



CISA 2030:
**DEFEND
HARDEN
PREVAIL**



OCTOBER 2026

TABLE OF CONTENTS

Foreword from DHS Secretary Markwayne Mullin	1
Welcome from CISA Acting Director Nick Andersen	3
Introduction	4
Pillar 1: DEFEND - Lead National Cyber Defense	5
Pillar 2: HARDEN - Prioritize National Infrastructure Security	6
Pillar 3: PREVAIL - Mobilize National Resilience	7
The Path Forward	8



SECRETARY
MARKWAYNE MULLIN

FOREWORD

250 years ago, Americans came together to fight for their way of life and to form a great new nation. In doing so, they faced and overcame challenges and hardships building off shared values and a desire for independence. Every day we face new challenges and threats to the homeland.

These new and evolving threats are stealthy. They prey on the critical infrastructure systems and networks that keep every aspect of our modern society secure and thriving, striking people at their most vulnerable moments and attempting to disrupt systems that we all rely on every day.

While many overlook the vital role America's critical infrastructure plays, it is fundamentally essential to the nation's security, public safety, and economy. It's often only when something goes wrong that we really appreciate what we have. Our great nation, the United States of America, cannot, and will not, allow unchecked access to the nation's critical infrastructure.

President Trump understood this when he created the Cybersecurity and Infrastructure Security Agency (CISA) as part of the Department of Homeland Security (DHS) in 2018. He charged CISA to bring together the nation's critical infrastructure and coordinate the security and resilience of the sectors that are so critical to national and economic security—failure was simply not an option.

Since the start of the President's second term, DHS has recommitted to protecting America's core services and infrastructure through CISA. This commitment is embodied in *CISA 2030: Defend, Harden, Prevail*.

As we mark America's 250th anniversary, the Department of Homeland Security stands resolute in its mission to protect the nation and uphold the values that define our country and the President's agenda. *CISA 2030: Defend, Harden, Prevail* serves as a call to action for every American to honor the courage of those who came before us and protect our way of life for those who will come after. We must unite at every level in defense of our shared future: federal, state, local, tribal, and territorial government, and owners and operators of businesses and critical infrastructure. Securing America for the next 250 years requires us to act decisively and embrace resilience as a fundamental American value. It's time to answer the call of history, standing shoulder to shoulder to keep America safe, strong, and free.

MARKWAYNE MULLIN

SECRETARY
DEPARTMENT OF HOMELAND SECURITY

This page intentionally left blank.



WELCOME

In his Foreword, Secretary Markwayne Mullin laid out the vision for a secure America. He urges each of us to take our place in history and unite in defense of our shared future. I, too, share this vision, and it is my privilege to carry it forward with purpose and speed.

The threat landscape we face today is not static. Nation-state actors and other malicious adversaries continue to grow more sophisticated in their efforts to compromise our networks, and there is no guarantee that a strong defense will eliminate intrusions. As President Trump has reminded us, resilience must be the foundation of our approach. We must ensure that when adversaries gain a foothold, we are prepared to detect them quickly, evict them decisively, and keep critical operations running without interruption.

This strategy reflects that reality. It commits CISA to strengthening the security of both the physical and cyber dimensions of our critical infrastructure, recognizing that the two can no longer be treated as separate domains. To execute President Trump's Cyber Strategy for America (March 2026) and Executive Order 14239, CISA will transition from passive defense to an aggressive, anticipatory stance that actively eliminates adversarial footholds in defense-critical infrastructure prior to weaponization against our systems. It also reaffirms CISA's role, as delegated by the Department, in leading the initiation and restoration of National Security and Emergency Preparedness communications — a responsibility that is essential to maintaining continuity of government and public safety during crises.

CISA 2030: Defend, Harden, Prevail is guided by three pillars to scope the agency's work where it will make the most impact:

- **DEFEND - Lead National Cyber Defense.** CISA must take up its cyber defense mission with renewed purpose, working with partners and setting conditions for decisive decision making when every moment counts.
- **HARDEN - Prioritize National Infrastructure Security.** CISA must focus sharply and ruthlessly prioritize our efforts in response to the threats that pose the highest risks and highest consequences.
- **PREVAIL - Mobilize National Resilience.** To counter and stay ahead of threats evolving at the speed of technology, CISA must be agile, scalable, and collaborative, partnering with and integrating the expertise of those who are on the front lines.

I call on everyone to do their civic duty and take every step necessary to deny our adversaries a single foothold or advantage that would impact our national security, prosperity, and way of life.

A handwritten signature in blue ink, reading "Nick Andersen".

NICK ANDERSEN

DIRECTOR (A)

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

INTRODUCTION

Today, as the United States enters a new era of technological innovation and economic growth, the Cybersecurity and Infrastructure Security Agency (CISA) stands at a crossroad in its cybersecurity and critical infrastructure mission. America's critical infrastructure—and the owners and operators who maintain it—is the backbone of U.S. economic strength, technological and manufacturing dominance, and national defense. Yet, our nation is faced with an increasingly complex environment, where compounding cyber, physical, and geopolitical threats increase the consequences of disruption across our most essential services. Our adversaries have, and will continue to, target our critical infrastructure with the aim of persistent access that can later be used to compromise vital systems when we need them the most.

U.S. competitiveness, national resilience, and the ability to deny our adversaries, require fundamentally changing how we operate as an agency. Eight years after its founding, the shifting scope of CISA's mission and unclear prioritization have come at the expense of the focus and agility required to respond to a dynamic and evolving threat landscape. We must transform our operational model to advance collective cyber defense, harden infrastructure most essential to our national and economic security, and mobilize our partnerships to strengthen collective resilience.

CISA 2030: Defend, Harden, Prevail is the roadmap to advance President Trump's *Cyber Strategy for America* and the *National Resilience Strategy*, and focus our mission for the American people.



PILLAR

DEFEND

LEAD
NATIONAL
CYBER DEFENSE

1

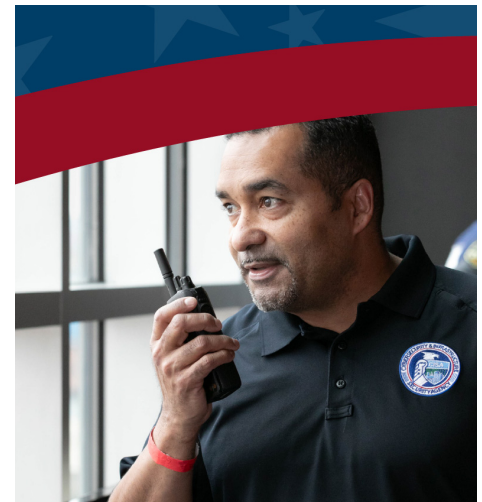


PILLAR

HARDEN

PRIORITIZE NATIONAL
INFRASTRUCTURE
SECURITY

2



PILLAR

PREVAIL

MOBILIZE
NATIONAL
RESILIENCE

3



DEFEND

LEAD NATIONAL CYBER DEFENSE

THE CYBER THREAT LANDSCAPE IS MORE COMPLEX AND INTERCONNECTED.

While advances in technology create opportunities for an enhanced cyber defense posture, technology is also expanding the attack surface—amplifying and accelerating cyber risks. The consequences of disruption are increasing, as our nation's critical infrastructure owners and operators face constant malicious threats and attacks from nation-state cyber threat actors and their criminal proxies. Our adversaries will continue to develop and deploy advanced capabilities, and we must work with partners to detect, disrupt, and mitigate cyber threats while helping rapidly remove adversaries from compromised systems.

We will lead our national cyber defense by working with partners to build confidence in the integrity of information security systems, the data those systems secure, the networks that carry it, and the infrastructure that enables it. As the operational lead for federal cybersecurity, we will set the conditions for decisive government action, direct defensive cybersecurity engagement with the public and private sectors, and unify our national cyber defenses in a way that shapes security outcomes faster than our adversaries can adapt and act. We will lead national level analysis and coordination to secure transformative technologies—such as super intelligence and quantum computing—that will revolutionize the way Americans live and work.

KEY OBJECTIVES

FORGE COLLECTIVE CYBER DEFENSE

CISA will integrate cyber defense capabilities of government, industry, State, Local, Tribal, and Territorial (SLTT) partners, and international organizations to improve understanding of threat activity, reduce national cyber risk and strengthen cyber defenses.

STRENGTHEN THE SECURITY AND RESILIENCE OF OPERATIONAL TECHNOLOGY (OT)

CISA will work alongside critical infrastructure owners and operators to modernize OT environments, improve asset visibility and anomaly detection, and assure OT supply chain integrity.

POSITION SOFTWARE SECURITY AS A STRATEGIC ADVANTAGE

The defense and operational continuity of our nation's most critical systems and assets depend on software that is secure, can withstand compromise, and recover rapidly. CISA will coordinate with partners to develop data-driven guidance and best practices to drive software security and supply chain transparency.

SECURE AMERICA'S TECHNOLOGY ECOSYSTEM

CISA will lead the assessment and rapid deployment of emerging technology that accelerates our collective cyber defense and ensures continuity of communications. We will partner across industry and government to secure innovative technologies that advance critical infrastructure operations, and work with owners and operators to ensure they are resilient against the threats these technologies pose.



HARDEN

PRIORITIZE NATIONAL INFRASTRUCTURE SECURITY

THE PROTECTION OF AMERICAN CRITICAL INFRASTRUCTURE IS A NATIONAL SECURITY AND ECONOMIC IMPERATIVE.

Our nation is built on and powered by millions of interconnected systems and assets that provide essential services such as energy, water, transportation, and telecommunications. We will build capacity across the critical infrastructure community by establishing frameworks that help Sector Risk Management Agencies (SRMA), owners and operators, as well as SLTT partners focus resources where they will have the greatest impact.

We will invest in intelligence-driven approaches that can be operationalized through intentional, coordinated action with, and by, our partners. We will deprioritize threat-agnostic, all-hazards approaches and embrace risk-informed, consequence-based analysis to focus attention, investment, and operational effort on the infrastructure whose disruption would have the greatest impact on public health and safety, continuity of the economy, and national security. We will make deliberate choices to prioritize and harden the nation's infrastructure whose disruption would have the most severe consequences.

KEY OBJECTIVES

INTEGRATE INTELLIGENCE ACROSS CRITICAL INFRASTRUCTURE SECURITY OPERATIONS

CISA will coordinate with the Intelligence Community, industry, and government agencies to mature our intelligence-to-operations pipeline. This requires targeted investments in modernized tools and technologies to improve cyber defense, enable real-time decision making and alerts, and accelerate operational response across the critical infrastructure community.

ENABLE RISK-INFORMED PRIORITIZATION

CISA will maintain and analyze infrastructure data to perform prioritization that ensures resources have the greatest possible impact on the security of our national infrastructure. CISA will support the White House in developing the National Risk Register and other prioritization efforts that articulate and quantify risk to our national infrastructure, related systems, and its users.

PARTNER FOR OPERATIONAL IMPACT

CISA will leverage intentional, action-oriented partnerships to advance meaningful and measurable security improvements across the critical infrastructure community. CISA will build distributed collaboration frameworks that empower and enable SRMAs, regions, states, communities, and owners and operators to advance infrastructure security through localized action.

FORTIFY THE NATION'S MOST IMPORTANT INFRASTRUCTURE

CISA will work alongside the critical infrastructure community and other key partners to strengthen infrastructure's ability to withstand malicious cyber activity so that essential services continue running for the American people.



PREVAIL

MOBILIZE NATIONAL RESILIENCE

DEFENDING OUR NATION FROM CYBER AND PHYSICAL ATTACKS TO CRITICAL INFRASTRUCTURE REQUIRES A MORE AGILE, COLLABORATIVE, AND DISTRIBUTED APPROACH, GROUNDED IN TRUSTED PARTNERSHIPS AND INFORMED BY LOCAL EXPERTISE.

As critical infrastructure risks evolve, and threats become faster, more technical, and more asymmetric, the U.S. requires a new operational model—one built for speed, adaptability, and shared responsibility. Our ability to defeat our adversaries cannot be constrained by decades-old technologies, processes, and functions. National critical infrastructure resilience can no longer be defined simply by how we respond to disruption, but by the model we build to withstand it.

We will transform capabilities, simplify core services, and develop cutting-edge technology solutions that accelerate our ability to quickly mobilize national resilience in the face of systemic disruption. We will strengthen continuity of operations through coordinated planning efforts. We will forge stronger and more distributed public-private partnerships that drive smart security investments, modern solutions, and collective action.

KEY OBJECTIVES

ADVANCE SECURE AND RESILIENT REGIONAL CAPABILITIES

CISA will equip its advisors to be the cyber and physical security workforce of today and tomorrow. CISA will invest in the security and resilience of our nation's critical infrastructure communities with tools calibrated to national cyber defense and the prioritization of national infrastructure security. CISA will build capacity through our ten regional offices to enable rapid mobilization against a persistent threat landscape.

STRENGTHEN NATIONWIDE INTEROPERABILITY AND CONTINUITY OF NATIONAL SECURITY/EMERGENCY PREPAREDNESS (NS/EP) COMMUNICATIONS

CISA will strengthen interoperability nationwide by providing priority voice, video, data, and information services to ensure continuity of communications. CISA will expand priority telecommunications services utilizing next-generation capabilities, including 5G/6G and commercial satellite constellations, to ensure resilient and redundant emergency connectivity.

MODERNIZE PLANNING AND EXERCISE CAPABILITIES

CISA will leverage advanced analytics, emerging technologies, intelligence, and cross-sector collaboration to continuously assess readiness, develop actionable joint planning efforts, improve mission continuity, and strengthen the foundation of our national resilience.

BUILD NEXT-GENERATION, INTEROPERABLE INFRASTRUCTURE

CISA will accelerate collective defense by investing in scalable, encrypted, and resilient infrastructure that enables integrated operation, protects emergency communications, and ensures continuity of essential functions in the event of disruption.



THE PATH FORWARD:

WE WILL DELIVER ON OUR PROMISE TO THE AMERICAN PEOPLE TO PROTECT THE NATION'S CRITICAL INFRASTRUCTURE AND LEAD NATIONAL CYBER DEFENSE. WE WILL FOCUS OUR ORGANIZATION, PEOPLE, AND TECHNOLOGY TO MEET THE DEMANDS OF TODAY AND THE THREATS OF TOMORROW.

WITHIN

60 days

CISA will

begin a programmatic review that will focus on our core services and capabilities to achieve our key objectives.

WITHIN

180 days

CISA will

deliver an approach for implementation and measurement of outcomes aligned to our guiding pillars and key objectives.

WITHIN

365 days

CISA will

deliver an update on its progress against implementation.

This page intentionally left blank.

CISA 2030:

**DEFEND
HARDEN
PREVAIL**

