ONE CISA: COLLABORATION, INNOVATION, SERVICE, ACCOUNTABILITY

CISA

STRATEGIC PLAN

2023–2025

PUBLICATION: SEPTEMBER 2022 | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Contents

MESSAGE FROM THE DIRECTOR

I am proud to share the 2023–2025 CISA Strategic Plan, the first comprehensive Strategic Plan since CISA was established as an Agency in 2018. The Strategic Plan represents a forward-leaning, unified approach to achieving our vision of ensuring secure and resilient critical infrastructure for the American people.

At CISA, we lead the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure that Americans rely on every hour of every day. The risks we face are complex, geographically dispersed, and affect a diverse array of our stakeholders, including federal civilian government agencies, private sector companies, state, local, tribal, and territorial (SLTT) governments, and ultimately the American people. It is our duty to work with our stakeholders to mitigate these risks to preserve our national security, economic stability, and the health and safety of all our citizens.

Our Strategic Plan lays out four ambitious goals that we must achieve to address the diverse and dynamic challenges facing our nation.

First, we will spearhead a national effort to ensure the defense and resilience of **cyberspace**. In our role as America's cyber defense agency, we must build the national capacity to defend against, and recover from, cyberattacks. We must work 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. And we must partner with the private sector and SLTT governments to detect and mitigate cyber threats and vulnerabilities before they become incidents.

Second, we will **reduce risks to, and strengthen the resilience of, America's critical infrastructure**. Our 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. We will proactively reduce risk to infrastructure and systems while also building our stakeholders' capacity to safeguard their infrastructure from cyber and physical threats and risks. During incidents and major disasters, we stand ready to assist our stakeholders and ensure that government officials and public safety personnel can communicate quickly and efficiently.

Third, we will **strengthen whole-of-nation operational collaboration and information sharing**. At the heart of CISA's mission is partnership and collaboration. Securing our nation's cyber and physical infrastructure is a shared responsibility. We are challenging traditional ways of doing business and actively working with our government, industry, academic, and international partners to move toward more forward-leaning, action-oriented collaboration. We are also committed to growing and strengthening our agency's regional presence to more effectively deliver the assistance our stakeholders need.

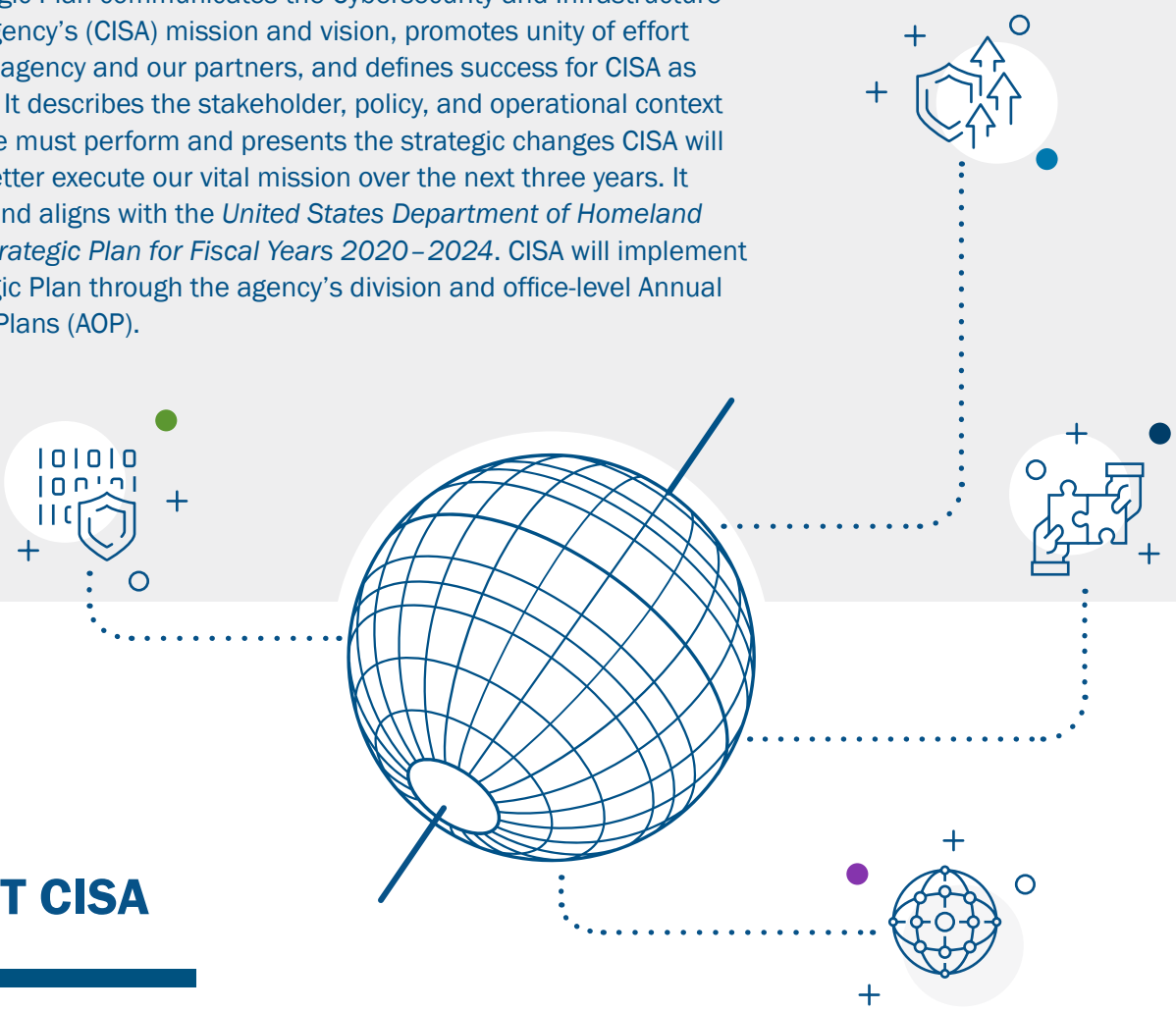
And fourth, foundational to our success, we will **unify as One CISA through integrated functions, capabilities, and workforce**. We will succeed because of our people. We are building a culture of excellence based on core values and core principles that prize teamwork and collaboration, innovation and inclusion, ownership and empowerment, and transparency and trust. As one team unified behind our shared mission, we will "work smart" to operate in an efficient and cost-effective manner.

There is much work to be done. CISA is at the center of a national call to action, and our world-class team is ready to deliver on our mission, working closely with a diverse group of partners across all sectors. Together, we will make essential progress to address the risks facing the nation and ensure the security and reliability of the critical services and infrastructure on which the nation depends.

Jen Easterly
Director

PURPOSE

This Strategic Plan communicates the Cybersecurity and Infrastructure Security Agency's (CISA) mission and vision, promotes unity of effort across the agency and our partners, and defines success for CISA as an agency. It describes the stakeholder, policy, and operational context in which we must perform and presents the strategic changes CISA will make to better execute our vital mission over the next three years. It builds on and aligns with the *United States Department of Homeland Security Strategic Plan for Fiscal Years 2020–2024*. CISA will implement the Strategic Plan through the agency's division and office-level Annual Operating Plans (AOP).



ABOUT CISA

Established by the *Cybersecurity and Infrastructure Security Agency Act of 2018*, **CISA serves as both America's cyber defense agency and as the national coordinator for critical infrastructure security and resilience**. This vast mission space necessitates engagements and partnerships with stakeholders worldwide as well as a strong domestic, regional presence. The threats we face—digital and physical, human-made, technological, and natural—are more complex, and the threat actors more diverse, than at any point in our history. CISA is at the center of mobilizing a collective defense as we lead the nation's efforts to understand, manage, and reduce risk to our critical infrastructure. Through all our efforts, we will remain vigilant about preserving the American people's privacy, civil rights, and civil liberties.

We count among our stakeholders the Federal Civilian Executive Branch (FCEB); state, local, tribal, and territorial (SLTT) governments; the private sector; Sector Risk Management Agencies (SRMAs); non-governmental organizations; non-profits; the American public; international partners; and academia.

CURRENT RISK LANDSCAPE

Our agency must execute this Strategic Plan in a complex landscape of ever-evolving risks to the nation's infrastructure and networks. Our increasingly interconnected, global cyberspace presents profound challenges in which we face 24/7/365 asymmetric, cyber threats with large scale real-world effects. Regardless of mission, industry, or sector, all organizations share the same overarching concerns. These include increasing adversary sophistication, capability, and boldness; an expanding cyberattack surface created through highly connected and interdependent technologies; and the need to rapidly increase the pool of highly skilled cyber talent for today and the foreseeable future. Outpacing our rivals' and adversaries' cyber capabilities is a national security imperative.

Cyber threat actors use increasingly sophisticated capabilities to undermine the U.S. economy and democracy, steal intellectual property, and sow discord. They take advantage of the operational boundaries between government organizations; the complexity of cyber infrastructure that spans public and private networks; and sponsorship by foreign adversaries. The urgency of CISA's cyber defense mission has never been more apparent than in our approach to defending the nation from the cyber

SHIELDS UP

CISA has been engaged in a Shields Up campaign since late 2021. In the face of potential spillover effects to the U.S. homeland related to the Russia-Ukraine crisis, the agency has been encouraging organizations of all sizes to take immediate steps to improve their cybersecurity and protect their critical assets. This campaign has included more than 100 briefings to thousands of stakeholders and a proactive effort to drive traffic to CISA.gov/Shields-Up. The Shields Up web page includes steps organizations can take to be more cyber secure; free cybersecurity resources for critical infrastructure partners; and guidance on how organizations can prepare themselves to mitigate the impact of potential foreign influence operations and mis-, dis-, and mal-information. Since its launch in February 2022, the Shields Up web page quickly became the most popular page on CISA.gov.

threat posed by Russia immediately after the invasion of Ukraine in early 2022. We facilitated effective collaboration with public and private sector partners to ensure vigilance in the face of potential malicious cyber activity targeting the nation's infrastructure, and we rapidly shared valuable information with those partners to help build our collective readiness. But our work is far from finished. Mitigating cyber threats requires a continuous, whole-of-nation approach that spans all stakeholders.

The diversity, complexity, and sheer expanse of our nation's physical infrastructure also poses unique challenges. Securing critical infrastructure, public gatherings, election polling places, and key facilities from the threats of terrorist attacks and targeted violence remains a key priority. The risks posed by a changing climate are equally daunting. As climate events grow more extreme, we can expect natural hazards, scarcities, and system stresses to place further strain on our nation's infrastructure, which will require greater emphasis on resilience. Such risks also heighten the pressures on local or regional emergency responders and government officials during incidents and events. They must have resilient, interoperable communications systems in place before the next disaster hits.

Of course, threats and risks are not confined to a single system or entity. Infrastructures that underpin our National Critical Functions (NCF) cross multiple sectors and continue to grow more interdependent. NCF are functions of government and the private sector so vital to the U.S. that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. The boundaries between the nation's cyber and physical infrastructure are therefore increasingly blurred. The convergence of cyber-physical technologies and systems that deliver our critical functions—from manufacturing to healthcare to transportation and beyond—means that single events can manifest in the loss or degradation of service across multiple industries. Operational technology (OT) and industrial control systems (ICS) pose unique risks that demand particular focus due to the heightened consequences of disruption and challenges related to deploying certain security controls at scale. While new and emerging technologies are vital drivers of innovation and opportunity, they can also present unanticipated risks. Similarly, unforeseen interdependencies can lead to systemic risk conditions and cascading impacts. Such an evolving environment requires a more unified approach than ever before.

In this dynamic risk landscape, we must be smart, innovative, and adaptable. Meeting these challenges requires an empowered workforce collaborating as a unified agency. We are committed to being the premier place to work in the federal government with a high-performing workforce. We also continuously strive to improve our business operations as we grow ever more integrated and agile. Together we serve as one team and "One CISA."

North Star

We see a country where the cyber and physical infrastructure that Americans rely on every hour of every day is safe, secure, and resilient.

This is CISA's north star—a guiding light for the numerous activities we undertake every day. It reminds us why our agency exists and why CISA's extraordinary people across the nation work tirelessly to achieve our vital mission.

We see a secure cyberspace that can support our way of life and make America the safest place to connect online. We see reliable delivery of critical services and functions to every home and business across our nation. And we see public and private sector organizations working as one team to defend against adversaries, preserve and protect national security, maintain a prosperous economy, and ensure the safety of all Americans.

OUR MISSION

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

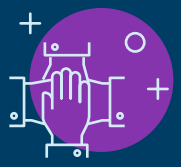
OUR VISION

Secure and resilient infrastructure for the American people.

CISA Core Values

CISA was designed to be something special and different. Not another bureaucracy, but something much more akin to a public-private collaborative. Our core values reflect this design and underpin everything we do at CISA:

Collaboration



Strong and vibrant partnerships are critical to everything we do; we will approach every engagement as an opportunity to build trust with our teammates, our partners, and our customers.

Innovation

We face threats at machine speed and adversaries unbounded by bureaucracy; we must move with creativity and agility at the speed of ideas to stay ahead of threats to our nation and our way of life, and we must be grounded in the strength of our resilience.

Service

We are defined by our dedication to selflessly serving the American people; more than a mission, our commitment is a calling to protect and defend the infrastructure Americans rely on every hour of every day.

Accountability

We will only succeed if every one of us takes active ownership of our mission, our words, and our actions. We will model the behavior we want to see in others; we will hold ourselves and our teammates responsible for our actions; and we will empower our workforce through trust, transparency, and radical honesty.

CISA Core Principles

Our core principles (See Figure 1) represent the ideal behaviors that will make us successful, both individually and collectively. They are rooted in our mission and vision, emanate from our core values, and define our culture: what we aim to cultivate in our organization, what we value, and what we aspire to be.

For more information on our core principles, please see www.cisa.gov/culture.

FIGURE 1. CISA Core Principles

In addition to our core values, which are woven throughout these principles, the overarching themes include trust, teamwork, empathy, imagination, inclusion, empowerment, ownership, and the power of resilience.

CISA places strong emphasis on culture because we believe it critical to fulfilling our mission. Living our core values every day and adopting our core principles with a growth mindset are the pathways to our success, and thus the success of our nation.

Strategic Plan Overview

This Strategic Plan defines four goals that will drive CISA to achieve our mission as a unified agency. Aligned with each goal are objectives detailing how we will accomplish these goals and measure our success. Figure 2 below depicts our strategic framework. In the sections that follow, representative outcomes and measurement approaches highlight what success looks like for each objective. CISA is developing specific measures of performance and effectiveness, which will be defined in our annual operating plans (AOPs). Identifying appropriate measures is not a simple task. It will require an ongoing effort throughout the performance period of the plan, and we will refine them as needed.

VISION

Secure and resilient infrastructure for the American people.

MISSION

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

GOAL 1

CYBER DEFENSE

Lead the national effort to ensure defense and resilience of cyberspace

OBJECTIVE 1.1
Enhance the ability of federal networks and systems to withstand cyberattacks and incidents

OBJECTIVE 1.2
Increase CISA's ability to actively detect cyber threats targeting America's critical networks

OBJECTIVE 1.3
Drive the disclosure and mitigation of critical cyber vulnerabilities

OBJECTIVE 1.4
Advance the cyberspace ecosystem to drive security-by-default

GOAL 2

RISK REDUCTION AND RESILIENCE

Reduce risks to, and strengthen resilience of, America's critical infrastructure

OBJECTIVE 2.1
Expand visibility of risks to infrastructure, systems, and networks

OBJECTIVE 2.2
Advance CISA's risk analytic capabilities and methodologies

OBJECTIVE 2.3
Enhance CISA's security and risk mitigation guidance and impact

OBJECTIVE 2.4
Build greater stakeholder capacity in infrastructure and network security and resilience

OBJECTIVE 2.5
Increase CISA's ability to respond to threats and incidents

GOAL 3

OPERATIONAL COLLABORATION

Strengthen whole-of-nation operational collaboration and information sharing

OBJECTIVE 3.1
Optimize collaborative planning and implementation of stakeholder engagements and partnership activities

OBJECTIVE 3.2
Fully integrate regional offices into CISA's operational coordination

OBJECTIVE 3.3
Streamline stakeholders' access to and use of appropriate CISA programs, products, and services

OBJECTIVE 3.4
Enhance information sharing with CISA's partnership base

OBJECTIVE 3.5
Increase integration of stakeholder insights to inform CISA product development and mission delivery

GOAL 4

AGENCY UNIFICATION

Unify as One CISA through integrated functions, capabilities, and workforce

OBJECTIVE 4.1
Strengthen and integrate CISA governance, management, and prioritization

OBJECTIVE 4.2
Optimize CISA business operations to be mutually supportive across all divisions

OBJECTIVE 4.3
Cultivate and grow CISA's high-performing workforce

OBJECTIVE 4.4
Advance CISA's culture of excellence

CISA CORE PRINCIPLES

People First • Do The Right Thing. Always. • Lead With Empathy • Seek And Provide Honest Feedback • Communicate Transparently And Effectively • Imagine, Anticipate, And Innovate To Win • Make It Count • Build And Cultivate Your Network • Play Chess • Stand In The Arena • Commit To A Lifetime Of Learning

CISA CORE VALUES

COLLABORATION || INNOVATION || SERVICE || ACCOUNTABILITY

FIGURE 2. Strategic Plan Overview

GOAL 1

Cyber Defense

SPEARHEAD THE NATIONAL EFFORT TO ENSURE DEFENSE AND RESILIENCE OF CYBERSPACE

CISA serves as America's cyber defense agency, spearheading the national effort to defend against cyber threat actors that target U.S. critical infrastructure, federal and SLTT governments, the private sector, and the American people. CISA must lean forward in our cyber defense mission toward collaborative, proactive risk reduction. Working with our many partners, it is CISA's responsibility to help mitigate the most significant cyber risks to the country's NCF, both as these risks emerge and before a major incident occurs.

CISA focuses on minimizing the impact of attempts to infiltrate, exploit, disrupt, or destroy critical infrastructure systems and networks and the NCF they enable. We will advance our work as the operational lead for Federal Civilian Executive Branch (FCEB) cybersecurity and as the federal cybersecurity shared services provider. We must ensure that federal civilian agencies have access to the best cybersecurity tools, incident response support, and risk management capabilities to safeguard the networks that support our nation's essential operations.

Since we cannot mitigate risks we cannot see, we will actively hunt for cyber threats and engage the cybersecurity community to drive disclosure and mitigation of critical vulnerabilities. Additionally, we must advance security in the broader cyber ecosystem. Driving toward a future where software and hardware are designed and built with security as a top priority is a necessity, particularly in ICS and OT, which directly underpin critical functions. Beyond secure technology, it is also essential to address workforce shortages in our cyber ecosystem, to include ensuring that our cybersecurity workforce reflects the diversity of our country and is ready to meet the breadth of challenges ahead.

As the nation's cyber defense agency, we understand that effective public and private sector partnerships and collaboration are mission critical and the only way to achieve a secure and resilient cyber ecosystem that powers an innovative and prosperous nation.

OBJECTIVE 1.1

ENHANCE THE ABILITY OF FEDERAL SYSTEMS TO WITHSTAND CYBERATTACKS AND INCIDENTS

CISA is dedicated to helping federal agencies make the bold changes necessary to improve the nation's cyber defense posture. We will do so by driving and facilitating the adoption of modern, secure, and resilient technologies; improving incident response capabilities; limiting supply chain risk to the federal government; and increasing visibility into cyber threats across federal networks. We will leverage our authorities to the maximum extent to drive and measure adoption of strong cybersecurity practices among federal civilian agencies. We will also help agencies build effective security programs by providing scalable and innovative services and capabilities.

REPRESENTATIVE OUTCOMES

1 | FCEB agencies are prepared for and able to rapidly recover from cyberattacks and incidents.

2 | FCEB agencies maintain mission continuity during and after cyberattacks and incidents.

MEASUREMENT APPROACH

CISA will measure adherence to, and effectiveness of, CISA cyber defense guidance, standards, and directives for federal agencies to improve the nation's cyber defense posture.

OBJECTIVE 1.2

INCREASE CISA'S ABILITY TO ACTIVELY DETECT CYBER THREATS TARGETING AMERICA'S CRITICAL INFRASTRUCTURE AND CRITICAL NETWORKS

Our nation is facing threats from highly sophisticated adversaries that seek persistent access to valuable systems and information. Our ability to detect and prevent these threats depends on significantly expanding our operational visibility. CISA will advance our capability to actively detect threats across federal and SLTT networks while working with industry partners to enhance our understanding of threats targeting private networks. We will continuously innovate our threat hunting capabilities to rapidly orchestrate threat identification and mitigation at scale.

REPRESENTATIVE OUTCOMES

1 | CISA increases production of actionable detection information for America's network defenders.

2 | America's network defenders proactively mitigate threats on their most critical networks before damaging intrusions occur.

MEASUREMENT APPROACH

CISA will measure the effectiveness of key efforts in network monitoring, cyber threat analytics, and cyber threat hunting to reduce the time-to-detect and time-to-remediate intrusions.

OPERATION WARP SPEED

Operation Warp Speed (OWS) was a public-private partnership initiated by the U.S. government to facilitate and accelerate the development, manufacturing, and distribution of COVID-19 vaccines. When Operation Warp Speed was launched in response to the COVID-19 pandemic, CISA was tasked with protecting the vaccine supply chain from cyber and physical threats.

CISA applied supply chain risk management techniques to prioritize the protection of suppliers and created a Task Force to develop and execute a strategy for ongoing outreach to 5,600+ healthcare delivery organizations identified as relevant to the COVID-19 response.

OBJECTIVE 1.3

DRIVE THE DISCLOSURE AND MITIGATION OF CRITICAL CYBER VULNERABILITIES

Recognizing that every piece of hardware and software contains vulnerabilities, we will serve as a trusted partner to coordinate disclosure of newly identified vulnerabilities in a manner that reduces the window for adversary exploitation. CISA will work closely with public and private entities and the cybersecurity research community to incentivize identification and reporting of previously unknown vulnerabilities, then leverage a broad array of capabilities to drive mitigation. Along with our partners, we will enable timely and coordinated vulnerability disclosure, provide recommendations, and amplify appropriate mitigation countermeasures using relevant channels and mechanisms. To decrease the frequency and magnitude of these vulnerabilities, we must also leverage our authorities and capabilities to identify unmitigated vulnerabilities, particularly affecting critical infrastructure, and drive urgent mitigation before exploitation occurs. Finally, we will work with the cybersecurity community to leverage lessons learned and implement recommendations from the Cyber Safety Review Board and other advisory bodies to elevate our nation's cybersecurity.

REPRESENTATIVE OUTCOMES

1 | Critical infrastructure owners/operators gain enhanced transparency of cybersecurity vulnerabilities.

2 | Critical infrastructure owners/operators are positioned to coordinate and integrate mitigations prior to exploitation.

MEASUREMENT APPROACH

CISA will measure the utilization and effectiveness of CISA's cyber vulnerability assessments and remediation services to increase identification and mitigation of vulnerabilities, reducing the window that adversaries have to exploit critical infrastructure.

CYBER SAFETY
REVIEW BOARD

The Cyber Safety Review Board (CSRB) was established in 2022 as an unprecedented public-private partnership to bring together government and industry leaders to conduct authoritative reviews and assess significant cyber events that impact the public and private sectors. During its inaugural review of the vulnerabilities in the log4j software library, the CSRB engaged with nearly 80 organizations and individuals to gather insights, inform findings, and develop actionable recommendations to prevent and respond more effectively to future incidents. The CSRB provides a unique and innovative forum for leading experts from government and industry to deliver recommendations designed to collectively elevate our nation's cybersecurity.

OBJECTIVE 1.4

ADVANCE THE CYBERSPACE ECOSYSTEM TO DRIVE SECURITY-BY-DEFAULT

Public and private network defenders across the country rely on many common tools, processes, and resources to perform their work. CISA fosters the development and adoption of state-of-the-art network defense and cyber operations tools, services, and capabilities to drive security-by-default in the technology ecosystem. We also support technology providers and network defenders as they work to ensure the security of software- and hardware-enabled products, services, networks, and systems. Recognizing that a secure cyber ecosystem is as much about people as about technology, we will support national efforts to empower the national cyber workforce to fill shortages in critical skills through our cyber education resources. Lastly, we recognize that technology products must be designed and developed in a manner that prioritizes security, ensures strong controls by default, and reduces the prevalence of exploitable vulnerabilities.

REPRESENTATIVE OUTCOMES

1 | Technology products widely used in the provision of NCF are secure and resilient by design.

2 | The nation's networks and systems are increasingly secure by default.

MEASUREMENT APPROACH

CISA will measure the adoption and effectiveness of secure development practices and control adoption for technology products and services.

GOAL 2

Risk Reduction and Resilience

REDUCE RISKS TO, AND STRENGTHEN RESILIENCE OF, AMERICA'S CRITICAL INFRASTRUCTURE

CISA coordinates a national effort to secure and protect against critical infrastructure risks. This national effort is centered around identifying which systems and assets are truly critical to the nation, understanding how they are vulnerable, and taking action to manage and reduce risks to them. We serve as a key partner to critical infrastructure owners and operators nationwide to help reduce risks and build their security capacity to withstand new threats and disruptions, whether from cyberattacks or natural hazards and physical threats. Critical infrastructure is divided into 16 sectors with each sector having a designated Sector Risk Management Agency (SRMA) responsible for helping owners and operators manage risk in that sector. CISA serves as the SRMA for eight of the 16 designated critical infrastructure sectors, fulfilling a unique partnership role for those sectors' risk management efforts.

CISA also supports the other SRMAs in their security and resilience efforts by assisting with the identification and management of risks, and providing access to CISA capabilities and resources. Both in its capacity as an SRMA for multiple sectors and as a supporter and facilitator of the other SRMAs, CISA has a pivotal role in securing our nation's most critical infrastructure.

To better meet the diverse needs of our stakeholders and focus our efforts on the nation's most critical infrastructure, CISA must further deepen its understanding of current and future critical infrastructure risks to the nation. We identify and analyze risks using NCF which are, simply put, what we need critical infrastructure to do to achieve national security, economic security, and public health and safety. We use the NCF to frame the analysis that tells us where risk concentrates in entities, assets, systems, technologies, and commodities so we can focus our efforts where they will have the greatest impact in reducing risk to the nation. This approach allows us to anticipate the sources of potentially cascading impacts and plan for effective mitigations in today's interconnected infrastructure environment. When threats and hazards do arise, we must be operationally ready to assist our partners with incident management and recovery, including during significant cyber incidents and major disasters. Through the strengthening of our voluntary partnerships and under applicable regulatory responsibilities, including the Chemical Facility Anti-Terrorism Standards (CFATS), CISA will advance security solutions that address the most pressing risks facing the nation's critical infrastructure. For example, through the CFATS program, high-risk chemical facilities are required to put in place measures to detect, delay, and respond to physical and cyberattacks such as establishing security officials; creating barriers and access control measures; implementing intrusion detection capabilities; and developing incident reporting, response and investigation programs for both physical and cyberattacks, among other measures.

NATIONAL CRITICAL FUNCTIONS AND CRITICAL INFRASTRUCTURE

NCF are functions of government and the private sector so vital to the U.S. that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

The set of NCF are organized into four areas—connect, distribute, manage, and supply—which identify the:

CONNECTIONS by technologies that enable critical communications and capabilities to send and receive data (e.g., internet connectivity),

DISTRIBUTION methods that allow the movement of goods, people, and utilities inside and outside the U.S. (e.g., electricity distribution or cargo transportation),

MANAGEMENT processes that ensure our national security and public health and safety (e.g., management of hazardous material or national emergencies), and

SUPPLIES of materials, goods, and services that secure our economy (e.g., clean water, housing, and research and development).

The NCF, therefore, allow CISA to understand where risk is concentrated across entities, assets, systems, technologies, and commodities, which allows us to prioritize our efforts.

OBJECTIVE 2.1

EXPAND VISIBILITY OF RISKS TO INFRASTRUCTURE, SYSTEMS, AND NETWORKS

CISA's efforts to understand critical infrastructure risk are predicated on gathering the right data and insights, which empowers CISA to drive assessments, analysis, and decision-making. This requires deepening our insights into the nation's cyber and physical critical infrastructure assets and systems, as well as identifying the potential and future sources of risk that could impact that infrastructure. CISA must reinvigorate our role as the national authority on, and central repository of, the nation's critical infrastructure data. We will advance our tools, doctrine, and operational capacity for assessing infrastructure criticality, comprehensively identifying critical infrastructure, and understanding how infrastructure is vulnerable. We will field innovative tools and advance partnerships to gain visibility into cyber and physical threats and vulnerabilities. We will continually identify nascent or emerging risks before they pose threats to our infrastructure. Finally, with the passage of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), CISA is on a path to improve the government's visibility into cyber incidents so that CISA and other agencies can work with stakeholders to take action to better protect themselves from similar incidents.

REPRESENTATIVE OUTCOMES

1 | CISA is the central repository for and national authority on critical infrastructure data.

2 | CISA identifies emerging and systemic risks before they pose threats to critical infrastructure.

MEASUREMENT APPROACH

CISA will measure increases in visibility and critical infrastructure security.

OBJECTIVE 2.2

ADVANCE CISA'S RISK ANALYTIC CAPABILITIES AND METHODOLOGIES

Foundational to the success of the cyber defense and infrastructure security missions is understanding national and sector level risk, especially those that are systemic to critical systems, networks, and infrastructure. We must mature CISA's risk analysis capabilities and methodologies to promote in-depth understanding of the risks we face. Building from the expanded visibility achieved through Objective 2.1, we will ensure that critical infrastructure information and identification efforts are incorporated into analytic methodologies to yield thorough, integrated analytic output that can guide agency decision making. Where CISA divisions house unique technical expertise, particular programs may have tailored risk analytic capabilities that complement cross-agency strategic level risk priorities.

REPRESENTATIVE OUTCOMES

1 | CISA has tailorable risk analytic capabilities and methodologies that promote in-depth understanding.

2 | CISA operations are guided and prioritized by a comprehensive understanding of the risk landscape.

MEASUREMENT APPROACH

CISA will measure the maturity of NCF risk analytics and the cross-agency accessibility of risk data. CISA will also measure its support to SRMAs in assessing risk to their sectors.

OBJECTIVE 2.3

ENHANCE CISA'S SECURITY AND RISK MITIGATION GUIDANCE AND IMPACT

To enhance the protection of critical infrastructure from threats, hazards, and risks, CISA provides stakeholders with security and risk mitigation guidance and assistance. To improve and expand our risk reduction impact, we will deliver actionable expertise and mitigations for addressing infrastructure security threats and hardening emergency communications systems, and we will issue authoritative guidance to drive effective IT network risk management. We will focus this guidance on risks that matter to our stakeholders and that CISA has identified as priority.

Where appropriate within CISA authorities, we will set standards and recommendations to guide security decisions, much like our efforts to establish performance goals and increase the cross-sector cybersecurity baseline. We will ensure security at high-risk chemical facilities consistent with CFATS and other applicable statutes. Where appropriate and warranted, we will also provide targeted technical assistance or assessments that measurably advance security and resilience.

MEASUREMENT APPROACH

CISA will measure the effectiveness and adoption of CISA's physical, emergency communications, and cybersecurity guidance for stakeholders.

REPRESENTATIVE OUTCOMES

1 | Stakeholders adopt CISA's critical infrastructure security guidance, standards, performance benchmarks, and risk management expertise.

2 | High-risk chemical facilities meet risk-based performance standards.

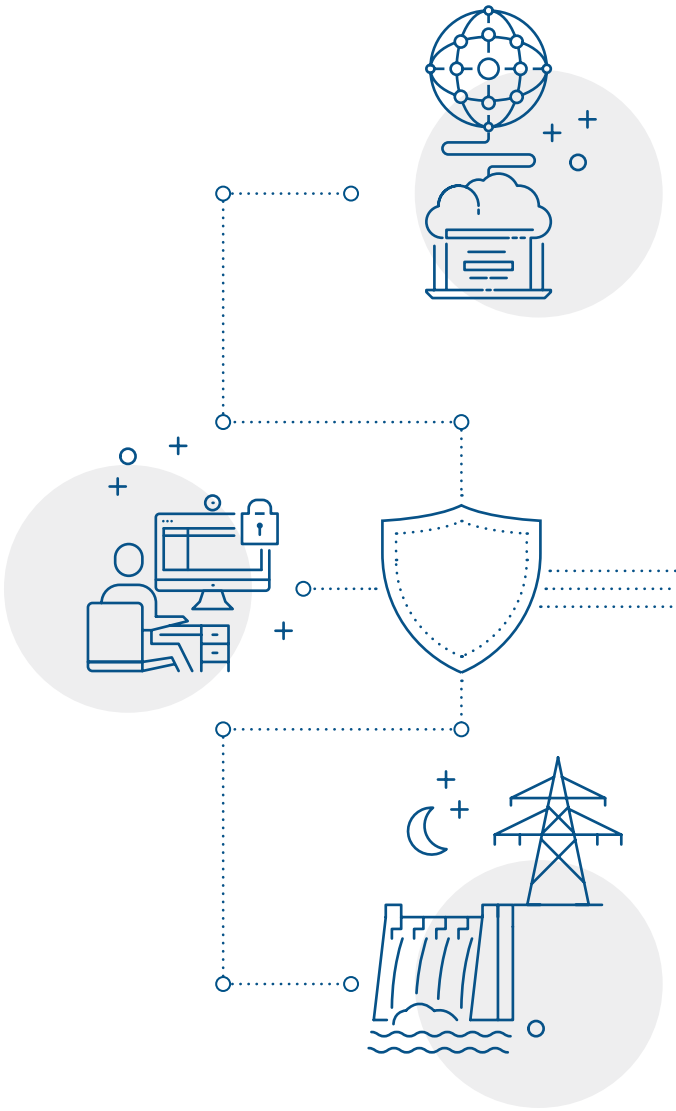
OBJECTIVE 2.4

BUILD GREATER STAKEHOLDER CAPACITY IN INFRASTRUCTURE AND NETWORK SECURITY AND RESILIENCE

CISA serves as a trusted partner in helping build the capacity of critical infrastructure owners and operators to make risk-informed decisions about their own security and resilience. To better serve their needs, we must appropriately scale CISA's key programs and risk related offerings in cybersecurity, infrastructure security, and emergency communications to meet our ever-growing stakeholder demand. This will include how we perform as an SRMA and the support that we provide to other Departments and Agencies in their SRMA roles. We will deliver impactful capabilities and services to meet our stakeholders' most pressing and evolving physical security challenges, which include insider threats, active shooter preparedness, bombing prevention, and security in public gathering places. We must also be responsive to emergent needs to tailor our offerings to address new risks, such as providing new emergency communications offerings specifically aimed at the cybersecurity risks that those systems face. Building capacity may also require broadening our offerings to new stakeholders and expanding cybersecurity services within CISA authorities to non-federal stakeholders.

MEASUREMENT APPROACH

CISA will measure the increase in and impact of key products and services available to different stakeholder groups.



REPRESENTATIVE OUTCOMES

1 | CISA's capacity building products and services are scalable to meet growing demand.

2 | SRMAs and other stakeholders recognize CISA's products and services as impactful, timely, and appropriately targeted to meet needs.

OBJECTIVE 2.5

INCREASE CISA'S ABILITY TO RESPOND TO THREATS AND INCIDENTS

CISA maintains a 24/7/365 operational posture and response coordination hub to respond to developing cyber and physical incidents or threats in a coordinated, integrated manner. We must bolster and expand our headquarters and regional capacity to support our stakeholders and interagency partners following physical threats and incidents, from terrorism and targeted violence attacks to major natural disasters. This will include CISA's role as an SRMA for eight critical infrastructure sectors and our support for other Departments and Agencies in their SRMA roles. During significant cyber incidents, CISA stands ready to support public and private entities' response, including deploying available incident response capabilities where appropriate, to limit negative impacts, minimize operational downtime, and enable rapid recovery. For events of national and regional significance such as natural disasters, we are similarly postured to deploy available assets and expertise, as appropriate, including supporting emergency responders through our responsibilities under Emergency Support Function 2 and Emergency Support Function 14 as outlined in the National Response Framework. Additionally, we will expand the reach of our vital emergency communications support services to ensure that first responder calls are connected and that public safety entities can rapidly communicate with each other during events.

REPRESENTATIVE OUTCOMES

1 | CISA supports our stakeholders' ability to respond quickly and appropriately to developing threats and incidents.

2 | CISA enables the continuity and resilience of critical infrastructure.

MEASUREMENT APPROACH

CISA will measure the efficiency and usage of key emergency communications services and CISA's incident response capabilities.

OBJECTIVE 2.6

SUPPORT RISK MANAGEMENT ACTIVITIES FOR ELECTION INFRASTRUCTURE

SLTT governments run elections. As the SRMA for the Election Infrastructure Subsector, CISA is the federal government's hub for understanding and characterizing risks to election infrastructure and ensuring election officials and their private sector partners have the information they need to manage risk to their systems. By virtue of our voluntary partnership with election officials and vendors, CISA gleans unique insights from the services and assessments we offer and the contributions of federal partners like the FBI, the U.S. Election Assistance Commission, and the Intelligence

ELECTION SECURITY AND RESILIENCE

CISA's election security mission can serve as a model for effective integration of the agency's capabilities around a key issue area. Following the designation of Election Infrastructure as a critical infrastructure subsector in 2017, the agency (at the time as the National Protection and Programs Directorate) used a task force model to orient and prioritize key organization functions around securing election infrastructure, addressing an unfamiliar set of issues in service of a stakeholder group it had little experience working with previously. It was first able to draw on existing expertise within the organization to build partnerships with election officials and other key stakeholders that would facilitate the infrastructure and risk analysis necessary to understand the problem set. It then engaged a variety of internal analytic and operational resources to drive the development of innovative solutions that improved its ability to respond to election stakeholder needs—for example, the development of customized Last Mile products to help local election officials prepare for and respond to incidents impacting their infrastructure, or implementation of new capabilities like Crossfeed and the Remote Penetration Test that could scale more effectively to enable election offices to understand and address their cybersecurity vulnerabilities. It also worked to counter mis- and disinformation through initiatives such as the CISA Election Security Rumor vs. Reality website.

Community. We use such insights to drive the agency's guidance and inform risk management operations. Evolving along with the risk landscape, our support has grown from a cybersecurity focus to a broader risk management approach that balances cyber, physical, and operational security. This includes contextualizing existing resources and capabilities for effective application to the Election Infrastructure Subsector's risk management activities, as well as developing novel products for the subsector's unique risk profile. CISA also supports state and local officials as they address mis- and disinformation in their communities. Empowering trusted voices is critical to ensuring that accurate information is available on our core democratic processes.

REPRESENTATIVE OUTCOMES

1 | CISA's services, products, and guidance are responsive to stakeholder needs and improve iteratively based on its evolving understanding of risks to election infrastructure.

2 | Lessons learned from risk and vulnerability trends are applied across the Election Infrastructure Subsector.

MEASUREMENT APPROACH

CISA will measure the extent of its reach to SLTT and private sector election stakeholders with products and guidance appropriate for their risk profile and organizational capabilities.

GOAL 3

Operational Collaboration

STRENGTHEN WHOLE-OF-NATION OPERATIONAL COLLABORATION AND INFORMATION SHARING

Trusted, sustained, and effective partnerships between government and the private sector are the foundation of our collective effort to protect the nation's critical infrastructure. Our safety and security rely on the shared commitments and investments made across critical infrastructure sectors. Through our partnerships with federal agencies and others, CISA will expand and strengthen these shared commitments, provide products and services that make continued investment in infrastructure security and resilience the smart and easy choice, and enhance information sharing and collaboration at the local, regional, and national levels. We will use our full suite of convening authorities and relationship management capabilities to expand and mature partnerships with stakeholders and facilitate information sharing.

We will approach every partnership with humility, transparency, gratitude, and a firm resolution to add value wherever possible.

This requires local, regional, and national presence and active engagement. It also requires developing a recognizable CISA brand and that we reliably deliver on our brand promise to defend and protect critical infrastructure. We will work through the partnership structure defined in the National Infrastructure Protection Plan ("National Plan") to engage SRMAs and critical infrastructure sector partners, fulfilling our responsibilities as the national coordinator for critical infrastructure security and resilience. We will also conduct local, regional, and national stakeholder outreach through a robust, flexible, and highly capable regional presence. Comprising this presence will be functional experts and supporting personnel who deliver CISA products, services, and information while also collecting the stakeholder feedback necessary to continuously refine and improve our offerings and inform our focus areas. Throughout our engagements—whether one-to-many or one-to-one—we will provide value to the public, our partners, and stakeholders while aggressively protecting their privacy, civil rights, and civil liberties.

OBJECTIVE 3.1

OPTIMIZE COLLABORATIVE PLANNING AND IMPLEMENTATION OF STAKEHOLDER ENGAGEMENTS AND PARTNERSHIP ACTIVITIES

To optimize the value of engagements and partnerships for both CISA and our stakeholders, we must plan, prioritize, and coordinate stakeholder engagements within our agency, SRMAs, and across the broader stakeholder community. We will build our CISA brand among the stakeholders we serve, with the goal of fostering confidence in the value we bring. We will use stakeholder data and insights, customer demand signals, operational requirements, and leadership priorities to guide the development of national and regional level outreach campaigns; prioritize targeted regional, topic-specific, and sector-based engagements; and tailor individual customer engagements. We will fulfill legislative and policy mandates to lead sector-based engagement as an SRMA and as the national coordinator for critical infrastructure security and resilience. We will engage and partner across the full breadth of CISA's stakeholders as defined earlier, which also include disadvantaged groups.

REPRESENTATIVE OUTCOMES

1 | CISA engagements, partnerships, and coordination (in its national coordinator for critical infrastructure security and resilience role) are targeted, purposeful, and prioritized.

2 | CISA has new and strengthened stakeholder relationships.

MEASUREMENT APPROACH

CISA will measure the effectiveness of strategic stakeholder engagements and partnership activities.

OBJECTIVE 3.2

FULLY INTEGRATE REGIONAL OFFICES INTO CISA'S OPERATIONAL COORDINATION

CISA regional office staff are critical to successful outreach; they improve access to CISA's products and services, build partnerships, and develop nationwide risk reduction and resilience capacity. We will increase integration between headquarters (HQ) and the regional staff that provide nationwide CISA touchpoints. We will establish processes for coordinating engagement activities between HQ divisions and regions and mutually support operational relationship management. To optimize the delivery of CISA's programs, products, and services, we will strengthen links between our existing national level partnership management framework and regions, directly extending elements such as Sector and Government Coordinating Councils (SCC and GCC), into the regions as appropriate. CISA will also create the internal business management forums, mechanisms, and processes that make nationwide stakeholder engagement planning and coordination simple, efficient, and mutually beneficial.

REPRESENTATIVE OUTCOMES

1 | CISA HQ and Regional Operations share a common operating picture.

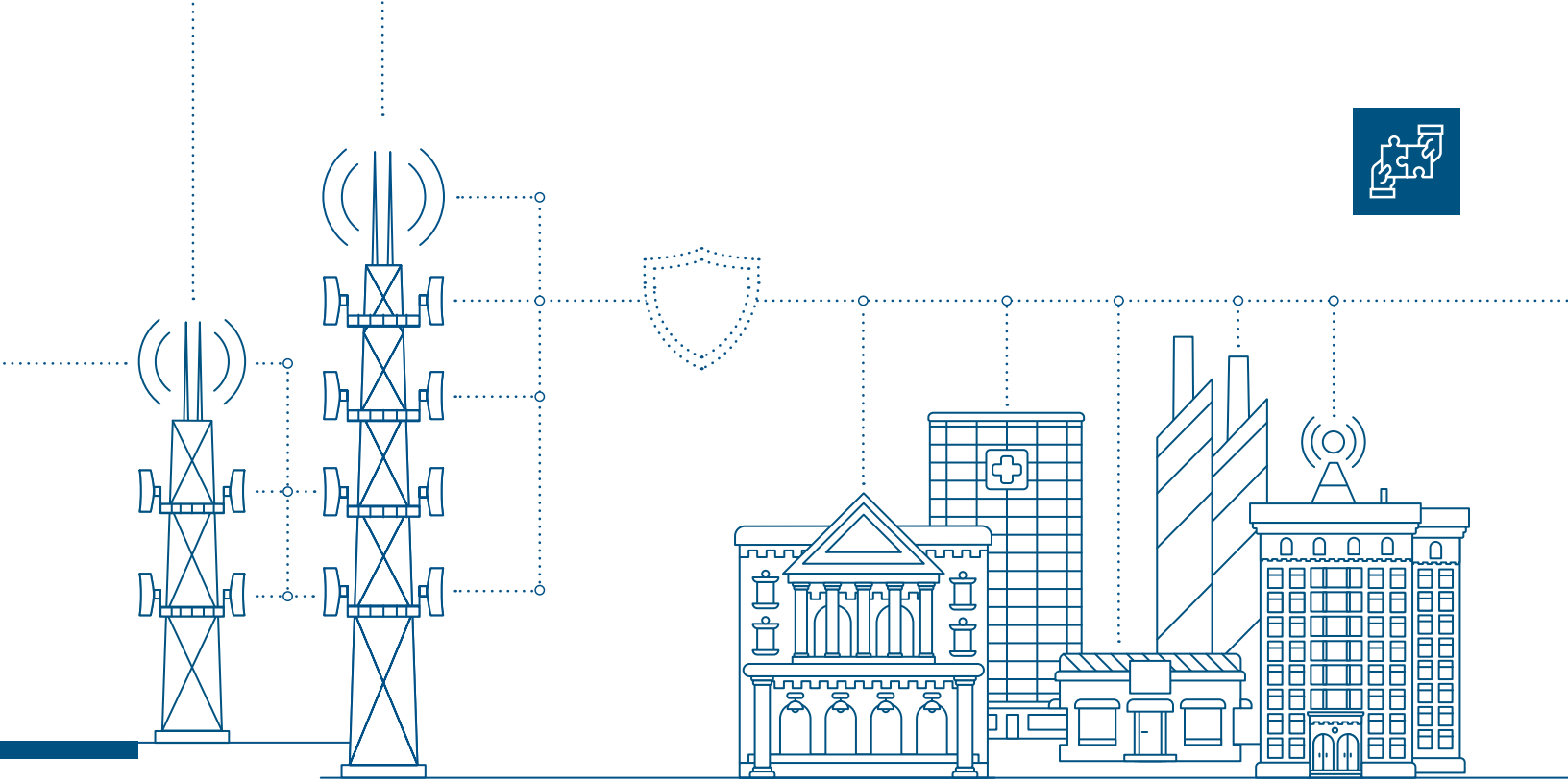
2 | The issues and concerns of local and regional stakeholders are appropriately raised within CISA and coordinating organizations.

MEASUREMENT APPROACH

CISA will measure the integration of regional and HQ coordination activities and the impact of regional stakeholder engagement.

JAMX22

The 2022 JamX counter-jamming event assessed the impact of jamming on public safety communications systems and mission response, and identified gaps in training. CISA developed the Public Safety Communications and Cyber Resiliency Toolkit to assist in evaluating current resiliency capabilities, identifying ways to improve resiliency, and developing plans for mitigating the effects of potential resiliency threats.



OBJECTIVE 3.3

STREAMLINE STAKEHOLDER ACCESS TO AND USE OF APPROPRIATE CISA PROGRAMS, PRODUCTS, AND SERVICES

CISA's programs, products, and services give our stakeholders the insights necessary to make timely, informed decisions about cyber and physical infrastructure risk reduction, defense, and resilience at the asset, system, and enterprise levels. To enable efficient and accessible use of these resources, CISA will strive to provide them to our customers on their terms. Wherever possible and suitable, we will offer our customers tailored product information, access, and delivery, based on their specific needs and circumstances. To this end, our catalog of resources will be consistently available, accurate, tailorable, engaging, and easy to access. We will market our programs, products, and services broadly and consistently across the agency to increase our reach among our core stakeholder groups, while looking to grow equitable access and use by underrepresented communities and non-traditional stakeholders.

REPRESENTATIVE OUTCOMES

1 | Stakeholders can quickly find and access relevant and appropriate CISA products and services.

2 | CISA proactively informs stakeholders of relevant and appropriate products and services.

MEASUREMENT APPROACH

CISA will measure the quality and accessibility of Division programs, products, and services.

OBJECTIVE 3.4

ENHANCE INFORMATION SHARING WITH CISA'S PARTNERSHIP BASE

To improve situational awareness for both CISA and our stakeholders, we must enhance multidirectional communications with external partners, including timely incident reporting and the sharing of threats and vulnerabilities, intelligence and intelligence requirements, as well as other information and data. Facilitating greater information sharing requires that we continue to build out new collaboration structures such as the Joint Cyber Defense Collaborative (JCDC), which works closely with SRMAs and Federal Cyber Centers. We are also maturing existing structures such as the Federal Senior Leadership Council (FSLC), Information Sharing and Analysis Organizations (ISAOs), Information Sharing and Analysis Centers (ISAC), SCCs, and GCCs. These will better position stakeholders for timely response to incidents. Enhancement refers to accelerating the speed, improving the accuracy, and enabling the effectiveness of information sharing and collaboration, while using CISA's authorities to preserve privacy, civil rights, and civil liberties.

REPRESENTATIVE OUTCOMES

1 | Stakeholders have access to timely, relevant, and accurate information to inform decision making.

2 | CISA's data handling and information sharing protects privacy, civil rights, and civil liberties.

MEASUREMENT APPROACH

CISA will measure the value of multidirectional information sharing with CISA partners.

JOINT CYBER DEFENSE COLLABORATIVE

CISA established the JCDC in 2021 to drive down cyber risk to the nation by combining the visibility and insight of the private sector with the federal cyber ecosystem. With more than 22 of America's largest cybersecurity and technology companies, and several government agencies, the JCDC provides a platform for true operational collaboration and engages in an unprecedented level of public-private proactive planning.

OBJECTIVE 3.5

INCREASE INTEGRATION OF STAKEHOLDER INSIGHTS TO INFORM CISA PRODUCT DEVELOPMENT AND MISSION DELIVERY

Insights from external stakeholders improve the CISA products and services that enable mission delivery. Some stakeholders provide direct feedback in the form of interviews and post engagement feedback requests. Others provide more indirect insights, such as through co-working with our partners or via lessons learned from assessment data over time. We will actively seek feedback from our stakeholders to ensure that we continuously refine and improve our product offerings to deliver tangible value as a trusted expert in the cyber and physical infrastructure domains. We will increase integration of stakeholder insights, information, and data to assist in decision making and the prioritization, development, modification, and tailoring of our products, services, and areas of focus.

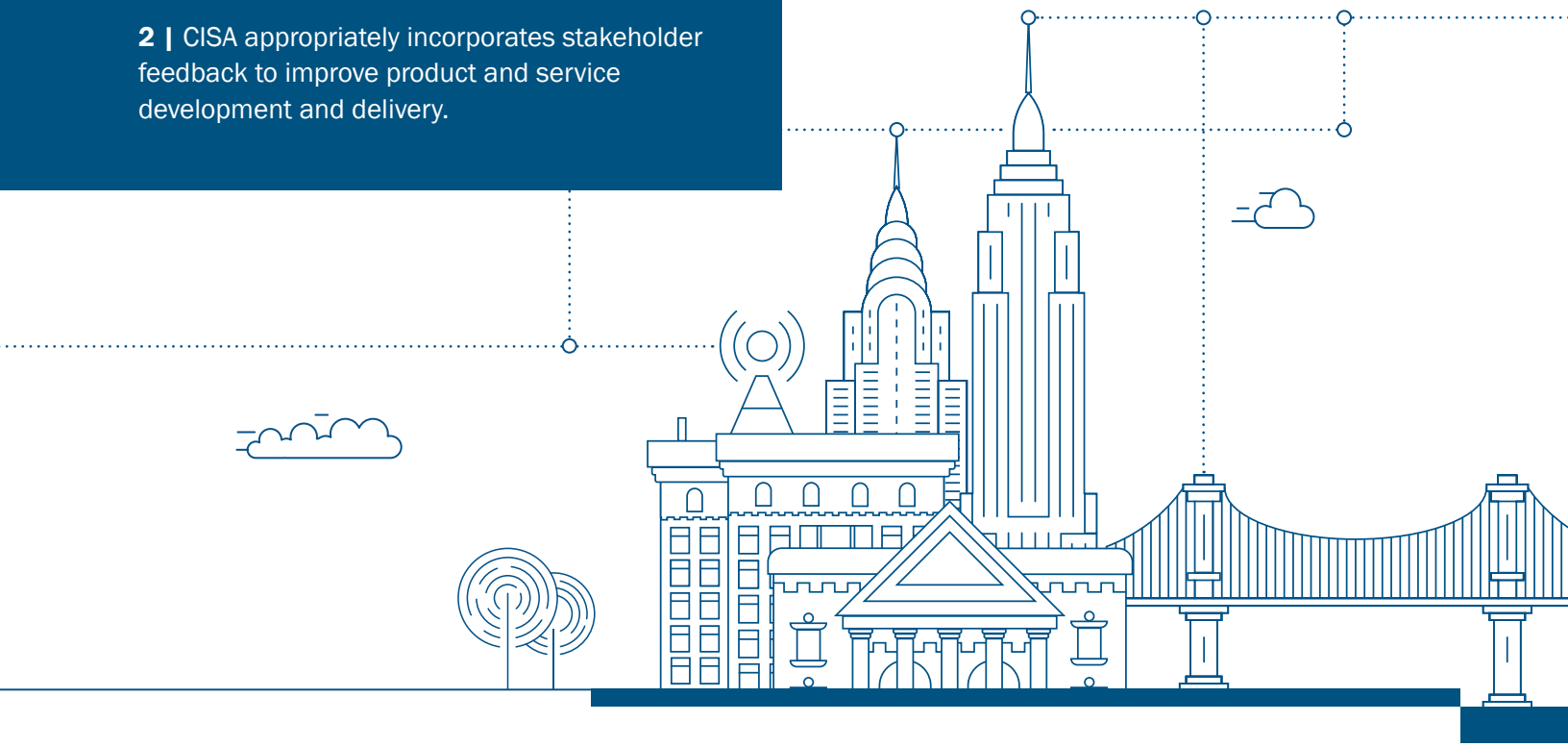
REPRESENTATIVE OUTCOMES

1 | Stakeholders have opportunities to provide feedback reflecting needs, interests, and priorities.

2 | CISA appropriately incorporates stakeholder feedback to improve product and service development and delivery.

MEASUREMENT APPROACH

CISA will measure stakeholder satisfaction and feedback to inform continuous improvements.



GOAL 4

Agency Unification

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

CISA must unify as an agency to work together as One CISA. This means we must streamline existing operations and adopt agile, new technologies that will enable customer service and improved timely, modern, and secure services. Through enhanced governance, management, and prioritization, we will break down organizational silos, grow the value of our services, and increase stakeholder satisfaction.

Additionally, we must enable and empower our workforce. People are CISA's most valuable asset. CISA is focused on creating an organizational culture where people love what they do, respect their colleagues, are empowered by their leaders, and feel like they are making a difference every day. We prioritize culture as key to success in our mission—

success that depends more upon unlocking the power and potential of people than of technology. CISA is building a culture of excellence that prizes core values and core principles, including teamwork and collaboration, innovation and inclusion, ownership and empowerment, and transparency and trust. Even as we focus on cultivating our workforce of today, it is important to recognize that our efforts also play an important role in helping build the workforce of tomorrow, especially a strengthened cyber workforce to meet our cyber defense challenges.

OBJECTIVE 4.1

STRENGTHEN AND INTEGRATE CISA GOVERNANCE, MANAGEMENT, AND PRIORITIZATION

CISA strives to mature and strategically address silos that prevent efficient delivery of our mission, without sacrificing the value gained through aggregated expertise, clear lines of accountability, and team identity. We will achieve this by implementing cross-Mission Enabling Office (MEO) meetings and exchange programs at all levels of CISA, and establishing governance and management structures that provide the necessary data and processes to enable prioritized decisions. CISA will work to delineate lines of effort and assign organizational and/or individual responsibility to drive collective decision making, and document and integrate processes to ensure standardization and utilization of best practices.

We will better integrate the Planning, Programing, Budgeting, Execution, and Evaluation (PPBEE) process into CISA governance processes and decisions to continue to be good stewards of public funds, provide effective internal controls for essential operational functions (e.g., payroll, invoicing, etc.), and support wise investment decisions. As CISA grows, we will strategically provision additional MEO resources such that CISA expands capacity, as necessary, to better achieve our mission.

REPRESENTATIVE OUTCOMES

1 | CISA translates leadership vision into prioritized action.

2 | CISA strategically and transparently allocates resources to support efficient delivery across the CISA enterprise.

MEASUREMENT APPROACH

CISA will measure effective and transparent oversight of funding and the degree to which programs and processes are standardized and integrated across the CISA enterprise.

OBJECTIVE 4.2

OPTIMIZE CISA BUSINESS OPERATIONS TO BE MUTUALLY SUPPORTIVE ACROSS ALL DIVISIONS

CISA business operations are critical to the organization's ability to function as one agency. As needs dictate, we will streamline existing operations and adopt agile, new technologies that will enable customer service and improved timely, modern, and secure services. Across CISA, we will advance and increase the utilization of products, services, and resources that prove to be effective—including secure, innovative, and interoperable technology solutions—to enable operational success. We will focus on integrating our systems and data to improve situational awareness, provide actionable information to support leadership decisions, improve processes and collaboration, and mature information sharing and data management across CISA.

REPRESENTATIVE OUTCOMES

1 | CISA senior leaders and operators have consistent and timely situational awareness, and actionable information.

2 | CISA integrates systems, processes, data, and architecture across the entire organization.

MEASUREMENT APPROACH

CISA will measure how effectively internal systems, processes, and architecture are enhancing multidirectional support across the entire organization.

OBJECTIVE 4.3

CULTIVATE AND GROW CISA'S HIGH-PERFORMING WORKFORCE

The nation needs excellence from CISA. We must deliver it. Our workforce must have the right credentials, expertise, and skills, and we must demonstrate their application of these skills in the quality of their work. We will build upon our success in cultivating and growing a workforce and culture that attract and retain our nation's most talented cyber and infrastructure defenders. We will implement a world-class talent ecosystem that spans recruiting, hiring, training, recognition, advancement, retention, and succession planning. To prevent future shortages that threaten our ability to compete, we will proactively seek, identify, and foster prospective talent from non-traditional places. We recognize and are prepared to meet the challenge of finding talented people from all areas and backgrounds with the aptitude and attitude to succeed. We will prioritize and leverage the DHS Cyber Talent Management System to modernize our recruiting and hiring efforts.

To foster employee retention, we must ensure equal access to professional development and educational opportunities for employees and leaders at all levels. We will deepen our mentoring and coaching programs across the organization, while rewarding exceptional CISA performers. Operating with One CISA voice, we will create an environment where high-performing teams can thrive by increasing transparency and operational effectiveness. We will create equitable outcomes for our workforce by creating more robust career paths and developing greater cross-component work opportunities for career advancement. This will also best enable CISA's workforce succession planning to ensure well-trained cyber defenders today as well as a strong pipeline of future cyber defense leaders.

CISA CYBER INNOVATION FELLOWS INITIATIVE

CISA's Cyber Innovation Fellows initiative offers private sector cybersecurity experts the opportunity to participate on the agency's cybersecurity operational teams, benefiting CISA's mission and their own professional development. Fellows will help design how CISA implements its cybersecurity programs and services, and will devise new approaches to legacy programs supporting federal cybersecurity, including AI, Machine Learning, and cloud security.


Nextgov

CISA is Seeking Cybersecurity Innovation Fellows

By Frank Konkel, Executive Editor, Nextgov JUNE 7, 2022

SECURITY

CISA launches Cyber Innovation Fellow initiative

June 14, 2022

MEASUREMENT APPROACH

CISA will measure the hiring and retention of the CISA workforce, and the utilization and impact of employee opportunities for training and growth.

REPRESENTATIVE OUTCOMES

1 | CISA hires, trains, and retains a skilled, diverse, and high-performing workforce.

2 | CISA recognizes, promotes, and provides a meaningful career track for our personnel.

OBJECTIVE 4.4
ADVANCE CISA'S CULTURE OF EXCELLENCE

The strength of CISA's culture is critical to our mission and foundational to our success as One CISA. We will continue building our culture through promulgation of our core values and core principles. Our culture will be incorporated in our day-to-day tasks, mission-enabling functions, service to our partners and stakeholders, and in our everyday behaviors. We will prioritize an environment of psychological safety where people can be their authentic selves; where they feel cared for, supported, empowered, and always treated with dignity and respect; where they feel a sense of ownership for mission; and where accountability and responsibility are welcome. We will prioritize wellness and resilience across our agency by systematically mitigating burnout and providing access to mental health resources. Advancing an organizational culture of fairness and justice requires that leaders at CISA promote transparency and equity around rewards, decision outcomes, communications, and employee treatment. To drive organizational performance, CISA will cultivate an environment where feedback, learning, growth, and innovative perspectives are welcomed and cherished. Capitalizing on our culture of excellence, CISA will be a recognized leader in the cyber community and a premier destination to work within the federal government.

REPRESENTATIVE OUTCOMES

1 | CISA is nationally recognized for our role in cyber defense and protection of critical infrastructure.

2 | CISA's cultural foundation of wellness, psychological safety, innovation, accountability, and enthusiasm for the mission is recognized, practiced, and reinforced.

MEASUREMENT APPROACH

CISA will measure improved psychological safety, diversity, and reduced burnout of the CISA workforce, which is imperative to enabling an innovative and motivated culture.

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

CISA | STRATEGIC PLAN 2023–2025

ONE CISA: COLLABORATION, INNOVATION, SERVICE, ACCOUNTABILITY