



# CISA

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

2022  
YEAR IN  
REVIEW



## **MISSION**

We lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

## **VISION**

Secure and resilient critical infrastructure for the American people.

## LETTER FROM CISA LEADERSHIP

Protecting our nation's critical infrastructure is foundational to our national security. That critical infrastructure includes everything from healthcare, water, and education to chemical, transportation systems, telecommunications, energy, and much more. And it's under constant risk from a wide array of threats. That makes CISA's work to understand, manage, and reduce risk to the cyber and physical infrastructure that Americas rely on every hour of every day so important.

In that context, we're pleased to share our 2022 CISA Year in Review which lays out the tremendous work by our teammates and partners over the past year. Organized around the four goals outlined in our Strategic Plan, it highlights key achievements toward our vision of ensuring secure and resilient critical infrastructure for the American people.

Just a few of these highlights include the launch of our nationwide Shields Up campaign to safeguard domestic critical infrastructure from potential cyber attacks stemming from Russia's invasion of Ukraine; the tremendous growth of our Joint Cyber Defense Collaborative (JCDC), a paradigm shift from partnership to real-time operational collaboration; a comprehensive cyber hygiene effort to help Americans people stay safe online; our first-ever School Safety Summit;

and a full month dedicated to championing Emergency Communications. Separately, we launched our first CISA Attaché office in London and are working closer than ever with our partners across the globe. We stood up our Cybersecurity Advisory Committee to help us evolve CISA into the cyber defense agency the nation deserves, and we separately welcomed recommendations from the nation's first Cyber Safety Review Board. We developed and published groundbreaking new Cybersecurity Performance Goals to provide a common set of cyber practices for businesses large and small, and we provided support to state and local election officials to help them ensure the safety and security of the 2022 midterm elections.

We accomplished all of this and much more through a unified spirit of collaboration and with a constant focus on building our CISA People First culture. We're especially proud of our work over the past year to promote the mental health and wellbeing of our team.

Over the course of the last year, we've been grateful every single day for the opportunity to serve with incredible teammates and partners. We're proud of what we have achieved to date and relentlessly optimistic about our future. We know that 2023 will be another exciting and productive year.

With Gratitude,



**JEN EASTERLY**  
DIRECTOR



**NITIN NATARAJAN**  
DEPUTY DIRECTOR



**BRANDON WALES**  
EXECUTIVE DIRECTOR



**KIERSTEN TODT**  
CHIEF OF STAFF

# TABLE OF CONTENTS

|   |    |
|---|----|
| Letter from CISA Leadership   | i  |
| Introduction  | 1  |
| Cyber Defense – Leading the National Effort to Ensure Defense and Resilience of Cyberspace                          | 2  |
| Risk Reduction and Resilience – Reducing Risks To and Strengthening Resilience of America’s Critical Infrastructure | 9  |
| Operational Collaboration – Strengthening Whole-Of-Nation Operational Collaboration and Information Sharing         | 14 |
| Agency Unification – Unifying As One CISA Through Integrated Functions, Capabilities and Workforce                  | 19 |
| Conclusion  | 24 |

## INTRODUCTION

**W**hat is it about the **Cybersecurity and Infrastructure Security Agency (CISA)** that makes it special? Is it the unique mission? The CISA Culture that draws a talented and increasingly diverse workforce? Or the innovative and collaborative approach we apply to our work with organizations and stakeholders from across the country and around the world?

We would say that it's all that...and more.

Take a tour through the following pages to see how CISA worked with our partners to drive down risk and build resilience to cyber and physical threats in FY 2022. This year's report is organized around the four goals outlined in the 2023-2025 CISA Strategic Plan: Cyber Defense, Risk Reduction and Resilience, Operational Collaboration, and Agency Unification. The plan clearly lays out our mission and vision and sets the path for where we will prioritize our efforts over the coming years, and, importantly, how we will measure our performance, with a focus on outcomes, not just activity. This last piece is a challenge as anyone in the business of security will know, as you're essentially making investments so bad things *don't* happen. That said we specifically added the word "reduce" into our mission statement this past year to hold

ourselves to a higher standard of accountability for truly improving the resilience of our infrastructure.

Our Strategic Plan focuses not only on "how" CISA works to reduce risk and build resilience, but also on how the agency is unifying as "One CISA" through integrated functions, capabilities, and workforce. Ultimately, the work you see in this Year in Review is grounded in CISA's core values of Collaboration, Innovation, Service, and Accountability and reflects the efforts of thousands of incredible teammates at CISA working selflessly day in and day out to protect and defend our nation. It's been a terrific year for us and our amazing partners...and we're just getting started!

# CYBER DEFENSE

LEADING THE NATIONAL EFFORT TO ENSURE DEFENSE AND RESILIENCE OF CYBERSPACE

CISA leads the national effort to ensure the defense and resilience of cyberspace. In our role as America's Cyber Defense Agency, CISA works to build the national capacity to defend against, and recover from, cyber intrusions. This includes working with federal partners to bolster their cybersecurity and incident response postures and safeguard the federal

civilian executive branch networks that support our nation's essential operations. It also includes partnering with the private sector and state, local, tribal and territorial governments to detect and mitigate cyber threats and vulnerabilities before they become incidents.

```

mirror_mod.use_z = True
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True

```

```

selection at the end -add back the deselected
mirror_ob.select= 1
modifier_ob.select=1
modifier_ob.scene.objects.active = modifier_ob
print("selected" + str(modifier_ob)) # modifier
mirror_ob.select = 0
key = key.context.selected_objects[0]
key.objects[one.name].select = 1

```

```

print("please select exactly two objects, no more")
OPERATOR CLASSES -----

```

```

class MirrorOperator(Operator):
    """Mirror to the selected object"""
    def execute(self, context):
        mirror_x = context.selected_objects[0]
        mirror_x

```

```

def execute(self, context):
    context.active_object is not None

```

# SHIELDS UP

## SAFEGUARDING AMERICANS AGAINST RETALIATORY OR SPILLOVER CYBER INCIDENTS STEMMING FROM RUSSIA'S GROUND WAR IN UKRAINE

CISA started a campaign in late 2021 to warn critical infrastructure owners and operators to put their “Shields Up” and protect their systems from potential Russian cyber attacks intended to deter the United States from assisting Ukraine

against Russia's unprovoked invasion. The campaign included **hundreds of briefings to thousands of stakeholders** across the nation, as well as a [webpage](#) hosting CISA's information on the threat environment, along with technical details and mitigations for network defenders on the latest malicious activity; guidance for every American on how they can stay safe online; and free cybersecurity resources. Since its launch in February 2022, the Shields Up webpage quickly became the most popular page on CISA.gov.

## NEW CYBERSECURITY PERFORMANCE GOALS RELEASED TO ELEVATE CYBERSECURITY ACROSS ALL CRITICAL INFRASTRUCTURE SECTORS

In October 2022, CISA released a set of cross-sector [Cybersecurity Performance Goals](#) (CPGs) to establish a common set of fundamental cybersecurity practices for critical infrastructure, with a particular focus on helping small- and medium-sized organizations—many of which form the supply chain of our major corporations—improve their cybersecurity efforts. Developed at the direction of the White House, the CPGs lay out highly impactful actions organizations can take to mitigate many common threats to critical infrastructure Information Technology (IT) and Operational Technology (OT) environments. The CPGs are based on extensive feedback from hundreds of organizations across the government and the private sector, including our international partners. Along with the CPGs themselves, CISA released an accompanying checklist that helps organizations prioritize each Goal by cost, impact, and complexity. The

voluntary goals both meaningfully reduce risks to critical infrastructure operations and promote the security and resilience of essential services upon which the American people depend.

| GOAL ID | IMPACT | COST | COMPLEXITY | CURRENT ASSESSMENT | YEAR 1 ASSESSMENT | NOTES |
|---------|--------|------|------------|--------------------|-------------------|-------|
| 1.0     | High   | Low  | Low        | Not Started        | Not Started       |       |
| 1.1     | High   | Low  | Low        | Not Started        | Not Started       |       |
| 1.2     | High   | Low  | Low        | Not Started        | Not Started       |       |



## SECURING OUR FEDERAL ENTERPRISE

As the operational lead for federal civilian cybersecurity, CISA works every day to advance the security and resilience of government systems. In 2022, we made revolutionary advances in this mission. Using new authorities and resources provided by Congress, we deployed new technologies across **nearly 50 federal agencies**, with more coming online every month. These technologies provide an unsurpassed level of visibility into threats and incidents targeting federal networks, allowing faster detection and reducing damaging impacts from our adversaries. We made the critical decision to sunset the legacy EINSTEIN program, which used government technologies to detect threats targeting federal networks, and have launched a new effort to provide modern, agile capabilities using commercial shared services.

We have also pivoted many of the resources historically used for the EINSTEIN program into building our new analytic environment, which will allow our operators and partners to analyze and correlate cyber risk information to identify trends and drive more effective remediation—an effort that will culminate in deployment of a Joint Collaborative Environment (JCE). We also used our authorities to issue **Binding Operational Directive 22-01**, which has transformed how organizations within the federal government and around the world prioritize vulnerabilities by driving a focus on those weaknesses that threat actors are actually using to cause harm. Finally, we took significant steps to implement new authorities from Congress to conduct persistent threat hunting and “red team” assessments, launching new programs that will allow greater confidence in the security of the highest-risk federal systems.



## COORDINATING VULNERABILITY DISCLOSURE

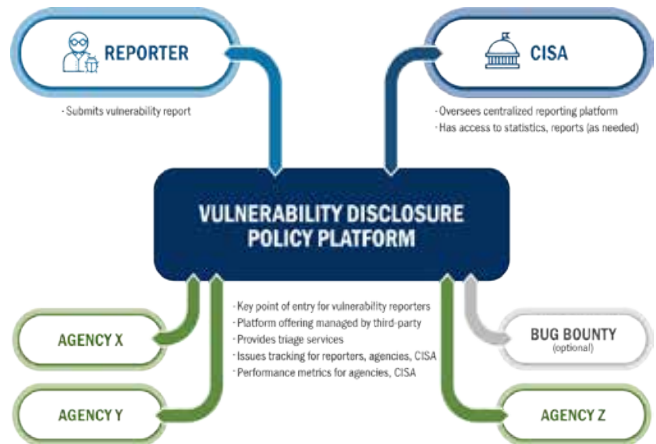
At CISA, we often say that cybersecurity is a team sport. Coordinated Vulnerability Disclosure, or CVD, is a key example of how this team effort can work. CVD is the process of coordinating mitigation or remediation and public disclosure of newly identified cybersecurity vulnerabilities in products and services with the affected vendors.

To help ensure users and system administrators receive clear and actionable information in a timely manner while simultaneously reducing the adversaries' opportunity to respond, we work to ensure that the affected vendors and the vulnerability reporter all disclose simultaneously. CVD demonstrates how important it is for vulnerability reporters and affected vendors to work together to ensure owners and operators can promptly and effectively remediate vulnerabilities in their environments. The CVD process provides a way to unite the cyber community through teamwork and collaboration in order to protect each other and the public from potential threat activity.

CISA sponsors the Vulnerability Information and Coordination Environment (VINCE) as a means to support the CVD process for cybersecurity researchers across the globe to report, communicate, and coordinate the mitigation of vulnerabilities with U.S. and international vendors.

### MORE THAN 700 COORDINATED VULNERABILITY DISCLOSURES IN 2022

In 2022 CISA coordinated 713 CVD cases and produced 416 vulnerability advisories. CVD has streamlined the patch development and deployment process for millions of devices annually due to the direct communication between vulnerability researchers and vendor(s) and/or service provider(s). This process reduces uncertainties and inaccuracies with the vulnerability information and the provided remediation guidance, instilling trust that the cyber ecosystem has in CVD-coordinated security advisories.





## JOINT CYBER DEFENSE COLLABORATIVE

### JOINT CYBER DEFENSE COLLABORATIVE (JCDC) MARKS FIRST YEAR, GROWS MEMBERSHIP

Established by Congress in 2021, the Joint Cybersecurity Defense Collaborative (JCDC) aims to fundamentally transform how we reduce cyber risk to our country: through continuous operational collaboration between trusted partners in the public and private sectors and by conducting rigorous planning to address the most significant threats before damaging intrusions occur. By bringing together government partners like the FBI, the National Security Agency (NSA), and U.S. Cyber Command with private sector partners, we have developed a new platform to drive down risk to the nation at scale.

With representation from nearly all the 16 critical infrastructure sectors, the JCDC has already improved communication and cooperation between industry and government, leading to significant additions to the known exploited vulnerabilities catalog and contributions to cybersecurity advisories. In FY22, upon the discovery of the Log4Shell vulnerability in Apache Log4j software, JCDC shared indicators of compromise, threat activity, and intelligence with and among JCDC members to enable partners to act quickly on this threat affecting software broadly used in a variety of consumer and enterprise services, websites, and applications—as well as in operational technology products—to log security and performance information. Additionally, JCDC and international partners collaborated to quickly release a joint cybersecurity advisory to share technical details and recommended mitigations to the broader cybersecurity community, helping the community to better understand and manage the threat posed by Log4Shell and related vulnerabilities.

CISA and JCDC members also developed and exercised a Russia-Ukraine Tensions Plan to guide collective operational posture and prepare synchronized defensive actions to mitigate harmful impacts to U.S. critical infrastructure from potential Russian cyber-attacks intended to deter the United States from assisting Ukraine against Russia's unprovoked invasion.

In April 2022, JCDC expanded to include Industrial Control Systems (ICS) security vendors, integrators, and distributors. These critical industry experts will help further increase the U.S. government's focus on the cybersecurity and resilience of industrial control systems and operational technology (ICS/OT).

CISA's Joint Cyber Defense Collaborative (JCDC) has formed relationships with over **150 Computer Emergency Response Teams (CERTs) worldwide** and collaborates through operational networks that provide unparalleled situational awareness of threat activity and allows us to coordinate actions with foreign partners to counter those threats in real time. Over the past year, CISA has continued to publish an increasing number of joint cybersecurity advisories with international partners and has increased its work with nations like Estonia, Latvia, Lithuania, Poland, Georgia, the Czech Republic, Ukraine, and those across Eastern Europe. These joint advisories have been tremendously beneficial during the Shields Up campaign.



## CISA CYBERSECURITY ADVISORY COMMITTEE

In December 2021, CISA announced and launched our inaugural Cybersecurity Advisory Committee (CSAC) meeting. The CSAC is a federal advisory committee comprised of **22 private sector leaders** across diverse professions and communities. The Committee was created to provide recommendations on the development and refinement of CISA's cybersecurity programs and policies. In FY22 the CSAC held **four quarterly meetings** and **94 subcommittee meetings** and provided CISA's Director with **53 recommendations** that will keep us well-positioned to address threats in a rapidly changing cybersecurity landscape.

## CYBER INNOVATION FELLOWS INITIATIVE

In June 2022, CISA launched the first-of-its-kind Cyber Innovation Fellows Program, offering private sector cybersecurity experts a unique opportunity to contribute to and engage with CISA's cybersecurity operational teams. The program marks another important milestone in our engagement with a broader community of experts whose training and expertise, creativity, and desire to make a difference in improving global cybersecurity will make valuable contributions to our mission. As of December, we have selected **six fellows** who will join us in early 2023.



## CYBER SAFETY REVIEW BOARD

The Cyber Safety Review Board (CSRB) was established to review and assess significant cybersecurity events so government, industry and the broader security community can better protect our nation's networks and infrastructure. The Board's first report, released July 14, reflects

its inaugural review of the vulnerabilities in the Log4j software library. Log4j software is integrated into millions of systems, and a vulnerability in such a ubiquitous piece of software impacts companies, organizations, and governments all over the world. The CSRB engaged with nearly **80 organizations and individuals** to gather insights, inform findings, and develop **19 actionable recommendations** for government and industry to address the continued risks posed by vulnerabilities in the Log4j open-source software library.

# RISK REDUCTION AND RESILIENCE

REDUCING RISKS TO AND STRENGTHENING RESILIENCE OF AMERICA'S CRITICAL INFRASTRUCTURE

The nation's safety and security depend on the ability of critical infrastructure to prepare for and adapt to changing conditions and to withstand and recover rapidly from disruptions. CISA works to proactively reduce

risk to infrastructure and systems while also building our stakeholders' capacity to safeguard their infrastructure from these risks.


## FIRST-OF-ITS-KIND CYBERSECURITY GRANTS FOR STATE, LOCAL, TERRITORIAL GOVERNMENTS

CISA and the Federal Emergency Management Agency (FEMA) collaborated on a **first-of-its-kind State and Local Cybersecurity Grant Program** to help under-resourced state, local, and territorial (SLT) partners build cyber resiliency.

This innovative program was established by the State and Local Cybersecurity Improvement Act, part of the Infrastructure Investment and Jobs Act, to help address the unique challenges state and territorial governments face when defending against cyber threats. Since the grant was announced, CISA's cybersecurity advisors and cybersecurity state coordinators have provided direct support to SLT CIOs, CISOs and Emergency Managers to answer grant application questions.

## CYBER STORM RECOGNIZED AS THE NATION'S CYBERSECURITY EXERCISE

This past spring, CISA held our eighth Cyber Storm exercise. Held biennially, Cyber Storm brings together the public and private sectors to simulate discovery of and response to a significant cyber incident impacting the Nation's critical infrastructure. It provides the framework for the most extensive government-sponsored cybersecurity exercise of its kind and is part of our ongoing efforts to assess and strengthen cyber preparedness of the nation. This was the first Cyber Storm exercise conducted pursuant to the requirements of the FY21 National Defense Authorization Act, which called for National Cyber Exercises to examine national response to a significant cyber-attack impacting critical infrastructure. As the most successful Cyber Storm to date, the exercise included **more than 2,000 participants from 33 federal agencies, nine states, 100 private sector companies, and 16 partner countries** to drive improvements in cybersecurity policy and plans.



**CYBER STORM VIII**  
NATIONAL CYBER EXERCISE

**BACKGROUND**

The Cyber Storm exercise series provides a venue for the federal government, state and local government, the private sector, and international partners to come together to simulate response to a large-scale, coordinated, significant cyber incident impacting the nation's critical infrastructure. Cyber Storm VIII, planned for Spring 2022, will allow participants to exercise their cyber incident response plans and identify opportunities for coordination and information sharing. Cyber Storm exercises have historically engaged more than 1,000 distributed players over the course of three days of live exercise play. Building on the success and momentum of Cyber Storm 2020 and lessons learned from real-world events, Cyber Storm VIII is positioned to meaningfully prepare participants for response to emerging and evolving threats.

**ENHANCING CYBER INCIDENT RESPONSE CAPABILITIES**

The cyber threat landscape continues to expand and advance, requiring public and private sectors to constantly evaluate their cyber incident response capabilities. Building on the outcomes of previous iterations, Cyber Storm VIII will examine all aspects of cyber incident response including potential or actual physical impacts of a coordinated cyber attack targeting critical infrastructure. Cyber Storm VIII provides a unique opportunity for organizations to evaluate their internal cyber incident response plans, while coordinating with those at the federal, state, and private sector levels. Together, participants will identify areas for growth and improvement to strengthen our national cyber resiliency.

**Figure 1: Cyber Storm Exercise Series Benefits**

- Builds on the outcomes of previous exercises and changes to the cybersecurity landscape
- Continually evaluates and improves the capabilities of the cyber response community
- Promotes public-private partnerships and strengthens relationships between the federal government and partners
- Integrates new critical infrastructure sectors and tools available to provide real-time and integration

**CYBER STORM VIII PARTICIPATION**

- Cyber Storm VIII includes organizations across federal, state, and international governments and the private sector
- Participating organizations will work directly with CISA to understand CISA's role and capabilities in a cyberattack.
- Participants operate in working groups to meet organization- and sector-specific objectives and improve coordination capabilities through the exercise.
- Benefits of participation include improved understanding of current cyber risks, awareness of incident response resources, strengthened relationships with counterparts, and refined communications strategies.

CISA | DEFEND TODAY. SECURE TOMORROW

[cisa.gov](https://cisa.gov) [cyberstorm@cisa.dhs.gov](mailto:cyberstorm@cisa.dhs.gov) [LinkedIn.com/company/cisagov](https://www.linkedin.com/company/cisagov) [@CISAgov](https://twitter.com/CISAgov) [Facebook.com/CISA](https://www.facebook.com/CISA) [@cisagov](https://www.instagram.com/cisagov)

## INAUGURAL NATIONAL SUMMIT ON K-12 SCHOOL SAFETY AND SECURITY FOCUSES ON SAFE AND SUPPORTIVE LEARNING ENVIRONMENTS

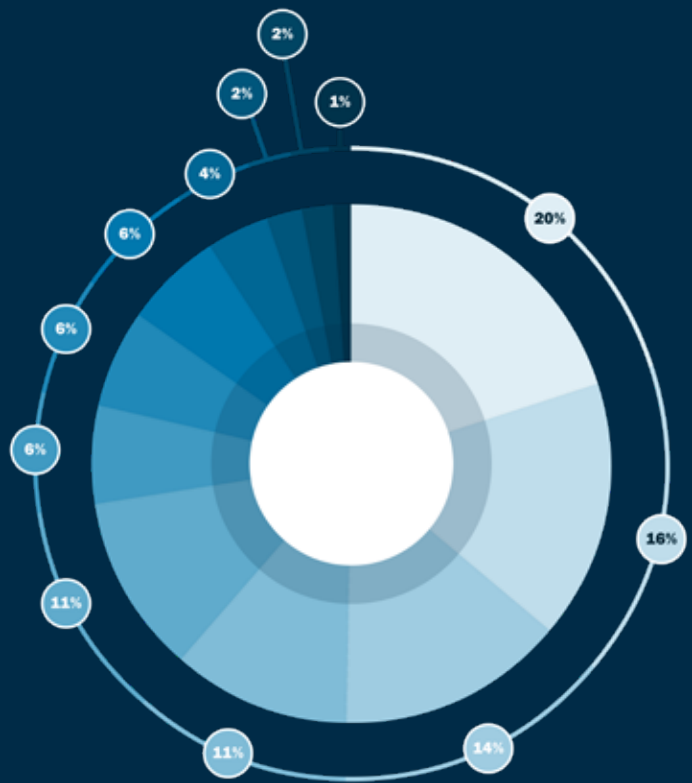
From November 1-3, CISA brought together federal, state, and local school leaders to share actionable recommendations that enhance safe and supportive learning environments in kindergarten through grade 12 (K 12) schools. This first-of-its-kind virtual event fostered a nationwide dialogue on school safety, providing a venue to share resources, products, and tools to support schools in implementing and strengthening their security postures. Based on the post event survey, **96%** of Summit participants

indicated they are either extremely likely or likely to apply one or more resources or strategies presented within their school or district, and **88%** of Summit participants indicated they either strongly agree or agree the Summit exceeded their expectations.

### SCHOOL SAFETY SUMMIT PARTICIPATION

**A range of individuals from across the country with a passion for improving school safety participated in the Summit.**

- ▶ **7,874** individuals registered for the Summit.
- ▶ **93%** of Summit participants indicated their work primarily served a school or district within the K 12 community.
- ▶ The Summit had participation from the K 12 community in **all 50 states**, the District of Columbia, the Northern Mariana Islands, American Samoa, the Virgin Islands, and Puerto Rico. More than **300** Summit participants were international attendees.
- ▶ **55%** of Summit participants indicated their primary job role was serving directly at a school or district level.





## OPERATION FLASHPOINT

### OPERATION FLASHPOINT HELPS RETAILERS REPORT AND ADDRESS SALES OF POTENTIALLY DANGEROUS CHEMICALS

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), expands outreach and support to encourage our private sector partners 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. The BMAP/Operation Flashpoint Team visited **more than 8,368 retail spaces across the country during FY22** as part of its outreach campaign.




## CHEM LOCK

### NEW VOLUNTARY CHEMICAL SECURITY INITIATIVE LAUNCHED

In November 2021, CISA launched ChemLock, a new voluntary chemical security initiative. The ChemLock program provides facilities that possess dangerous chemicals with tailored, scalable, no-cost services and tools to improve their chemical security posture. CISA gained our 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.

### OUTREACH TO HISTORICALLY BLACK COLLEGES AND UNIVERSITIES (HBCU)

In response to the threats to HBCUs throughout 2022, CISA mobilized resources such as its Protective Security Advisors (PSA) to **reach out to all 108 Historically Black Colleges and Universities across the country** to provide support.

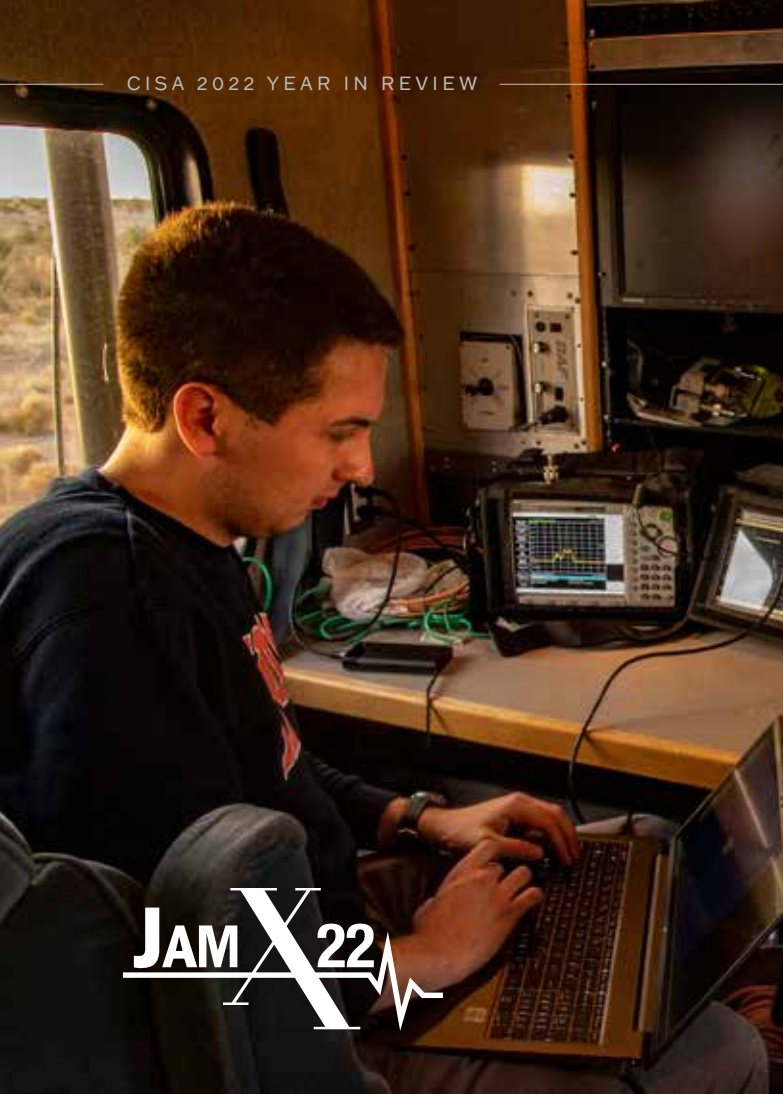
As a result, we developed new relationships with **56 HBCUs** and received requests for assistance from **37 HBCUs**.

Additionally, we **conducted 27 courses in bombing prevention, trained more than 1,300 participants, and delivered over 1,500 products**.

CISA also conducted an active shooter preparedness webinar **across the 16 affected states and communities with 348 registered attendees**.

## EXERCISING TO BUILD RESILIENCE FOR PUBLIC SAFETY COMMUNICATIONS: JAMX22

In April 2022, CISA, along with the Department of Homeland Security (DHS) Science and Technology Directorate (S&T), co-hosted JamX22, an event that assessed the impact of jamming on public safety communications systems and mission response and identified gaps in training with our public safety communications partners. The 2022 event continued efforts from the 2016 and 2017 First Responder Electronic Jamming Exercises. As part of our role, CISA participated in the JamX22 VIP Demonstration and developed the Public Safety Communications and Cyber Resiliency Toolkit to assist public safety agencies and others responsible for communications networks in evaluating current resiliency capabilities, identifying ways to improve resiliency, and developing plans for mitigating the effects of potential resiliency threats.



**JAM X22**

### EDUCATING THE AMERICAN PEOPLE ABOUT SIMPLE STEPS TO STAY SAFE ONLINE

As part of our efforts to raise awareness of cyber hygiene and what every American can do to stay safe online, we launched a campaign to highlight the importance of Multifactor Authentication, including urging implementation of phishing-resistant MFA and how to use it.

As part of this campaign, we also promoted 4 Steps to Keep you Cyber Safe:

- ▶ **Implement multifactor authentication** on your accounts and make it significantly less likely you'll get hacked.

- ▶ **Update your software.** In fact, turn on automatic updates.
- ▶ **Think before you click.** More than 90% of successful cyber attacks start with a phishing email.
- ▶ **Use strong passwords, and ideally a password manager** to generate and store unique passwords.





## INFRASTRUCTURE SECURITY MISSION ACCOMPLISHMENTS IN 2022:

**ACTIVITIES AND TRAINING**

- ▶ **Conducted 163 exercises around the nation with 14,260 total participants.** FY22 had 54 more exercises than FY21. 87% of respondents stated exercises enhanced individual or organizational preparedness.
- ▶ **Conducted nearly 1,830 Chemical Facility Anti-Terrorism Standards inspections across the country, which represents 57% of high-risk facilities, well exceeding the target of 35%.** The CFATS program has assisted **more than 10,000 facilities** since the program began.
- ▶ Documented **2,500+ IED-related incidents; supported 27+ Special Events;** and conducted **791 C-IED and Risk Mitigation** training courses for **18,330 participants.**
- ▶ Trained its **150,000th person** in counter-IED measures and techniques.
- ▶ The School Safety Task Force provided **11** trainings, for over **4,937** participants.

**PRODUCTS**

- ▶ **Distributed 142,400+ C-IED Awareness Products.**
- ▶ **Delivered 114 Active Shooter Preparedness webinars** to critical infrastructure, international, law enforcement, emergency response, interagency, and private sector stakeholders with **over 32,600 registrants** and had **139,835 website visits to [cisa.gov/active-shooter-preparedness](https://www.cisa.gov/active-shooter-preparedness).**
- ▶ **Released the K-12 School Security Guide (3rd ed., 2022)** and companion products which provide a comprehensive doctrine and systems-based methodology to support schools in conducting vulnerability assessments and planning to implement layered physical security elements across K-12 districts and campuses. The guide was **downloaded more than 2,400 times in its first six months.**
- ▶ **Delivered 120 Infrastructure Visualization Platform products** and **collaborated on 42 Regional Resiliency Assessments Projects.** These collaborative assessment efforts with the owners and operators of critical infrastructure led to the identification of facility security and resilience vulnerabilities and proposed recommendations for mitigating those vulnerabilities. In addition, CISA supported **over 200 Infrastructure Survey Tool (IST) assessments.** Of the facilities undergoing the IST, 92% responded they were likely to integrate vulnerability assessment or survey information into their security and resilience enhancements.

# OPERATIONAL COLLABORATION

STRENGTHENING WHOLE-OF-NATION OPERATIONAL COLLABORATION  
AND INFORMATION SHARING

Collaboration is at the heart of everything we do at CISA because, securing our nation's cyber and physical infrastructure is a shared responsibility. Everyday, CISA is actively working with our government, industry, academic, and international partners to move toward more forward-leaning, action-

oriented collaboration and we do so with humility, transparency, gratitude, and a firm resolution to add value wherever possible. CISA is also committed to growing and strengthening the agency's regional presence to more effectively deliver the assistance our stakeholders need.



## CISA GOES GLOBAL

The cybersecurity threats we face are borderless. In 2022 we expanded our collaboration with the international community. For example, we formalized operational cooperation with several international partners through Joint Work Plans (JWPs) and Memorandums of Understanding (MOUs), including the United Kingdom, Australia, Singapore, Israel, the United Arab Emirates (UAE), and Ukraine.

In July, CISA opened our **first Attaché office**. Based in London, to serve as a focal point for international collaboration between CISA, UK government officials, and other federal agency officials. We also hosted onsite liaisons from the **UK's National Cyber Security Centre and the Australian Signals Directorate**.

Through State Department funded foreign assistance, CISA implements international capacity building, technical assistance, and enhanced information sharing for efforts like: sustaining support to the Government of Ukraine as they counter cyber aggression from Russia; partnering with the Philippines' Anti-Terrorism Council to support their National Action Plan for soft target protection; engaging across the Western Hemisphere through our partners at the Organization of American States; supporting intersections to the Indo-Pacific Economic Framework across Asia; and mitigating vulnerabilities in the Balkans.

CISA is at the forefront of international efforts to prevent chemical terrorist incidents. CISA, along with the Defense Threat Reduction Agency, INTERPOL and the FBI, founded and co-implement the Global Congress on Chemical Security and Emerging Threats. In 2022, the Global Congress facilitated dialogue between **more than 220 chemical security experts from 72 countries**, including policymakers, law enforcement, regulators, industry, academia, think tanks, military, NGOs, and international organizations

Through State Department sponsored Embassy Science Fellowships, CISA engaged with our partner in the Dominican Republic recommend emergency communications' public notification improvements in anticipation of cybersecurity challenges associated with technology upgrades to Next Generation 9-1-1. CISA separately executed six U.S. Department of State-funded international capacity building programs reaching **more than 1,000 participants from 31 total countries** in FY22. The projects, workshops, and training focused on cyber hygiene best practices, resources to combat cybersecurity threats, ransomware threat mitigation, cyber workforce development strategies, Industrial Control Systems training, vulnerability assessments, and a case study on Operation Warp Speed.

### CISA OFFICE FOR BOMBING PREVENTION

CISA's Office for Bombing Prevention collaborated with Romania, Mexico, Canada, the European Union, and the United Kingdom in addition to our work here in the U.S.

Notably, for the second consecutive year, CISA worked with the U.S. Embassy in Mexico City and the Department of State's Export Control and Related Border Security (EXBS) Program to provide training to government officials in Mexico.

## DELIVERING CISA SERVICES ACROSS THE COUNTRY

CISA implements a significant portion of our operational mission through 10 regional offices which provide direct services to CISA stakeholders across the country. These regional offices are essentially microcosms of CISA that deliver and coordinate community-based solutions on behalf of the agency. These include prevention, protection, mitigation, response, and recovery solutions for cyber, physical, and emergency communications risks impacting critical infrastructure around the nation. Additionally, the agency provides situational awareness, information sharing, technical assistance, outreach, vulnerability notifications, and incident response coordination. Last, but not least, through Chemical Facility Anti-Terrorism Standards, our regionally based Chemical Inspectors engage chemical facilities and other stakeholders to secure potentially dangerous chemicals throughout the Nation.

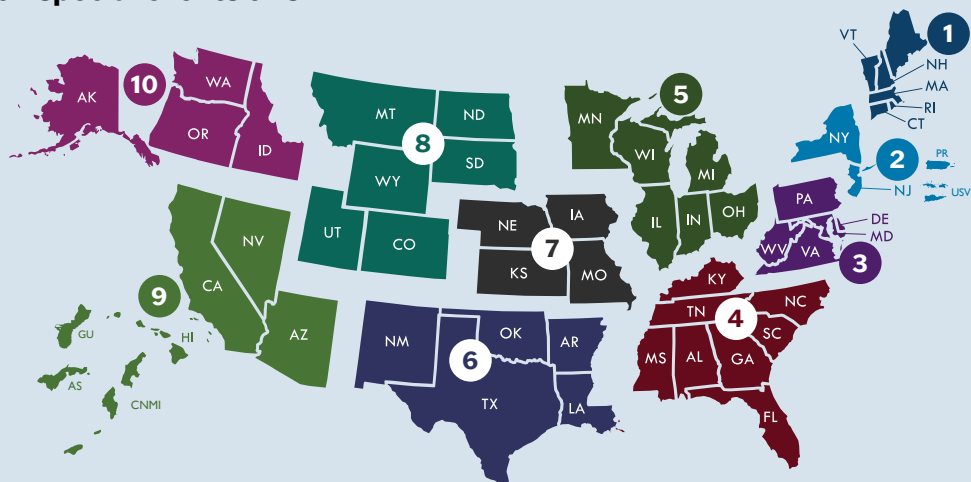
During response operations CISA deployed staff to support state, local, tribal and territorial government partners, providing emergency communications, critical infrastructure recovery coordination, and advanced technical services to assist with federal response and recovery operations. For example, **CISA Regional Offices supported 194 incidents and 197 special events this past year.**

### OUR “NO WRONG DOOR” APPROACH

- ▶ Nationwide hybrid security advisor cadre
- ▶ Advisors trained on all aspects of cyber, physical, emergency communications security
- ▶ Ensures CISA stakeholders receive the services they need when they are needed

Over the past year, CISA has expanded our support for each state to have a Cybersecurity State Coordinator (CSC), additional CSAs, Protective (Physical) Security Advisors, and regional staff to seamlessly pivot to address emerging threats and vulnerabilities.

In 2022, CISA marked a significant milestone when we fully integrated CISA’s Emergency Communications Coordinators (ECCs) into the agency’s Regional Office field forces, furthering operational capabilities and capacity where the demand was highest. Through these programs, we helped ensure public safety, national security, and emergency preparedness communities can communicate seamlessly and securely.



[cisa.gov/cisa-regions](https://cisa.gov/cisa-regions)

## FOSTERING INTEROPERABLE EMERGENCY COMMUNICATIONS

Throughout 2022, CISA continued to pioneer in the realm of priority communications. We partnered with Idaho National Laboratory on an exciting Proof of Concept that tested the patented “CRIUS” CommCube technology. This effort promotes resilient route diversity of national security and emergency preparedness communications to provide an alternate communication pathway when networks are congested, damaged, or even destroyed. CISA, the National Association of State 911 Administrators, the National Council of Statewide Interoperability Coordinators, and the 911 Program Office at the National Highway Traffic Safety Administration held a series of interoperability workshops open to all states. Representatives from 38 states and the District of Columbia discussed emergency communications interoperability with public safety representatives within their state. The workshop brought state emergency leadership together to communicate and collaborate effectively; develop statewide goals and actionable steps for states to work toward improving emergency communications interoperability; and facilitated state conversations on how to deepen and enhance emergency communications governance structures to facilitate greater interoperability and decision-making.

**CISA focused on securing the public’s most direct route to emergency services, the Nation’s emerging Next Generation 911**

**system.** Production of guidance, including “Two Things Every 911 Center Should Do to Improve Cybersecurity” and the “911 Cyber Incident Response Case Studies Suite” based on real-world events are helping administrators better prepare for and respond to cyber incidents. In recognition of the criticality of this effort, CISA received initial funding within the FY22 appropriation in support of a **new program dedicated to ensuring Next Generation 911 systems align with NIST cybersecurity standards**, while preserving the ability to work with all forms of data, video and information services. Public safety officials partnered with CISA to release **cybersecurity educational materials tailored to the public safety operational environment** such as the “First 48: What to Expect When a Cyber Incident Occurs” document and the Guide to Getting Started with a Cyber Risk Assessment.

Emergency communications are paramount during disasters, and this year CISA captured and shared lessons learned from events such as the Nashville bombing and Midwest derecho as well as serving as emergency communications specialists during hurricanes, floods, and other disasters. **CISA personnel deployed extensively** during the year to support national security events, the southern border, and Hurricane Ian.

We also **facilitated six Network Security Information Exchange (NSIE) meetings** during FY22. NSIE industry and government members, including international partners, share information regarding threats to and vulnerabilities of the public network affecting national security and emergency preparedness telecommunications.

### AS PART OF OUR EMERGENCY COMMUNICATIONS MISSION THIS YEAR, CISA:

- ▶ Added **123,236** new Wireless Priority Services users to CISA Priority Services.
- ▶ Completed **214 requests** for technical assistance in **46 states** for a total of **5,000 participants**.
- ▶ Conducted **112** Communications Unit focused Training courses for a total of **1,680** students.
- ▶ Facilitated **34** strategic workshops that advanced interoperable, cyber-secure and resilient emergency communications in 27 states.
- ▶ **Expanded Cybersecurity service offerings** to include webinars, workshops and a rapid cybersecurity assessment.
- ▶ Engaged with public safety officials on the National Emergency Communications Plan by responding to **more than 500** requests and inquiries.

## CYBER INCIDENT REPORTING FOR CRITICAL INFRASTRUCTURE ACT OF 2022 SET TO SIGNIFICANTLY ENHANCE CYBERSECURITY EFFORTS

Many of the cybersecurity incidents that have occurred over the past decade could have been prevented by the simple sharing of timely, quality information following previous incidents. This is a critical gap that the President and Congress aimed to close through the enactment of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

As required by CIRCIA, CISA has started to develop regulations requiring covered entities to report covered cyber incidents and related ransom payments to CISA. In line with the agency's commitment to collaboration, CISA sought the ideas and perspectives from stakeholders across the spectrum—including the public, the private sector, and other government representatives—by conducting listening sessions across the country and accepting written feedback in advance of publishing the Notice of Proposed Rulemaking.

- ▶ CISA triaged 37,875 cyber incident reports, acting on 2,609 incidents requiring CISA's assistance.

## CISA PARTNERS WITH THOUSANDS OF ELECTION OFFICIALS TO HELP PROMOTE SECURE ELECTIONS

Securing our nation's election infrastructure requires true partnership. CISA has been working with state and local election officials to be sure they have access to the resources, tools, capabilities, and information they need to build resilience against all threats. CISA worked with all 50 states, the **District of Columbia, and the U.S. territories** to secure the 2022 election. This work included hundreds of election infrastructure security assessments and cybersecurity vulnerability scanning in hundreds of jurisdictions. We also included work with the **3,400-member Election Infrastructure Information Sharing and Analysis Center**,

which provides real-time, actionable threat and mitigation information to help state and local election officials understand the risk environment.

Through the first three quarters of FY 2022, we conducted trainings, exercises, panel presentations, keynote speeches, and more around the nation to reach **more than 5,000 local, state, federal, international, and private sector entities with a role in election security and resilience**.

Tabletop the Vote, CISA's annual National Elections Exercise, included **more than 1,100 participants from 48 states, 16 federal agencies, and 18 sector partners**, addressing cyber and physical security challenges to election infrastructure.

# AGENCY UNIFICATION

UNIFYING AS ONE CISA THROUGH INTEGRATED FUNCTIONS, CAPABILITIES, AND WORKFORCE

Foundational to our success, the agency is unifying as One CISA through integrated functions, capabilities, and workforce. The agency is building a culture of excellence

based on core values and core principles that prize teamwork and collaboration, innovation and inclusion, ownership and empowerment, transparency and trust.



## BUILDING A WINNING CISA CULTURE

CISA is a great place to work because of our people and our culture. [CISA's Core Values](#) represent the fundamental tenets of the organization and guide all our actions: Collaboration, Innovation, Service, Accountability. The agency's Core Principles represent the ideal behaviors that will make our workforce individually and collectively successful. They are rooted in CISA's mission and vision, emanate from the agency's Core Values, and define our Culture: What we aim to cultivate in our organization, what we value, and what we aspire to be.

In our effort to build a unique culture at America's youngest federal agency—one that truly puts People First, cultivates psychological safety, and incubates innovative ideas—we launched a three-phased Culture Sprint to help manifest our Core Principles into our everyday lives.

- **In Phase One**, we launched a series of Psychological Safety Workshops, which were open to all CISA employees and contractors, and required for all supervisors. These workshops focused on the concept of psychological safety, the mission imperative of cultivating a culture where everyone is free to be their authentic self at work and treated with dignity and respect, and the innovative power that comes from a culture where psychological safety is a norm.
- **In Phase Two**, we held CommUNITY Circles, which further explored the concepts discussed in the workshops. These Circles offered the opportunity for employees to share how they are implementing the lessons from the workshops into their workplace as we build the foundation of CISA's People First culture.
- **And, in Phase Three**, we graduated 119 CISA employees from a 6-week Culture Cohort. This cohort laid the groundwork to unleash the innovative power of our workforce, launching a unique employee-driven innovation hub. Moving forward, this platform will enable employees to propose novel concepts for how to help build CISA into the agency that the nation deserves.





## 2022 DECLARED CISA'S YEAR OF MENTAL HEALTH AND WELLBEING

The COVID-19 pandemic took a toll on mental health for millions of Americans and was a key driver of workplace burnout over the past several years, something reflected in numerous engagements with our CISA workforce. That is why we committed to making 2022 the Year of Mental Health and Wellbeing—because we believe that mental health IS health. To that end, we pursued a series of efforts to review our existing support to employees, expand existing resources wherever possible, and launch novel new initiatives.

- **Educating Ourselves & Combatting Stigmas.** A key first step toward addressing mental health challenges is to raise awareness, create a conversation, and address misperceptions. To do so, we hosted ten Town Halls with world-renowned wellness experts, medical professionals, and mental health advocates, including Yale Professor Laurie Santos, burnout prevention author Jennifer Moss, and wellness thought leaders Guy Winch and Morra Aarons-Mele. These discussions focused on the science behind mental health, practical tips on how to prevent and combat burnout, and the imperatives for any organization to safeguard wellbeing in its workforce.
- **Taking Action.** While visibility is critically necessary, we also knew that it was in and of itself insufficient. To take action on what we learned, we highlighted existing resources for employees and spearheaded new initiatives. This included launching CISA CARES, a consolidated resource hub for employees to leverage wellness services, rolling out the Headspace mindfulness app free-of-charge for employees, and establishing Meditation Rooms for employees to reserve throughout the workday.

A recent employee survey noted that these efforts were both relevant and useful, we plan to continue championing mental health and wellness as priority focus areas in the years to come.



## AN ONGOING COMMITMENT TO DIVERSITY, EQUITY, INCLUSION, AND ACCESSIBILITY

CISA is dedicated to advancing, welcoming, and celebrating all forms of diversity from neurodiversity, diversity of gender identity, race, ethnicity, sexual orientation, age, religion, disability, and social and economic background. Diversity of experience equals diversity of thought and that makes us better problem solvers.

In FY22, we instituted a mandatory instructor-led, two-session training—Stronger Together: The Power of Diversity & Inclusion, which was completed by over 2100 employees. Training topics included: “Language Matters,” “Making the Case for Inclusive Diversity,” “Practicing Inclusive Diversity,” “Making the Unconscious Conscious,” “Values Training,” “Identifying and Reducing Bias,” “5 Habits of Inclusivity,” and “Structured Tools to Combat Bias.”

In addition, we stood up an External Civil Rights and Civil Liberties (ECRCL) function to ensure the agency executes our mission while preserving individual liberty, fairness, and equality under the law. As one of its first actions, the ECRCL team created CISA’s first Language Access Plan, setting CISA on a path to develop and implement reasonable efforts to eliminate or reduce barriers to persons with limited English proficiency to accessing CISA resources, services, activities, and events.

We are also dedicated to working across the broader community to ensure individuals from every background and walk of life have an equal opportunity to work in the field of cybersecurity.

Our country and our global networks are strongest when our workforce reflects the full diversity of the American people. We continue to seek new ways to promote diversity and inclusion both at CISA and across the cybersecurity community at large.



- We partnered with [Girls Who Code](#) to develop pathways for young women to pursue careers in cybersecurity and technology. This partnership will seek to tackle diversity disparities by working to heighten the awareness of cybersecurity and technology careers and working with employers to build tangible pathways for young women, especially young women of color, to get hands-on experience in the private sector, the non-profit sector, or government.
- As part of our mission to recruit diverse cybersecurity talent and build the workforce of the future, we awarded \$2 million to two innovative organizations for development of cyber workforce training programs. The [NPower](#) and [CyberWarrior](#) organizations, which received the awards, focus on the unemployed and underemployed; underserved communities in urban and rural areas; as well as traditionally underserved populations, to include veterans, military spouses, women, and people of color.



- We joined forces with [CYBER.ORG](#) and [Girl Scouts of the USA](#) to create a Cyber Awareness Challenge. Through the challenge, girls across the country are given direct access to fun activities that will strengthen their skills and interest in cybersecurity.
- Our Cybersecurity Defense Education and Training Program (CDET), through [CYBER.ORG](#), initiated a partnership with nine Historically Black Colleges and Universities (HBCU) through [Project REACH | Cyber.org](#). The partnering institutions include Morgan State University, Claflin University, Langston University, University of Arkansas at Pine Bluff, Stillman College, Shaw University, Voorhees College, Lane College, and Bowie State University. For each HBCU partner, CYBER.ORG is working to develop partnerships with three surrounding high schools that receive Title-I funding and serve historically underrepresented students to build cybersecurity course pathways.

## STANDING UP A NEW PROCUREMENT CAPABILITY

As a young agency, CISA did not initially have its own internal contracting capabilities and was supported by the Department of Homeland Security headquarters oversight for its contracting requirements activity within CISA. In FY 22, Congress took the important step to fund positions to stand up a contracting office in CISA. Additionally, the Executive Director of the DHS Office of Procurement Operations, as the Head of Contracting Activity, delegated the necessary authorities to CISA's new Chief of the Contracting Office. The development of this office and the delegated procurement authorities now allows CISA to directly coordinate the planning, execution, and administration of the agency's contracts. As a direct result of this new authority, CISA's internal procurement processes are becoming more efficient, with better alignment among the CISA portfolios to ensure optimal and streamlined contracting vehicles. Our new procurement office is able to engage with CISA programs early, as they discuss contract requirements, which helps reduce turnaround times for contracting actions. Notably, we continue to focus on managing our procurement spending through our Strategic Sourcing program and leveraging Best in Class (BIC) contract vehicles to eliminate redundancies, increase efficiencies, and deliver value and savings to taxpayers. For vendors wanting to do business with us, our new procurement capability enables industry to directly interact with our Contracting Officers and Program Offices on specific contract requirements. As we look to 2023, CISA will take advantage of this new authority to begin developing a small business program to help small businesses learn how to do business with us.



# CONCLUSION

LOOKING BACK, FORGING AHEAD

It is hard to believe CISA just turned four years old on November 16, 2022. Over the course of FY22, we accomplished much to advance our vision of secure and resilience infrastructure, while laying the groundwork for ever deeper and increasingly substantial efforts in the coming years. Many of the projects launched this past year—like the cybersecurity grant program for state, local and territorial governments, implementation of CIRCIA, and the Cybersecurity Performance Goals—are multi-year efforts that will mature and expand in FY23 and beyond. We'll see a tribal version of the cybersecurity grant program launched in 2023, tailored to the Native American community. The relationships developed through our international engagements will continue to mature and bear fruit as we confront the ever-evolving cyber-threat landscape. Building on CISA's Strategic Plan, the agency will produce supporting strategies, including the Stakeholder Engagement Strategic Plan that was released

in October and a Cybersecurity Strategic Plan to be released in early 2023, to guide our efforts over the coming years. Through CISA's regional presence, we will continue to support the federal response to major disasters like Hurricane Ian, where we provided information on critical infrastructure impacts, facilitated infrastructure prioritization and restoration efforts, and kept communication channels open for emergency responders. And (!), we will be launching a completely updated website to ensure our resources, information and assistance is readily available to all our partners and stakeholders.

As we saw in 2022, things move fast here. Heading into the new year, be sure to follow us on social media to stay current on new developments, engage CISA directly through our regions or headquarters programs, and take part in the many information sharing opportunities we offer, both in-person and virtually.



## ABOUT CISA

The Cybersecurity and Infrastructure Security Agency (CISA) is the newest agency in the federal government, established in 2018 to be America's Cyber Defense Agency. We serve as the National Coordinator for critical infrastructure security and resilience, leading the effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day. As the majority of our nation's critical infrastructure is owned and operated by the private sector, operational collaboration is foundational to our efforts. We work with a wide array of partners across the globe—from every industry, to federal, state, local, tribal, territorial, and international governments, to non-profits, academia, and the research community—connecting them together and to the resources, tools, and information that will help them fortify their security and resilience against current and emerging threats.



CISA.GOV



LINKEDIN.COM/COMPANY/CISAGOV



@CISAGOV | @CISACYBER | @CISAJEN



FACEBOOK.COM/CISA



@CISAGOV



@CISAGOV