Cybersecurity and Infrastructure Security Agency

2019 HIGHLIGHTS

DEFEND TODAY, SECURE TOMORROW

U.S. DEPARTMENT OF HOMELAND SECURITY

CISA
CYBER+INFRASTRUCTURE

DECEMBER 2019

Table of Contents

ABOUT CISA

> Meeting their Constitutional duties to provide for the common defense, Congress and the Administration established CISA, an agency to lead the national effort to protect our critical infrastructure. An agency to bring to bear all of the instruments of national power in this endeavor. Where there may be a lack of leadership, CISA will step up. Where there may be a lack in national capability, CISA will provide. Through partnership and cooperative defense, as an ally to the national values of civil liberties and prosperity, we will protect the American way of life.

Christopher Krebs
Message from the Director,
CISA Strategic Intent, 2019

Mission

1 Lead the national effort to understand and manage cyber and physical risk to our critical infrastructure.

Vision

2 Secure and resilient critical infrastructure for the American people.

The Nation's Risk Advisor

Established November 16, 2018, the Cybersecurity and Infrastructure Security Agency (CISA) is the Federal lead for national risk management of cybersecurity and physical infrastructure. CISA works with partners across government and industry to defend against today's urgent threats and hazards and collaborates to build more secure and reliant infrastructure and address long-term risks for tomorrow.

Many critical infrastructure risks are complex, dispersed both geographically and across a variety of stakeholders, and challenging to understand and address. This is where CISA fits in as a central coordinator of analysis, planning, and response, especially in areas where there is no other designated Federal Government leader.

Second Annual National Cybersecurity Summit Reflects Progress and Priorities for the Future

CISA held the second annual National Cybersecurity Summit September 18-20 in National Harbor, Maryland. The event drew more than 1,000 cybersecurity leaders and experts across every level of government, industry, and academia to discuss ways to collectively defend against the threats of today and secure against the risks of tomorrow.

The event offered more than 40 breakout sessions across five tracks: Protect 2020; Defend Today; Secure Tomorrow; Insights; and Partnerships in Action. A wide range of topics were covered, including:

- DHS Acting Deputy Secretary David Pekoske's opening address on the shared responsibility of government and industry to protect critical infrastructure,
- A discussion between Senator Mark Warner (D-VA) and CISA Director Krebs on threats associated with 5G and China, and
- A moderated panel with CISA Director Krebs and cybersecurity reporters exploring how media approaches elections.

In addition, beginner and experienced cyber analysts participated in an exciting "Capture The Flag" exercise using puzzles and clues to determine how attackers were accessing a regional electrical utility's IT network and how to stop them.

The Summit proved to be informative and an excellent forum for private and public stakeholders to meet and share experiences.

Guiding Principles

- **Leadership and Collaboration:** CISA's leadership is one of our primary benefits to stakeholders and the Nation, but without successful collaboration with our partners, we cannot achieve our mission.
- **Risk-Prioritization:** CISA's foremost responsibility is to safeguard the American people and we prioritize our efforts at all levels to focus on the greatest threats and vulnerabilities facing the homeland.
- **Results Oriented:** CISA must focus our efforts on having the greatest impact for the investment made to demonstrably reduce risk, respond to requirements put forth by our partners, and work toward defined common objectives.
- **Respect for National Values:** Our work to protect national critical functions must reflect the ultimate purpose of enabling an open and prosperous society.
- **Unified Mission and Agency:** We are one mission and one agency. We fundamentally focus on risk management, however it presents itself**,** whether through cyber, physical, human factors, or supply chain.

About This report

CISA 2019 Highlights is designed to provide a selection of key achievements and successes during the Agency's inaugural year. The priorities looking ahead for the Agency can be found in the *Strategic Intent* document at www.cisa.gov/strategic-intent. *CISA 2019 Highlights* is not intended to provide a comprehensive summary of activities, nor does it reflect the full scope, breadth, and depth of CISA's myriad programs, initiatives, and partnerships.

CISA BY THE NUMBERS

A Commitment to Training

CISA has conducted more than **11,041** training sessions—in class, online, and via independent study—reaching over **117,401** participants

Protecting Against Active Shooters

877,565

page views of the Active Shooter webpage

Defend Today, Secure Tomorrow

Conducted more than

2,800

infrastructure and cybersecurity assessments and exercises

Stopping Cyber Attacks in Their Tracks

3,583,230

Unique indicators–sharing cyber threat indicators between the Federal Government and our private sector partners in real time

Protecting Public Spaces

Engaged more than

1,700 places of worship, hotel, sport, K-12, and shopping facilities to perform security visits and assess potential vulnerabilities

Creating Safer Schools

Conducted nearly

1,200 engagements with state departments of education, school districts, and K-12 facilities

ELECTION SECURITY
for the Nation, by the Nation

> “2018 was the most secure election in modern history, and 2020 is going to be even better.”
>
> **Christopher Krebs**
> CISA Director

A functioning democratic society depends on fair and secure elections. Responding to Russia’s campaign in 2016 to undermine Americans’ faith in the democratic process, CISA made protecting our Nation’s elections systems a top priority.

CISA is responsible for assisting state and local governments, and the private sector organizations that support them, with their efforts to enhance the security and resilience of our election infrastructure. **While CISA is the lead federal agency responsible for securing our elections, state and local election officials on the ground in communities around the country are responsible for governing, managing, and securing our election process.** Consistent with long-standing partnerships with states and localities, we worked closely with election officials throughout 2018 and 2019 to augment their efforts by sharing cybersecurity threat information and offering resources, including tabletop exercises, network and system assessments, and technical assistance.

Throughout our efforts, we’ve worked with essential partners including the National Association of Secretaries of State, the National Association of State Election Directors, and the U.S. Election Assistance Commission, along with individual state and local election officials throughout the country. We’ve provided alerts and warnings, held classified and unclassified threat briefings, and provided voluntary cyber and physical assessments at no cost to state and local governments.

In June of 2019 CISA hosted its second ‘**Tabletop the Vote**’ exercise to improve preparedness, information sharing, response, and recovery. The exercise was attended by 47 states, three territories, more than a thousand local officials, their private sector partners and Federal Government representatives.

Our objective is to reduce the likelihood of compromises to election infrastructure confidentiality, integrity, and availability, which are essential to the conduct of free and fair democratic elections.

Leading up to the 2018 midterm elections, CISA established an election security plan with more than 500 CISA employees supporting election security preparedness nationwide. We designated a mission manager and a deputy mission manager; deployed Protective Security and Cybersecurity Advisors to work with election officials across the country; established steady communications with state, local, tribal, and territorial partners; deployed members of our cyber threat Hunt and Incident Response Team to states and localities; and set up two Election Day situational awareness rooms.

We also deepened our partnerships and worked even more closely with trusted third parties—including the Multi-State Information Sharing and Analysis Center (MS-ISAC), the Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), and key private sector vendors—to analyze relevant cyber data, facilitate information exchange, enhance outreach, and share threat information.

Leading to the 2020 Presidential election, we continue to coordinate with federal, state, local, and private sector partners nationwide to support state and local election officials. We have increased our engagement with election officials across the country and are committed to working with them to increase the resilience of the election process. We offer training sessions, intelligence, incident response services, and more; election officials in all 50 states are working with us in some way.

In partnership, EI-ISAC and CISA have deployed Albert Sensors, intrusion detection systems, in all 50 states, 2 territories, and 97 localities in preparation for the 2020 election.

We are also committed to dispelling the fog that disinformation spreads as part of #Protect2020, a hashtag we developed for quick updates.

Foreign interference is malign action taken by foreign governments or actors. It is designed to sow discord, manipulate public discourse, discredit the electoral system, bias the development of policy, or disrupt markets to undermine the interests of the United States and our allies.

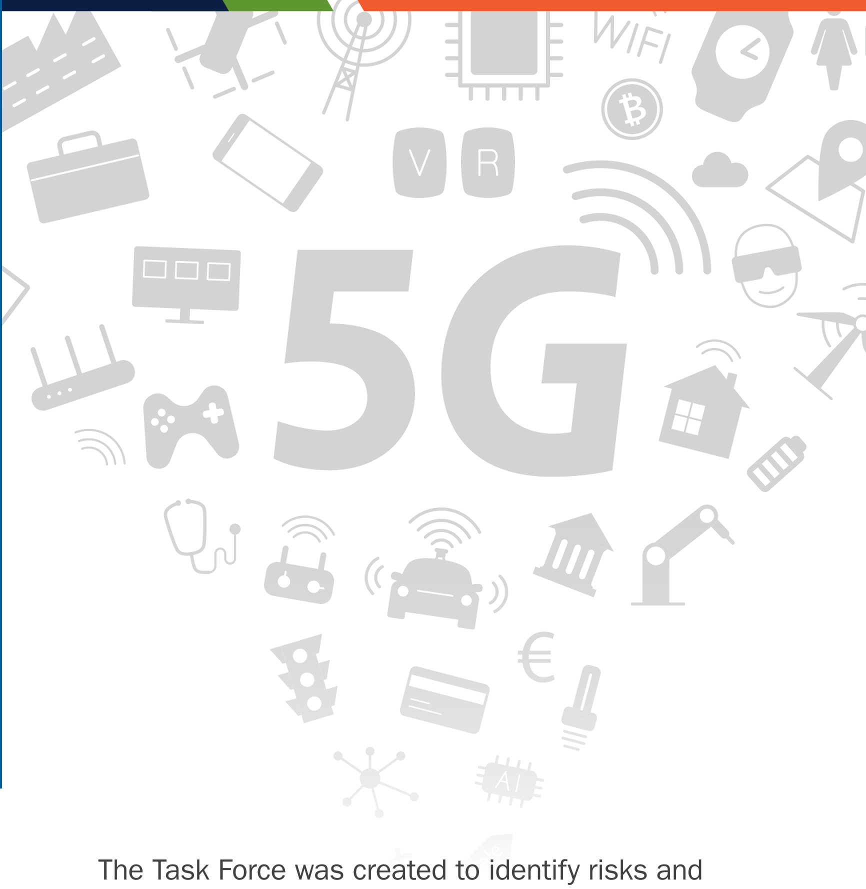
To counter foreign interference, we created an easily understood, tongue-in-cheek infographic entitled *The War on Pineapple: Understanding Foreign Interference in 5 Steps*.

In collaboration with federal, state, and local partners, we are working on ***The State and Local Election Counter Information Operations Playbook***. The playbook is designed to provide election officials with tools to identify, report, and respond to information operations.

Our country has made tremendous strides since 2016, and we are relentless in our commitment to collaborate with those on the front lines of administering our elections to secure election infrastructure from risks. We will remain transparent as well as agile in combating threats and securing our physical and cyber infrastructure.

5G:

Its potential and peril



Fifth generation wireless, or "5G" as it's commonly called, portends potential *and* peril for the Nation. With faster, more reliable wireless communications connections for users, 5G can provide the extra bandwidth needed to advance the Internet of Things—a network linking not just phones and computers but also robots, cars, and all manner of sensor-equipped consumer products and infrastructure. It can underpin a new era of "smart cities"—in which energy grids, traffic signals, and emergency services are linked to reduce inefficiencies and response delays.

However, if the underlying network is not secure, or if 5G components are manufactured by untrusted companies, U.S. entities could be exposed to risks introduced by malicious software and hardware, counterfeit components, and component flaws caused by poor manufacturing processes and maintenance procedures.

CISA established the **Information and Communications Technology (ICT) Supply Chain Risk Management Task Force**, a public-private partnership with members of the information technology and telecommunications industries working alongside federal partners.

The Task Force was created to identify risks and develop solutions to help manage risk to the global ICT supply chain, including the challenges 5G technology presents. One line of Task Force effort underway is the identification of processes and criteria for risk-based evaluation of ICT suppliers, products, and services.

CISA also recently issued a report, *Overview of Risks Introduced by 5G Adoption in the United States*, reviewing the dangers of a 5G network developed by untrustworthy companies. The report cited:

> *"The use of 5G components manufactured by untrusted companies could expose U.S. entities to risks introduced by malicious software and hardware, counterfeit components, and component flaws caused by poor manufacturing processes and maintenance procedures. 5G hardware, software, and services provided by untrusted entities could increase the risk of compromise to the confidentiality, integrity, and availability of network assets. Even if U.S. networks are secure, U.S. data that travels overseas through untrusted telecommunications networks is potentially at risk of interception, manipulation, disruption, and destruction."*

The Federal Government manages these vulnerabilities and increases the security of communications networks as 5G is adopted by:

- Encouraging continued development of trusted 5G technologies, services, and products.
- Encouraging continued trusted development of future generations of communications technologies.
- Promoting international standards and processes that are open, transparent, and consensus-driven, and that do not place trusted companies at a disadvantage.
- Limiting the adoption of 5G equipment with known or suspected vulnerabilities.
- Continuing engagement with the private sector on risk identification and mitigation efforts.
- Ensuring robust security capabilities for 5G applications and services.

The 5G issue is a multi-faceted challenge requiring a similarly multi-faceted approach, which CISA brings to this work. Working with industry partners, we are leading 5G risk mitigation efforts across the Federal Government to ensure that the United States can fully benefit from all the advantages 5G connectivity promises.

Our economic security and national security fundamentally depend on it. Through our unique authorities, CISA is leading the effort to ensure security is built into all parts of 5G (and not bolted on after the fact) by enabling a meaningful dialog on all facets of the needed security.

Valuable Partnership Across The Pond

In today's interconnected world, cybersecurity and critical infrastructure security requires strong trusted public and private partnerships around the world with 2019 being an eventful year for CISA's international security cooperation. This Spring launched CISA's first-ever cybersecurity personnel exchange with the UK's National Cyber Security Centre (NCSC). Having a CISA cyber expert embedded within the Cyber Security Centre and an NCSC cyber expert embedded within CISA has led to improved collaboration on threat assessments, technical standards and advice as well as incident management practices. The exchange has been a boon to the US-UK partnership and serves as a template for CISA's future international footprint.

Be Aware: Drones Can Spy and Steal Secrets

Theft of corporate data, trade secrets, and personal information occurs in many digital ways, and one of the newest methods is through spying unmanned aircraft—specifically, Chinese-made drones. Although unmanned aircraft systems can provide various benefits, U.S. intelligence and security officials have repeatedly warned about the cyber and data security risks associated with information or communications technologies designed, manufactured, or sold by commercial enterprises operating under the control or influence of a foreign authoritarian state.

That's why, in May, we alerted partners and stakeholders to the inherent risk of data theft posed by unmanned aircraft systems made in China. Our notice, titled *"Chinese Manufactured Unmanned Aircraft Systems,"* informed the public that U.S. officials have "strong concerns about any technology product that takes American data into the territory of an authoritarian state that permits its intelligence services to have unfettered access to that data or otherwise abuses that access." In a nutshell, China imposes stringent obligations on its citizens and businesses to support national intelligence activities, meaning China can require its domestic manufacturers and technology companies to share information gathered overseas, in America and elsewhere, with the Chinese government on demand.

Additionally, CISA formed the Cross Sector Unmanned Aircraft Systems Security Working Group to study the security threat of Chinese-manufactured drones and similar devices. The group will explore issues such as incident baseline and reporting, security operations, emergency action plans, damage assessment, nefarious indicators, and tracking best practices.

We urge American companies to be aware of whether your unmanned aircraft systems data is being stored by the drone vendor or other third parties. And if it is being stored, find out how, where, and for how long.

INDUSTRIAL CONTROL SYSTEMS: The real frontier for cybersecurity

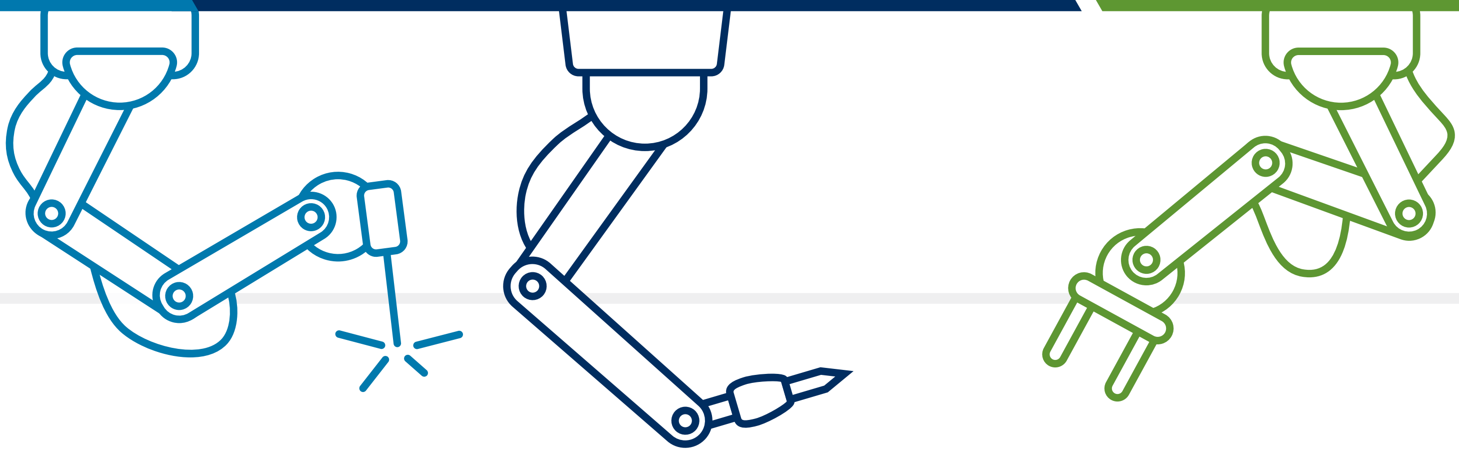
> “Industrial control systems are at the center of our efforts for protecting strategic critical infrastructure.”
>
> **Christopher Krebs**
> CISA Director

Much of critical infrastructure shares a common operational characteristic: a dependence on industrial control systems (ICS). These systems use data to control, monitor, and manage core industrial operations for a wide array of critical infrastructure, spanning transportation systems, telecommunications networks, industrial manufacturing plants, electric power generators, oil and natural gas pipelines, and even the Internet of Things. Increasingly, these systems are accessed through the internet, making them more vulnerable to attack and manipulation. And ICS, which involves the use of data to control industrial operations, is less developed than other areas of information technology in terms of including adequate security.

CISA leads the Federal Government’s unified effort to work with the ICS community to reduce risk to our critical infrastructure by strengthening ICS security and resilience. We have long recognized and prioritized securing these operations, as such systems, if attacked, can be manipulated to cause considerable damage to infrastructure—and people.

ICS Security Issues Are Global

In April 2019, LockerGoga ransomware made a splash in the media when an international organization’s industrial control systems (ICS) were infected, bringing their operations to a halt. CISA’s relationship with international partners enabled us to immediately receive information on LockerGoga and share that information with all of CISA’s partners in a matter of hours. CISA quickly distributed machine-readable products to help our partners protect their networks and systems against the threat. In the months following the initial LockerGoga ransomware attack, international partners continued to share information with CISA, enabling us to develop new products, refine existing ones, and contact partners that were targeted by actors using LockerGoga. Relationships and information sharing make all the difference in cybersecurity, allowing all of us to make meaningful impact across the cyber defense ecosystem when we work together at speed.



CISA is focusing on a unified strategic initiative that will move beyond reactive measures to more proactive ICS security focused on four interrelated and cross cutting pillars.

- First, we ask for greater contributions from the ICS community. In turn, we are delivering more value to them. One example of this collaboration is the CISA and FBI joint technical alert about Russian government malicious cyber activity targeting energy and other critical infrastructure sectors. Information derived from this coordinated work with the private sector is extremely valuable for the ICS community.
- Second, CISA is driving affordable technology innovation across the community to mature collective ICS cyber defense capabilities. We are driving technology developments to harden the cybersecurity defenses of legacy control systems, while building increased security into new ICS development and increasing data visibility.
- Third, CISA is taking the concepts of a cyber kill chain and defense-in-depth and assessing how to apply them to ICS. Recognizing that more facilities are connecting ICS to their internet-accessible networks, we are partnering with the public and private sectors to gather data, analyze, and assess data to improve cybersecurity.
- Fourth, CISA is driving more informed, proactive cybersecurity investments that will lead to stronger ICS security. We can do this by moving to anticipate risk, identifying and removing barriers, and understanding the impact of our actions on the risk landscape.

Each pillar supports specific objectives that require incremental, evolutionary, or disruptive actions. With our partners, we are making significant inroads in securing the ICS environments upon which our critical infrastructure relies. Collectively, with owners and operators, law enforcement, intelligence, and international partners, CISA is striving to reduce risk in a converging cyber-physical landscape.

ICS Joint Working Group: Collaboration and Resources for All

The Industrial Control Systems Joint Working Group marked a milestone this year, celebrating its 10th year hosting face-to-face meetings with the ICS community. The Working Group is a partnership supporting information sharing and collaboration among federal agencies and departments and private asset owners/operators of ICS to reduce risk to the Nation's industrial control systems across all critical infrastructure sectors. Since 2009, the Working Group has held biannual face-to-face meetings, webinars, and workshops to increase information sharing and partner collaboration in research, development, and implementation of secure industrial control systems, making use of the experience of academics, researchers, vendors, consultants, and government experts. Webinars included ways to ensure operational integrity and persistent threat-based security for ICS.

PROTECTING .GOV:
Network Defender

“

On behalf of USAID, I would like to thank your team for its thorough assessment of USAID’s information security infrastructure and high value systems. Not only was the [CISA] assessment team professional and knowledgeable about the task at hand, it provided the Agency with an informative analysis of the results and took the time to help us understand areas that need improvement.

The lessons learned and detailed reports provided to USAID’s Security Operations Center (SOC), Computer Security Incident Response Team (CSIRT), and to senior leadership will assist us in strengthening our security posture. Recommendations made in the assessment will guide USAID to make smart and strategic improvements in the areas of cyber protection, detection, identification, response, and recovery, thereby enhancing our cyber resilience against new threats that arise.

”

Jay Mahanand
Chief Information Officer
USAID, July 11, 2019

Emergency Directive 19-01: “Thwart Domain Name Tampering Now”

CISA issued its first emergency directive (ED 19-01), “Mitigate DNS Infrastructure Tampering” January 22, 2019.

In concert with government and industry partners, CISA had been tracking incidents of Domain Name System (DNS) infrastructure tampering across worldwide networks. Partners in the internet security community first informed us of this activity. We saw attackers using compromised credentials to try to redirect and intercept e-mail traffic across multiple federal agency services and networks. We knew an urgent response was needed to thwart such potentially harmful actions as we saw cyber attacks intent on gaining access to platforms used to manage domain name system records. In the DNS, also known as the “phone book of the internet,” a domain name is the address where internet users can access your website.

By issuing the directive, CISA sought to work with agencies to detect and prevent additional impacts on agencies and systems. To avert damage to federal clients, CISA directed fast, preventative actions based on the best practices for enterprise DNS management. Additionally, when it became aware that multiple executive branch agency domains were being tampered with, CISA notified the domain owners immediately.

CISA required departments and agencies, within 10 business days, to:

- Audit DNS records;
- Change DNS account passwords;
- Add multi-factor authentication to DNS accounts; and
- Monitor certificate transparency logs to ensure authenticity of certificate requests.

BOD 19-02: “Fix Those Weaknesses Before Barbarians Storm Your Gates”

Time is of the essence in all things digital. As federal agencies continue to expand their internet presence and operate more connected and complex systems, it is more critical than ever for federal agencies to rapidly fix vulnerabilities that otherwise could allow malicious actors to compromise federal networks through faulty, public-facing systems.

Recent reports from government and industry partners show that the average time between discovery and exploitation of a vulnerability is decreasing as today’s adversaries are more skilled, persistent, and able to exploit known vulnerabilities.

CISA recognized federal agencies need to act quickly to reduce unauthorized access to federal systems. In April, CISA issued Binding Operational Directive 19-02, “Vulnerability Remediation Requirements for Internet-Accessible Systems,” to cut remediation time of critical vulnerabilities from 30 days to 15 days. The amount of time to fix “high” serious, but not critical, vulnerabilities was reduced to 30 days.

We push ourselves as we push our federal clients. If agencies cannot remediate vulnerabilities in the specified timeframes, we will send a partially populated remediation plan identifying all overdue, in-scope vulnerabilities to the agency point of contact for validation and population, to be returned within three working days of receipt.

Tailored Assistance for State, Local, Tribal, and Territorial Governments

State, local, tribal, and territorial governments find themselves targeted by cyber attacks almost as often as the Federal Government. While partners in our cyber battles, non-federal governments face their own budget and implementation constraints. To share our experience, we developed "CISA Insights" that take applicable cybersecurity guidance from emergency or binding operational directives and other sources and tailor the guidance for all government entities and private industry organizations. These recommendations also include lessons learned, implementation considerations, and resource considerations for organizations in deciding on next steps for their security programs.

This information comes from our experience addressing the same issues across federal executive departments and agencies. As cybersecurity recommendations in directives are not “one size fits all,” customized recommendations ensure that state, local, tribal, and territorial government partners and private industry have tailored guidance to help them address cyber risk management issues in adaptable ways for their organizations.

Although state, local, tribal, and territorial governments and private industry are the target audience for the "CISA Insights," the guidance is applicable to other partners, such as international governments and industries, public-private partnerships, and cross-industry consortiums.

Ransomware is a Scourge: CISA Insights

Recently we've seen more and more instances of business and government being attacked by ransomware. It is a scourge for which CISA provides a host of no-cost services to government partners at all levels, to help them prepare and protect their systems. Successful ransomware attacks can be especially debilitating if they affect critical citizen-facing or revenue-generating services. Medical and other health practices have been known to go bankrupt after ransomware attacks. Law enforcement and other local and state government offices have been forced to spend money they could ill afford to restore systems.

To help fortify state, local, tribal, and territorial governments, CISA works with them to respond to and recover from ransomware incidents—including offering onsite assistance. CISA coordinates with state and local government staff to:

- Identify areas where their cybersecurity practices could be strengthened.
- Assist in developing governance documentation and reviewing response plans.
- Identify critical systems and services and provide recommended recovery actions.
- Work among onsite government offices assisting in response, remediation, recovery, and restructuring efforts, including with partners such as the Federal Bureau of Investigation, local law enforcement, and vendors.

Government partners provided CISA with malware samples, enabling CISA to develop products to help all partners protect their networks against ransomware attacks.

“

Chass,

I wanted to send this quick note as a follow up to the Port of Portland visit on July 8, 2019. These official meetings with private-sector owners, local, state, tribes and federal partners are priceless!

Over the past 12 months I have heard nothing but positive remarks every time DHS-CISA does one of these data collections. Communication, networking, and sharing of data, as well as the current planning progress has brought our communities together which provides me the information I need to share with officials including Governor Kate Brown.

I've used this type of meeting and the FEMA airport assessments as examples when giving presentations and testimony.

Also, the marine partnerships have started on the back of the R-RAP, in fact the U.S. Coast Guard rep (James Merten) stated that his work directly is being impacted by the R-RAP in a positive manner and that we (us) are saving him years of work.

As I stated at the meeting, the sea and river ports that are being looked at in the R-RAP will allow us in the years ahead (post R-RAP) to address infrastructure issues and the Columbia river will play a major role in kick-starting our short and long-term recovery efforts.

Lastly, I appreciate the willingness of you and your team to keep me in the loop as the sponsor of the Oregon R-RAP.

Stay safe, stay focused.

”

Mike Harryman, MA
Office of Governor Kate Brown
State Resilience Officer

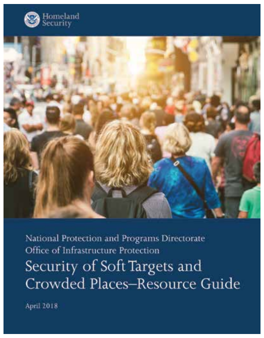
PROTECTING SOFT TARGETS and crowded places

Locations such as transportation centers, parks, restaurants, shopping centers, and entertainment and special event venues are easily accessible, attract large numbers of people on a predictable basis, and are often vulnerable to attacks using simple tactics and readily available weapons. CISA works with partners to identify, develop, and implement innovative and scalable measures to mitigate risks to these venues, which often play an integral role in the country's economy. CISA provides partners at every level a wide range of resources, programs, and training to increase awareness and promote effective strategies and tactics to counter threats, including bombs/improvised explosive devices (IEDs) and active shooters, such as the examples that follow.

New Security of Soft Targets and Crowded Places Resource Guide

https://www.cisa.gov/securing-soft-targets-and-crowded-places

CISA published an updated *Soft Targets and Crowded Placed Resource Guide* in April 2019 to reflect recent attacks and help prepare stakeholders for threats ranging from bombings and active shooters to drones. The guide raises awareness of and access to the wide range of free DHS capabilities supporting risk mitigation for businesses, government, first responders, and individuals and organizations across the Nation. Resources include guides, information materials, in-person and online training tools, videos, and websites in the categories of addressing the basics of security; identifying suspicious behavior; protecting against unmanned aircraft systems; preparing and responding to active assailants; and preventing and responding to bombings.


Homeland Security
National Protection and Programs Directorate
Office of Infrastructure Protection
Security of Soft Targets and Crowded Places–Resource Guide
April 2018

> "The ability to train our staff in a program of this quality gives them additional tools to enhance our services to both our clients and our guests, while making public assemblies safer."

Jay Brock
Senior Vice President
Operations and Training,
Contemporary Services Corporation

Working with Faith-Based Communities

CISA teamed with the Secure Community Network (SCN) in April to host a tabletop exercise involving Jewish community leaders from across the Nation, federal and state law enforcement, and interagency partners. The exercise examined the potential response to a notional event focused on threats of violence, including scenarios based on current events. The exercise was the latest in several initiatives to improve threat information sharing, conduct training and exercises, and develop and disseminate technical resource documents.

CISA partnered with the DHS Center for Faith and Opportunity Initiatives and the White House to conduct the Faith-Based Safety and Security Symposium with nearly 200 key faith-based leaders and government representatives. The event focused on the importance of securing faith-based communities from all types of violence and exchanging best practices used by faith-based groups for information sharing, preparedness, response, and recovery. Partnership and collaboration are essential to building secure and resilient communities. The need to preserve the right to peacefully congregate and practice a religion of choice is integral in the Constitution, and an attack against such facilities is a direct threat to American democracy. The Symposium took place September 25, which was National Awareness Day for the "If You See Something, Say Something" campaign that works with partners year-round to inspire, empower, and educate the public on the importance of reporting suspicious activities.

Bombing Prevention

CISA has trained state and local entities such as the New York Police Department and the Port Authority of New York through a national Train-the-Trainer pilot program. The Counter-IED Train the Trainer program aims to improve interagency cooperation and expand distribution of awareness products and services for personnel and agencies, critical infrastructure owners and operators, and public and private sector stakeholders.

CISA expanded an effective counter-improvised explosive device (IED) awareness training initiative to the private sector. In June CISA trained staff from Contemporary Services Corporation (CSC) in Bombing Prevention Awareness and Protective Measures. CSC is the largest U.S. public event crowd management and security provider, covering stadiums, arenas, ballparks, festivals, theaters, and other large venues. The trainings enable participants to teach the two courses and six other one-hour, awareness-level courses. A CSC staff member taught the first courses led by a private sector partner in August—Response to Suspicious Behaviors and Items for Bombing Prevention and Introduction to the Terrorist Attack—to approximately 70 students.

CISA expects **10 CSC trainers** and **50 departments** to participate in the Train The Trainer initiative by the end of calendar year 2019, and to process at least **1,500-2,000 students** through the program by the end of 2020.

Partnering with Chemical Facilities to Keep Our Communities Safe

The Chemical Facility Anti-Terrorism Standards (CFATS) program regulates and works with businesses and other organizations to reduce the risks associated with certain hazardous chemicals and prevent them from being exploited in a terrorist attack.

CFATS applies to facilities across many industries that produce, store, or distribute any of more than 300 chemicals of interest that present security issues. CISA Chemical Security Inspectors work with and inspect facilities across the country—approving security plans and verifying the implementation of security measures.

CFATS at a Glance FY19

Number of inspections performed	**1,799**
Number of top screens reviewed	**2,669**
Number of security plans reviewed/approved	**520**
Number of compliance assistance/tech consults provided	**512**
Number of outreach engagements performed	**1,985**

Active Shooter Training

CISA's Active Shooter Preparedness and Security Program provides comprehensive resources that help public and private sector stakeholders develop effective emergency action plans, identify potential behavioral indicators, mitigate the impacts of an attack, and quickly recover from an incident.

In FY 2019 (through July 31):

- The program conducted 26 in-person Active Shooter Workshops with 3,250+ participants. By year end, it will complete 42 workshops with about 5,000 participants.
- Nearly 673,000 learners completed the "What Can You Do" Independent Study Guide.
- Nearly 673,000 users accessed the Active Shooter Preparedness Website for information.

In addition to 30+ traditional Active Shooter Preparedness Workshops across the country, in March, CISA partnered with the Foundation of Shalom Park in Charlotte, NC, to host an 8-hour workshop, with nearly 140 participants from 87 houses of worship, K-12 schools and higher-education institutions, chemical facilities, financial institutions, transportation services, hospital and healthcare facilities, and manufacturing plants. Participants gained valuable emergency action planning information from qualified instructors and emergency planning professionals, and unique first-hand perspectives from active shooter survivors and first responders through innovative video interviews. They also had the opportunity to develop and customize draft emergency-action plans for their own organizations through collaborative breakout sessions.

Los Angeles Dodgers Full-Scale Exercise

March 8, 2019
Los Angeles, California

The Los Angeles Dodgers Full-Scale Exercise was designed to enhance security and resiliency of the Los Angeles Dodgers and the City of Los Angeles by testing emergency response procedures; establishing best practices in response efforts; and improving awareness of tools, resources, needs, and the operations of both stadium officials and first responders. The outcome of the exercise not only increased the resiliency of Dodger Stadium, but also informed future decision making and enhanced preparedness and response planning efforts of local response agencies.

More than 700 participants, including CISA and Dodgers executive leadership, security, and operations personnel, and local first responders from Los Angeles Fire and Police Departments came together to test tactical response and coordination to a complex coordinated attack at Dodger Stadium. The exercise focused on both public and private sector abilities to respond to the simulated events, which included managing crowds, VIPs, and people with special needs; evacuation and shelter-in-place decisions; integrating public-sector emergency medical teams with on-site medical providers; and integrating on-site, off-duty uniformed law enforcement with responding, on-duty law enforcement. The exercise also aimed to foster a greater understanding of all of the stakeholders' capabilities and build relationships between private and public sector partners in the Los Angeles area.

“

There is a lot that goes on behind the scenes to ensure that our fans enjoy an exceptional and seamless experience at Dodger Stadium. In line with that, we take the security of our fans, staff and players very seriously. This is why we feel it's important to work with our partners at CISA and in the community around the stadium to invest the time and resources into planning and testing our security and emergency procedures. In the unlikely event that something was to happen at Dodger Stadium, having gone through this exercise puts us in a better position to respond as a unified team.

”

Stan Kasten
President & CEO, Los Angeles Dodgers

EMERGENCY COMMUNICATIONS

for safer, better-prepared communities

> “The information the State Markers provide is a huge value-add in understanding how to develop and operationalize the Statewide Communication Interoperability Plan.”

Jason Bryant
Kansas Statewide Interoperability Coordinator

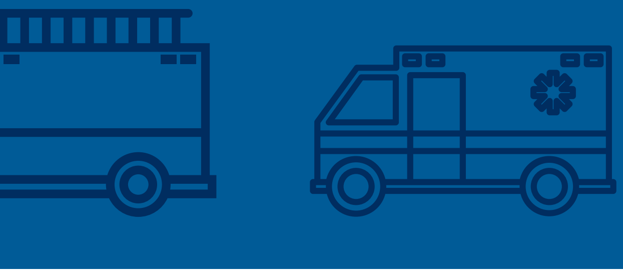
Ensuring operable and interoperable communications and real-time information sharing among responders during all threats and hazards is paramount to the safety and security of Americans. From a small-scale incident to a significant natural or manmade disaster, responders depend on the seamless flow of voice, video, and data communications to respond to and recover from events that threaten lives and property.

CISA leads the Nation’s public safety and national security and emergency preparedness communications efforts. The Agency provides training, coordination, tools, and guidance to help its federal, state, local, tribal, and territorial government and industry partners develop their emergency communications capabilities and increase interoperability.

Stakeholder-Focused Updates to the Nation’s Strategy for Emergency Communications

www.cisa.gov/NECP19

National Emergency Communications Plan Vision: Enable the Nation’s emergency response community to communicate and share information securely across communications technologies in real-time, including all levels of government, jurisdictions, disciplines, organizations, and citizens impacted by any threats or hazards event.



National Collaboration for a New NECP

CISA collaborated with SAFECOM and the National Council of Statewide Interoperability Coordinators to update the *National Emergency Communications Plan* (NECP), released September 25, 2019. Over two years, CISA engaged 3,500+ representatives from public safety agencies, non-governmental organizations, and other groups through interviews, public webinars, working groups, and a national feedback initiative. CISA drew on this input, along with lessons learned from 2008 and 2014 NECP implementation, and real-world events to craft new goals, objectives, and success indicators.

State Interoperability Markers Program Enables National Baselining

CISA partnered with the National Council of Statewide Interoperability Coordinators to develop 25 indicators of interoperability maturity aligned with the SAFECOM Continuum of “initial,” “defined,” or “optimized” maturity. CISA then led a State Interoperability Markers Workshop in July 2019, using Kansas as a test case for a state evaluation. Thanks to the program, states and territories can assess themselves against the markers, providing the first-ever national baseline. This data helps states and territories identify gaps to inform strategic and financial planning and enables CISA to tailor support to enhance their interoperable communications capabilities.

Special Event Support

Large public events pose a number of security challenges. CISA supports special events through its regional offices, which offer a range of services such as site security assessments, cybersecurity support, interoperable communications, training, exercise facilitation and technical expertise. Working together with a wide range of federal and state, local, tribal, and territorial response agencies and industry partners, CISA’s regional teams often begin collaborating on major events more than a year in advance of an event. CISA has supported events like the Super Bowl, Boston Marathon, Rose Bowl and Parade, and many other high-profile events.

CISA Event Support At Work

Protective Security Advisors supported 19 National Special Security Events and Special Event Assessments during calendar year 2019.

A CISA Emergency Communication Coordinator supported Super Bowl LII by developing the Communications Concept of Operations and quick reference cards for field personnel and provided onsite event support.

In 2019 CISA staff engaged over 1,700 places of worship, hotel, sport, K-12, and shopping facilities performing security visits in order to assess potential vulnerabilities and inform security representatives of options to consider to reduce the impacts of an attack.

CONCLUSION:

AN AGENCY FOR THE 21ST CENTURY —AND BEYOND!

We need excellent mission support to address the advanced threats and hazards of today. This means that not only do we need staff expertise (continually enhanced through training and collaboration with functional experts), but we also need an internal organizational structure and operating processes that enable our staff to deliver optimum service to and on behalf of the Nation. We are undertaking a CISA 2020 internal change management campaign to unify the agency, enhance mission effectiveness, and improve the overall CISA employee experience to support our mission as effectively as possible.

CISA mission functions must deliver customer-focused support in order for CISA operations to secure and enhance the resilience of the Nation's infrastructure. Across all our mission support elements, CISA will identify and apply lessons learned from across the Federal Government and private industry. We will ensure mission operators and partners receive new capabilities in a timely, effective manner to address evolving threats. We will create a culture that fosters and rewards innovation.

Effective mission support is essential to defending today and securing tomorrow. Our desired outcome is to exceed Federal Government averages on mission support performance.

As the preceding pages of selected highlights attest, we have accomplished a great deal during our first year. We were able to achieve all this and more, through the efforts of the great CISA workforce—dedicated, talented, and committed people who work day in and day out on behalf of the Nation—and in partnership with you. We couldn't have done this without you, our partners and stakeholders among all levels of government, all industry sectors, the intelligence and defense communities, academia, and our international allies. Thank you. And thank you to Congress and the Administration, for enabling us to more effectively serve the Nation as the Cybersecurity and Infrastructure Security Agency.

CISA
CYBER+INFRASTRUCTURE

WWW.CISA.GOV