IT Security | Supply Chain | OT Security | Insider Threat | Physical Security | Interoperable Communications

COVID-19 COMMUNICATION PRODUCTS

DEFEND TODAY,
SECURE TOMORROW

LAST UPDATED: 27 JULY 2020

Joint Alerts

NEW Innovative Practices and New Solutions Guide

- On July 22, CISA released a new guide that advises election officials on how to ensure they are adequately prepared for their state and local elections during the COVID-19 pandemic.
- This guide is part of a series of best practices created by the Election Infrastructure Government Coordinating Council and Subsector Coordinating Council's Joint COVID Working Group. Election officials have implemented innovative practices and new solutions through the 2020 primary election season in response to COVID-19. The guides offer illustrations of operations that are possible, either as principal solutions or as backup options, for the 2020 general election.

NEW COVID-19 Recovery CISA Tabletop Exercise Package (CTEP)

- On July 17, CISA released a new exercise package to assist private sector stakeholders and critical infrastructure owners and operators across all sectors in assessing recovery and business continuity plans and addressing key questions related to organizational recovery from the COVID-19 Pandemic.

Public Advisory - Malicious Activity Targeting COVID-19 Research Development

- On July 16, in response to malicious activity targeting COVID-19 research and vaccine development in the United States, United Kingdom (UK), and Canada, CISA, the UK's National Cyber Security Centre (NCSC), Canada's Communications Security Establishment (CSE), and the National Security Agency (NSA) released a "Joint Cybersecurity Advisory" to expose an advanced persistent threat. A malicious cyber actor is using a variety of tools and techniques to target organizations involved in COVID-19 research and vaccine development.
- CISA encourages users and administrators to review the Joint Cybersecurity Advisor as well as the following Malware Analysis Reports for more information, and to apply the mitigations provided.
  - SOREFANG
  - WELLMESS
  - WELLMAIL

Joint CISA and FCC Letter

- On May 26, CISA and the Federal Communications Commission (FCC) sent a letter to the nation's governors encouraging them to provide necessary access and resources to communications workers helping to keep Americans connected during the COVID-19 pandemic. The letter also highlights CISA's recent guidance on the Essential Critical Infrastructure Workforce and 911 Centers During the Pandemic.

Avoid Scams Related to Economic Payments, COVID-19

- On May 21, CISA, along with the Department of the Treasury, Internal Revenue Service (IRS), and United States Secret Service (USSS) issued a joint alert warning Americans to be on the lookout for criminal fraud related to economic impact payments—particularly fraud using coronavirus lures to steal personal and financial information, as well as the economic impact payments—and for adversaries seeking to disrupt payment efforts.
- The alert contains several resources to help defend, mitigate and report suspicious cyber activity, especially emails that could be attempted phishing attacks.

FBI and CISA Warn Against Chinese Targeting of COVID-19 Research Organizations

- On May 13, the FBI and CISA issued a public service announcement to warn organizations researching COVID-19 of likely targeting and network compromise by the People's Republic of China. Healthcare, pharmaceutical and research sectors working on COVID-19 response are the prime targets of this activity and should take the necessary steps to protect their systems.

Joint CISA and UK Tip on COVID-19 Cyber Threat Exploitation

- On May 5, CISA and the UK's National Cyber Security Centre (NCSC) released a joint advisory to address an increase in malicious activity with themes related to COVID-19. Malicious cyber actors are targeting individuals, small and medium enterprises, and large organizations worldwide through COVID-19-related scams and phishing campaigns. At the same time, the surge in teleworking has increased the use of potentially vulnerable services.

Cyber Warning Issued for Key Healthcare Organizations in UK and USA

- On May 5, CISA and the UK's NCSC released a joint advisory to address the large-scale "password spraying" campaigns against healthcare bodies and medical research organizations.

Joint Bulletin: Physical Security Considerations for the Healthcare Industry During COVID-19 Response

- On April 24, CISA, the Department of Health and Human Services, and the FBI jointly released a bulletin regarding potential threats to the healthcare industry and resources on how to mitigate these threats.

CISA Alert AA20-099A: COVID-19 Exploited by Malicious Cyber Actors

- On April 8, CISA and the UK's NCSC issued a joint alert which provides information on exploitation by cybercriminals and advanced persistent threat (APT) groups during the COVID-19 pandemic.

UK and US Security Agencies Issue COVID-19 Cyber Threat Update

- On April 8, CISA, in partnership with the UK's NCSC, released a joint advisory on the growing number of cybercriminals and other online malicious groups exploiting the COVID-19 outbreak. In addition to alerting people to the threat, the advisory directs them to resources available to counter it.

CISA Current Activity: FBI Releases Guidance on Defending Against VTC Hijacking and Zoom-bombing

- On April 2, the FBI released an article on defending against video-teleconferencing (VTC) hijacking (referred to as "Zoom-bombing" when attacks are to the Zoom VTC platform). The FBI released this guidance in response to an increase in reports of VTC hijacking.

Cyber Alerts

CISA: AA20-107A: Continued Threat Actor Exploitation Post Pulse Secure VPN Patching

- On April 16, CISA released this alert to update administrators on the issue of threat actors who successfully exploited CVE-2019-11510 and stole organizations' credentials. The alert warns administrators that these threat actors will still be able to access—and move laterally through— the organization's network even after it has patched this vulnerability if the organization did not change those stolen credentials.

The United States Issues an Advisory on North Korean Cyber Threats

- On April 15, the U.S. Departments of State, Homeland Security, and Treasury, and the FBI issued an advisory to raise the awareness of the cyber threat posed by North Korea. The advisory highlights North Korea's malicious cyber activities around the world, identifies U.S. government resources that provide technical and threat information, and includes recommended measures to counter the cyber threat.

Enterprise VPN Security Alert

- On March 13, CISA released this alert to provide information on virtual private network (VPN) security as more organizations implement remote work options—or telework—which require a VPN solution to connect employees to an organization's information technology (IT) network.

Defending Against COVID-19 Cyber Scams Alert

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

Infrastructure Security

Letters to Faith-Based Communities

- On April 8, CISA issued letters to members of faith-based communities about the need to remain vigilant, and expressed its commitment to supporting their efforts in maintaining safe and secure houses of worship and related facilities during a time when stressors caused by the pandemic may contribute to an individual's decision to commit an attack or influence their target of choice.

Emergency Communications

Guidelines for 911 Centers

- On May 15, these guidelines were developed to support public safety partners across all levels of government when developing plans and actions regarding governance, procedures, staffing, and cleaning and disinfecting in response to a pandemic. *Guidelines for 911 Centers* includes:
  - Guidelines for Executives: 911 Center Pandemic Recommendations—emphasizes the importance of communications centers, accentuates the particular risk of a pandemic to resiliency of 911 operations, communicates executive-level action, and provides a description of available guidance for 911 administrators
  - Guidelines for 911 Centers: Pandemic Planning—highlights governance, resource planning, and contingency considerations from a holistic perspective during a pandemic
  - Guidelines for 911 Centers: Pandemic Operating Procedures—provides recommendations on how to organize, train, and care for personnel while operating through a pandemic
  - Guidelines for 911 Centers: Cleaning and Disinfecting During a Pandemic—presents cleaning and disinfecting guidance specific to public safety and resources for 911 centers during a pandemic

Priority Telecommunications Services

- As of May 6, CISA provided Priority Telecommunications Services to approximately 70,000 additional users, increasing connectivity for essential critical workers access to Government Emergency Telecommunications Service (GETS), Wireless Priority Services (WPS), and Telecommunications Service Priority (TSP).

Election Security

COVID-19 Elections Working Group

- In March, CISA, in partnership with the U.S. Election Assistance Committee, created a COVID-19 working group within its election sector coordinating councils. This working group is a joint effort between the private sector and the government to identify information needed by election officials to support the expansion of vote-by-mail that many states are looking to implement as well as improve the safety of polling places in a COVID-19 environment.

Supply Chain

CISA and INL Release Commercial Routing Assistance App

- On May 6, CISA and the Idaho National Laboratory (INL) launched a new "Commercial Routing Assistance (CRA) tool for truckers and other commercial drivers in the United States. The free app incorporates coordinated data streams and plots multiple routing options so commercial operators can plan and manage vehicle movements across multiple states quickly in times of disasters or other restrictions. CISA and INL also released a Commercial Routing Assistance Fact Sheet.

Building Collective Resilience for the ICT Supply Chain

- On May 5, CISA released a blog to provide information on how individual companies and organizations can build and implement an effective information and communications technology (ICT) supply chain risk management program to improve their overall security posture during COVID-19.

Tools and Resources

State, Local, Tribal, and Territorial COVID-19 Disinformation Toolkit

- CISA issued a toolkit to state, local, tribal, and territorial officials to bring awareness to misinformation, disinformation, and conspiracy theories appearing online related to COVID-19's origin, scale, government response, prevention, and treatment.
- Disinformation around the pandemic has consisted of false information and unsubstantiated rumors regarding the origin of the virus, and the facts and data regarding the pandemic.
- This toolkit helps state and local officials convey timely, trusted, and verified COVID-19 details and developments to their constituents so that disinformation cannot be created and spread by bad actors. It also includes communication strategies to help regional offices share verified information with their constituents.

Webinar – Critical Infrastructure Hurricane Response During a Pandemic

- On June 18, CISA hosted 2020 Hurricane Season Preparedness Webinar to discuss the CISA's role in hurricane preparedness and response, while in a COVID-19 environment. The webinar covered risks to interdependent critical infrastructure systems and the federal approach to infrastructure response and recovery.
- The event took place from 10:30 a.m. to noon ET, and featured speakers from CISA, the Federal Emergency Management Agency (FEMA), and the National Oceanic and Atmospheric Administration.
- This webinar was for infrastructure stakeholders at the local, regional, and national levels, including government and industry decision makers who are involved in response and recovery.

Coronavirus Web page

- On May 2, CISA updated the Coronavirus web page to include a new FEMA resource. The COVID-19 Pandemic Operational Guidance for the 2020 Hurricane Season to help emergency managers and public health officials best prepare for disasters, while continuing to respond to and recover from coronavirus. CISA initially launched the Coronavirus web page to ensure that the public and private sectors have the information they need to ensure America's cyber and infrastructure security during the COVID-19 pandemic.

Updated Guidance on Essential Critical Infrastructure Workers During COVID-19

- On May 19, CISA released an update to the Guidance on Essential Critical Infrastructure Workers During COVID-19 (ECIW). ECIW 3.1 provides clarity around many individual worker categories and updates existing language to better reflect terminology used in food and agriculture industries.
- CISA originally released the guidance on March 19 to help state and local jurisdictions and the private sector identify and manage their essential workforce while responding to COVID-19.
- Subsequent versions were introduced to include additional services and industries that were deemed essential after receiving feedback and suggestions from its partners.

Telework Guidance K-12 Schools

- On May 13, CISA published video conferencing guidance and a tip sheet for K-12 schools. The conferencing guidance is for school districts and campus IT administrations, as well as teachers and staff to help them think through cybersecurity issues. The tip sheet provides a graphic and easy to read summary of the guidance. These resources can be found at www.schoolsafety.gov, as well as www.cisa.gov/telework.

CISA Insights – COVID-19 Disinformation Activity

- On May 8, CISA released a new *CISA Insights* to address the false and misleading information related to the coronavirus (COVID-19). This *CISA Insights* provides an overview of coronavirus disinformation and steps that can be taken to reduce the risk of sharing inaccurate information with your friends and family.

Telework Guidance and Resources

- On April 24, CISA launched telework guidance and resources on its website to help agencies and organizations that have implemented more telework in response to COVID-19. In addition to the "TIC 3.0 Interim Telework Guidance," the web page also includes information on:
  - Telework Best Practices from DHS and the National Security Agency

  - Video Conferencing Tips
  - Cybersecurity Recommendations for Critical Infrastructure Using Video Conferencing
  - Cybersecurity Recommendations for Federal Agencies Using Video Conferencing
  - Guidance for Securing Video Conferencing

Critical Infrastructure Operations Centers and Control Rooms Guide for Pandemic Response

- On April 23, CISA released guidance geared toward all 16 critical infrastructure sectors identified by the federal government. The guide provides considerations and mitigation measures for operation centers and control rooms but can be applied further to any critical node that is required to continue functioning in a pandemic environment.

Trusted Internet Connections (TIC) 3.0 Interim Telework Guidance

- On April 8, CISA released interim Trusted Internet Connections (TIC) guidance to aid agencies in securing their network and cloud environments. The "TIC 3.0 Interim Telework Guidance" supports the current surge in teleworking and use of collaboration tools amongst the federal workforce.

Implementing Safety Practices for Critical Infrastructure Workers Who May Have Had Exposure to a Person with Suspected or Confirmed COVID-19

- In April, CISA and the Centers for Disease Control and Prevention released interim guidance to aid critical infrastructure workers in 16 different sectors of work and provide information on what critical infrastructure workers should do if they have been exposed to COVID-19.

CISA Insights Risk Management for Novel Coronavirus (COVID-19)

- On March 18, CISA released a new CISA Insights to help executives think through physical, supply chain, and cybersecurity issues that may arise from the spread of COVID-19.

COVID-19 Action Team

- CISA.CAT@CISA.DHS.GOV

FEMA Mission Assignment

- CISA has been activated as part of ESF-2 (Communications) and ESF-14 (Cross Sector Business and Infrastructure) to provide 24/7 support at FEMA's National Response Coordination Center (NRCC) and in the 10 CISA regions.