CISA
CYBER+INFRASTRUCTURE

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

COMMUNITY BULLETIN

Alerts & Announcements

CISA Support for COVID-19

The Cybersecurity and Infrastructure Security Agency (CISA) is closely monitoring and responding to the evolving Coronavirus outbreak, also known as COVID-19.

As the nation's risk advisor, CISA is sharing the readiness information below to assist partners and stakeholders as they deal with organizational and workforce impacts from COVID-19, to include: identifying mission essential functions, updating incident response plans, factoring in workforce changes in a distributed environment, and guarding against the possibility of malicious cyber actors taking advantage of public concern by conducting phishing attacks and disinformation campaigns.

In addition, CISA continues to work closely with its federal partners in a whole of Nation effort to detect and slow the spread of COVID-19 in the United States. This effort is led by the Department of Health and Human Services through the Centers for Disease Control (CDC), with all other agencies, including CISA, in a support role.

The first and best source of authoritative information on COVID-19 is coronavirus.gov, which includes situation reports, guidance, and more. There are a variety of other sources of information to support you and your businesses during this time:

- What the U.S. Government is Doing: https://www.usa.gov/coronavirus
- What DHS/CISA is Doing: https://www.dhs.gov/coronavirus; https://www.cisa.gov/coronavirus
- CDC Guidance for Businesses and Employers: https://www.cdc.gov/coronavirus/2019-ncov/community/guidance-business-response.html
- What Our Partners are Doing: https://staysafeonline.org/covid-19-security-resource-library/

CISA Updates Guidance on Essential Critical Infrastructure Workers During COVID-19

On March 28, 2020, CISA released updated guidance to help state and local jurisdictions and the private sector identify and manage their essential workforce while responding to COVID-19.

This guidance states:

> “If you work in a critical infrastructure industry, as defined by the Department of Homeland Security, such as healthcare services and pharmaceutical and food supply, you have a special responsibility to maintain your normal work schedule.”

Version 2.0 provides clarity around a range of positions needed to support the critical infrastructure functions laid out in the original guidance and the dependencies on their supply chains – including essential sanitation and hygiene productions and services, and manufacturing of critical products.

This guidance is not a federal mandate, and final decisions remain at the state and local levels, who must make determinations of how to balance public health and safety with the need to maintain critical infrastructure in their communities.

CISA executes the Secretary of Homeland Security’s responsibilities as assigned under the Homeland Security Act of 2002 to provide strategic guidance, promote a national unity of effort, and coordinate the overall Federal effort to ensure the security and resilience of the Nation's critical infrastructure.

The list of Essential Critical Infrastructure Workers was developed in coordination with Federal agencies and the private sector as a guide to help decision-makers within communities understand how to ensure continuity of essential functions and critical workforce as they consider COVID-related restrictions in certain communities (e.g., shelter-in-place).

The list can also inform critical infrastructure community decision-making to determine the sectors, sub sectors, segments, or critical functions that should continue normal operations, appropriately modified to account for CDC workforce and customer protection guidance. These critical functions include, but are not limited to, systems that support healthcare personnel (e.g., doctors, nurses, laboratory personnel, etc.), the food industry (e.g., retail groceries and pharmacies), communication providers (e.g., operators, call centers, IT data centers), defense systems support, law enforcement, public works, and other essential operations. Workers who support these critical functions are necessary to keep critical systems and assets working.

“As the nation comes together to slow the spread of COVID-19, everyone has a role to play in protecting public health and safety. Many of the men and women who work across our nation’s critical infrastructure industries are hard at work keeping the lights on, water flowing from the tap, groceries on the shelves, among other countless essential services,” said Christopher Krebs, CISA Director. “As the nation’s risk advisor, this list is meant to provide additional guidance to state and local partners, as well as industry, building on the President’s statement that critical infrastructure industries have a special responsibility to keep normal operations. We’re providing recommendations for these partners as they carry out their mission to keep their communities safe, healthy, and resilient. And on behalf of CISA, we thank the brave men and women who continue these essential jobs in challenging times.”

The list of Essential Critical Infrastructure Workers was developed using existing data and analysis, including publicly available analysis done by the President’s National Infrastructure Advisory Council in 2007.

CISA will use this list to support federal, state, local, tribal, and territorial government response to COVID-19. To view the full list of Essential Critical Infrastructure Workers and to learn more about our efforts, visit https://www.cisa.gov/coronavirus.

CISA Insights: Risk Management for Novel Coronavirus

CISA released an Insights document titled, “Risk Management for Novel Coronavirus (COVID-19),” detailing steps to help executives think through physical, supply chain, and cybersecurity issues that may arise as a result of this ongoing public health concern.

Read the CISA Insights at CISA.gov/insights, or download a PDF version from the CISA Insights publication page: https://go.usa.gov/xdHjV.

COVID-19 Cyber Alert

On March 6, 2020, CISA released an alert warning individuals to remain vigilant for scams related to COVID-19.

CISA warns that Cyber actors may send emails with malicious attachments or links to fraudulent websites to trick victims into revealing sensitive information or donating to fraudulent charities or causes. Exercise caution in handling any email with a COVID-19-related subject line, attachment, or hyperlink, and be wary of social media pleas, texts, or calls related to COVID-19.

Review a detailed list of precautions on the CISA Alerts page: https://www.us-cert.gov/ncas/current-activity/2020/03/06/defending-against-covid-19-cyber-scams

Enterprise Virtual Private Network (VPN) Security Concerns, Mitigations

On March 13, 2020, CISA released an alert encouraging organizations to adopt a heightened state of cybersecurity when considering alternate workplace options for their employees. Remote work options—or telework—require an enterprise VPN solution to connect employees to an organization's IT network.

Review a detailed list of considerations and mitigations on the CISA Alerts page: https://www.us-cert.gov/ncas/alerts/aa20-073a

CISA Urges Administrators to Patch Remote Code Execution Vulnerability

CISA is urging users and administrators to review Microsoft's Advisory on CVE-2020-0688, a remote code execution vulnerability, and apply the necessary patches as soon as possible. A remote attacker can exploit this vulnerability to take control of an affected system that is unpatched.

Although Microsoft disclosed the vulnerability and provided software patches for the various affected products in February 2020, advanced persistent threat actors are targeting unpatched servers. According to recent open-source reports, Microsoft Exchange Servers affected by CVE-2020-0688 continue to be an attractive target for malicious cyber actors.

Read the full advisory on Microsoft's Security Guidance site: https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2020-0688

Featured Resources

CISA Creates New Guidance Portal

CISA relies on guidance documents to express and disseminate its views, interpret statutory and regulatory provisions, and implement various programs.

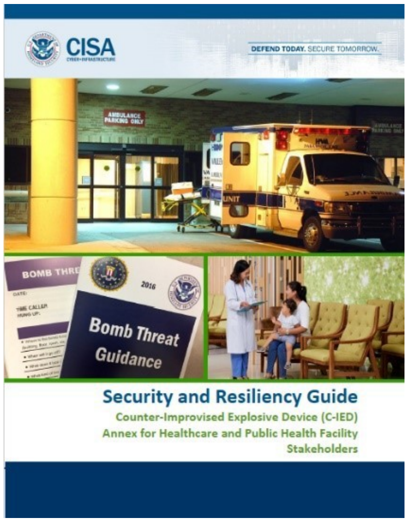
Consistent with Executive Order 13891, “Promoting the Rule of Law Through Improved Agency Guidance Documents,” CISA has created the CISA Guidance portal to provide information and access to all Agency guidance documents on which the Agency relies.

Visit the CISA Guidance webpage to view the relevant guidance documents for the Protected Critical Infrastructure Information (PCII) program and the Chemical Facility Anti-Terrorism Standards (CFATS) program: https://go.usa.gov/xdHKY.

Readers can also review the full executive order on the White House website: https://www.whitehouse.gov/presidential-actions/executive-order-promoting-rule-law-improved-agency-guidance-documents/.

CISA Addresses Improvised Explosive Device Security Challenges Facing Healthcare Stakeholders

CISA published an Annex for Healthcare and Public Health Facility Stakeholders that describes the actions that management and staff at healthcare facilities can take to understand and improve their ability to perform counter-Improvised Explosive Device (C-IED) activities and make critical security decisions.



Security and Resiliency Guide
Counter-Improvised Explosive Device (C-IED)
Annex for Healthcare and Public Health Facility Stakeholders

The annex complements CISA’s Security and Resiliency Guide: Counter-IED Concepts, Common Goals, and Available Assistance (SRG C-IED) by tailoring C-IED guidance and resources to those in the healthcare industry.

Past incident data shows that bomb threats are likely to occur in healthcare settings on a frequent basis. Healthcare facilities must take preventative action to ensure their own preparedness for a potential IED incident as part of their overall security management efforts.

By connecting with local authorities, developing plans to identify issues and support incident response, training employees, and reporting concerns to emergency authorities, many incidents may be mitigated or avoided.

To enhance C-IED preparedness, download and share the Annex for Healthcare and Public Health Facility Stakeholders PDF from CISA’s website: https://go.usa.gov/xdHWp. For questions about the products, email OBP@cisa.dhs.gov.

Learn more about CISA’s Security and Resiliency Guide through the CISA Publications Library: https://go.usa.gov/xdHW7.

CISA is Hiring!

We’re hiring Cybersecurity Advisor Positions! These positions, located throughout the nation, provide direct support to an assigned state/region and will work as part of a regional based team that is composed of physical and cybersecurity experts as well as regional support personnel. Regions vary in size but can contain between 4-6 cybersecurity advisors. Multiple positions across the United States are available. View the entire job announcement for full details.

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!

- #Coronavirus has been detected in locations across the world. The latest readiness info from @CISAgov tackles physical, supply chain, and cybersecurity issues: https://go.usa.gov/xdHjV
- Due to the large amount of speculation regarding #COVID19, this is a reminder to rely on OFFICIAL sources for accurate information. Help control the spread of rumors by sharing this page: https://www.fema.gov/coronavirus-rumor-control
- State and local election officials are actively monitoring #coronavirus and how to keep elections safe. Check with them for updates on whether your election day information has changed: nass.org/initiatives/trustedinfo-2020
- If you see disinformation about #coronavirus don't rt, fwd or share – even if you're trying to debunk the source. You could unknowingly amplify. Instead, you can help by sharing the facts from trusted sources like coronavirus.gov or @fema: More: fema.gov/coronavirus-rumor-control
- As we all adjust our behavior in light of the #COVID19 threat, the Nation's critical #infrastructure is more visible that ever. There are some functions that are critical to our way of life and the men and women who carry out these functions ensure our Nation's resilience to #coronavirus. What are these critical functions? Medical/Health, Communications, IT, Food, Transportation & Logistics, Energy, Water & Wastewater, Law Enforcement, Public Works, some gov't Ops, Hazmat, Essential Financial Services. Our Nation depends on these functions daily and that's why it is paramount that the people carrying out these roles are able to safely continue working. We recently released a guide for state & local jurisdictions and the private sector to help them manage their workforce: cisa.gov/identifying-critical-infrastructure-during-covid-19

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.

OTHER RESOURCES:
About Us | Getting Started | Cybersecurity Framework | Assessments | Events and Media | Privacy
STAY CONNECTED:

SUBSCRIBER SERVICES:
Manage Preferences | Unsubscribe | Help

This email was sent to kathleen.donnelly@associates.hq.dhs.gov using GovDelivery Communications Cloud on behalf of: United States Computer Emergency Readiness Team (US-CERT) · 245 Murray Lane SW Bldg 410 · Washington, DC 20598 · (888) 282-0870

GOVDELIVERY