisor Condoleezza Rice in the George W. Bush Administration.

Learn More About the New Director Here

CISA and FBI Launch "Operation Flashpoint" to Raise Awareness about Bomb Attack Prevention

CISA and the FBI announced a new pilot program called “Operation Flashpoint” tobuild awareness in communities across the U.S. about how to prevent bomb attacks.

At the pilot’s launch in Clinton, Miss., CISA and FBI officials highlighted the threat posed by domestic violent extremists and others who can build improvised explosive devices (IEDs) from common household items found at retail stores across the country. Approximately 250,000 businesses in the U.S. sell, use or distribute materials that can be used to build bombs.

IEDs pose a significant threat in the U.S. In 2020 alone, there were 2,061 total bomb threat, suspicious package, and device-related incidents across the nation. Major bombings can cause mass casualty events and cost hundreds of millions of dollars. The 90-day Operation Flashpoint pilot, which will include events in other cities including Columbia, S.C.; Louisville, Ky.; and Orlando/Tampa, Fla., encourages businesses and the public to voluntarily report suspicious activities, such as buying large amounts of chemicals and materials (or a combination of these) that can be used to build bombs.

“Operation Flashpoint is a major milestone in implementing U.S. policy to thwart bomb threats,” said Dr. David Mussington, Executive Assistant Director for CISA’s Infrastructure Security Division. “It shows the strong unity in the federal government, between the Department of Justice and the Department of Homeland Security, to safeguard citizens and critical infrastructure.”

The pilot seeks to reduce the threat of IED attacks by helping businesses detect the illegitimate acquisition, theft, or diversion of dangerous chemicals, and by encouraging retailers to report suspicious activity by calling 1-855-TELL-FBI (1-855-835-5324). Follow #OperationFlashpoint through the summer on Twitter: @CISAgov and @CISAInfraSec.

Learn More About Operation Flashpoint Here

CISA Releases New Guidance for Screening Patrons at Public Venues

Developed in coordination with Commercial Facilities Sector stakeholders, the *Public Venue Security Screening Guide* offers options to consider when using screening procedures at public venues for a variety of events: concerts, sporting events, fairs, festivals, conventions, theme parks, and other events or functions where Americans gather.

The *Public Venue Security Screening Guide* is for any organization or venue that uses screening procedures within the Commercial Facilities Sector and its subsectors: Gaming, Lodging, Media & Entertainment, Outdoor Events, Public Assembly, Sports Leagues, Real Estate, or Retail.

This product is the third in a series of document updates that includes the *Public Venue Bag Search Procedures Guide* (2019) and the *Public Venue Credentialing Guide* (2020).

Stakeholders may contact the CISA Commercial Facilities Sector Management Team at CFSTeam@cisa.dhs.gov with any questions.

Learn More About Public Venue Security Screening Here

CISA Hosts Webinar on Inclusive Governance Structures

On May 26, CISA presented the Implementing the National Emergency Communications Plan (NECP) webinar, “It Takes a Village: Leveraging the Whole Community to Make Critical Emergency Communications Decisions.” The webinar provided information on how the NECP advocates for inclusive governance bodies when developing strategic, operational, and contingency plans related to emergency communications.

While emergency communications governance often involves traditional disciplines or sectors, capabilities can be improved with the collaboration of representatives from additional systems or response functions (e.g., chief information officers, elected officials, public works, public health, utilities, natural resources or parks and recreation, and building inspectors).

The webinar featured two use cases. The first was on tribal emergency communications decision-making groups presented by representatives from the Mille Lacs Band of Ojibwe and the state of Minnesota. In addition, a representative from the Mid-America Regional Council shared best practices and lessons learned from integrating cyber equities into strategic planning for effective emergency communications. More than 200 participants attended to learn about expanding the membership of governance structures and the importance of collaboration between jurisdictions, agencies, and organizations across the Emergency Communications ecosystem.

For a copy of the slide deck, which includes a list of related resources, please send a request to necp@cisa.dhs.gov.

Learn More About Inclusive Governance Structures Here

New Cybersecurity Requirements for Critical Pipeline Owners and Operators

On May 27, the Department of Homeland Security's (DHS) Transportation Security Administration (TSA) announced a new Security Directive that will enable DHS to better identify, protect against, and respond to threats to critical companies in the pipeline sector. The Security Directive will require critical pipeline owners and operators to report confirmed and potential cybersecurity incidents to CISA and to designate a Cybersecurity Coordinator to be available 24/7. This Security Directive highlights the critical role CISA plays as the nation's leader in cyber defense.

Learn More About Pipeline Cybersecurity Requirements Here

Events

Partner Webinar: Cyber Awareness Training for Your Business

Join the Small Business Administration (SBA) for a webinar that will focus

Partner Webinar:

Assessment Policies, Strategies, and Practices for Cybersecurity Hiring

Webinar: Cybersecurity Community Capacity Building

Join CISA for a webinar to explore models for on the latest online threats such as phishing, malware, and ransomware.

Date: July 21, 2021

Time: 12:00 p.m. ET

Learn More Here

Join the National Initiative for Cybersecurity Education (NICE) for a webinar on developing assessment-based approaches to identifying and hiring cybersecurity talent.

Date: July 27, 2021

Time: 1:30 p.m. ET

Learn More Here

building resilient cyber systems, case studies on public-private information sharing, and best practices for distributed and community-based cyber capacity building.

Date: July 27, 2021

Time: 2:00 p.m. ET

Learn More Here

Featured Programs and Resources

CISA Develops Catalog of Bad Practices

As recent incidents have demonstrated, cyberattacks against critical infrastructure can have significant impacts on the critical functions of government and the private sector. All organizations, and particularly those supporting designated critical infrastructure or National Critical Functions (NCF) should implement an effective cybersecurity program to protect against threats and manage risk in a manner commensurate with the criticality of those NCFs to national security, national economic security, and/or national public health and safety.

CISA is developing a catalog of Bad Practices that are exceptionally risky, especially in organizations supporting critical infrastructure or NCFs. Entries in the catalog will be listed here as they are added.

1. Use of unsupported (or end of life) software in service of critical infrastructure and NCFs is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. This dangerous practice is especially egregious in internet accessible technologies.

2. Use of known/fixed/default passwords and credentials in service of Critical Infrastructure and NCFs is dangerous and significantly elevates risk to national security, national economic security, and national public health and safety. This dangerous practice is especially egregious in internet accessible technologies.

While these practices are dangerous for critical infrastructure and NCFs, CISA encourages all organizations to engage in the necessary actions and critical conversations to address Bad Practices.* To learn more, visit cisa.gov/badpractices

**This list is focused and does not include every possible inadvisable cybersecurity practice. The lack of inclusion of any particular cybersecurity practice does not indicate that CISA endorses such a practice or deems such a practice to present acceptable levels of risk.*

Understanding Vulnerabilities of Positioning, Navigation, and Timing

UNDERSTANDING VULNERABILITIES OF
POSITIONING, NAVIGATION, and TIMING

Positioning, Navigation, and Timing (PNT) services are integral for many operations across the critical infrastructure sectors and for many of these operations, the Global Positioning Navigation (GPS) is the primary source of PNT. Although an invisible utility, the risk of disruption to or loss of GPS (or other PNT sources) is very visible and can have adverse, cascading impacts to the global economy and the lives of people around the world.

To help facilitate dialogue on the need to strengthen the Nation's resilience from the impact of PNT disruptions, CISA's National Risk Management Center (NRMC) published the ***Understanding Vulnerabilities of PNT* fact sheet**. This fact sheet provides an overview of critical infrastructure dependencies on PNT services (e.g., earth drilling, waterway surveillance, and power generation) as well actions critical infrastructure owners/operators and equipment manufacturers can take to adopt responsible uses of PNT services and contribute meaningfully to national resilience.

To download this resource and for more PNT resources, visit cisa.gov/pnt.

CISA Releases New Mis, Dis, Malinformation Resource Library

From conspiracy theories related to COVID 19 to believable audio clips and videos crafted to spread false information, malicious actors use a variety of tools to cause chaos, confusion, and division.

CISA is charged with building national resilience to mis , dis , and malinformation (MDM) and foreign influence activities targeting our democratic way of life, and the critical infrastructure and functions on which it relies. To this end, CISA recently launched the MDM Resource Library. Individuals, state, local, tribal, and territorial (SLTT) governments, the private sector, academia, and others can use these voluntary tools to understand the threat of foreign influence activities and how to mitigate associated risks.

Visit the Mis , Dis, Malinformation Resource Library**.**

CISA Develops New Tools of Disinformation Resources

TOOLS OF DISINFORMATION

Inauthentic Content

Key Terms

Examples of Inauthentic Content

Disinformation actors use a variety of tools to influence their victims, stir them to action, and create consequences.

CISA developed the Tools of Disinformation: Inauthentic Content (available in English and Spanish) to illustrate the tactics used by disinformation actors such as manipulating audio and videos, conducting forgeries, and developing proxy in order to undermine public confidence and sow confusion. It also provides examples on how to recognize these tactics to help individuals minimize the spread of disinformation.

For more Mis, Dis, and Malinformation Resources, visit: CISA.gov/mdm resource library.

CISA Develops Disaster Access Management and Re-Entry Tabletop Exercise

In support of the Critical Infrastructure Cross Sector Council and its members' desire to implement a common access management approach for use during large scale disasters and other emergencies, CISA has developed a Disaster Access Management and Re Entry Tabletop Exercise (TTX). The Disaster Access Management and Re Entry TTX focuses on the following concepts:

- Coordination of state and local access management plans and business re entry procedures with private sector stakeholders.
- Review of intelligence and information sharing processes with local or regional critical infrastructure owners / operators to enable stabilization of community lifelines.
- Examination of recovery and business continuity plans and procedures following a large scale incident to enable access for essential workers.

The TTX can be applied to any significant incident (e.g., flooding, hurricane, wildfire, pandemic, etc.) where state or local authorities may need to establish restricted areas or emergency zones to protect public health and safety, while coordinating with the private sector to support or restore community lifelines. The Access Management and Re Entry TTX is part of CISA's Critical Infrastructure Tabletop Exercise Program (CTEP).

CISA Releases New Chemical Facility Anti-Terrorism Standards Information

On June 23, CISA published two revised information collection requests (ICRs) in the Federal Register that support the Chemical Facility Anti Terrorism Standards (CFATS) program.

The first is a soliciting public comment on ICR 1670 0014. This ICR supports CISA's collection of information for various processes of the CFATS program, such as redeterminations, compliance assistance, and verifying information submitted on Top Screens (i.e., sale of a facility or removal of COI), among others. In this Federal Register notice, CISA is requesting approval to continue collection of information to support these efforts, as well as proposing several minor updates that reflect the passage of the Cybersecurity and Infrastructure Security Act of 2018.

In addition, CISA published a soliciting public comment on ICR 1670 0029, which supports CISA's collection of information related to screening affected individuals for terrorist ties, which is implemented via the Personnel Surety Program (PSP). In this Federal Register notice, CISA is requesting approval to continue collection of information to support these efforts and proposing several minor updates that reflect the passage of the Cybersecurity and Infrastructure Security Act of 2018.

Thank you for your continued interest and support as CISA continues to enhance the CFATS program. For general questions about the ICRs, please contact CFATS@hq.dhs.gov.

CISA Releases New Ransomware Readiness Assessment

The Cyber Security Evaluation Tool (CSET®) is a stand alone desktop application that guides asset owners and operators through a systematic process of evaluating Operational Technology and Information Technology.

On June 30, a CISA Current Activity announced the CSET was updated to include a new module: Ransomware Readiness Assessment (RRA). The RRA is a self assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident.

After completing the evaluation, the organization will receive reports that present the assessment results in both a summarized and detailed manner. The organization will be able to manipulate and filter content in order to analyze findings with varying degrees of granularity.

CISA strongly encourages all organizations to take the CSET Ransomware Readiness Assessment, available at Ransomware Readiness Assessment CSET v10.3.

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!

- Check out the new guidance from @CISAgov on bad cybersecurity practices that threaten our critical infrastructure: https://www.cisa.gov/BadPractices

- Want to learn more about cyber hygiene services? @CISAgov has the resources you need: https://www.cisa.gov/cyber-hygiene-services

- Save the date! @CISAgov will be hosting a community capacity building webinar on July 27. Register here: https://cyber-capacity-building.eventbrite.com