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.