ONE CISA: COLLABORATION, INNOVATION, SERVICE, ACCOUNTABILITY

CISA

CYBERSECURITY

STRATEGIC PLAN

FY2024–2026

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Contents

EXECUTIVE SUMMARY

Our nation is at a moment of opportunity. The *2023 U.S. National Cybersecurity Strategy* outlines a new vision for cybersecurity, a vision grounded in collaboration, in innovation, and in accountability. Now is the moment where our country has a choice: to invest in a future where collaboration is a default rather than an exception; where innovation in defense and resilience dramatically outpaces that of those seeking to do us harm; and where the burden of cybersecurity is allocated toward those who are most able to bear it. We must be clear-eyed about the future we seek, one in which damaging cyber intrusions are a shocking anomaly, in which organizations are secure and resilient, in which technology products are safe and secure by design and default. This is a shared journey and a shared challenge, and CISA, as America's cyber defense agency, is privileged to serve a foundational role in the global cybersecurity community as we achieve measurable progress to our shared end state.

We know that the stakes are high. Our nation relies on connected technologies every hour of every day to enable essential services, from drinking water to electricity to financial systems. In recent years, this dependence has deepened even further, as many Americans now rely on connectivity for most aspects of their daily lives. Malicious cyber actors recognize our dependence on technology and constantly attempt to exploit this reliance for financial or strategic gain. Too often, they succeed. Their success is enabled by an environment of insecurity, in which our enterprises are too difficult to defend, and our technology products are too vulnerable to protect.

But we also know the steps to take. We must change how we design and develop technology products, such that exploitable conditions are uncommon and secure controls are enabled before products reach the market. We must quickly detect adversaries, incidents, and vulnerabilities, and enable timely mitigation before harm occurs. We must help organizations, particularly those that are "target rich, resource poor," take the fewest possible steps to drive the most security impact. Recognizing that we will not prevent every intrusion, we must ensure that our most essential services are resilient under all conditions, with particular focus on under-resourced communities where loss of key services can have the greatest impact. Most importantly, we must do it together, recognizing that true collaboration is the only path toward a more secure future.

To this end, our Cybersecurity Strategic Plan outlines three enduring goals:

GOAL 1: ADDRESS IMMEDIATE THREATS. We will make it increasingly difficult for our adversaries to achieve their goals by targeting American and allied networks. We will work with partners to gain visibility into the breadth of intrusions targeting our country, enable the disruption of threat actor campaigns, ensure that adversaries are rapidly evicted when intrusions occur, and accelerate mitigation of exploitable conditions that adversaries recurringly exploit.

GOAL 2: HARDEN THE TERRAIN. We will catalyze, support, and measure adoption of strong practices for security and resilience that measurably reduce the likelihood of damaging intrusions. We will provide actionable and usable guidance and direction that helps organizations prioritize the most effective security investments first and leverage scalable assessments to evaluate progress by organizations, critical infrastructure sectors, and the nation.

GOAL 3: DRIVE SECURITY AT SCALE. We will drive prioritization of cybersecurity as a fundamental safety issue and ask more of technology providers to build security into products throughout their lifecycle, ship products with secure defaults, and foster radical transparency into their security practices so that customers clearly understand the risks they are accepting by using each product. Even as we confront the challenge of unsafe technology products, we must ensure that the future is more secure than the present—including by looking ahead to reduce the risks and fully leverage the benefits posed by artificial intelligence and the advance of quantum-relevant computing. Recognizing that a secure future is dependent first on our people, we will do our part to build a national cybersecurity workforce that can address the threats of tomorrow and reflects the diversity of our country.

As we progress toward these goals, we must embody the hacker spirit, thinking creatively and innovating in every aspect of our work. The ongoing work of CISA's workforce—our threat hunters, vulnerability analysts, operational planners, regionally deployed cybersecurity advisors, and others—epitomize this collaborative spirit.

Each day, our team members work shoulder to shoulder with the cybersecurity community to address our most pressing cyber risks. We know we cannot achieve lasting security without close, persistent collaboration among government, industry, security researchers, the international community, and others. Even as we are accountable for national cybersecurity, we must align accountability across the ecosystem, such that cybersecurity is considered a foundational business risk at every organization and technology manufacturers prioritize product safety. Cyber incidents have caused too much harm to too many American organizations. Working together, we can change this course. Working together, we can create a new model. We know the path and we've collectively begun the right steps. Now is the time to focus, prioritize, and accelerate—recognizing that our adversaries are not going to wait.

Our Strategic Intent

In alignment with the *2023 National Cybersecurity Strategy* and the *Fiscal Year 2023–2025 CISA Strategic Plan*, this *CISA Cybersecurity Strategic Plan* describes how we will execute our cybersecurity mission and advance our cybersecurity capabilities. Within CISA, this Plan will serve as a keystone for implementation, resource, and operational planning, as further executed through our Annual Operating Plans. Externally, it will help stakeholders understand and participate in our long-term cybersecurity planning and prioritization.

OUR MISSION IS WELL-SUMMARIZED IN THE NATIONAL STRATEGY:

"Defending the systems and assets that constitute our critical infrastructure is vital to our national security, public safety, and economic prosperity … We aim to operationalize an enduring and effective model of collaborative defense that equitably distributes risk and responsibility and delivers a foundational level of security and resilience for our digital ecosystem."

THIS IS OUR NORTH STAR.

As we implement our Strategic Plan, changes to the threat and technology environments may require periodic re-evaluation of strategic priorities. However, the fundamental security shifts toward which we will drive, and the long-term investments defined by this Plan will endure.

CISA's approach to cybersecurity is grounded in five fundamental precepts:

CYBERSECURITY IS A WHOLE OF CISA MISSION: While our Cybersecurity Division provides unique technical expertise and executes many of the agency's core cybersecurity authorities, every organization, every team, every person in CISA contributes to our cybersecurity mission—recognizing that at times cybersecurity risks are most effectively addressed through non-digital means, such as investing in functional resilience under all conditions. In particular, our growing regional teams are essential to our aim of providing responsive and actionable assistance to organizations in every corner of our country.

CYBERSECURITY IS A WHOLE OF GOVERNMENT MISSION: Within the U.S. government, CISA serves a unique role—a role that depends on close collaboration with our interagency partners. We maintain invaluable operational partnerships with agencies such as the Federal Bureau of Investigation, the National Security Agency, U.S. Cyber Command, and the Sector Risk Management Agencies, and coordinate closely with the Office of the National Cyber Director, the Office of Management and Budget, and the National Security Council to advance national priorities and strategic imperatives. We must continue to institutionalize these partnerships so that they endure and eliminate any gaps in cohesion that could be exploited by our adversaries.

CYBERSECURITY IS A WHOLE OF NATION MISSION: The breadth of our cybersecurity challenge exceeds the capacity of any one organization. We will succeed or fail as a community. We will work toward a model where collaboration is the default response, where information about malicious activity, including intrusions, is presumed necessary for the common good and urgently shared between industry and government, and where government and industry work together with reciprocal expectations of transparency and value. Most

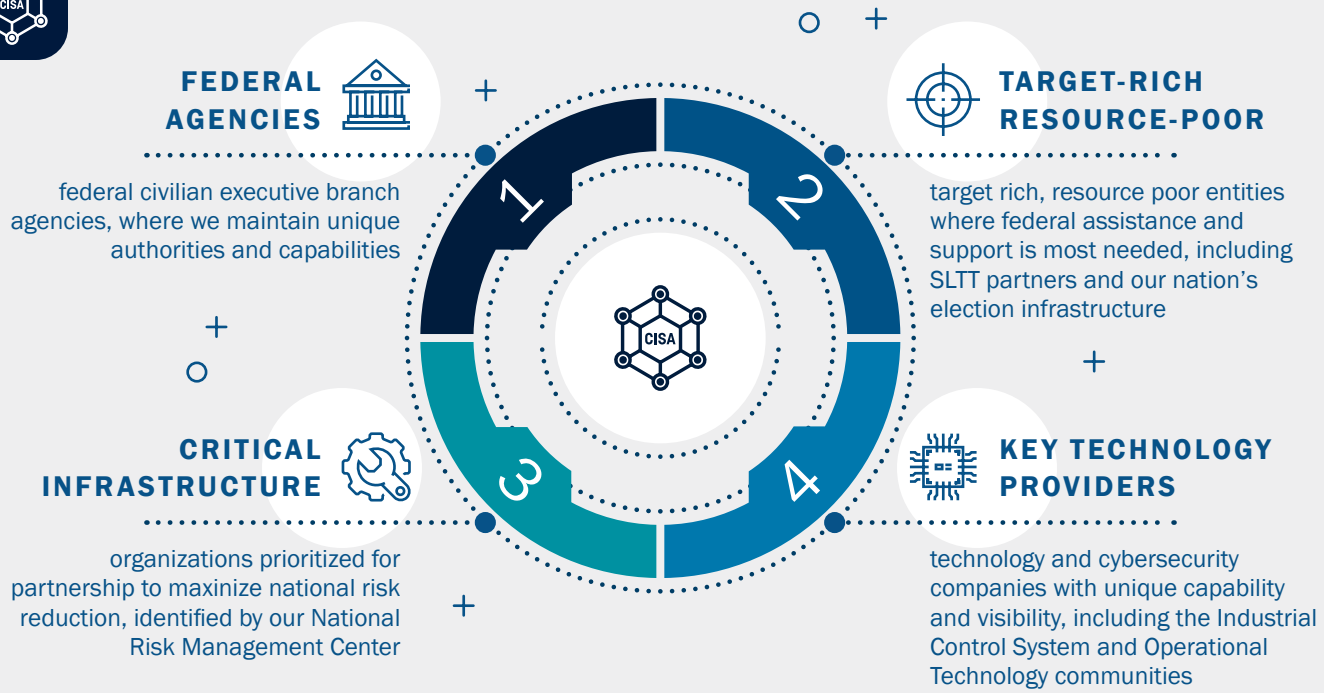


FIGURE 1. Priority Stakeholders

importantly, our success is based on the trust of our partners. At every turn, we will prioritize maintaining trusted relationships that allow us to serve as a unique partner and source of expertise. We also recognize that cybersecurity is a whole-of-society mission, in which every individual and organization has a role to play.

PRIORITIZE OUR RESOURCES WITH RIGOR AND HUMILITY: Like any organization, CISA's resources are finite, and we must prioritize our actions to achieve the greatest impact for the American people. We will focus our activities on four broad sets of stakeholders: (1) federal civilian executive branch agencies, where we maintain unique authorities and capabilities; (2) target rich, resource poor entities where federal assistance and support is most needed, including SLTT partners and our nation's election infrastructure; (3) organizations that are uniquely critical to providing or sustaining National Critical Functions, leveraging the analytic capabilities of our National Risk Management Center; and (4) technology and cybersecurity companies with capability and visibility to drive security at scale, including the Industrial Control System and Operational Technology communities. While we will not limit our support and engagement to these groups, prioritization will allow us to make prudent tradeoffs where necessary to maximize our contributions.

ACHIEVE IMPACT OR FAIL FAST: We recognize that cybersecurity risk to our country is too high, and that the American people expect CISA to play a central role in driving positive change. We must ensure that all of our efforts have a measurable impact in reducing cybersecurity risk, whether directly or indirectly, and rigorously leverage available data in determining whether our intended impacts are being achieved. Where we determine that a given program, service, or capability is not resulting in expected impacts, we will be disciplined in "failing fast" and making best use of our resources to pivot with agility.

CISA'S CYBERSECURITY

Goals and Objectives

Our Cybersecurity Strategic Plan includes goals and associated objectives that will be executed through Annual Operating Plans, assigning each CISA organization responsibilities for key milestones and metrics. Importantly, our three goals do not operate in isolation, as shown below.

GOAL 1 | Our understanding of immediate and emerging threats will enable us to prioritize investment in the security controls, product attributes, and services that most effectively reduce risks.

GOAL 2 | As we provide guidance and services that help organizations prioritize reductions in enterprise risk, we will more clearly define the risks that can be most effectively addressed by safer products.

GOAL 3 | As we advance security across the product lifecycle, we will force threat actors to adopt more time-consuming and expensive tactics, reducing the prevalence of attacks.

FIGURE 2. CISA Cybersecurity Strategic Plan Goals

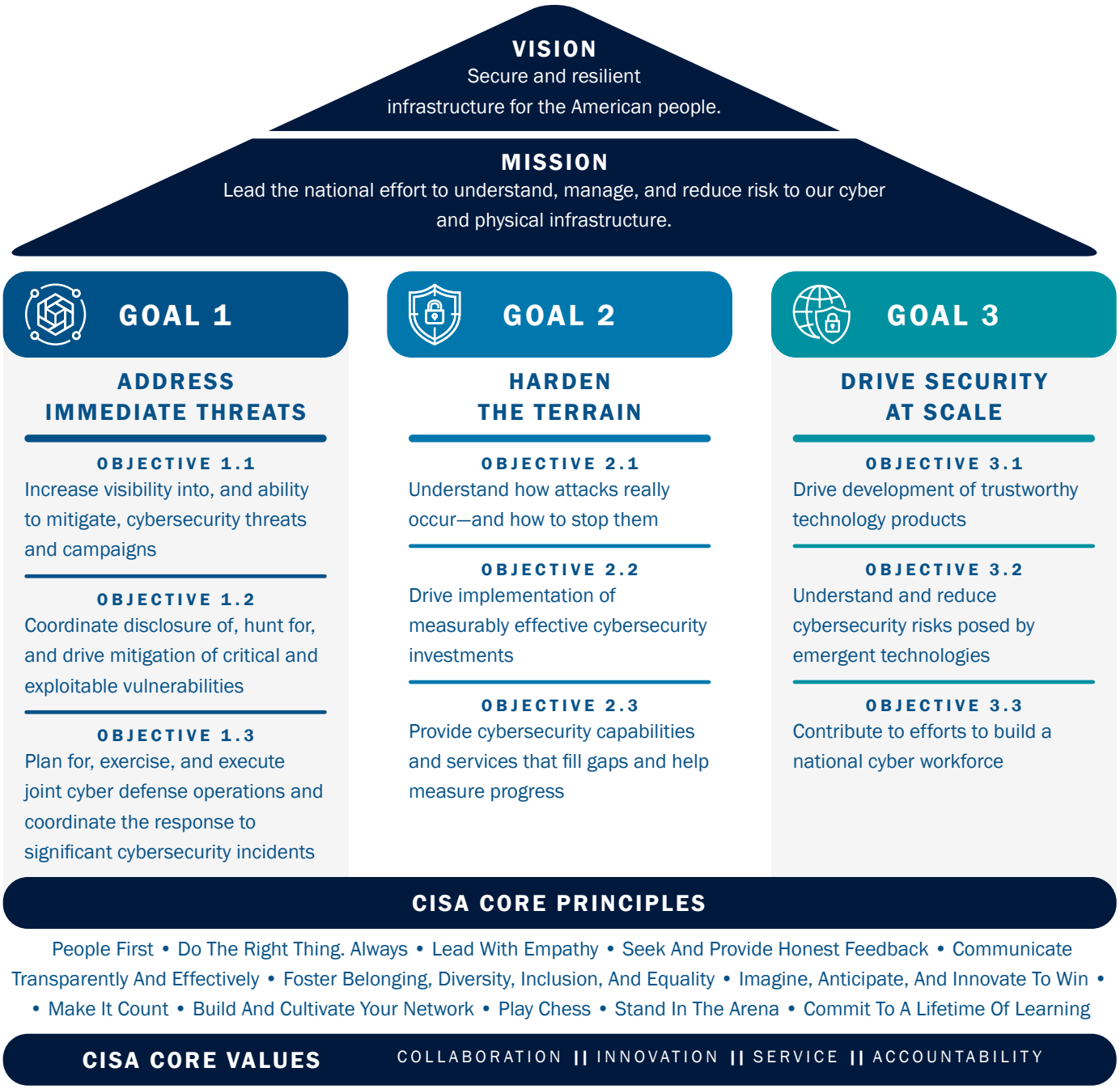


FIGURE 3. CISA Cybersecurity Strategic Plan Overview

To the contrary, our work to address immediate threats will enable us to prioritize investment in the security controls, measures, and capabilities that most effectively reduce risks. In turn, as we provide guidance and services that help organizations reduce their enterprise risk, we will be able to more clearly define the attributes of a safe and secure technology product. Finally, as we advance security across the product lifecycle, we will force threat actors to adopt more time-consuming and expensive tactics, reducing the prevalence of attacks. It is only through this virtuous cycle that we will make necessary progress.

GOAL 1

Address Immediate Threats

Today, it is too easy for malicious cyber actors to target American organizations. Our adversaries launch repeated campaigns against government agencies and critical infrastructure entities. Seemingly omnipresent vulnerabilities in widely used software and systems make these campaigns far too successful. In sum, too many American organizations are soft targets. To compound the challenge, we collectively lack visibility into the extent of adversary activity targeting our country. We must increase the costs borne by transgressors and increase friction for malicious activities by leading a national effort defined by speed and scale: when an adversary compromises an American network, they are rapidly detected and evicted before damage occurs; when an exploitable condition manifests, it is similarly detected and remediated before an intrusion takes place. No single organization can achieve this goal alone. We will lead a national effort toward collective defense, working shoulder-to-shoulder with federal government agencies, SLTT governments, the private sector, the security community, international allies, and others to make American networks a challenging and expensive target for our adversaries.

OBJECTIVE 1.1

Increase visibility into, and ability to mitigate, cybersecurity threats and campaigns

Today, our cybersecurity community, CISA included, lacks visibility of necessary breadth and depth into cybersecurity intrusions and adversary campaigns. We must achieve the ability to rapidly detect adversary activity and enable rapid eviction, denying malicious actors the persistent access they often seek, whether on-premises or in the cloud. We will achieve this visibility by all available means: through our own sensors and capabilities; by leveraging commercial and public data sources, and by partnering with the private sector, government agencies, and international allies. Our necessary gains in operational visibility must be underpinned by state-of-the-art tools, modern analytic infrastructure, trusted partnerships, and the world's best analytic workforce. All this data must be seamlessly integrated across CISA and rapidly shared in real-time in a machine-readable manner with government, private sector, and international partners to provide operators with accurate, actionable information—a vision we will execute leveraging the Joint Collaborative Environment. Working collaboratively with our partners, we must identify and mitigate threat campaigns before significant damage occurs.

ENABLING MEASURE

We will measure the breadth of our visibility into threat activity across critical infrastructure and government networks by building a coalition that leverages all available capabilities—our own and those of our partners.

MEASURE OF EFFECTIVENESS

We will use our increasing visibility to track progress in reducing the number and impact of incidents affecting critical infrastructure and government networks and the dwell time of our adversaries for each incident.

1 | Reduction in our time-to-detect adversary activity affecting federal agencies and critical infrastructure partners.

2 | Reduction in the time-to-remediation across each identified intrusion.

3 | Reduction in impact of incidents affecting CISA stakeholders.

OBJECTIVE 1.2

Coordinate disclosure of, hunt for, and drive mitigation of critical and exploitable vulnerabilities

Most intrusions today are perpetrated using known vulnerabilities or exploiting weak security controls. This makes life too easy for our adversaries. As a nation, we must urgently progress to a model in which pervasive vulnerabilities and security weaknesses in critical infrastructure and government networks are considered intolerable. While much progress in this area must be driven through deployment of technology that is safe and secure by design and default, we will also take near-term steps to reduce the prevalence of exploitable vulnerabilities by providing authoritative instruction on prioritized mitigations, hunting for exploitable vulnerabilities in domestic networks, and using all possible levers to widely publicize and drive remediation. We must gain a persistent understanding of vulnerabilities across our nation's critical infrastructure and government networks in order to enable more timely remediation before intrusions occur. We must also encourage, catalyze, and support the security research community and product security teams to ensure that vulnerabilities are discovered and fixed before adversaries can use them to cause harm. The uncoordinated or premature disclosure of significant vulnerabilities can lead to opportunities for easy exploitation by threat actors across all sectors of government and the economy. To this end, we will work closely with vendors, integrators, system owners, the security research community, and other key partners to incentivize identification and reporting of previously unknown vulnerabilities, enable timely and coordinated vulnerability disclosure, and drive mitigation before compromise occurs.

ENABLING MEASURE

1 | We will measure the breadth of our visibility into vulnerabilities, particularly those known to be exploited by adversaries, across critical infrastructure and government networks, whether through our own capabilities or that of our partners.

2 | We will increase trust and collaboration with the research community and the private sector by expanding participation in Coordinated Vulnerability Disclosure efforts.

MEASURE OF EFFECTIVENESS

1 | Reduction in the time-to-remediate Known Exploited Vulnerabilities across critical infrastructure and government networks.

2 | Increase in percentage of recommendations from CISA's vulnerability and risk assessments adopted by assessed organizations.

3 | Reduction in the number of vulnerabilities disclosed without appropriate coordination or provision of necessary mitigations.

OBJECTIVE 1.3

Plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents

No single organization can effectively manage, understand, and address the breadth of cyber incidents and threats facing our country. Through our Joint Cyber Defense Collaborative and our expanding regional teams, we will serve as an integrator and force multiplier, bringing together government, private sector, and international partners to measurably reduce cyber risk. We will invest in persistent collaboration defined by reciprocal expectations of transparency and value and minimizing friction to enable scale and data-driven analysis. We will develop, exercise, and execute cyber defense plans that enable effective responses to urgent threats while retaining focus on longer-term risks that require sustained investment. To

most effectively realize our collaboration and planning capabilities, we will update, exercise, execute, and maintain the National Cyber Incident Response Plan (NCIRP) to ensure that the breadth of our nation's capacity is effectively coordinated and leveraged in reducing the impact of cyber incidents. We will accelerate coordination with our government partners that maintain the ability to impose costs on our adversaries so that decisions to target American networks are met with appropriate consequences. Recognizing the borderless nature of cyber defense, we will maximize our role as America's Computer Emergency Response Team (CERT) to serve as an operational exemplar to the international community and forge a coalition of national cyber defense organizations to act in concert in protecting against shared threats.

ENABLING MEASURE

1 | We will expand the breadth and depth of our persistent collaboration model by increasing both the number of participating organizations and the operational value derived by each participant.

2 | We will increase the number of cyber defense plans and the alignment of each plan to high-priority risks identified by our public and private stakeholders.

MEASURE OF EFFECTIVENESS

1 | Increase in the volume of unique, timely, and relevant information shared by industry or government partners through our persistent collaboration channels.

2 | Increase in specific actions codified in cyber defense plans adopted by industry and government partners.

3 | Increase in post-incident after-action reports demonstrating that actions developed in cyber defense plans reduced negative outcomes.

GOAL 2

Harden the Terrain

Today, CISOs and cybersecurity professionals across the country are arguing for adoption of stronger controls, investment in modern technologies, and deprecation of legacy IT. Too often, CISOs are losing this argument, to the detriment of cybersecurity and, at times, national security. Starting with the federal civilian executive branch, we must shift the balance of risk management and security investment decisions across the country. We will achieve this change by providing clear, actionable guidance, by using all available levers to influence risk decisions of organizational leaders, by providing best-in-class services that help "target rich, resource poor" entities address gaps in their security programs, and by continuously measuring the state of American cybersecurity to understand areas for needed focus and investment, all informed by our understanding of the adversaries.

OBJECTIVE 2.1

Understand how attacks really occur—and how to stop them

Every organization has a finite cybersecurity budget, but the ways to expend such limited resources are nearly infinite. CISA must inform, guide, and drive adoption of the most impactful cybersecurity measures by first understanding how attacks occur—not just the initial access, but how the attacker exploited a web of unsafe technology products and inadequate security controls to achieve their objective. We will base this understanding on a variety of sources, including our own visibility into federal civilian executive branch systems, our partners' visibility into critical infrastructure systems, insights from the research community, and incident reporting—voluntary today and supplemented by mandatory reporting under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) in future years. We will focus on understanding how the success achieved by attackers differs by sector or organizational profile, and whether such differences are caused by factors such as a lack of resources, information, or expertise that CISA and our partners can help rectify. This knowledge is a prerequisite for us to proactively drive pro-security decisions and inform and justify security decisions made by all levels of government and across the private sector.

ENABLING MEASURE

We will develop a robust capacity to analyze information about cybersecurity intrusions and adversary adaptation, and derive insights into which security measures were, or could have been, most effective in limiting impact and harm.

MEASURE OF EFFECTIVENESS

Increase in the percentage of recommendations in CISA's guidance and directives that are directly based upon specific data showing how adversaries successfully execute intrusions and the most effective mitigations to stop them.

OBJECTIVE 2.2

Drive implementation of measurably effective cybersecurity investments

We must provide timely, accurate, actionable, and achievable guidance that helps organizations prioritize investment in controls and mitigations that address how attacks actually occur and how adversaries are evolving. For federal civilian executive branch agencies, we will fully exercise our directive authorities to drive toward a common security baseline and execute agency improvement plans to address tailored gaps. We will ensure that our guidance remains relevant in a changing technology environment, with particular focus on ensuring secure adoption of cloud computing resources. For organizations across the country, we will provide guidance that supports prudent investment, including machine-readable technical information by default. At the center of these efforts are the Cybersecurity Performance Goals (CPGs), which can help critical infrastructure and other entities make risk management decisions that achieve high-priority security outcomes and consider aggregate risk to the nation. We will work with a variety of partners across government and industry to promote adoption and take steps to align incentives that address constraints limiting further progress.

ENABLING MEASURE

We will develop guidance that is directly responsive to how intrusions occur and how adversaries are adapting, and that drives investment toward the most impactful security measures, including by regularly updating the Cross-Sector Cybersecurity Performance Goals, collaboratively developing Sector-Specific Cybersecurity Performance Goals, and leveraging our Binding Operational and Emergency Directives to drive urgent investment toward the most impactful measures.

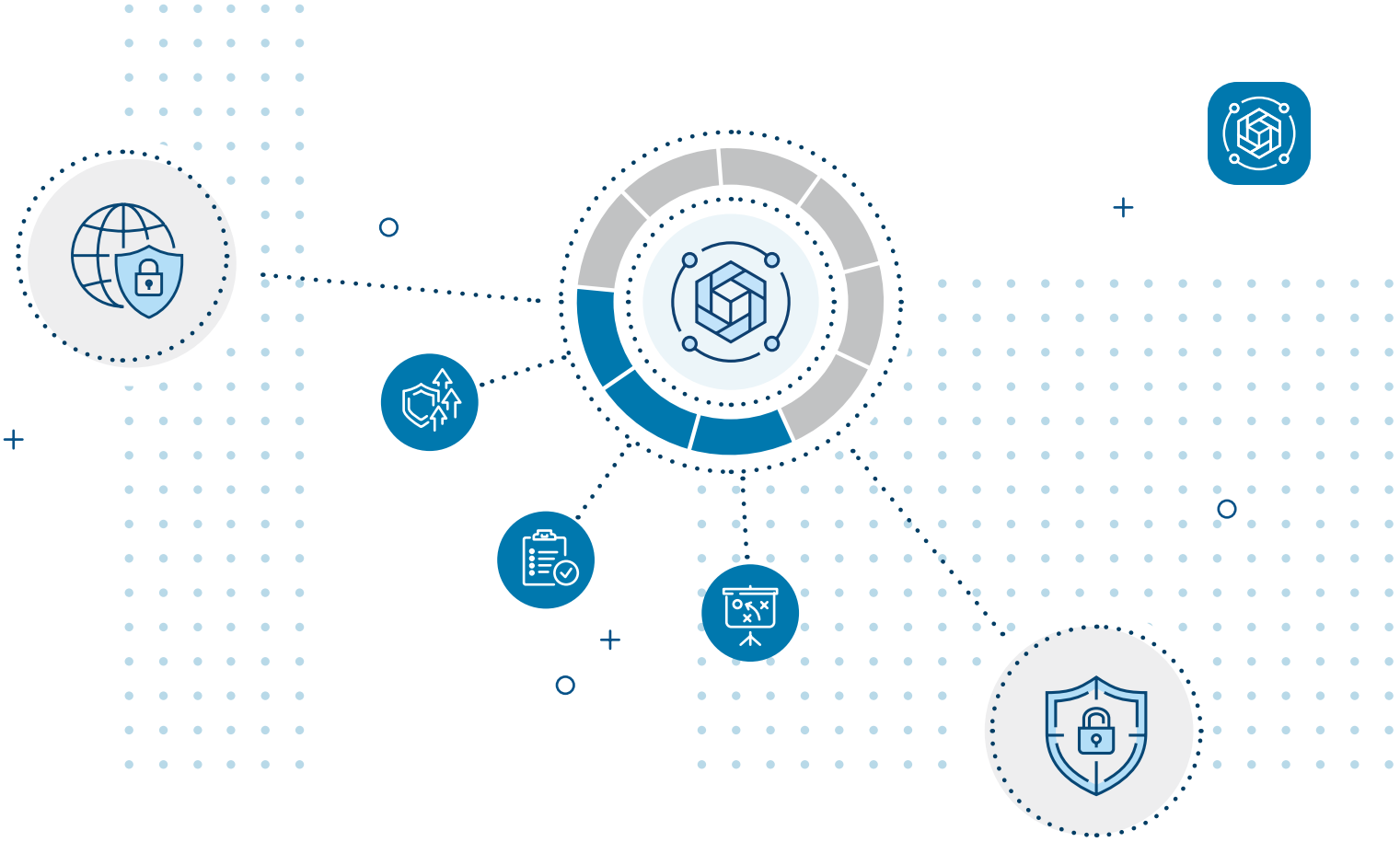
MEASURE OF EFFECTIVENESS

1 | Increase in the average number of Cybersecurity Performance Goals effectively adopted by organizations across each critical infrastructure sector.

2 | Where possible, reduction in confirmed impactful incidents in organizations that have adopted a higher number of Cybersecurity Performance Goals.

3 | Increase in the number of organizations outside of the FCEB that have adopted applicable requirements in CISA directives.

4 | Increase in the percentage of FCEB agency adoption of CISA directive requirements.



OBJECTIVE 2.3

Provide cybersecurity capabilities and services that fill gaps and help measure progress

Our nation benefits from a robust commercial market for cybersecurity capabilities and services, which CISA cannot and will not seek to supplant or duplicate. Instead, CISA will provide modern cybersecurity capabilities and services in three cases: (1) for federal civilian executive branch agencies, where our authorities and resources enable provision of centralized and shared services that offer necessary visibility, expedited risk reduction, and significant cost savings; (2) for target rich/resource poor organizations, where limited resources and sustained adversary interest provide a compelling justification for government assistance to the degree our authorities allow; and (3) to measure the state of American cybersecurity and associated trends, which is necessary to guide actionable and impactful information sharing, guidance, and direction.

In the first case, this will include continuing to expand and modernize the Continuous Diagnostics and Mitigation program, which now provides extraordinary visibility across nearly every federal civilian executive branch agency and enables host-level persistent hunting and response, and our Cybersecurity Shared Services Office, which provides a broadening portfolio of commercial services from Protective DNS Resolution to Vulnerability Disclosure Platforms. In the second case, we will provide cybersecurity assessments and, in cases where our authorities allow us, shared services that meet identified capability gaps and are

consumable by our partners, guiding target rich/resource poor entities to alternative providers when necessary, benefitting from relationships and scale offered by our regional teams. In the final category, we will leverage commercial Attack Surface Management and similar capabilities to both help our partners identify exploited or exploitable conditions and gain a better picture into security trends across the country. In all cases, our strong bias will be to leverage commercially-available tools and services; only when no viable capabilities exist in the commercial market will we consider developing an in-house capability. Our capabilities and services will be designed with scalability as a top priority, leveraging the breadth and capability of our regional cybersecurity workforce and focusing on delivering measurable value to every participating partner. These capabilities will be underpinned by modern analytic infrastructure, executed through our Cyber Analytics and Data System (CADS) for our own operators and expanding into the Joint Collaborative Environment (JCE) to incorporate data and analysis from our partners across government and the private sector.

ENABLING MEASURE

We will expand and modernize our cybersecurity capabilities and services to cover more partners and address a more complete set of risks.

MEASURE OF EFFECTIVENESS

We will define measures of effectiveness for every capability and service, to include:

1 | Protective DNS Service: Number of malicious domain requests blocked.

2 | Continuous Diagnostics and Mitigation: Percentage increase in agencies that have fully automated key vulnerability and asset management processes and can report advanced measurements such as time-to-remediate, scan frequency, and scan quality.

3 | Attack Surface Management: Percentage decrease in prevalence of, and time-to-remediate, vulnerabilities in all participating organizations and percentage increase in visibility across all sectors.

4 | Vulnerability Disclosure Platform: Increase in vulnerabilities identified via agency Vulnerability Disclosure Platforms prior to adversary exploitation.

5 | DotGov program: Increase in eligible organizations enrolled in DotGov.

6 | CyberSentry: Number of potential threats detected by the CyberSentry capability prior to identification by participating entity.

GOAL 3

Drive Security at Scale

As a society, we can no longer accept a model where every technology product is vulnerable the moment it is released and where the overwhelming burden for security lies with individual organizations and users. Technology should be designed, developed, and tested to minimize the number of exploitable flaws before they are introduced to the market. We must think about cybersecurity as a safety issue and ask more of the most capable and best-positioned actors in cyberspace—technology providers—to build security into products throughout their lifecycle, ship products with secure defaults, and foster radical transparency when known weaknesses are present in software, hardware, systems, and supply chains. Even as we confront the challenge of unsafe technology products, we must ensure that the future is more secure than the present—including by looking ahead to reduce the risks posed by adoption of artificial intelligence (AI) and the advance of quantum-relevant computing. Recognizing that a secure future is dependent first on our people, we will do our part to build a national cybersecurity workforce that reflects the diversity of our country.

OBJECTIVE 3.1

Drive development of trustworthy technology products

As noted in the National Cybersecurity Strategy, "poor software security greatly increases systemic risk across the digital ecosystem and leaves Americans bearing the ultimate cost." We will partner with like-minded organizations across government and industry to drive progress toward a world in which a technology product must be safe before it can be sold. We will focus first on defining what it means for a technology product to be safe and secure, collaboratively developing guidance and technical criteria to help customers choose safe products and manufacturers to deliver accordingly. Recognizing that technology manufacturers will need to prioritize areas for improvement, we will take a data-driven approach to identify those practices that drive down the most risk and address entire classes of attacks, such as using memory safe coding languages. We will take steps to advance transparency, including through adoption of Software Bills of Materials and rigorous vulnerability disclosure practices. Even as we maintain our voluntary, trust-based model of collaboration, we will strive to ensure that regulators and other government entities with compulsory authorities leverage technically sound and effective practices developed together with our partners across the private sector, ideally enabling harmonization across both U.S. and global regulatory regimes.

ENABLING MEASURE

We will produce and regularly update criteria and practices to develop and maintain products that are secure by design and default, and work with partners to assess the extent to which technology products adopt these clearly defined practices.

MEASURE OF EFFECTIVENESS

1 | Increase in the number of technology providers that have published detailed threat models, describing what the creators are trying to protect and from whom.

2 | Increase in the number of technology providers that have regularly and publicly attested to implementation of specific controls in the Secure Software Development Framework (SSDF).

3 | Increase in the number of technology providers that have published a commitment to ensure that product CVE entries are correct and complete.

4 | Increase in the number of technology providers that have published a secure-by-design roadmap, including how the provider is making changes to their software development processes, measuring defect rates, and setting goals for improvement, and transitioning to memory-safe programming languages.

5 | Increase in the number of technology providers that regularly publish security-relevant statistics and trends, such as MFA adoption, use of unsafe legacy protocols, and the percentage of customers using unsupported product versions.

OBJECTIVE 3.2

Understand and reduce cybersecurity risks posed by emergent technologies

The current technology environment poses of a variety of cybersecurity challenges: widespread use of products no longer supported by their vendor, complex network architectures that create gaps for adversaries, resource constrained organizations that are unable to deploy modern security controls. Even as we address these characteristics that challenge nearly every organization, we must recognize that the technology environment of the near future may present even great risks. While we collectively cannot predict the future technology environment with precision, we know that AI and cryptanalytically-relevant quantum computers (CRQCs) will fundamentally change aspects of how we secure our critical data and systems from cybersecurity threats. We will collaboratively work to ensure that our own work benefits from responsible use of emergent technologies, that we help the developers of emergent technologies protect their systems and data from malicious use, and that we help protect organizations from adversarial use of these technologies.

ENABLING MEASURE

We will provide guidance and support to help organizations understand, leverage, and reduce harms that accrue from malicious use of AI, CRQCs, and other emergent technologies.

MEASURE OF EFFECTIVENESS

Increase in the publication and adoption of guidance to:

1 | Help organizations safely use AI to advance cybersecurity.

2 | Protect AI systems from adversarial manipulation or abuse, building upon NIST's AI Risk Management Framework.

3 | Protect critical infrastructure organizations from adversarial AI systems.

4 | Publish evaluation of potential cryptographic vulnerabilities in critical infrastructure, particularly focused on ICS/OT systems.

5 | As verifiably quantum-safe products enter the market, increase in migration to quantum-safe cryptography by Systemically Important Entities and FCEB agencies.

OBJECTIVE 3.3

Contribute to efforts to build a national cyber workforce

Our nation remains challenged by intersecting gaps: a shortage of qualified candidates for many cybersecurity roles and a profound lack of diversity in the cybersecurity workforce. Addressing these gaps remains a challenge for cybersecurity teams across the country, in many ways posing a risk to national security. We will work closely with the Office of the National Cyber Director (ONCD) to implement a national cybersecurity workforce and education strategy. We will seek opportunities to bolster the national cyber and cyber-adjacent workforce—focusing both on ensuring the current cybersecurity workforce has the skills needed for a changing risk and threat environment and expanding the pipeline for the future workforce, from "K to Gray."

ENABLING MEASURE

We will invest in programs and initiatives in support of the National Cybersecurity Workforce Strategy that both support a current cybersecurity workforce that meets the challenges of today and helps build a deep and diverse workforce of tomorrow.

MEASURE OF EFFECTIVENESS

1 | Increase in the number of cybersecurity students trained in courses offered or funded by CISA.

2 | Increase in the percentage of cybersecurity courses offered or funded by CISA that target underrepresented populations.

3 | Increase in the number of organizations provided with training and resources to deliver cybersecurity training.

Conclusion

The next three years will set a new course for CISA and for national cybersecurity. It is a bold and expanded path, but this work is essential to a safe and secure cyberspace for all Americans. Given the untenable cyber risks our country, our businesses, and our communities face, we have no other choice. Together with our partners, we hope to look back on 2023 as the point when the trajectory of national cybersecurity risk began to change for the better.

Through the implementation of this strategy, we will first focus our efforts and energy to ensure our core cybersecurity functions are executed to the greatest effect. We must get the fundamentals right. We will optimize our cyber defense operations to identify, prevent, and address acute threats and vulnerabilities, and mitigate incidents more quickly. We will provide innovative shared services to directly address risks as well as actionable and practical guidance that helps defenders prioritize investments to address the most likely and impactful threats.

But we know this is not enough. We will drive progress toward a future where technology is purposely designed, built, tested, and maintained to significantly reduce the number of exploitable flaws before it is introduced to the market for broad use. We will take steps to shift the burden for security to those who can bear it.

And we will do to it together. The risks are severe and mounting, the hurdles are high. But they are surmountable. Through our shared efforts, we will shift the arc of national risk and create a safer future for generations to come.

Appendices

APPENDIX 1
Alignment with the CISA Strategic Plan

CISA STRATEGIC PLAN GOAL 1 **CYBER DEFENSE**	CISA CYBERSECURITY STRATEGIC PLAN OBJECTIVES
1.1. Enhance the ability of federal systems to withstand cyberattacks and incidents	**All Objectives**
1.2. Increase CISA's ability to actively detect cyber threats targeting America's critical infrastructure and critical networks	**1.1.** Increase visibility into, and ability to mitigate, cybersecurity threats and campaigns
1.3. Drive the disclosure and mitigation of critical cyber vulnerabilities	**1.2.** Coordinate disclosure of, hunt for, and drive mitigation of critical and exploitable vulnerabilities
1.4. Advance the cyberspace ecosystem to drive security-by-default	**3.1.** Drive development of trustworthy technology products
	3.2. Understand and reduce cybersecurity risks posed by emergent technologies
	3.3. Contribute to efforts to build a national cyber workforce
CISA STRATEGIC PLAN GOAL 2 **RISK REDUCTION AND RESILIENCE**	CISA CYBERSECURITY STRATEGIC PLAN OBJECTIVES
2.1. Expand visibility of risks to infrastructure, systems, and networks	**1.1.** Increase visibility into, and ability to mitigate, cybersecurity threats and campaigns
	2.1. Understand how attacks really occur—and how to stop them
2.2. Advance CISA's risk analytic capabilities and methodologies	**2.1.** Understand how attacks really occur—and how to stop them
2.3. Enhance CISA's security and risk mitigation guidance and impact	**1.1.** Increase visibility into, and ability to mitigate, cybersecurity threats and campaigns
	1.2. Coordinate disclosure of, hunt for, and drive mitigation of critical and exploitable vulnerabilities

APPENDIX 1

Cybersecurity Strategic Plan alignment

CISA STRATEGIC PLAN GOAL 2 **RISK REDUCTION AND RESILIENCE**	CISA CYBERSECURITY STRATEGIC PLAN OBJECTIVES
2.3. Enhance CISA's security and risk mitigation guidance and impact	**1.3.** Plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents
	2.2. Drive implementation of measurably effective cybersecurity investments
	2.3. Provide cybersecurity capabilities and services that fill gaps and help measure progress
	3.2. Understand and reduce cybersecurity risks posed by emergent technologies
2.4. Build greater stakeholder capacity in infrastructure and network security and resilience	**2.3.** Provide cybersecurity capabilities and services that fill gaps and help measure progress
2.5. Increase CISA's ability to respond to threats and incidents	**1.1.** Increase visibility into, and ability to mitigate, cybersecurity threats and campaigns
	1.3. Plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents
2.6. Support risk management activities for election infrastructure	**All Objectives**
CISA STRATEGIC PLAN GOAL 3 **OPERATIONAL COLLABORATION**	CISA CYBERSECURITY STRATEGIC PLAN OBJECTIVES
3.1. Optimize collaborative planning and implementation of stakeholder engagements and partnership activities	**1.3.** Plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents
3.2. Fully integrate regional offices into CISA's operational coordination	**1.3.** Plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents
	2.3. Provide cybersecurity capabilities and services that fill gaps and help measure progress
3.3. Streamline stakeholder access to and use of appropriate CISA programs, products, and services	**1.3.** Plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents

APPENDIX 1

Cybersecurity Strategic Plan alignment

CISA STRATEGIC PLAN GOAL 3 **OPERATIONAL COLLABORATION**	CISA CYBERSECURITY STRATEGIC PLAN OBJECTIVES
3.3. Streamline stakeholder access to and use of appropriate CISA programs, products, and services	**2.3.** Provide cybersecurity capabilities and services that fill gaps and help measure progress
3.4. Enhance information sharing with CISA's partnership base	**1.1.** Increase visibility into, and ability to mitigate, cybersecurity threats and campaigns
	1.2. Coordinate disclosure of, hunt for, and drive mitigation of critical and exploitable vulnerabilities
	1.3. Plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents
	2.1. Understand how attacks really occur—and how to stop them
	2.2. Drive implementation of measurably effective cybersecurity investments
3.5. Increase integration of stakeholder insights to inform CISA product development and mission delivery	**1.3.** Plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents
	2.3. Provide cybersecurity capabilities and services that fill gaps and help measure progress
CISA STRATEGIC PLAN GOAL 4 **AGENCY UNIFICATION**	CISA CYBERSECURITY STRATEGIC PLAN OBJECTIVES
4.1. Strengthen and integrate CISA governance, management, and prioritization	N/A
4.2. Optimize CISA business operations to be mutually supportive across all divisions	N/A
4.3. Cultivate and grow CISA's high-performing workforce	N/A
4.4. Advance CISA's culture of excellence	N/A

APPENDIX 2

Alignment with the National Cybersecurity Strategy

NATIONAL CYBERSECURITY STRATEGY PILLAR ONE | **DEFEND CRITICAL INFRASTRUCTURE**	CISA CYBERSECURITY STRATEGIC PLAN OBJECTIVES
1.1. Establish cybersecurity requirements to support national security and public safety	**2.1.** Understand how attacks really occur—and how to stop them
	2.2. Drive implementation of measurably effective cybersecurity investments
	2.3. Provide cybersecurity capabilities and services that fill gaps and help measure progress
	3.3. Contribute to efforts to build a national cyber workforce
1.2. Scale public-private collaboration	**1.1.** Increase visibility into, and ability to mitigate, cybersecurity threats and campaigns
	1.2. Coordinate disclosure of, hunt for, and drive mitigation of critical and exploitable vulnerabilities
	1.3. Plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents
1.3. Integrate federal cybersecurity centers	**1.3.** Plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents
1.4. Update federal incident response plans and processes	**1.3.** Plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents
1.5. Modernize federal defenses	**All Objectives**

Alignment with the National Cybersecurity Strategy

NATIONAL CYBERSECURITY STRATEGY PILLAR TWO | **DISRUPT AND DISMANTLE THREAT ACTORS**	CISA CYBERSECURITY STRATEGIC PLAN OBJECTIVES
2.1. Integrate federal disruption activities	**1.1.** Increase visibility into, and ability to mitigate, cybersecurity threats and campaigns
	1.3. Plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents
2.2. Enhance public-private operational collaboration to disrupt adversaries	**1.1.** Increase visibility into, and ability to mitigate, cybersecurity threats and campaigns
	1.3. Plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents
2.3. Increase the speed and scale of intelligence sharing and victim notification	**1.3.** Plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents
2.4. Prevent abuse of U.S.-based infrastructure	**1.3.** Plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents
2.5. Counter cybercrime, defeat ransomware	**All Objectives**
NATIONAL CYBERSECURITY STRATEGY PILLAR THREE | **SHAPE MARKET FORCES TO DRIVE SECURITY AND RESILIENCE**	CISA CYBERSECURITY STRATEGIC PLAN OBJECTIVES
3.1. Hold the stewards of our data accountable	N/A
3.2. Drive the development of secure internet of things devices	**3.1.** Drive development of trustworthy technology products
3.3. Shift liability for insecure software products and services	**1.2.** Coordinate disclosure of, hunt for, and drive mitigation of critical and exploitable vulnerabilities
	3.1. Drive development of trustworthy technology products

Alignment with the National Cybersecurity Strategy

NATIONAL CYBERSECURITY STRATEGY PILLAR THREE | **SHAPE MARKET FORCES TO DRIVE SECURITY AND RESILIENCE**	CISA CYBERSECURITY STRATEGIC PLAN OBJECTIVES
3.4. Use federal grants and other incentives to build in security	**2.1.** Understand how attacks really occur—and how to stop them
	2.2. Drive implementation of measurably effective cybersecurity investments
	2.3. Provide cybersecurity capabilities and services that fill gaps and help measure progress
	3.3. Contribute to efforts to build a national cyber workforce
3.5. Leverage federal procurement to improve accountability	**2.1.** Understand how attacks really occur—and how to stop them
	2.2. Drive implementation of measurably effective cybersecurity investments
	3.1. Drive development of trustworthy technology products
3.6. Explore a federal cyber insurance backstop	**2.1.** Understand how attacks really occur—and how to stop them
	2.2. Drive implementation of measurably effective cybersecurity investments
NATIONAL CYBERSECURITY STRATEGY PILLAR FOUR | **INVEST IN A RESILIENT FUTURE**	CISA CYBERSECURITY STRATEGIC PLAN OBJECTIVES
4.1. Secure the technical foundation of the internet	**1.3.** Plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents
	2.2. Drive implementation of measurably effective cybersecurity investments
	3.1. Drive development of trustworthy technology products
	3.2. Understand and reduce cybersecurity risks posed by emergent technologies

Alignment with the National Cybersecurity Strategy

NATIONAL CYBERSECURITY STRATEGY PILLAR FOUR | **INVEST IN A RESILIENT FUTURE**	CISA CYBERSECURITY STRATEGIC PLAN OBJECTIVES
4.2. Reinvigorate federal research and development for cybersecurity	**1.1.** Increase visibility into, and ability to mitigate, cybersecurity threats and campaigns
	1.2. Coordinate disclosure of, hunt for, and drive mitigation of critical and exploitable vulnerabilities
	1.3. Plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents
	2.2. Drive implementation of measurably effective cybersecurity investments
	3.1. Drive development of trustworthy technology products
	3.2. Understand and reduce cybersecurity risks posed by emergent technologies
4.3. Prepare for our post-quantum future	**2.2.** Drive implementation of measurably effective cybersecurity investments
	3.2. Understand and reduce cybersecurity risks posed by emergent technologies
4.4. Secure our clean energy future	**1.3.** Plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents
	2.2. Drive implementation of measurably effective cybersecurity investments
	3.1. Drive development of trustworthy technology products
4.5. Support development of a digital identity ecosystem	**3.1.** Drive development of trustworthy technology products
4.6. Develop a national strategy to strengthen our cyber workforce	**3.3.** Contribute to efforts to build a national cyber workforce

Alignment with the National Cybersecurity Strategy

NATIONAL CYBERSECURITY STRATEGY PILLAR FIVE | **FORGE INTERNATIONAL PARTNERSHIPS TO PURSUE SHARED GOALS**	CISA CYBERSECURITY STRATEGIC PLAN OBJECTIVES
5.1. Build Coalitions to Counter Threats to Our Digital Ecosystem	**1.3.** Plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents
5.2. Strengthen International Partner Capacity	**1.3.** Plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents
5.3. Expand U.S. Ability to Assist Allies and Partners	**1.3.** Plan for, exercise, and execute joint cyber defense operations and coordinate the response to significant cybersecurity incidents
5.4. Build Coalitions to Reinforce Global Norms of Responsible State Behavior	N/A
5.5. Secure Global Supply Chains for Information, Communications, and Operational Technology Products and Services	**3.1.** Drive development of trustworthy technology products

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

CISA | CYBERSECURITY STRATEGIC PLAN FY2024–2026

ONE CISA: COLLABORATION, INNOVATION, SERVICE, ACCOUNTABILITY