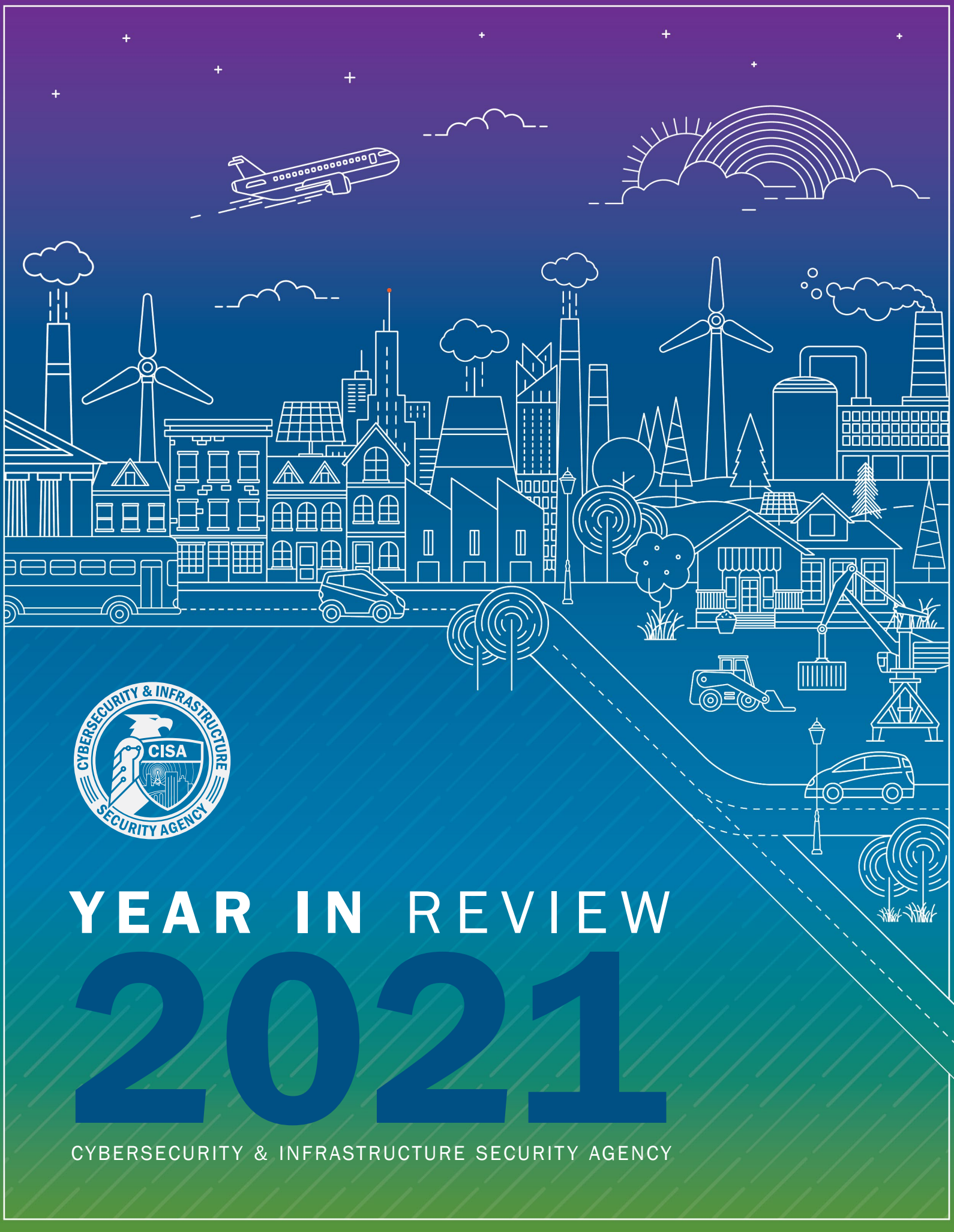


YEAR IN REVIEW

2021

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

CISA YEAR IN REVIEW 2021 | Maturing Partnership into Operational Collaboration

CONTENTS

01

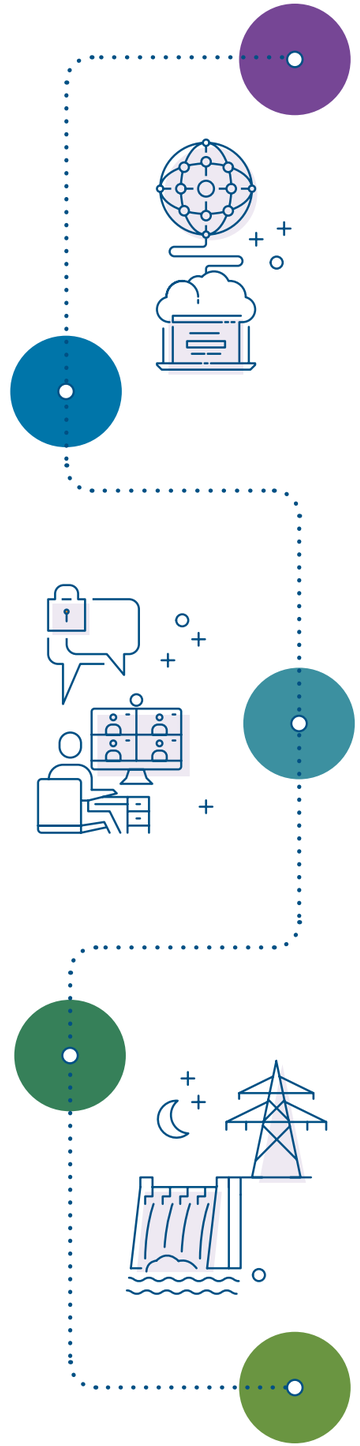
Introduction

As 2021 dawned, the nation faced a range of tough issues, including the ongoing COVID pandemic, civil unrest around the country—and even at the U.S. capitol—and mis- and dis-information campaigns. At the same time, increasingly disruptive cyberattacks demonstrated the very real impact of the virtual environment on physical infrastructure, starting with the Solar Winds supply chain compromise that was first recognized in December 2020.

While the nation grappled with the impacts of these issues, CISA deepened its public-private partnerships to expand operational collaboration with external partners. Under new leadership and a new Administration, this shift could be seen in the agency's response to cyber and physical incidents over the past year, as well as new initiatives like the Joint Cyber Defense Collaborative (JCDC) that CISA launched to unify cyber defense capabilities that are currently spread out across multiple federal agencies, many state and local governments, and countless private sector entities.

The following pages provide insight into CISA's work across its mission space in 2021, following the outline of the Director's Strategic Intent:

- **PARTNERSHIPS:** We will sustain our trusted and effective partnerships between government and the private sector, which are the foundation of our collective effort to protect the Nation's critical infrastructure.
- **FEDERAL CYBERSECURITY:** We will continue to drive fundamental cross-agency organizational change to reduce the cybersecurity risk to the Federal Civilian Executive Branch.
- **CRITICAL INFRASTRUCTURE SECURITY:** We will bolster our efforts to secure cyber, physical, and communications critical infrastructure and sustain the operations that are vital to the American people.
- **INDUSTRIAL CONTROL SYSTEMS (ICS):** We will maintain our operational focus on ICS entities and move forward with the implementation of sensors and other capabilities.
- **PUBLIC GATHERING SECURITY:** In fulfilling our role as a national coordinator for critical infrastructure and as a Sector Risk Management Agency ourselves, we will continue to lead the effort to reduce the risk and impact of attacks against public gatherings and crowded places.
- **CLIMATE RESILIENCE:** We will ensure operational readiness in the regions to support information sharing among federal, state, and local partners in preparation for extreme climate events.
- **THE CISA WORKFORCE:** We will continue to attract and retain world-class talent through a talent management ecosystem that spans recruiting and hiring, to onboarding and integration, training, recognition and promotion, and succession planning and retention.



A YEAR OF **FIRSTS**

In August 2021, CISA Launched the Joint Cyber Defense Collaborative (JCDC), creating an entirely new function that unites partners across government and industry to coordinate cybersecurity planning, share information and issue jointly developed guidance to help reduce cyber risk. At the end of 2021, the JCDC Alliance partners include

15 of the nation's largest cybersecurity, technology and infrastructure companies,

including the major Internet Service Providers, Cloud Service Providers, and Cybersecurity Companies. **(At the time of this report's release, that number has grown to over 20).**

CISA released its **first international strategy**, CISA Global, a strategic guide for the agency's international efforts. In coordination with the State Department's Office of the Coordinator for Cyber Issues, CISA hosted the agency's first ever International Partner Call for

293 participants from more than 75 countries

to provide background and mitigation resources on the recent supply chain compromise.

With the increasing availability of a vaccine for COVID-19, CISA completed its first cybersecurity sensor deployment supporting a COVID-19 fill & finish vaccine manufacturer. This is the first of several entities outfitted with CISA's sensing capabilities to

hunt for malicious cyber activity targeting key entities within the COVID-19 supply chain.

CISA doubled monitoring services deployed to key entities in the vaccine supply chain in support of the national pandemic response. These entities can be characterized as small to medium-sized businesses that fell below the thresholds for services as defined by the Federal COVID response effort, but through CISA analysis were determined as critical to vaccine manufacturing and scaled production activities.

CISA launched ChemLock, a new

voluntary chemical security initiative.

The Chemlock program provides facilities that possess dangerous chemicals tailored, scalable, no costs services and tools to improve their chemical security posture. CISA gained its chemical security expertise from more than a decade of working with high-risk chemical facilities under the Chemical Facility Anti-Terrorism Standards (CFATS) regulatory program.

With the release of BOD 22-01 on Reducing the Significant Risk of Known Exploited Vulnerabilities, CISA established the

first ever catalog of Known Exploited Vulnerabilities,

fundamentally transforming how the federal government (and the nation as a whole) prioritized vulnerability mitigation efforts. This catalog became a key tool during the log4j response.

As part of the log4j response, CISA created

an authoritative source of impacted systems for a specific vulnerability for the first time.

CISA created this Github repository of known vulnerable products, which served as the authoritative source for public and private organizations, and published an open-source scanner to help organizations identify exposure to vulnerable versions of log4j.

CISA hosted the first **Cross Sector Space System Critical Infrastructure Working Group** to assess the risk to space systems and to understand the risk to National Critical capabilities. The Working Group is comprised of

13 government and 20 industry organizations & 22 Subject Matter Experts

(SMEs) that will identify and develop strategies to minimize risks to space systems that support the nation's critical infrastructure. In partnership with the Office of Space Commerce and the DHS Office of Strategy, Policy, and Plans (PLCY), CISA also moderated the inaugural space cybersecurity symposium.

CISA issued its first three administrative subpoenas in April and May 2021,

implementing a key authority in the FY21 National Defense Authorization Act.

This new authority has empowered CISA to identify vulnerabilities resident on critical infrastructure systems and has directly led to the engagement of key stakeholders to drive remediation of identified vulnerabilities.

CISA released a first-of-its-kind "Business Case for Security" guide

to provide unique insights into costs (i.e., operational, budgetary, and reputational) associated with deliberate disruptions to operations and corresponding recommendations for security professionals to communicate the importance of investing in security to C-suite leadership.

02

Partnerships

Collaboration is at the heart of CISA's mission, and CISA strengthens its operational efforts through strong domestic and international relationships that lead to valuable and actionable information-sharing. CISA collaborates through both formal and informal mechanisms like our longstanding work with Sector Coordinating Councils (SCCs) and Government Coordinating Councils (GCCs) through which the federal government and private industry collaborate, plan, and share information within and across 16 critical infrastructure sectors. Under the FY21 National Defense Authorization Act (NDAA), CISA also established the Joint Cyber Defense Collaborative (JCDC), which integrates the unique cyber capabilities of government at all levels, the international community, the private sector, and others to reduce cyber risk through collective cyber defense operations. The JCDC addresses two critical challenges: creating a more inclusive and operationally integrated community of cyber defenders to plan, exercise, and fight together; and galvanize cybersecurity community action. Additionally, on December 1st, (2021), Director Easterly announced the appointment of the intial

23 members to serve on CISA's newly established Cybersecurity Advisory Committee.

Members present recommendations and advise the Director to strengthen the cybersecurity mission of the agency through the development, refinement, and implementation of policies, programs, planning, and training. The Committee held its first meeting on December 10.

We also collaborate via informal and situational partnerships like CISA's work with the Federal Emergency Management Agency (FEMA) to develop the "Building Private-Public Partnerships Guide." This document provides guidance and best practices for state, local, tribal, and territorial (SLTT) jurisdictions to establish and maintain private-public partnerships to coordinate whole of society mitigation, response, and recovery planning and preparedness efforts. The recommendations in the guide can also help these jurisdictions develop, manage and scale private-public partnerships to strengthen their respective health and safety, economic security, and community resilience.

Through the Enduring Security Framework (ESF), CISA also partnered with the National Security Agency (NSA) and the Office of the Director of National Intelligence (DNI) to release a paper which identifies and assesses risks and vulnerabilities introduced by 5G ("Potential Threat Vectors to 5G Infrastructure"). The ESF 5G Threat Model Working Panel, a subgroup within the ESF, examined three major threat vectors in 5G: standards, the supply chain, and threats to systems architecture—to develop a summary and technical review of threats posed by 5G adoption in the United States and sample scenarios of 5G risks. Lastly, in partnership with DHS Science and Technology Directorate and the private sector, CISA funded efforts to develop the Position, Navigation and Timing (PNT)

PARTNERING TO BUILD THE WORKFORCE

CISA partnered with the National Science Foundation (NSF) and the Office of Personnel Management (OPM) to host the 2021 CyberCorps®: Scholarship for Service (SFS) Virtual Job Fairs in March and September. The job fairs provide a forum for college students in the SFS program to seek employment from federal, state, local, tribal, and territorial governments.

conformance framework which serves as a guide for building more secure and resilient PNT end user equipment. As a result of this partnership, DHS published anti-spoofing algorithms for GPS receivers. These algorithms are available on the CISA GITHUB site.

In June 2021, CISA and the Federal Bureau of Investigation (FBI) launched a 90-day pilot for a joint initiative called “Operation Flashpoint.” Operation Flashpoint enhances CISA’s Bomb-Making Materials Awareness Program (BMAP) and expands outreach and support to encourage U.S. private sector entities that sell Explosive Precursor Chemicals to take voluntary measures to properly secure these chemicals and to report and or prevent suspicious transactions. In response to several cyber incidents, CISA worked with high-risk chemical facilities and facilities that possess dangerous chemicals to identify potential vulnerabilities and share mitigation measures to ensure the security of those chemicals.

This past year, CISA also assisted U.S. Cyber Command’s (USCYBERCOM) Training and Exercises Directorate (J7) as they updated their Joint Advanced Cyber Warfare Course (JACWC) to become the new Joint Cyberspace Fundamentals Course (JCFC). The JCFC effort shifted the course focus from a comprehensive overview of roles and capabilities to a more strategic overview of the policy, legal authorities, strategy, and operations related to USCYBERCOM and cyber warfare. In April, CISA supported a USSOUTHCOM-led Joint Cyber Combatant Command Assistance Team (JCCAT) to assess current capabilities and assistance needs of key Colombian government cyber entities in Bogota.

On a regional and local level, CISA partnered with the Cybercrime Support Network to develop National Information Exchange Model (NIEM) Cyber Domain content for **38 state, local, tribe, and territorial (SLTT) entities**. The new cyber information sharing standard will ensure a coordinated community effort to increase

PARTNERSHIPS

Collaborating to Advance a Software Bill of Materials (SBOM)

CISA convened the first SBOM-a-rama conference, bringing together hundreds of participants across government and industry to work together to advance the cause of the Software Bill of Materials, a key Cyber EO deliverable and ever more critical in light of the log4j vulnerabilities.

Collaborating on Critical Infrastructure Security

As part of CISA’s ongoing work to strengthen our nation’s critical infrastructure, the agency held

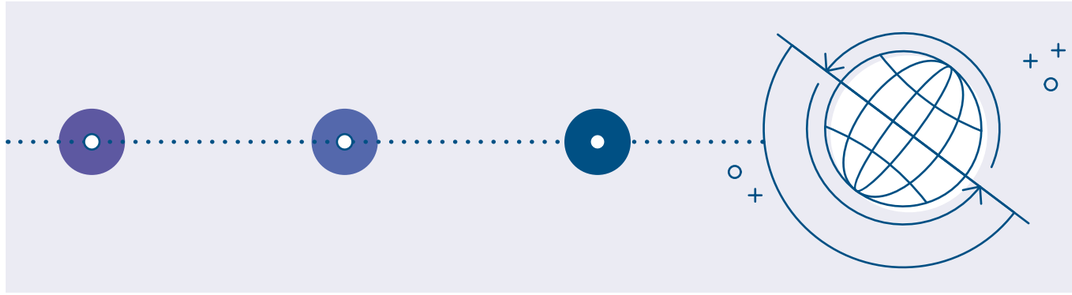
411 meetings in FY 21

under the Critical Infrastructure Partnership Advisory Council (CIPAC) framework, a forum in which the government and private sector entities, organized as coordinating councils, can jointly engage in a broad spectrum of activities to support and collaborate critical infrastructure security and resilience efforts.

visibility of cyber risks through consistent data and information sharing. Additionally, through its Dallas, TX based Region 6 team, CISA facilitated a planning meeting for the World Petroleum Congress with the City of Houston Emergency Management, Galveston County Emergency Management, U.S. Coast Guard Incident Management Division Chief, and the Federal Bureau of Investigation (FBI) Special Events Coordinator. This meeting offered a forum for these key partners to discuss the development of a response and communication framework. CISA’s Philadelphia, PA, based Region 3 team coordinated with the U.S. Department of Health and Human Services (HHS), which is the Sector Risk Management Agency (SRMA) for public health, to collaborate on outreach to large pharmacy chains engaged in administering the COVID-19 vaccine. The region brought together federal partners from CISA and other parts of DHS, along with HHS and FBI to engage with pharmacy chain senior leadership. This initiated a “top down” approach in understanding of threats, protective measures, and critical information sharing.

CISA’s partnership activities extended across the globe, and we were grateful to our international partners for their willingness to engage. Throughout 2021, CISA signed cybersecurity Memoranda of Understandings with close partners, concluded bilateral Work Plans operationalizing and aligning mutual efforts to counter cyber threats, hosted a series of targeted training and capacity building opportunities to build the cyber resiliency of geostrategic partners, and participated in multilateral engagements to influence and offset malign influences. CISA continued to develop and enrich priority international partnerships that resulted in bidirectional information sharing, often of a timely and sensitive nature enabling CISA action to mitigate and minimize harm from cyberattacks. Below are some salient snapshots of CISA’s 2021 international engagements.

Between February and March 2021, as part of our country’s bilateral collaboration with Mexico, CISA delivered counter improvised explosive device (C-IEC) trainings to Mexico’s Naval Secretariat, Secretariat of National Defense, Ministry of Security and Citizen Protection, and Federal Protective Service, as well as to participants from the National Coordination of Civil Protection and General Prosecutor’s Office. Conducted in partnership with the U.S. Department of State’s Export Control and Border Security (EXBS) Program, the training represented OBP’s first training delivery in Spanish. This training also represents the first-ever collaboration between DHS and State/EXBS Mexico. The courses utilized the expertise and cooperation of a range of U.S. government agencies to deliver training and technical assistance to the Mexican government. In March, CISA also became the only non-African member of the Africa Computer Security Incident Response Teams (CSIRT) Working Group funded by the Department of State Office of the Coordinator for Cyber Issues and organized by the Software Engineering Institute (SEI’s) CERT division. In July, CISA and the Israel National Cyber Directorate



(INCD) approved a bilateral Work Plan establishing four lines of collaboration including: operations; 5G and supply chain security; cyber hygiene; and emerging technologies. In August, CISA signed a Memorandum of Understanding with Singapore's Cyber Security Agency, announced by Vice President Harris. During October through December, CISA deployed its first-ever Cyber Fellows to South Korea, Paraguay and Ireland through its inaugural participation in the Department of State's Embassy Science Fellows (ESF) program.

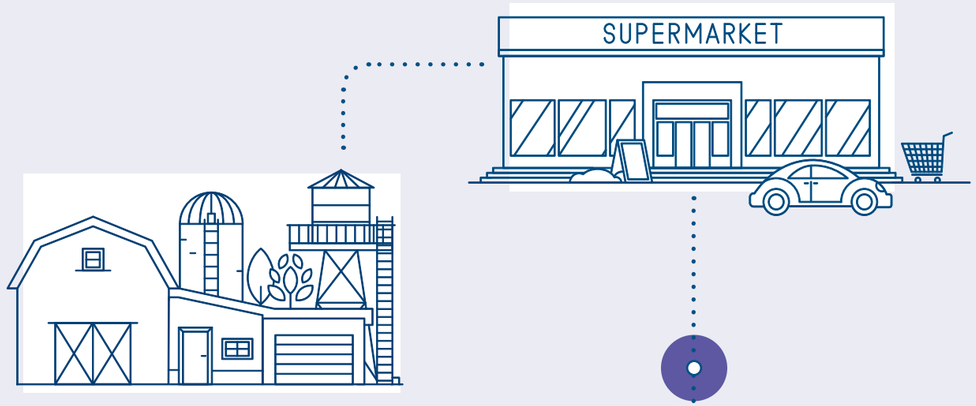
In an example of how CISA coordinated both internationally and across the interagency, in July, CISA participated in the DHS-led, State Department Counterterrorism (CT) Bureau-sponsored, Soft Target Security Workshop for law enforcement and government representatives from across South-eastern Europe. The workshop was the first of its kind and included over **100 international participants** from **ten countries**, and sessions were translated into **six languages**.

> **In one of the most collaborative and global products we have released to date, CISA released an 8-seal Cyber Security Alert**

in November, as part of the global response to the log4j vulnerability. This product included joint seals with the NSA and the FBI, as well as the full U5 community—including two agencies from New Zealand.

ENGAGING STAKEHOLDERS TO SUPPORT IMPLEMENTING THE NATIONAL EMERGENCY COMMUNICATIONS PLAN (NECP)

CISA undertook extensive stakeholder engagement activities to support implementation of the National Emergency Communications Plan (NECP). This included hosting **six public webinars** for more than **2,000 total participants** on key implementation issues including ransomware, inclusive governance, human factors, priority services, continuity, and emerging technology.



PARTNERING FOR INNOVATIVE TECHNOLOGY

Over the past two years CISA has developed a comprehensive approach to partnering with DHS Science & Technology (S&T) Research & Development (R&D) to meet CISA's priorities for innovative technology.

In FY21 CISA stakeholders are actively participating in **33 ongoing R&D projects totaling over $45M**.

The success of CISA's collaboration with DHS S&T was instrumental in receiving an additional **$157.5M** in the Infrastructure Investment and Jobs Act for future critical infrastructure security and resilience research and development.

DELIVERING ON INTERDEPENDENCY

The collective efforts of CISA, the U.S. Indo-Pacific Command (INDOPACOM), and the Hawaii partnerships, under the Interdependencies of Critical Energy Infrastructure (ICEI) Memorandum of Understanding (MOU), produced a tangible deliverable with the publication of the "Hawaii Critical Infrastructure Interdependency Analysis Guide". This milestone of the ICEI roadmap, which was set forth back in June 2019, was successfully completed despite the challenges presented by the global pandemic's impact on physical collaboration and travel requirements. With this deliverable, the ICEI partners in the Pacific Region have set themselves on a solid path of identifying critical infrastructure (CI) and CI interdependencies/dependencies throughout the State of Hawaii as envisioned in the ICEI MOU.

UNIFYING OUR MESSAGE

CISA released an 8-seal Cyber Security Alert on Log4j-Related Vulnerabilities, which included joint seals from the NSA and the FBI, as well as the full U5 community—including two agencies from New Zealand, making it one of the most collaborative products we have released to date and highlighting CISA's growing engagement with key international partners.

03

Federal Cybersecurity

CISA continues to drive fundamental cross-agency organizational change to reduce the cybersecurity risk to the Federal Civilian Executive Branch (FCEB). By providing innovative technology capabilities, first-rate services, and real-time information, CISA helps federal agencies manage sophisticated cybersecurity risks.

With the release of its Cybersecurity Executive Order (Cyber EO), the White House recognized CISA as a key cybersecurity partner. Under the Cyber EO, CISA was tasked to stand up and lead the Endpoint Detection and Response (EDR) initiative. In fewer than 5 months, CISA rapidly engaged with and assessed federal agencies' EDR capability needs and moved from planning to executing to fill agency capability gaps. Moreover, as part of the Cyber EO, CISA published groundbreaking guidance to drive security advances across the federal government and nation, including the Cloud Security Technical Reference Architecture and the Zero Trust Maturity Model. Finally, CISA developed new contracting clauses that will dramatically increase security for federal vendors and provide CISA with deeper insight into security risks.

As part of the DOTGOV Act of 2020, CISA was required to take ownership of administering the .gov top-level domain (TLD). This transfer to CISA from General Services Administration (GSA) was executed in 2021 and has been a significant step in the agency's role in federal cybersecurity. The .gov TLD exists so the public can readily identify the online services of bona fide U.S.-based government organizations. Since the TLD underpins communication with and within federal government institutions, all aspects of .gov administration have cybersecurity significance.

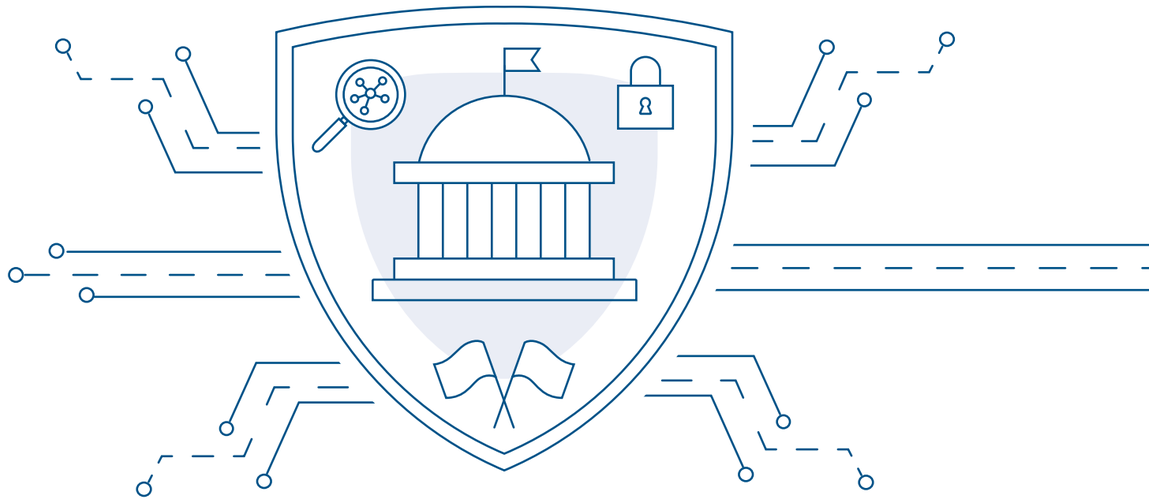
Additionally, TLD is critical infrastructure for SLTT governments throughout the country and central to the availability and integrity of thousands of online services relied upon by millions of users. Of note, CISA provides this service free of charge to SLTT governments, including election officials and others.

ENHANCING THE NATIONAL SECURITY POSTURE

On May 12, 2021, President Biden signed Executive Order 14028: Improving the Nation's Cybersecurity, designed to enhance the national cybersecurity posture, and improve protection of the nation's critical infrastructure and federal networks.

CISA completed all **35 tasks** assigned to the agency to improve information sharing, modernize federal cybersecurity standards, and enhance software supply chain security.

CISA products in support of the E.O. include the Cloud Security Technical Reference Architecture (CSTRA) and the CISA Zero Trust Maturity Model, which has become a prominent reference in the Federal Zero Trust Strategy.



SUPPORTING **NATIONAL CYBERSECURITY**

CONDUCTING CYBERSECURITY EXERCISES ON A NATIONAL SCALE

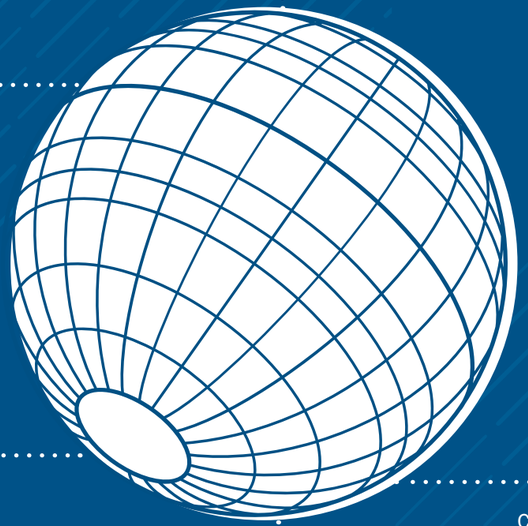
Cyber Storm, CISA's premier biennial cybersecurity exercise, was designated as the National Cybersecurity Exercise required by Section 1744 of the FY21 National Defense Authorization Act (NDAA). Cyber Storm's designation as the National Cybersecurity Exercise is reflective not only of the maturity and impact of the exercise on a national scale, but also of the broad participation in the exercise which includes federal, state, and local governments, private sector entities representing multiple critical infrastructure sectors, and international partners from more than 15 countries.

ADVISING ON THE COLONIAL PIPELINE DARKSIDE THREAT

CISA and the Federal Bureau of Investigation (FBI) released a Joint Cybersecurity Advisory (AA21-131A) in response to a ransomware attack on Colonial Pipeline by a threat actor known as DarkSide. The advisory also included technical details regarding the nature of the attack, as well as potential mitigation steps that critical infrastructure owners could take to segment and protect IT and OT networks.

TRANSLATING CYBERSECURITY AWARENESS

The White House, all 50 states, Washington, D.C., and four territories (American Samoa, Guam, Puerto Rico, U.S. Virgin Islands) signed proclamations declaring October as Cybersecurity Awareness Month. As part of efforts commemorating 18th year of Cybersecurity Awareness Month, CISA translated numerous Cybersecurity Awareness Month materials developed by the agency's partner, National Cyber Security Alliance, into Arabic, Chinese, Portuguese, French, and Spanish.



INCREASING INTEREST IN PRODUCTS

CISA publishes TLP:WHITE products as part of the National Cyber Awareness System. Each operational product offers a variety of information for users with varied technical expertise. Those with more technical interest can read the Alerts, Analysis Reports, Current Activity, or Bulletins. The number of pageviews per product has steadily gone up in the last few years. In Q1 of 2019, there were 36,816 page views of Activity Alerts. In 2020, that number rose to 353,275, and for Q1 2021, that number had again risen to 578,649, a 63.8% increase from the previous year and an incredible 1,471.7% increase over 2019 figures.

IDENTIFYING VULNERABILITIES IN PUBLIC-FACING INTERNET CONNECTIONS

CISA initiated a pilot program to scan publicly available internet connections of 700+ key entities in the vaccine manufacturing, production, and distribution supply chain to identify vulnerable Internet Protocol (IP) addresses and inform those entities of possible risks.

SUPPORTING REGIONAL CYBERSECURITY

CISA continues to assist critical SLTT and private critical infrastructure owners and operators in reducing the risk to their systems and assisting them with responses efforts during cyber events. Examples of efforts this year include:

- In response to the Ransomware Attack on the Crystal Valley Cooperative in Mankato Minnesota, CISA cybersecurity field personnel shared indicators of compromise from a Co-Op ransomware incident that occurred in another state. CISA assisted the Cooperative as they worked with third parties such as RSM and Emisoft to restore systems, including drawing a connection between the success of the ransomware attack to an open patch on a legacy system. The coordinated effort resulted in the restoration of affected systems in under a week and mitigated risk impacting 120 grain storage locations, 16,000 Co-Op farmers, feed manufacturing, and Bio-Fuels production.

- CISA cyber security field personnel partnered with a large shipping company in the development of a cybersecurity "Regional Action Template". This template included an incident management communication plan and functional exercise plans. The plan will assist the large shipping company in their corporate regional response to cybersecurity incidents and will enhance the overall security posture of the company.

- As part of its Implementing the National Emergency Communications Plan (NECP) Webinar Series, CISA partnered with the City of Tulsa, Oklahoma, to conduct a webinar titled, "Addressing the Ransomware Threat to Emergency Communications." Over 500 participants joined the webinar to learn more about critical topics such as:

  - What ransomware is and how to protect emergency communications systems
  - What to do if a mission-critical system is attacked by ransomware
  - Resources and actions to prepare for and recover from ransomware attacks

04

Critical Infrastructure Security

Critical infrastructure describes the systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. In addition to bringing significant technical expertise to its critical infrastructure security efforts, CISA also works extensively with government and private sector partners and collaborates with stakeholders on training, exercises, assessments and other resources.

For example, the CISA Gateway program completed its multi-year migration to a Federal Risk and Authorization Management Program (FedRAMP) High government cloud (GovCloud) environment. The Gateway program provides a suite of infrastructure protection and resilience tools and applications that partners across the CISA mission space can use to help secure infrastructure and respond to risks and threats. By migrating CISA Gateway to the cloud, CISA is achieving multiple benefits, such as enhanced cybersecurity protections and increased capacity for CISA Gateway and its users.

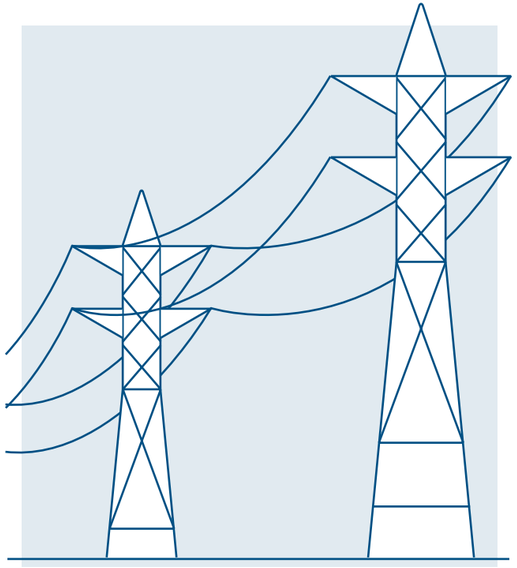
In close collaboration with Chemical Sector partners, CISA also developed the Chemical Sector Security Awareness Training resource to address fundamental security priorities for chemical facilities. Similarly, CISA released the Surveillance and Suspicious Activity Indicators Guide for Dams and Levees, which provides information on surveillance objectives and indicators of, methods of reporting and other actions to take to counter surveillance and suspicious activity.

As the COVID-19 pandemic continued to impact the U.S., CISA released the "COVID-19 Vaccine Points of Distribution Physical Security" action guide to provide managers and organizers with information about potential physical threats and corresponding risk mitigation solutions. Additionally, CISA doubled its monitoring services deployed to key entities in the vaccine development, manufacturing, and distribution supply chain in support of the national pandemic response. These small to medium-sized businesses fell below the thresholds for services as defined by the Federal COVID response effort, but through CISA analysis were determined as critical to vaccine manufacturing and scaled production activities.

Much of the nation's critical infrastructure relies on systems and networks that are connected to the internet, making cybersecurity integral to critical infrastructure security. CISA works extensively to provide information and resources to support cybersecurity across the nation to help government and private sector entities identify, mitigate, and protect against a wide array of cyber threats to critical infrastructure.

To help improve cybersecurity among critical infrastructure entities, and in response to growing ransomware attacks, CISA played a key role in developing stopransomware.gov, a dedicated website to provide a one-stop shop for ransomware resources from across the U.S. government and a simplified way for victims to report ransomware incidents. Additionally, CISA released the third version of its Strategic Technology Roadmap (STR), a public guide for organizations in government and industry. The STR is intended to help maintain and evolve technological superiority over our nation's adversaries, to protect and defend against critical infrastructure risks, and to ensure emergency communications are available when they are needed. The STR also guides CISA's technology investments with a foundation based on rigorous research and identifying innovative technologies and best practices for industry and government cybersecurity and communications capabilities to achieve the agency's mission needs.

As part of CISA's efforts to counter misinformation, disinformation, and mal-information (MDM), the agency released two new public products this year. Bug Bytes is second graphic novel in the Resilience Series and is available in both English and Spanish. Bug Bytes and Real Fake, its predecessor graphic



novel released in 2020, communicates the dangers and risks associated with dis- and misinformation through fictional stories that are inspired by real-world events. The other product released this year is "Tools of Disinformation: Inauthentic Content" which highlights the tactics used by disinformation campaigns, such as manipulating audio and videos, conducting forgeries, and developing proxy websites, to undermine public confidence and sow confusion.

HIGHLIGHTS IN CRITICAL INFRASTRUCTURE SECURITY

ACHIEVING SAFETY ACT COVERAGE AS A QUALIFIED ANTI-TERRORISM TECHNOLOGY

CISA's Empowered Trainer Initiative (ETI) Counter-Improvised Explosive Device (C-IED) Train-the-Trainer (TtT) Program received Block Designation in 2021, as a qualified anti-terrorism technology (QATT) under the "Support Anti-Terrorism by Fostering Effective Technologies (SAFETY) Act" of 2002, supporting CISA's private sector partners' efforts to create safe and secure environments and venues while leveraging liability protections provided by the SAFETY Act.

PROVIDING ELECTION SECURITY SUPPORT TO STATES

CISA's mission includes helping the nation carry out safe and secure elections. on November 2, 2021, the agency provided support on the day of state off-year general elections held across multiple states (CO, ME, NJ, PA, TX, VA, WA).

MITIGATING RISKS TO PIPELINES

Through its National Risk Management Center, CISA coordinated with the Transportation Security Agency (TSA), pipeline owners and operators, and other federal partners to make significant progress in identifying and mitigating cyber vulnerabilities in the pipeline ecosystem. In FY 21, this Pipeline Cybersecurity Initiative (PCI) team supported the delivery of Validated Architecture Design Review assessments to **53 pipelines, more than five times as many** as the past 3 years combined.

SUPPORTING CRITICAL COMMUNICATIONS

CISA engaged over **750 subscriber organizations** and others within the communications community during the May 2021 Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) User Council meeting. Along with CISA's Telecommunications Service Priority (TSP), these three services address the fundamental needs for the critical infrastructure community to place priority voice phone calls in a severely damaged and/or congested network, as well as allow priority repair and installation of new voice and data circuits serving in critical sites impacted by events. CISA also provisioned 30 emergency and essential Telecommunications Service Priority (TSP) circuits on behalf of the U.S. Department of State and U.S. Secret Service as world leaders gathered in New York City for the 76th session of the United Nations General Assembly (UNGA).

IMPROVING PERSONNEL SURETY IN REGULATED CHEMICAL FACILITIES

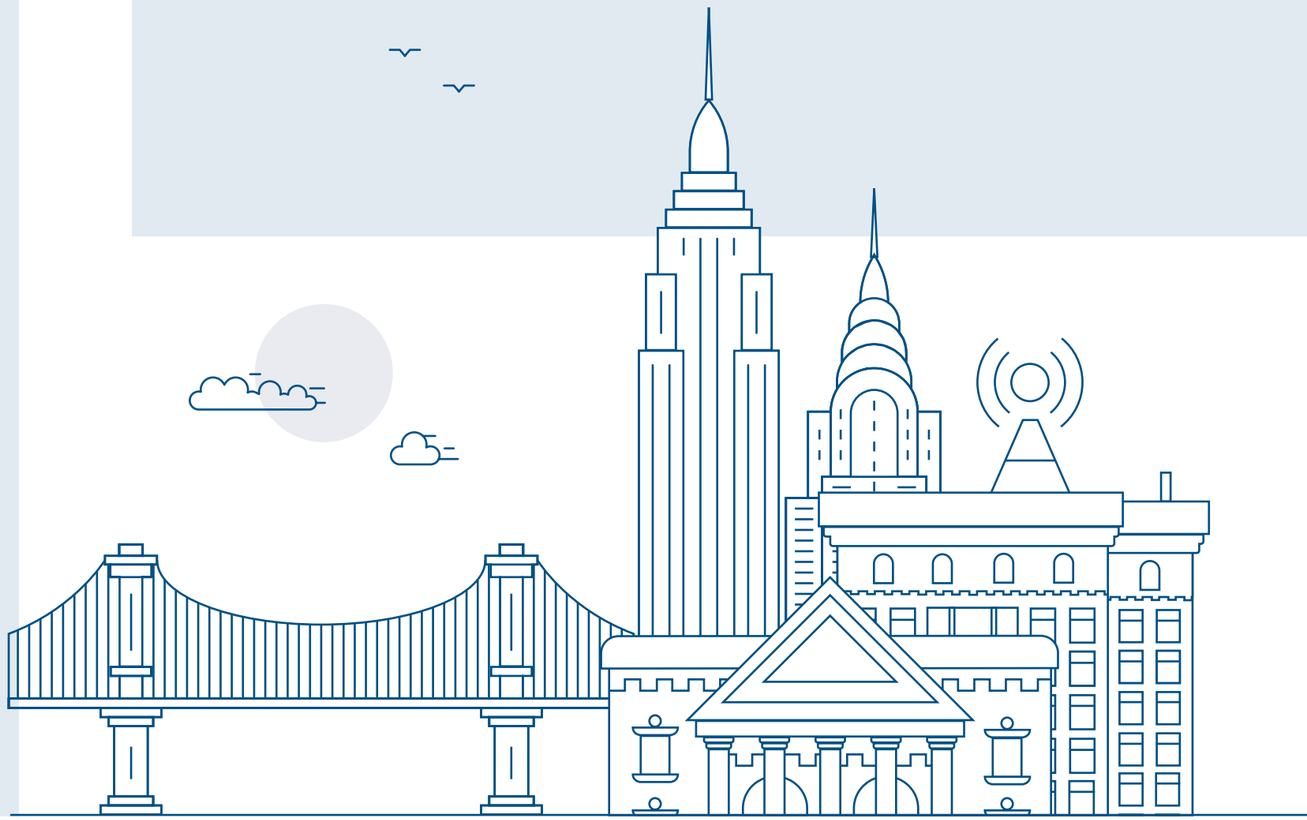
Through its Office of Chemical Security, CISA notified all high-risk facilities to implement the Personnel Surety Program (PSP) by the second quarter of FY22. As of November 2021, **more than 2,900 out of 3,300** high-risk facilities had added RBPS 12(iv) to their security plans with **more than 331,000** individual names having been vetted against the Terrorist Screening Database.

ASSESSING SECURITY IN THE NATIONAL CAPITAL REGION

CISA led interagency efforts to develop the "National Capital Region (NCR) Executive Branch Security Assessment" after the January 6th incident at the Capitol Building. The effort determined whether current security frameworks, agreements, and capabilities of NCR Executive Branch departments and agencies are sufficient to address the dynamic risk environment in the Washington, DC, area and identified capability gaps along with tangible actionable recommendations to enhance security.

MITIGATING RISK AROUND IMPROVISED EXPLOSIVE DEVICES

Through its Office for Bombing Prevention, CISA provided **more than 600 in-person and virtual** counter-IED and risk mitigation trainings for **18,000+** public and private stakeholder partners. These counter-IED training engagements were bolstered by CISA's **857** Bomb-making Materials Awareness Program (BMAP) outreach activities and **56,000+** unique views to CISA's "What to Do" video series that teaches viewers how to respond in the even they receive a bomb threat.

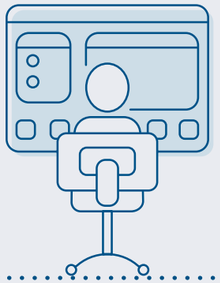


05

Industrial Control Systems (ICS)

Industrial Control Systems are increasingly internet-enabled, offering efficient and effective ways to remotely operate and control critical infrastructure like utilities. CISA continues to maintain an operational focus on ICS entities. The agency is moving forward with the implementation of sensors and other capabilities by partnering with and serving the ICS community to reduce risk to these unique, potentially high-risk systems.

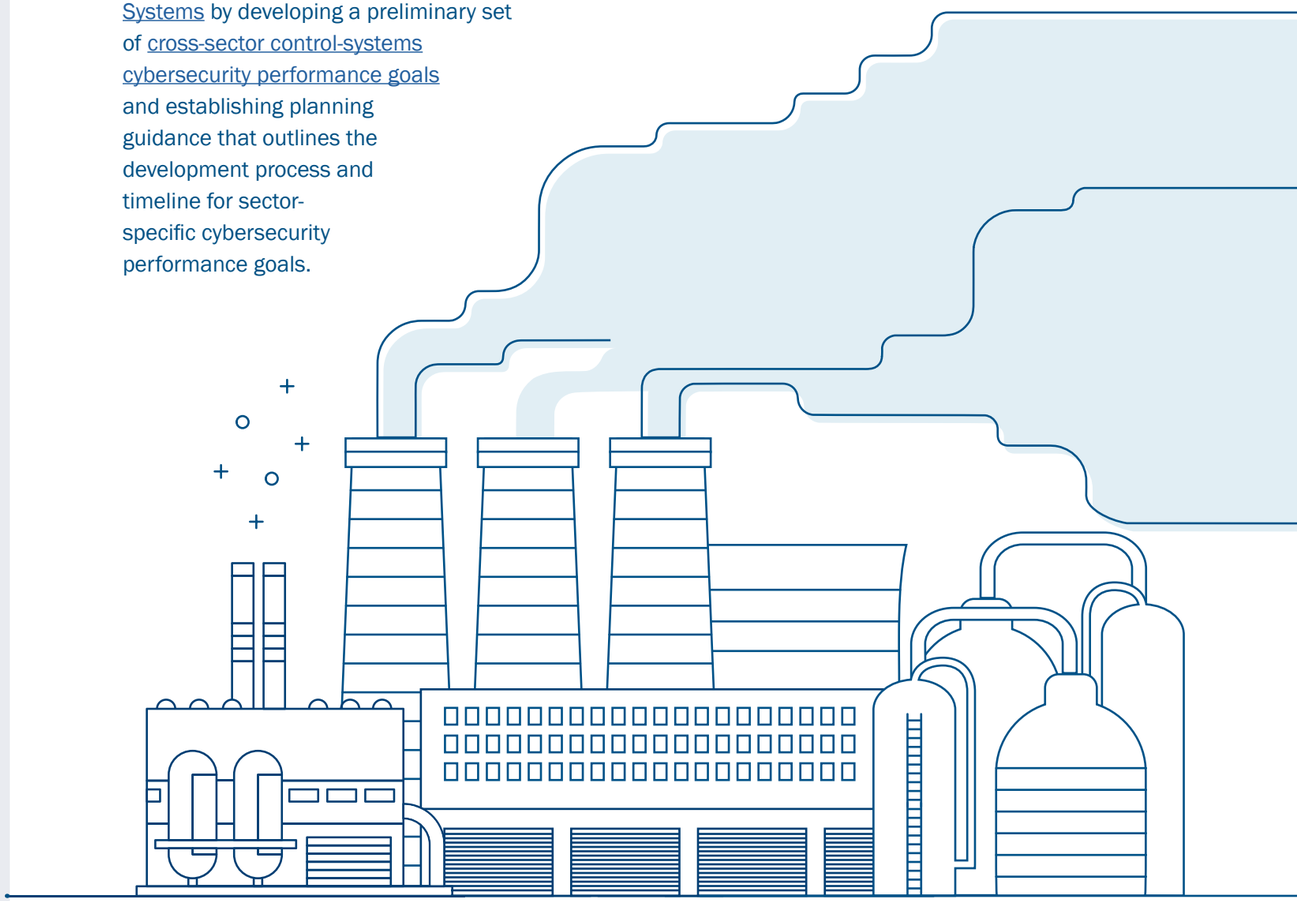
In 2021, CISA gained Congressional authorization for CyberSentry, a program meant to provide CISA and key partners with a comprehensive view of cyber-risks to our nation's most consequential critical infrastructure entities. Since then, CISA has expanded the list of CyberSentry organizations on the path for adoption. Moreover, CISA matured the ICS Control Environment Laboratory Resource (CELR) public-private partnership to advance our understanding of cyber-risks to auto and rail industries, creating state of the art emulation and simulation environments.



TRAINING TO SECURE US-JAPAN INDUSTRIAL CONTROL SYSTEMS

CISA delivered training at the U.S.-Japan Industrial Control Systems (ICS) Cybersecurity Week attended by **67 participants** from **15 countries** across the Indo-Pacific region. Held virtually due to COVID-19, the training offered an overview of ICS security and how to proactively identify vulnerabilities and how to conduct intrusion detection and countering cyber-attacks against ICS infrastructure, among other topics. This training was a result of collaboration between the Japan's Ministry of Economy, Trade and Industry (METI) and CISA, State Department, and the Department of Energy, with support from the European Union.

Of note this year, in collaboration with the National Institute of Standards and Technology (NIST), CISA responded to the National Security Memorandum (NSM) on Improving Cybersecurity for Critical Infrastructure Control Systems by developing a preliminary set of cross-sector control-systems cybersecurity performance goals and establishing planning guidance that outlines the development process and timeline for sector-specific cybersecurity performance goals.



06

Public Gatherings Security

In fulfilling its role as a national coordinator for critical infrastructure and as a Sector Risk Management Agency for multiple sectors, CISA continues to lead the effort to reduce the risk and impact of attacks against public gatherings.

One of the agency's most significant contributions to mitigating the threat of Domestic Violent Extremists was the Mitigating Attacks on Houses of Worship Security Guide released this year. The guide presents new analysis drawn from a series of incidents at houses of worship over the past decade and offers a range of mitigation solutions designed to achieve a robust and layered approach to security. The guide also won the **Society for Technical Communication's Best in Show award** during its 2020–2021 competition, against 54 public and private sector submissions.

The agency released several other new products and resources including: *Employee Vigilance through the Power of Hello*, a new resource series to help non-security professionals within public gathering locations identify and respond effectively to suspicious behavior; the *De-Escalation Series for Critical Infrastructure Owners and Operators*, which helps the private sector recognize the warning signs of someone on the pathway to violence; and a new "Securing Public Gatherings" webpage to provide organizations with a single place to access resources that inform capacity building efforts and risk-based decision-making. Additionally, to help mitigate risks to the Commercial Facilities Sector, CISA released the *Public Venue Security Screening Guide*, a compilation of recommendations and best practices for developing and implementing security screening procedures at large event venues.

As chair of the Interagency Security Committee (ISC), CISA also released the "ISC Best Practices Subcommittee Compendium—Protecting Against Violent Civil Disturbance: Considerations for Federal Facilities." The document provides a compiled list of mitigation considerations to support Federal department and agency security efforts that facility security officials can use to plan and prepare for as well as mitigate the threat from violent civil disturbances.

In July, the DHS and U.S. Department of State co-led the "Southeastern Europe Soft Target Security Workshop," during which representatives from across CISA presented on a range of topical issues including vulnerability assessments, active shooter preparedness, bombing prevention, small, unmanned aircraft systems security, insider threat mitigation, exercises, school safety, faith-based community security, and ransomware. The virtual event provided a forum through which 10 participating countries exchanged information regarding the evolving threat environment and risk mitigation solutions associated with public gatherings.

CISA also provided regional support to metropolitan police, state security operation centers, command posts and in region operations commands for many Special Event Assessment Rating Events and planning efforts such as the Super Bowl, Presidential Inauguration, Chicago and NY Marathons, 2022 World Games, NASCAR Races, Kentucky Derby, Major League Baseball World Series, and the Macy's Thanksgiving Day Parade to name a few. For many of these events, CISA regional personnel serve as the Deputy Federal Coordinator and are engaged in the security planning and day of monitoring activities.

KEY WAYS CISA WORKED TO SECURE PUBLIC GATHERINGS IN 2021

Training to secure public gatherings. CISA conducted several trainings and events in 2021 to support efforts to secure public gatherings. Highlights include:

- More than 90 Active Shooter Preparedness webinars with more than **11,000 human capital and security professionals** to provide information regarding behavioral indicators, potential attack methods, emergency action plan creation, and how to quickly recover from an incident.
- In partnership with the FBI, held a virtual "Faith-Based Safety and Security Symposium," which convened more than **1,000 faith-based representatives** to discuss the security of houses of worship and the safe reconstitution of in-person services during the pandemic.
- CISA conducted seven virtual courses on bombing prevention for United Nations security professionals at **12 locations worldwide**. The UN's Department of Security and Safety (UNDSS) provides security for over **36,000 staff members**, **58,000 dependents** and **1,000 VIPs** (including government leaders). CISA trained the UNDSS to prevent IED attacks against critical infrastructure, which are a serious threat to the UN.
- In FY21 CISA planned and executed **18 exercises** with more than **2,000 participants** in support of DHS and CISA priorities to enhance the security and resilience of soft targets and public gatherings.

Addressing new, emerging, and ongoing threats facing the K-12 academic community. CISA launched two public awareness initiatives to support K-12 safety and cybersecurity:

- The 2021 School Safety Webinar Series, a monthly program hosted in coordination with the Federal School Safety Clearinghouse that covers a range of school safety topics and the resources and best practices available to create safer and more resilient school systems.
- The "2021 Virtual School" cybersecurity campaign, a communications effort to promote online safety and security for students and schools continuing to operate in a virtual environment.

07

Climate Resilience

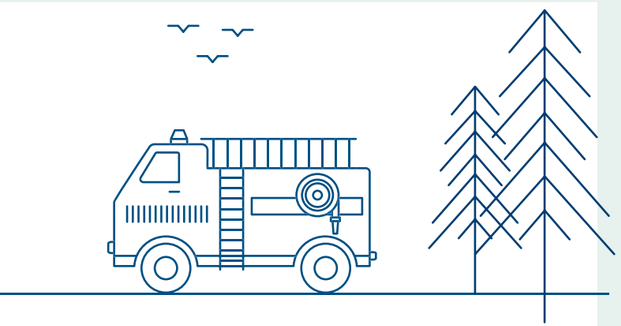
President Biden's Executive Order on Tackling the Climate Crisis at Home tasks DHS with considering the implications of climate change to Nation Critical Functions, along with other strategic focus areas. CISA is heeding the call to help the nation understand and plan for climate-related risks through its on-the-ground presence in 10 regions nationwide, its National Risk Management Center, and the agency's partnerships SLTT governments, and local communities.

Through its 10 regions, CISA continued its work to ensure operational readiness in the regions to support information sharing among federal, state, and local partners in preparation for a variety of threats, including extreme climate events that may impact critical infrastructure.

At the national level, CISA finalized the National Critical Functions (NCF) Framework and completed initial Functional Decomposition of all 55 NCFs to enhance understanding of any given function's individual components, concentrations of risk, critical processes, and dependencies across the NCF ecosystem. CISA also stood up the Federal Risk Management Working Group to coordinate and implement interagency risk mitigation measures. Adoption of the NCF Framework continues and it is referenced in the National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control System

and the Executive Order on Tackling the Climate Crisis at Home and Abroad.

CISA also published its Methodology for Assessing Regional Infrastructure Resilience, the culmination of a multi-year effort to publish an assessment methodology for use by critical infrastructure security and resilience partners. This methodology reflects lessons learned from the implementation of more than 100 regional infrastructure assessments over the course of a decade via the Regional Resilience Assessment Program (RRAP). The methodology complements the growing body of work on infrastructure resilience, filling a knowledge gap by capturing practical knowledge



gained from more than ten years of real-world experience conducting dozens of regional assessments.

Over the course of the year, CISA hosted or developed several exercises designed to support efforts to improve processes and overall resilience to major climate events. CISA's Emergency Services Section coordinated with the Agency's Exercises program to develop a Disaster Access Management and Re-Entry Tabletop Exercise (TTX) to support the Critical Infrastructure Cross-Sector Council and its members' desire to implement a common access management approach for use before, during, and after large-scale disasters and other emergencies. The TTX provides an exercise template to assist SLLT government entities, in coordination with private sector and critical infrastructure stakeholders, assess or develop their access management plans and business re-entry procedures. Continuing the efforts, in May 2021, CISA, in conjunction with CPS Energy, the San Antonio Office of Emergency Management, Bexar County Office of Emergency Management, and Bexar County Public Works, conducted a virtual tabletop exercises (VTTX) to engage participants in collaborative discussions of actions to be taken during and after a major storm event in the San Antonio area. The "Texas Torrent: 2021" Alamo Area Community Flood Resilience Tabletop Exercise hosted approximately 123 virtual from local, state, and federal partners.

In October, the Infrastructure Resilience Planning Framework (IRPF) was released. The IRPF provides an approach for localities, regions, and the private sector to work together to plan for the security and resilience of critical infrastructure services in the face of multiple threats and changes. This resource, along with the Regional Resilience Assessment Methodology, will allow CISA to work with its partners in SLTT governments to help them incorporate resilience into planning and infrastructure operations.

Operationally, CISA supported Hurricane Ida response and recovery operations from August 25th–September 20th by coordinating with FEMA, CISA Region 6, SLTT, and industry partners to monitor critical infrastructure of concern supporting the coordination of recovery efforts as required. In particular, Emergency Support Function (ESF) #2 and Emergency Support Function (ESF) #14 were actively engaged, with the COMMS-ISAC partners working to restore critical communications. Additionally, a "Fiber Cut Task Force" was stood-up to coordinate messaging and products to make recovery and restoration crews aware of the hazards of cutting fiber which could in turn delay communications restoration. The effort was highly successful, and the products will be used in future weather-related storm recovery operations.

ASSESSING NATIONAL CRITICAL FUNCTIONS (NCFS)

In 2021, after adopting the National Critical Functions Framework as an agencywide risk-based prioritization method, CISA produced five (5) National Critical Functions Assessments. These assessed current impacts to NCFs and provided forecasts of potential cascading effects to critical infrastructure and connected NCF's. The completed assessments were released to external partners including the National Security Council, the White House, and Federal Inter-agency partners.

HIGHLIGHTING ONGOING MALICIOUS CYBER ACTIVITY WITH INFOGRAPHICS

CISA's National Risk Management Center released two infographics in October 2021 in support of a CISA/FBI joint cybersecurity advisory highlighting ongoing malicious cyber activity targeting the Water and Wastewater Systems Sectors. The infographics provided additional context of the potential of cyber risks within both of those sectors and available resources for the Supply Water and Manage Wastewater National Critical Functions.

DEVELOPING VITAL RESOURCES

CISA continues to develop vital resources to protect the nations critical infrastructure and provide climate resilience the agency moves into 2022.

08

CISA Workforce

CISA continues its efforts to attract and retain world-class talent through a talent management ecosystem that spans recruiting and hiring to onboarding and integration, training, recognition and promotion, and succession planning and retention. Through new tools and strong partnerships, CISA is also supporting broader efforts to build multi-talented, multi-skilled workforce for today and tomorrow.

In 2021, the agency undertook a number of technology innovation and modernization initiatives to ensure CISA's workforce has the right systems, tools, and data to perform the mission. The agency published its first CISA Enterprise Architecture, an integrated model representing the organizations, people, functions, programs, systems, and other key features of CISA. This document will serve as the corporate memory of the agency representing the three pillars of architecture: people, processes, and technology. CISA also published the first agency-level Target Architecture, outlining the future systems and tools our people will need to address threats. This will be used to inform investment decisions in major acquisition programs and in R&D to deliver innovative tools to our stakeholders. Additionally, the CISA Data Council delivered the first CISA Data Strategy, Data Governance Framework, and guidance documentation. Based on an agency-wide inventory, CISA identified data assets to both populate the department's data catalog to make this data available to analysts across the CISA mission divisions. This information will improve CISA's mission effectiveness by making the right data available to the right people at the right time.

CISA also developed a Cybersecurity Workforce Guide for current and future federal and SLTT staff looking to expand their cybersecurity skills and career options, and hosted events like its President's Cup Cybersecurity Competition to identify, challenge, and reward the best cyber talent in the federal government.

Week three of CISA's 4th Annual National Cybersecurity Summit focused on building the cyber workforce. During that week, the agency announced that it had awarded $2 million to two innovative organizations to help develop cyber workforce training programs. This effort focuses on unemployed, underemployed, and underserved audiences. The agency is also partnering with organizations like Girls Who Code to help more girls to pursue careers in cybersecurity and technology.

CISA continues to develop the workforce we need as an agency to execute our mission and build the pipeline for the future, while also helping close the gender gap and increase diversity.

In FY21, CISA participated in **47 recruiting events**, of which **27 focused on increasing workforce diversity**. As a result of these recruiting efforts, CISA's diversity increased in **four key categories**, with the most significant increases seen in the executive leadership team.

BETWEEN FY20 & FY21

SES Race and Ethnicity Increased from **10% to 19%**

Workforce Race and Ethnicity Increased from **33% to 34%**

SES Gender for Females increased from **23.8% to 29.8%**

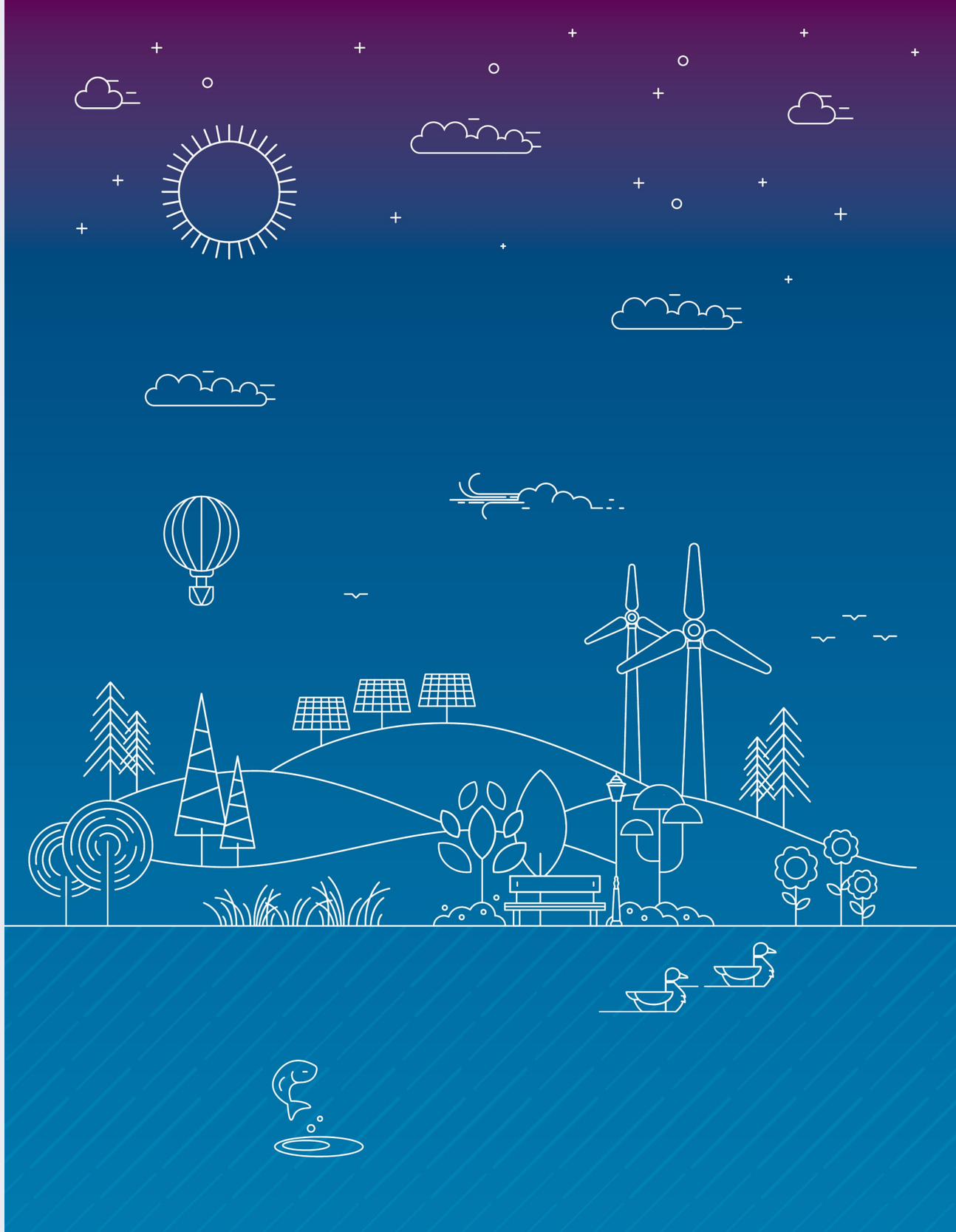
Workforce Gender for Females increased from **34.8% to 35.9%**

09

Conclusion

In many ways, 2021 closed with new iterations of issues similar to what the agency and the nation faced at the end of 2020: notably, the Log4j cybersecurity vulnerability that poses cyber risks on an unprecedented scale, potentially surpassing the impacts of the Solar Winds supply chain cyber incident identified in December 2020, as well as an ongoing COVID 19 pandemic that continues to disrupt traditional ways conducting work and business, education, and other areas that are vital to the nation's economy and security.

Despite these and other challenges, the situation has changed. CISA, the private sector, other government agencies, and the world better understand what they are up against. Our partnerships have matured and grown in significant ways, and there is more energy behind collective efforts to overcome and even stay ahead of the many threats we face.



10

Resources

EMERGENCY DIRECTIVES

CISA issued 5 Emergency Directives and one Binding Operational Directive over the past year, requiring certain federal agencies in the Executive Branch to take specific actions.

ED 22-02: Mitigate Apache Log4J Vulnerability

ED 21-04: Mitigate Windows Print Spooler Service Vulnerability

ED 21-03: Mitigate Pulse Connect Secure Product Vulnerabilities

ED 21-02: Mitigate Microsoft Exchange On-Premises Product Vulnerabilities

ED 21-01: Mitigate SolarWinds Orion Code Compromise

BINDING OPERATIONAL DIRECTIVES (BODs)

BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities

ALERTS, ADVISORIES, AND INSIGHTS

CISA published **59 alerts, advisories, and CISA Insights** in 2021, covering topics from persistent threats to cloud environments, infrastructure and supply chains to threat actors and malicious programs. Joint advisories were produced with our partners at home and abroad, including the Federal Bureau of Investigation (FBI), the National Security Agency (NSA), the Australian Cyber Security Centre (ACSC) and the U.K. National Cyber Security Centre (NCSC).

JAN 8 Detecting Post-Compromise Threat Activity in Microsoft Cloud Environments Alert (AA21-008A)

JAN 13 Cloud Security Observations: Attackers Exploiting Poor Cyber Hygiene

JAN 25 Unauthorized Drone Activity Over Sporting Venues security notice

JAN 27 Information on a virtual tabletop exercise to help organizations and individuals reduce risk of, respond to, and recover from civil unrest

JAN 27 National Terrorism Advisory System (NTAS) bulletin

FEB 8 TEARDROP Malware Analysis Report

FEB 8 SUNBURST Malware Analysis Report

FEB 11 Compromise of U.S. Water Treatment Facility Alert (AA21-042A)

FEB 17 AppleJeus: Analysis of North Korea's Cryptocurrency Malware Alert (AA21-048A)

FEB 24 Exploitation of Accellion File Transfer Appliance Alert (AA21-055A)

MAR 3 Mitigate Microsoft Exchange Server Vulnerabilities Alert (AA21-062A)

MAR 9 Mitigating and Remediating advanced persistent threat (APT) – Compromised Networks Outline

MAR 9 CISA Insights: Remediating Networks Affected by the SolarWinds and Active Directory/M365 Compromise: Risk Decisions for Leaders

MAR 10 FBI-CISA Joint Advisory on Compromise of Microsoft Exchange Server

MAR 13 Added seven Malware Analysis Reports (MARs) to Mitigate Microsoft Exchange Server Vulnerabilities Alert (AA21-062A)

MAR 17 Trickbot Malware Alert (AA21-076A)

MAR 18 Detecting Post-Compromise Threat Activity Using the CHIRP IOC Detection Tool Alert (AA21-077A)

MAR 29 Risk Management Process for Federal Facilities: An Interagency Security Committee Standard (RMP)

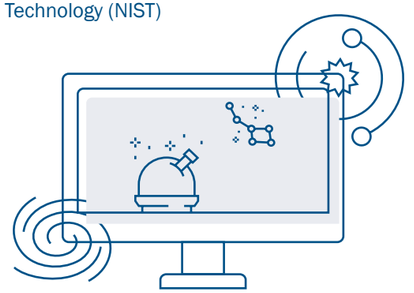
APR 2 Joint Cybersecurity Advisory with the FBI about known Fortinet FortiOS vulnerabilities CVE-2018-13379, CVE-2020-12812, and CVE-2019-5591

APR 7 Trusted Internet Connections (TIC) 3.0 Traditional Use Case and the TIC 3.0 Branch Office Use Case in accordance with the Office of Management and Budget (OMB) Memorandum (M) 19-26

APR 15 NSA-CISA-FBI Joint Cybersecurity Advisory on Russian SVR Targeting U.S. and Allied Networks

APR 20 Exploitation of Pulse Connect Secure Vulnerabilities Alert (AA21-110A)

APR 26 Defending Against Software Supply Chain Attacks, jointly with the National Institute of Standards and Technology (NIST)



APR 26 Russian Foreign Intelligence Service (SVR) Cyber Operations: Trends and Best Practices for Network Defenders Alert (AA21-116A)

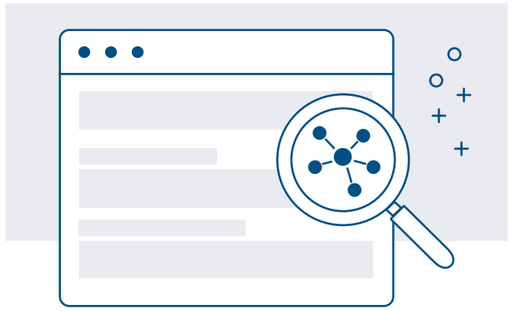
MAY 3 Security and Resilience Considerations for Mass Vaccination Sites White Paper

MAY 7 Joint NCSC-CISA-FBI-NSA Cybersecurity Advisory on Russian SVR Activity

MAY 11 Darkside Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks Alert (AA21-131A)

MAY 12 CISA Insights: Mitigating the Impacts of Doxing on Critical Infrastructure

MAY 14 Eviction Guidance for Networks Affected by the SolarWinds and Active Directory/M365 Compromise Analysis Report (AA21-134A)



MAY 19 Next Generation 911 Incident Related Imagery Impacts 101

MAY 27 Updates to Alert on Pulse Connect Secure

MAY 28 Sophisticated Spearphishing Campaign Targets Government Organizations, IGOs, and NGOs Alert (AA21-148A)

JUN 2 Best Practices for MITRE ATT&CK® Mapping

JUL 1 NSA-CISA-NCSC-FBI Joint Cybersecurity Advisory on Russian GRU Brute Force Campaign

JUL 4 CISA-FBI Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Attack

JUL 7 Malware Analysis Report (MAR) on DarkSide Ransomware

JUL 8 CISA Analysis: FY2020 Risk and Vulnerability Assessments and associated infographic Risk and Vulnerability Assessment (RVA) Mapped to the MITRE ATT&CK® Framework

JUL 19 CISA-FBI Joint Advisory Chinese State-Sponsored Cyber Operations: Observed TTPs Alert (AA21-200B)

JUL 19 Chinese State-Sponsored Cyber Operations: Observed TTPs Alert (AA21-200B)

JUL 19 Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department Alert (AA21-200A)

JUL 19 CISA Insights: Chinese Cyber Threat Overview for Leaders

JUL 20 Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013 Alert (AA21-201A)

JUL 21 13 malware analysis reports (MARs) as part of an ongoing response to Pulse Secure compromises

JUL 28 Top Routinely Exploited Vulnerabilities Alert (AA21-209A

AUG 2 CISA-NSA Joint Cybersecurity Technical Report Kubernetes Hardening Guidance

AUG 17 BadAlloc Vulnerability Affecting BlackBerry QNX RTOS Alert (AA21-229A)

AUG 21 Hurricane-Related Scams

AUG 24 Five Pulse Secure-Related MARs

AUG 31 Ransomware Awareness for Holidays and Weekends Alert (AA21-243A)

SEP 2 CISA Insights – Risk Considerations for Managed Service Provider Customers

SEP 16 APT Actors Exploiting Newly Identified Vulnerability in ManageEngine ADSelfService Plus Alert (AA21-259A)

SEP 22 CISA-FBI-NSA Joint Cybersecurity Advisory on Conti Ransomware

OCT 14 Ongoing Cyber Threats to U.S. Water and Wastewater Systems Alert (AA21-287A)

NOV 17 Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities Alert (AA21-321A)

OCT 18 BlackMatter Ransomware Alert (AA21-291A)

OCT 18 CISA-FBI-NSA Blackmatter Ransomware Advisory to Help Organizations Reduce Risk of Attack

DEC 2 APT Actors Exploiting CVE-2021-44077 in Zoho ManageEngine ServiceDesk Plus Alert (AA21-336A)

DEC 20 CISA-FBI holiday cyber safety public safety announcement (PSA)

PRODUCTS

CISA released **90 products** in a variety of formats, such as fact sheets, assessment tools and videos. These publications provided guidance on topics ranging from anti-terrorism standards to communications and infrastructure safety.

JAN 1 CFATS Risk Based Performance Standard 8

JAN 6 Advance notice of proposed rulemaking (ANPRM) for the Chemical Facility Anti-Terrorism Standards (CFATS) program

JAN 13 Cybersecurity Perspective Healthcare and Public Health (HPH) Response to COVID-19

JAN 14 Personal Security Considerations fact sheet

JAN 15 Houses of Worship (HOW) Self-Assessment Tool

JAN 27 Information on a virtual tabletop exercise to help organizations and individuals reduce risk of, respond to, and recover from civil unrest

FEB 3 Continuous Diagnostics and Mitigation (CDM) Agency-Wide Adaptive Risk Enumeration (AWARE) Video

FEB 5 Cactus League Table Top Exercise to protect spring training for fans

FEB 9 Cyber Safety video series in partnership with CYBER.ORG

FEB 19 Updated SAFECOM Fact Sheet in partnership with SAFECOM

FEB 19 FY2021 Emergency Communication Technical Assistance (TA) Planning Guide (TA/SCIP Guide)

FEB 19 SAFECOM Fact Sheet for Stakeholder Use

FEB 19 FY2021 Emergency Communication Technical Assistance (TA) Planning Guide (TA/SCIP Guide)

FEB 25 SAFECOM Guidance on Emergency Communications Grants (SAFECOM Guidance) in partnership with SAFECOM

FEB 26 Public Safety Unmanned Aircraft System (UAS) Resource Guide in partnership with SAFECOM and National Council of Statewide Interoperability Coordinators (NCSWIC)

FEB 26 Blog and infographics in collaboration with the Department of Health and Human Services (DHHS) identifying potential cyber security impacts on the COVID-19 vaccine supply chain

MAR 4 CISA-NSA: Guidance on Strengthening Cyber Defense Through Protective DNS

MAR 18 Released new forensics tool CHIRP as part of Detecting Post-Compromise Threat Activity Using the CHIRP IOC Detection Tool Alert (AA21-077A)

MAR 29 Risk Management Process for Federal Facilities: An Interagency Security Committee Standard (RMP)

MAR 31 Interagency Security Committee (ISC) 2020 Annual Report

APR 7 CISA 2020 Year in Review

APR 8 Aviary, a new companion resource to the Sparrow detection tool

APR 12 Vendor Supply Chain Risk Management (SCRM) template

APR 12 Contingency Considerations When Facing Reductions in Emergency Communications Budgets fact sheet

APR 12 Supply Chain Risk Management (SCRM) Essentials

APR 13 Updated Fire as a Weapon Action Guide

APR 12 Vendor Supply Chain Risk Management (SCRM) template

APR 12 Contingency Considerations When Facing Reductions in Emergency Communications Budget fact sheet

APR 15 COVID-19 Checklist: Securing Your Business and Clinical IT

APR 15 Domain-Based Message Authentication: Reporting and Conformance (DMARC) and Multi-factor authentication (MFA).

APR 22 Encryption in Three Minutes Video

APR 23 Updated 2021 Risk Management Process: An Interagency Security Committee Standard

APR 26 CISA-NIST Defending Against Software Supply Chain Attacks

MAY 3 COVID-19 Vaccine Distribution Security Concerns in the Last Mile Infographic

MAY 12 Printing While Working Remotely Capacity Enhancement Guide

MAY 12 Resilient Power Best Practices fact sheet

MAY 19 Next Generation 911 Incident-Related Imagery Impacts

MAY 20 Released the translated Employee Vigilance Through the Power of Hello in the 12 Asian American and Pacific Islander (AAPI) languages

JUN 2 Risk to Critical Infrastructure: Telecommunications Central Offices infographic

JUN 9 Rising Ransomware Threat to Operational Technology (OT) Assets fact sheet

JUN 11 Public Safety Answering Point (PSAP) Ransomware Poster

JUN 21 Communications and Cyber Resiliency

JUN 22 Funding Mechanisms Guide for Public Safety Communications

JUN 24 Bad Practices catalog

JUN 28 Positioning, Navigation, and Timing (PNT) fact sheet

JUN 29 SAFECOM Publishes Updated SAFECOM Interoperability Continuum and Frequently Asked Questions

JUN 30 New module in the Cyber Security Evaluation Tool (CSET®): Ransomware Readiness Assessment CSET v10.3

JUL 12 California Statewide Next Generation 911 Geographic Information System Use Case

JUL 14 State: Local: Tribal: and Territorial (SLTT) Indicators of Compromise (IOC) Automation Pilot Program Products

JUL 15 StopRansomware.gov launched by The White House, the Department of Homeland Security (DHS), and the Department of Justice (DOJ)

JUL 19 SAFECOM 2021 Strategic Plan

JUL 22 National Special Security Events (NSSE)/Special Event Assessment Rating (SEAR) Communications Planning Toolkit (Version 2.0)

JUL 30 Vulnerability Disclosure Policy (VDP) Platform

AUG 3 Chain of Custody and Critical Infrastructure Systems

AUG 6 Cybersecurity Workforce Training Guide

AUG 11 Leveraging Geographic Information Systems to Enhance Emergency Response

AUG 12 The Business Case for Security

AUG 13 Essential Critical Infrastructure Workforce Guidance, Version 4.1

AUG 16 Funding and Sustaining Land Mobile Radio (LMR) Systems Brochure

AUG 18 Protecting Sensitive and Personal Information from Ransomware-Caused Data Breach fact sheet

AUG 25 Sign up for a .Gov Domain: Information for Election Officials

SEP 8 Responding to Drone Calls: Guidance for Emergency Communications Centers (ECCs)

SEP 2 Released Public Venue Security Screening Guide

SEP 21 Autonomous Ground Vehicle Security Guide: Transportation Systems Sector

SEP 23 Draft IPv6 Considerations for TIC 3.0 guidance for public comment

SEP 23 De-Escalation Series for Critical Infrastructure Owners and Operators

SEP 27 Infrastructure Resilience Planning Framework (IRPF) for state, local, tribal and territorial governments

SEP 28 Insider Threat Mitigation Self-Assessment Tool

SEP 28 CISA-NSA Guidance on Selecting and Hardening VPNs

OCT 1 Provide Medical Care Critical Condition and Stakeholder Decision Support to Minimize Further Harm

OCT 7 Trusted Internet Connections 3.0 Remote User Use Case

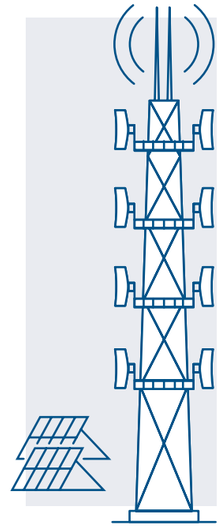
OCT 14 National Interoperability Field Operations Guide (NIFOG) version 2.0

OCT 14 Ongoing Cyber Threats to U.S. Water and Wastewater Systems Sector Facilities

OCT 14 Cyber Risks & Resources for the Water and Wastewater Systems Sector Infographic

OCT 20 Video addressing Project 25 (P25) funding issues and the future of the P25 standard

OCT 28 NSA-CISA Series on Securing 5G Cloud Infrastructures



OCT 29 National Emergency Communications Plan (NECP) Spotlights: Ensuring Interoperable Encrypted Communications

NOV 1 Approach for Developing an Interoperable Information Sharing

NOV 5 Strategies to Protect Our Critical Infrastructure Workforce

NOV 16 Federal Government Cybersecurity Incident and Vulnerability Response Playbooks

NOV 18 Launched Voluntary Chemical Security Program: ChemLock

NOV 19 Launched Infrastructure Dependency Primer

NOV 23 Holiday shopping tips including 12 videos providing resources and best practices for safely navigating websites

NOV 30 Four educational 5G videos

DEC 2 CISA-NSA Security Guidance for 5G Cloud Infrastructures Part III: Data Protection, the third of a four-part series created by the Enduring Security Framework (ESF)

DEC 15 National Critical Functions (NCFs) Status Update

DEC 16 CISA-NSA Ensure Integrity of Cloud Infrastructure, the fourth installment on securing the integrity of 5G infrastructures

DEC Developed Chemical Sector Awareness Training with sector partners

DEC Released Surveillance and Suspicious Activity Indicators Guide for Dams and Levees

ANNOUNCEMENTS

FEB 2 Pilot technology supporting phase 2 of the Next Generation Network Priority Service (NGN-PS)

MAR 8 Awarded a $1.2 million grant to the Center for Infrastructure Assurance and Security (CIAS) at The University of Texas at San Antonio (UTSA) to conduct a pilot program to help state, local, tribal and territorial governments identify high value assets (HVA) in order to prioritize resources and planning

MAR 8 Announced that CISA will oversee the .gov top-level domain (TLD) beginning in Apr. 2021

APR 14 Co-winner of the American Society for Public Administration's (ASPA) 2021 Public Integrity Award with the National Association of State Election Directors (NASED)

APR 27 Took over administration of the .gov top-level domain (TLD) and made .gov domains available at no cost to qualifying organizations

JUN 30 Joint bomb prevention initiative with the FBI: Operation Flashpoint

AUG 23 Signed a Memorandum of Understanding (MOU) with the Cyber Security Agency of Singapore (CSA)

OCT 4 CISA's Office of Bombing Prevention (OBP) marked its 15th year protecting the U.S. from incidents of terrorism and targeted violence

OCT 14 CISA, Crius Technology Group, and Idaho National Laboratory test emergency communications use of high voltage power lines

DEC 1 CISA announced the appointment of the initial 23 members who will serve on CISA's Cybersecurity Advisory Committee, a key authority granted to CISA under the National Defense Authorization Act (NDAA) for Fiscal Year 2021

BLOGS

CISA published **63 blogs**, covering topics that spanned CISA's mission and areas of interest, from **Enhancing Personal and Organizational Security During Civil Unrest** to **Approach for Developing an Interoperable Information Sharing Framework: Ensuring Future Interoperability and Data Sharing for Public Safety Communications Technology**.