2020 YEAR IN REVIEW

CONTENTS

CISA END OF YEAR REPORT: JAN 2020–DEC 2020

NEW MILESTONES IN CYBERSECURITY AND INFRASTRUCTURE SECURITY

EXECUTIVE OVERVIEW

Established in November 2018, the Cybersecurity and Infrastructure Security Agency (CISA) rose to meet multiple historic challenges in its first year, impacting individuals, communities, and Nations across the world. At the start of CISA's second year, our strategic priorities focused on election security, supply chain risks from cyber threats, protecting the .gov domain, soft target security, and critical infrastructure protection.

Early in 2020, Coronavirus-19 (COVID-19) emerged as a top priority for the Agency and the Nation. As the pandemic spread across the United States, nearly all CISA's employees transitioned to full time telework starting March 13, 2020, and retained mission continuity while maintaining the health and safety of employees and their families. Despite an abrupt transition to a fully virtual environment, CISA continued to engage with stakeholders and partners around the Nation and around the world to understand and mitigate risks to the Nation's cyber, physical, and emergency communications infrastructure.

MILESTONES AND ACCOMPLISHMENTS

CISA has spent years building trusted partnerships across the public and private sectors. This year, these partnerships demonstrated their value over and over. CISA also updated its approach to information sharing and situational awareness by streamlining and combining elements of the organization into an integrated, all-risks, cross-functional operation. These and other core capabilities created the essential structure CISA needed to succeed in the face of all the challenges that 2020 produced.

- **The 2020 Presidential election was the most secure election ever.** Starting immediately after the 2016 elections, CISA worked extensively to build trust-based relationships with more than 6,000 state and local election officials, all major technology vendors, and federal partners to ensure election officials had the information they needed to protect their systems and respond to any potential incidents. CISA helped the Nation's elections infrastructure owners and operators increase security by completing 19 infrastructure exercises, including multiple exercises with both state and National level stakeholders to protect the 2020 elections and election infrastructure.

6,000+ **Number of state and local officials engaged**

- **CISA helped counter disinformation and misinformation,** including foreign influence operations, threatening critical infrastructure such as the 2020 election and the nation's COVID-19 response.

CISA's Disinformation Toolkit has been downloaded more than 11,000 times and helped state, local, tribal, and territorial governments raise awareness of online efforts and conspiracy theories related to COVID-19's origin, scale, government response, prevention, and treatment.

11,000+ **Number of downloads**

- Officially launched in June 2020, **CISA Central** has been a critical part of CISA's unified approach to cyber, communications, and physical security responding to COVID-19, hurricanes, and other threats over the course of the year. Today, CISA Central is firmly established as the one-stop-shop for information sharing and situational awareness monitoring and serves as a "front door" to CISA for all stakeholders.
- With the **Essential Critical Infrastructure Workers Guidance,** CISA made "essential worker" part of the common vocabulary across the U.S. More importantly, this guidance provided much needed assistance for state, local, tribal, and territorial governments making time-sensitive decisions about who could access worksites during periods of quarantine and reduced movement.
- Critical resources like the **Telework Guidance and the related cisa.gov/telework** web page helped stakeholders address new cybersecurity vulnerabilities during mass moves to the online environment. The **Cyber Essentials and six associated toolkits** helped small businesses and smaller state, local, tribal, and territorial organizations build a culture of cybersecurity from the top down. **Trusted Internet Connections (TIC) 3.0 Interim Telework Guidance** offered further security recommendations in a remote work environment.
- CISA initiated and implemented **Priority Telecommunications Services (PTS)** alerts to provide first responders, major hospitals and alternate care facilities, medical research centers, and other critical manufacturing facilities with vital priority communication services for COVID-19 planning and response as the Nation shifted to a maximum telework environment. CISA expedited more than 90,000 activations and established telecommunication lines, which Increased usage by 50% for U.S. Navy hospital ships, Defense Health Service, and critical manufacturers like 3M.

50% **Increased PTS usage for U.S. Navy hospital ships, Defense Health Service, and critical manufacturers like 3M.**

- CISA inspected **1,300+** high-risk chemical facilities and gained long-term authorization for its **Chemical Facilities Anti-Terrorism Standards** (CFATS) program, which provided much-needed stability to CISA and chemical security stakeholders. The **Interagency Security Committee** that CISA chairs turned 25 years old this year, and CISA launched a virtual training program through the **School Safety Clearinghouse** to raise awareness of resources and tools available on **SchoolSafety.gov** to enhance school resilience.
- The Agency gathered critical infrastructure stakeholders in the U.S. as well as international partners to address key issues related to COVID-19 such as critical infrastructure impacting **13 partner countries,** prioritizing stakeholder needs and demands for facial coverings, and transatlantic cooperation on healthcare sector security. CISA's contributions helped COVID response efforts by sharing information about key industry partners involved in developing a COVID-19 vaccine and flagging information on malicious activities targeting those partners.
- CISA expanded its reach on cybersecurity by helping external audiences understand the threats, their role in cybersecurity, and actionable steps to take. Some examples of these efforts include a K-12 curriculum through a Cybersecurity Education and Training Assistance Program (CETAP) grant and CYBER.ORG that 21,000+ teachers used impacting more than 3 million K-12 students; CISA's **3rd Annual National Cybersecurity Summit,** this year taking it online as a series of four, weekly virtual events running Sept 16 - Oct 7.

15,000+ **People attended CISA's virtual National Cybersecurity Summit**

- **The Cyber Career Pathways Tool** launched on the **National Initiative for Cybersecurity Careers and Studies** (NICCS) website in August 2020 to develop future cybersecurity experts. This tool created and maintained in partnership with the Interagency Federal Cyber Career Pathways gained 31,000+ views since it launched. Additionally, the **CISA Services Catalog** provides users a sense of how cybersecurity, infrastructure security, and emergency communications intersect to form a holistic approach to risk management, directs users to the appropriate contact for each service, and assigns maturity levels to CISA services guide users toward higher tiers of resilience.
- On December 13th, CISA **Emergency Directive (ED) 21-01** was published, requiring Federal Civilian Executive Branch (FCEB) agencies to disconnect or power down all affected versions of SolarWinds Orion, which were being exploited by malicious actors, posing an unacceptable risk to FCEB agency networks. Within 72 hours of the ED, all FCEB agencies that reported using an affected version had disconnected them. On December 17th, CISA published an activity alert (AA20-352a), describing how an advanced persistent threat (APT) actor had exploited and compromised certain versions of SolarWinds Orion, and was also exploiting commonly used authentication mechanisms. This alert was intended to help public and private entities detect if this malicious activity could be on their networks and take appropriate actions, and has been updated several times as new information became available. CISA's **Supply Chain Compromise webpage** captured guidance and tools, including **Sparrow**, a free tool to help detect possible compromised accounts and applications in the Microsoft Office 365 environment.

CONCLUSION

CISA's staff worked through the historic events that packed 2020 and are unlikely to forget this landmark year. This year presented a collection of challenges, starting with a global pandemic on a scale not seen since 1918, along with mass shifts to telework, virtual school, and telehealth that highlighted and strained the Nation's telecommunications and IT sectors. It also included significant civil unrest that posed threats to people, federal buildings and other local infrastructure and wrapped up with a Presidential election unlike any other in the Nation's history. There were also increasing cyberattacks across the Nation's critical infrastructure—especially attacks focusing on health care systems, vaccine developers and supply chain, 911 call centers, and educational institutions. Yet through it all, CISA kept pace, delivering its core capabilities while adapting to new requirements simultaneously. Read on to see big-picture accomplishments from across CISA this past year.

JAN2020 — DEC2020

JAN14
EMERGENCY DIRECTIVE 20-02 ISSUED
Windows vulnerabilities that require immediate attention

FEB11
SCHOOLSAFETY.GOV LAUNCH

MAR13
COVID-19
CISA pivots full time telework and continues its mission

COVID OPERATIONS
- Coronavirus information page launched
- Published the Essential Critical Infrastructure Workers List and updated it as needed

APR29
LOGO LAUNCH

JUNE
CISA CENTRAL STANDS UP

JULY
SOCIAL MEDIA EXPANSION

JULY14
EMERGENCY DIRECTIVE 20-03 ISSUED
Mitigate Windows DNS Server Remote Code Execution Vulnerability from July 2020 Patch Tuesday

AUG10
CYBER STORM (VII) EXERCISE
More than 1000 players participated

AUG11
EMERGENCY DIRECTIVE 20-04 ISSUED
Mitigate Netlogon Elevation of Privilege Vulnerability from August 2020 Patch Tuesday

SEPT02
BINDING OPERATIONAL DIRECTIVE 20-01 ISSUED
Develop and Publish a Vulnerability Disclosure Policy

SEPT16
CYBERSUMMIT
CISA's 3rd annual National Cybersecurity Conference goes virtual

OCT
CYBERSECURITY AWARENESS MONTH

NOV03
ELECTIONS
Culmination of CISA's work with state and local elections officials, election systems and vendors

#PROTECT2020

NOV
INFRASTRUCTURE SECURITY MONTH
With focus on workforce safety and operations resilience

NOV16
HAPPY BIRTHDAY
CISA turned two years old

DEC13
SOLARWINDS
Issued Emergency Directive 21-01 Mitigate SolarWinds Orion Code Compromise

COVID-19 Coronavirus

CYBERSECURITY

42+ Guidance Products Released

CISA worked to accelerate the removal of COVID-related fraudulent domains from the internet **7,000+**

62+ Healthcare entities were notified of targeting and/or open critical vulnerabilities

STAKEHOLDER ENGAGEMENT

- Engagements increased visibility into healthcare sector's cybersecurity posture by **50%**
- Conducted web application **vulnerability scanning**
- Held **29+** Cross Sector Business and Infrastructure calls with **53,657+** participants
- Shared CISA COVID-19 guidance & resources with **34 countries & 7 international organizations**
- Distributed **29 technical reports** highlighting adversary indicators some jointly with allied (or international) partners
- Provided **24/7** support to FEMA's National Response Coordination Center & in **10** CISA Regions
- Assisted with **Cross Sector Coordination,** including transport of medical grade gases
- Provided actionable information to **254,220+ CISA.gov/Coronavirus visits**

TELEWORK GUIDANCE & RESOURCES

33,615

CISA.GOV/TELEWORK VISITS

5,300+

CISA Central responses to information requests

CRITICAL INFRASTRUCTURE

Supported development of updated **guidance** for Critical Infrastructure workers who may have been exposed to COVID

Coordinated with Chemical Sector partners to identify requirements for more than **8 million** facial cloth coverings

Completed 143+ virtual Technical Assistance sessions with SLTT stakeholders since COVID-19 pandemic began

Issued guidance to the faith-based community about COVID and **physical security**

Provided Priority **Telecommunications Services** to 74,000+ additional users

153,000+ users downloaded the GETS/WPS Dialer App

Responded to **3,200+** inquiries from stakeholders

The Essential Critical Infrastructure Workforce list's effectiveness is also borne out by its usage. From March to November 30 2020, the ECIW list was viewed on the CISA website more than **3.4 million** times and downloaded more than **455,000** times

The ECIW list was also shared with **24** countries and **6** international organizations. The ECIW was adopted in its totality by **14** states and was referenced by **20** states.

Analysis of key supply chain elements has enabled focused outreach to the most critical production and distribution entities

RESOURCES:

- Telework Guidance
- Risk Management Insights
- Cyber Scams
- UK/US Cyberattack Alert
- Disinformation Toolkit for SLTT
- VPN Security
- Exposed? Need to Go Back to Work?
- Election Resources
- Joint Health Care Community Bulletin
- Video Teleconference Guidance
- Guidance for Schools Using Video Conferencing
- Commercial Routing Assistance
- CISA-FBI Alert on Malicious Cyber Activity
- Critical Infrastructure Operations Centers and Control Room Guide for Pandemic Response

CYBERSECURITY DIVISION

SECURING FEDERAL NETWORKS

Worked to accelerate the removal of more than **7,000** fraudulent domains and have blocked more than **6,829** malicious domains from attacking our federal networks

Held more than **80** meetings with agency Chief Information Security Officers to establish priorities, examine challenges, and exchange ideas to enhance partnership

Named as the Cyber QSMO; awarded a contract for a vulnerability disclosure platform service & pre-enrolled +20 agencies; will improve how potential vulnerabilities on federal information systems are tracked, analyzed, reported, managed, and communicated

Issued four Emergency Directives for federal civilian agencies to take action to secure their networks, resulting in patching of more than **2.6** million systems

Webpages launched to provide guidance on the SolarWinds Supply Chain Compromise accessed more than **567,000** times in Dec 2020

Launched U.S. federal government's first online cybersecurity marketplace with

50+ services offered

Completed **61** High Value Asset assessments against **210 Tier-1 HVA** systems to improve cybersecurity on most critical systems

GOVDELIVERY

Informs and updates more than **1.5 million** CSD stakeholders

2,000+

Attendees in Continuous Diagnostics and Mitigation courses

21,000+

K-12 teachers accessed our curriculum, impacting more than **3 million K-12** students

EDUCATION & TRAINING

President's Cup Cybersecurity Competition had **249** teams, **1470** unique competitors across all **3** competitions

17 federal agencies participated in CISA's Federal Executive Institute (FEI) Cyber Executive Course

More than **2.5 million** page views on National Initiative for Cybersecurity Careers and Studies

26 federal organizations participated in Identify, Mitigate, and Recover (IMR) Incident Response Training series

GUIDING AND SUPPORTING INDUSTRY CYBERSECURITY

Issued Trusted Internet Connections (TIC) **3.0 Telework Guidance**

Released "**Securing Industrial Control Systems: A Unified Initiative**" strategy

Released 6 chapters of the **Cyber Essentials Toolkit**; guidance for IT and C-suite leaders to strengthen cybersecurity practices in their organization

802 new customers for **Cyber Hygiene** vulnerability scanning services, providing organizations with information on security gaps and configuration weaknesses on their Internet-facing devices

Worked with **80+ industry partners** on Continuous Diagnostics & Mitigation to provide visibility for more than

80% agency assets

- Developed and published more than **1,300** products
- ALERT AA20-014A had **146,710** page views

RESOURCES:

- ICS Strategy
- Cyber Essentials Toolkit
- Continuous Diagnostics Management
- Quality Services Management Office Cybersecurity Marketplace
- Emergency Directives
- Cyber Hygiene Services
- Supply Chain Compromise | CISA

INFRASTRUCTURE SECURITY DIVISION

ASSESSMENTS AND ANALYSIS – KEEPING OUR INFRASTRUCTURE SECURE

299 critical infrastructure security and resilience assessments completed using the Infrastructure Survey Tool (IST) providing stakeholders with comparative data to enhance their facilities physical and cyber security

1,300 high-risk facilities inspected under the Chemical Facility Anti-Terrorism Standards (CFATS)

28 Regional Resilience Assessments currently underway with critical infrastructure partners to characterize infrastructure systems and identify opportunities to enhance resilience to all hazards

30 products produced by the C-IED OSINT Collection Program, with more than **355,000-page views** on TRIPwire

Onboarded **700** new chemical facilities into the CFATS program

Relaunched the National Counter-Improvised Explosive Device (C-IED) Capabilities Analysis Database (NCCAD) in November, completing **90 assessments** in the last 2 months of 2020

EXPERIENCE & GUIDANCE

Performed **863** chemical security stakeholder engagements, compliance assistance visits, and audits

Launched the Chemical Security Seminar Series which hosted **1,600** attendees

Provided guidance to **1,000** faith-based leaders and a suite of resources to another **50,000** increasing their knowledge of security best practices for houses of worship

SECURITY & RESILIENT OPERATIONS

Delivered 82 Infrastructure Visualization Platform (IVP) assessments to stakeholders to enhance critical infrastructure security and response planning

Conducted **1,601** outreaches to public and private sector stakeholders through the Bomb-Making Materials Awareness Program (BMAP) and distributed the monthly BMAP Bulletin to **more than 100,000** subscribers

More than 800 stakeholders trained on the resources and tools offered by SchoolSafety.gov, which strengthen preparedness and resilience capabilities of schools

CAPACITY BUILDING

Conducted Cyber Storm 2020, the seventh iteration of CISA's biennial National cyber crisis exercise, which engaged **more than 2,000** participants across federal, state and local governments, international partners, and critical infrastructure owners and operators to strengthen cyber preparedness

In person and online efforts improved readiness to mitigate an active shooter event for **more than 550,000** participants

More than 31,000 successful completions of the online C-IED training video series

Distributed **more than 22,000** C-IED awareness products to support stakeholder C-IED programs

Supported **25** election security exercises, including the Nationwide Tabletop the Vote exercise

More than 93,000 successful completions of the Active Shooter Preparedness online training

Hosted **more than 600** C-IED trainings which reached **nearly 23,000** participants

Conducted **81** cyber and infrastructure security exercises, reaching **9,583** participants

More than 8,000 Interagency Security Committee trainings improved government facility risk management capabilities for **41** departments and agencies and **15** SLTT partner organizations across **30** states

RESOURCES:

- ISD Landing Page
- CFATS Landing Page
- Faith Based Organizations - Houses of Worship
- Active Shooter Preparedness
- Interagency Security Committee
- Insider Threat Mitigation Guide
- School Safety training

EMERGENCY COMMUNICATIONS DIVISION

OUR STAKEHOLDERS

The Emergency Communications Division's stakeholders continue to grow along with our partnerships and products to help our stakeholders remain safe and secure. Our largest stakeholders include:

- **19,966** Municipalities, Governors, Mayors, Public Works, Council Members, and Federally Recognized Tribal Nations
- **2.8M** Police and Fire Personnel
- **8,000** Power Plants and Wireline Carriers
- **825,000** EMS Professionals
- **6,200** Hospitals and Certified Emergency Managers
- **6,800** Banks

EMERGENCY RESPONSE

Completed **152** technical assistance engagements supporting **95** strategic state markers with **85** of those completed during the COVID-19 pandemic and trained more than **800** communications responders

Connected more than **1,900** Wireless Priority Service (WPS) calls and more than **2,700** Government Emergency Telecommunications Service (GETS) calls with **98%** call completion rates for two emergency events, including Hurricane Isaias

Provided emergency communications technical assistance in all **56** states and territories to address capability gaps, implement solutions, and provide training to enable the seamless flow of information during incident response

PRODUCTS RELEASED TO KEEP AMERICA SAFE, SECURE, AND RESILIENT

Partnered with the National Council of Statewide Interoperability Coordinators (NCSWIC) across **56** states and territories to identify **25** performance markers that enable state and territory leadership to make data-driven resource allocation decisions for programs, products, and services

Published Fiscal Year 2020 SAFECOM Guidance on Emergency Communications Grants, to include a new cybersecurity priority aligned with the 2019 National Emergency Communications Plan update and additional resources for emerging technologies

Developed various products, including:

- Ransomware Awareness/ Education Brief for public safety answering points
- NG911 Readiness Self-Assessment Tool
- Cyber Risks to Next Generation (NG911) white paper
- 911 and Land Mobile Radio Operations, and more

PRESIDENTIAL EMERGENCY PLANNING AND PREPAREDNESS

Helped the U.S. Secret Service (USSS) develop a National Special Security Event (NSSE) Spectrum deconfliction process for the Republican National Convention

Provided interoperable communications support to the Multi-Agency Coordination Center for the Democratic National Convention

Technical communications assistance to state and local public safety supporting Presidential Debates

Supported the District of Columbia and the USSS in inauguration planning activities

RESOURCES:

- Emergency Communications
- Funding and Sustainment
- Communications & Cyber Resiliency
- Priority Telecommunications Services
- Technical Assistance
- NG911

ELECTION SECURITY

RUMOR CONTROL

Debunked 23 rumors

Responded to **23** rumors to debunk common misinformation and disinformation narratives and themes that relate to the security of election infrastructure and related processes

Page was accessed more than **5.4 million times**

NATIONAL-LEVEL BRIEFINGS

Conducted 10 National-level briefings

3 classified briefings

7 unclassified threat briefings and update calls

OPERATIONAL SUPPORT

Hosted 3 operations center standups

Hosted in-person and/or virtual operations centers **three times**

March 3rd, June 2nd, and November 3rd, 2020

SERVICES PROVIDED

Provided more than 600 Cybersecurity services

including Risk and Vulnerability Assessments, Remote Penetration Testing, Validated Architecture Design Reviews, Phishing Campaign Assessments, Cyber Hygiene, and responses to other requests for technical assistance

PRODUCTS DEVELOPED

Developed more than 7,000 products

300+ publications and internal products like the #Protect2020 Strategic Plan, GCC and SCC publications, planning and guidance documents, public service announcements, risk assessments, infographics, risk posture documents, voluntary information sharing guidance, and risk profile/assessment tools

6,500+ unique “Last Mile” products (Election Security Snapshots and Election Day Emergency Response Guides) for state, local, and private sector partners

200+ CFI products like infographics, stakeholder toolkits, fact sheets, case studies, and daily/weekly reports on election and COVID-related disinformation

ENGAGEMENTS WITH STAKEHOLDERS

Engaged more than 600 stakeholders

250+ external stakeholder engagements, including GCC and SCC meetings, National stakeholder calls, conferences and speaking engagements, classified and unclassified threat briefings for partners, campaign/partisan organization engagements, National-level exercises, CISA internal stakeholder trainings/meetings, and Federal interagency roundtables

50+ congressional engagements (hearings, briefings, and member/staff updates)

100+ engagements with CFI partners, including social media, elections and disinformation experts, government/industry sync meetings, and engagements with individuals or organizations including researchers, civil society groups, private sector, academia, and international partners

200+ media engagements, including interviews, answering inquiries, and other efforts

RESOURCES:

- Campaign Checklist for Securing Your Cyber Infrastructure
- Cyber Incident Detection and Notification Planning Guide for Election Security
- Election Infrastructure Security Resource Guide
- Guide to Vulnerability Reporting for America’s Election Administrators
- Incident Handling Overview for Election Officials
- #Protect2020
- US Election Assistance Commission (EAC)
- Physical Security of Voting Locations and Election Facilities
- Election Disinformation Toolkit
- Mail-in Voting Processing Factors Map
- Securing Voter Registration Data
- Protecting Your Networks from Ransomware
- Mail-in Voting Election Integrity Safeguards Infographic
- Post Election Process Mapping Infographic
- Election Results Reporting Risk and Mitigations Infographic
- Election Risk Profile Tool

NATIONAL RISK MANAGEMENT CENTER

ELECTION SECURITY – DEFENDING OUR DEMOCRACY

Worked with **more than 6,000** state, local, and federal partners to ensure that election officials had the information they needed to protect their systems and respond to any incidents

Developed unique products like the Election Security Snapshots, the Election Day Emergency Response Guide, the #Protect2020 plan, and the Real Fake graphic novel to engage with a range of stakeholders

#PROTECT2020

SUPPLY CHAIN

Published the Information And Communications Technology Supply Chain Risk Management Task Force Year 2 Report

Released the first Supply Chain Risk Management (SCRM) essentials document, which was downloaded

more than 2,400 times

NATIONAL CRITICAL FUNCTIONS

Further developed the National Critical Functions framework as a novel approach to critical infrastructure risk assessment

- Piloted National NCF Risk Register, and established supporting risk database which included:
  - 7 sprints and releases
  - 65+ data points
  - 70+ features
- Completed stakeholder analysis for all 55 NCFs and mapping to 16 CISR sectors
- Developed the methodology, playbook for NCF decomposition analysis, and conducted an initial sprint for 19 of the NCFs
- Published definitions for the 55 National critical functions

RISK ANALYSIS AND BUILDING CYBERSECURITY RESILIENCE

600+ stakeholder engagements were held, ranging from speaking engagements to threat briefings for partners

600+ cybersecurity services were provided, including risk and vulnerability assessments, penetration testing, architecture reviews, and more for technical assistance

7,000+ products developed for state, local, tribal, territorial, and private sector partners

5G SECURITY AND RESILIENCE

CISA published a new resource, **Edge vs. Core - An Increasingly Less Pronounced Distinction in 5G Networks**, to inform stakeholders about how edge computing increases the risks of introducing untrusted components into 5G networks by moving core functions away from traditional network boundaries

Engaged with more than **390** state and local government partners through a series of workshops designed to provide education of **5G technology**, deployment best practices, discuss security and resilience concerns, and increase awareness of the digital divide at the state and local level

Released CISA **5G Strategy** which details the development and deployment of a secure and resilient 5G infrastructure, enhancing National security, technological innovation, and economic opportunity for the United States and its allied partners

PNT EMP/GMD

PNT

Primary drafter of the Executive Order (E.O) on Strengthening National Resilience through Responsible Use of Positioning, Navigation, and Timing (PNT) Services

EMP/GMD

Drafted DHS EMP Program Status Report as part of an update on efforts in support of Executive Order (E.O.) 13865

PARTNERSHIPS

Along with DHS and interagency partners, we developed the EMP Program Status Report in response to Executive Order 13865. This report was downloaded

7,400 times

Conducted eight cybersecurity assessments for pipeline owners and operators alongside the TSA. This number will grow to

52 in 2021

RESOURCES:

NRMC homepage

Election Security

5G Strategy

Supply Chain Risk Management

PNT

EMP/GMD

Pipelines

STAKEHOLDER ENGAGEMENT DIVISION

EVENTS

40,000 partners participated in **2,600** webinars hosted via the Homeland Security Information Network – Critical Infrastructure Community of Interest

Hosted working-level expert-to-expert workshop with Germany to build cyber capacity across the Nation and globe

Supported more than **350** Critical Infrastructure Partnership Advisory Council and cross-sector meetings, many covering CISA's 2020 emerging priorities

Managed the cybersecurity working group for the Council of Governors and state, local, tribal, and territorial officials

Hosted the 3rd annual National Cybersecurity Summit, which brought more than **15,000** virtual attendees across four key-topic areas

Coordinated and facilitated key engagements with critical infrastructure stakeholders such as the 2020 Dams Sector Information Sharing Drill, Critical Manufacturing Sector Regional Roundtables, and more

CAMPAIGNS

STOP. THINK. CONNECT.™

Managed a year-round campaign for public awareness that aimed to increase understanding of current cyberthreats and empower the public to take charge of their online safety and security

Cybersecurity Awareness Month

Worked with public and private sector partners throughout October to encourage cyber responsibility for individuals and organizations: "Do your part. #BeCyberSmart"

PRODUCTS DEVELOPED TO BUILD RESILIENCE

Shared over **7,000** new products via the Homeland Security Information Network

- Public Venues Credentialing Guide
- CISA Service Catalog v1.0
- NSTAC *Report to the President on Software-Defined Networking*
- Small and medium sized businesses survey and white paper
- Emergency Services Active Shooter Planning Resource Guide
- Telework Essentials
- CISA SLTT cyber information sharing program
- Trust in Smart City Systems Report
- Dams Sector Cybersecurity Framework Implementation Guidance
- Automated Indicator Sharing (AIS)
- Access Letter Template for SLTT and CI
- Internet of Things Acquisition Guidance
- Critical Manufacturing Sector Security Guide

And many more!

SUPPLY CHAIN

Established DHS, acting primarily through CISA, as the Information Sharing Agency for the Federal Acquisition Security Council, responsible for supply chain risk information sharing

INTERNATIONAL ENGAGEMENT

Shared CISA COVID-19 guidance and resources with 34 countries and seven international organizations

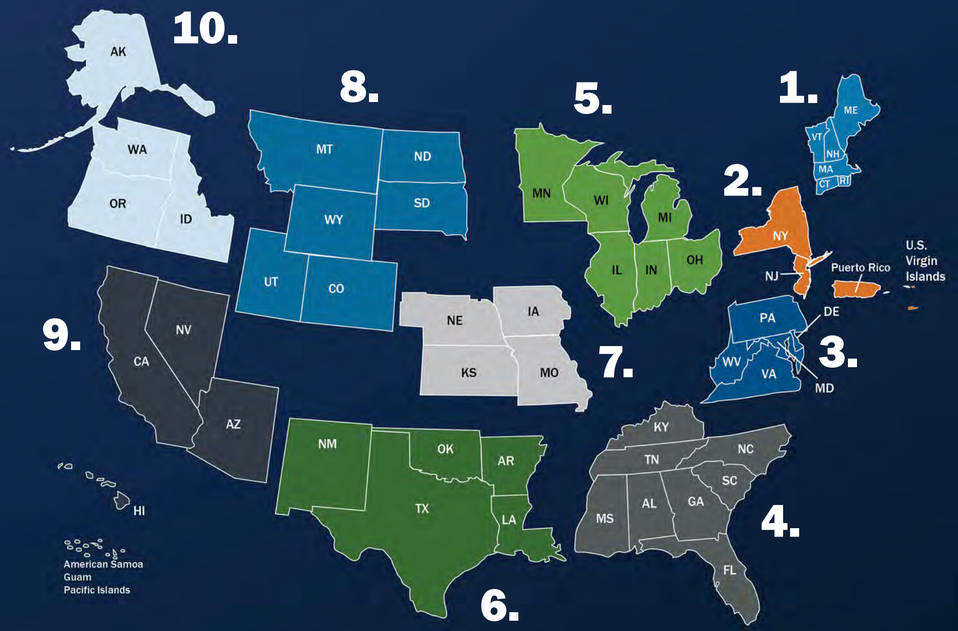
Joined the Organization of American States CSIRT Network and the Pacific Cyber Security Operational Network

RESOURCES:

- SED homepage
- CISA Services Catalog | CISA
- Cyber Awareness Month
- Cyber Essentials | CISA
- STOP. THINK. CONNECT.™
- Ransomware
- Infrastructure Security Month

INTEGRATED OPERATIONS DIVISION

REGIONAL OPERATIONS



- Conducted 3 Chemical Security Audits, **112** Authorization Inspections, **1,400+** Compliance Assistance visits, and **180** general Outreach engagements, plus more than **6,000** P-CFOIs
- Conducted **1,700+** security survey and assessments to include Security Assessments at First Entry, Regional Resilience Assessment Programs, Survey Tools, and Infrastructure Visualization Platforms
- Supported **85** Special Events via exercises, event execution, and incident support
- Provided **500+** security assistance training, presentations, planning support, and workshops to support public gatherings
- Provided **2,000+** Cyber Assessments, protective visits, exercises, and strategic engagements to include major initiatives to support elections and COVID-19 Tier 0 and Tier 1 providers

All of this while adapting our services to a COVID-19 environment

CISA INTEL

- Provided an integrated approach to cyber and physical threat monitoring as well as incident specific intelligence context and products to support mission functions
- Integrated CISA incident response data with Intelligence Community reporting to focus on CISA-mission relevant intelligence
- Embedded all-source intelligence analyst and reports officer with CISA's Threat Hunting teams

- Supported CISA's Elections Security efforts by providing classified intelligence research, production, coordination, and collaboration with the Intelligence Community throughout 2020
- Conducted **more than 50** Intel briefings for CISA leadership to ensure relevant information could support decision making

CISA CENTRAL

- Working with FEMA, provided Emergency Support Function 2 (Communications) and Emergency Support Function 14 (Cross-Sector Business and Infrastructure) in support of multiple natural disasters
- Established the COVID-Task Force to align and focus critical CISA resources to support the Federal Government's response to COVID
- Provided **24x7x365** operational reporting and situational awareness on incidents impacting critical infrastructure

RESPONSE AND REPORTING

Coordinated major events and operations such as the 2020 Election, CISA's COVID-19 response, and natural disasters to include **13 hurricanes**, **6** of which were at a Cat 3 or higher

Rapidly transitioned the Agency to a pandemic response environment and coordinated cross-sector activities to identify and mitigate risk to the National Critical Functions

Matured the role of a new Division within CISA to meet the demands of a dynamic operating environment

OPERATIONAL PLANNING, READINESS, AND CONTINUITY

Led CISA's Pandemic Response Team to ensure CISA could meet essential mission requirements during a global pandemic

Worked with CISA Divisions to create the 2020 Presidential Elections Security Operational Plan and the COVID Operational Plan & CONOPs

2020 YEAR IN REVIEW

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY
CISA