CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

STRATEGIC INTENT

"DEFEND TODAY,
SECURE TOMORROW"

CISA
CYBER+INFRASTRUCTURE

AUGUST 2019

Table of Contents:

Message FROM THE Director

> **AMERICA'S RESPONSE TO THE CHALLENGES AND OPPORTUNITIES OF THE CYBER ERA WILL DETERMINE OUR FUTURE PROSPERITY AND SECURITY.**
>
> National Security Strategy of the United States of America, December 2017

There are moments in the history of our Nation when Congress and the President deem it necessary to create a new executive agency to serve the American people. The establishment of the Department of Homeland Security itself was one of these moments. Sixteen years later, we recognized that there must be a single organization to lead efforts to build national resilience. Today, that new agency is the Cybersecurity and Infrastructure Security Agency, the Nation's Risk Advisor.

CISA is necessary because the twenty-first century brings with it an array of challenges that are often difficult to grasp and even more difficult to address. We immediately think of our reliance on networked technologies, or perhaps our interdependent supply chain, as significant risk factors—how well do we really know the things we're relying on and do we understand what happens when we lose them? Making matters more complicated, it's not just human-driven threats; we must also plan and prepare for Mother Nature, as well as for the fact that sometimes technology just fails and bad things happen as a result.

In no arena is this framing of the CISA mission more relevant than our election security work. The CISA team engaged in the defense of the 2018 elections across every organizational division, working with all 50 states and across the Federal Government. Our focused efforts to defend democracy clearly demonstrate that CISA is capable of surging to confront emerging threats and support our partners, wherever and whomever they may be.

Meeting their Constitutional duties to provide for the common defense, Congress and the Administration established CISA, an agency to lead the national effort to protect our critical infrastructure. An agency to bring to bear all of the instruments of national power in this endeavor. Where there may be a lack of leadership, CISA will step up. Where there may be a lack in national capability, CISA will provide. Through partnership and cooperative defense, as an ally to the national values of civil liberties and prosperity, we will protect the American way of life.

This document is the keystone for our new agency. I call on the entire CISA workforce and all of our partners to bring this vision into being. Let's stand side-by-side as we defend the homeland. Let's work together to secure tomorrow. Join me as we make history.

Christopher Krebs
Director

INTRODUCTION

This document lays out the strategic vision and operational priorities of the CISA Director. It provides a general approach for how we execute our responsibilities and serves as a reference point for our employees and partners to guide our work and create unity of effort. It aims to position us to successfully meet our mission in the coming years and decades. It serves as the interim strategy as we develop a longer-term strategic plan.

The common framework of goals and outcomes helps organize our mission execution and inform management decisions—including operations planning, requirements generation, budget formulation, and performance management. These are high-level outcomes that we will constantly seek to achieve; specific actions and milestones will appear in operational and organizational plans. These goals and outcomes give us a constant foundation for capability and direction as threats and the mission space dramatically evolve.

CISA AT A GLANCE

WE ARE THE NATION'S RISK ADVISORS

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure.

WHO WE ARE

CISA works with partners across government and industry to defend against today's threats and collaborates to build more secure and resilient infrastructure for the future.

- PARTNERSHIP DEVELOPMENT
- INFORMATION AND DATA SHARING
- CAPACITY BUILDING
- INCIDENT MANAGEMENT & RESPONSE
- RISK ASSESSMENT AND ANALYSIS
- NETWORK DEFENSE
- EMERGENCY COMMUNICATIONS

STRATEGIC CONTEXT

In today's globally interconnected world, our critical infrastructure and American way of life face a wide array of serious risks. Nation-state adversaries and competitors seek to advance their objectives through a variety of hybrid tactics, including subtle actions that significantly weaken the foundations of U.S. power, degrade society's functions, and increase adversaries' ability to hold our critical infrastructure at risk. Extreme weather events and other natural hazards seem ever-present in today's headlines. All the while, the heightened threat from terrorism and violent crime remains. It is increasingly local and often aimed at soft targets like malls, theaters, stadiums, and schools.

The critical functions within our society are "systems of systems" with complex interdependencies and systemic risks that can have cascading effects during all types of incidents. As networked devices further weave into our lives and businesses, their vulnerabilities provide additional attack vectors for nation states and criminals. Global supply chains introduce the risks of malicious activity in software and hardware, disruptions from physical attacks or natural events, and manipulation for political and economic purposes. Aging, outdated, and under-resourced infrastructures are a challenge across the country. During any emergency, communication between first responders and between decision-makers is at risk from disruption or lack of interoperability.

Many of these risks are complex, dispersed both geographically and across a variety of stakeholders, and challenging to understand and address. This is where CISA fits in as a central coordinator of analysis, planning, and response, especially in areas where there is no other designated Federal Government leader.

MISSION, VISION, & APPROACH

MISSION: Lead the national effort to understand and manage cyber and physical risk to our critical infrastructure.

VISION: Secure and resilient critical infrastructure for the American people.

GUIDING PRINCIPLES

The following core principles must be built into everything we do. Each principle is essential to achieving the vision of CISA and building the culture within which the agency will thrive.

1 LEADERSHIP AND COLLABORATION.

Many of the risks we face today came about precisely because so many entities had a stake in the problem set, yet no single one had ultimate responsibility. CISA's leadership is one of our primary benefits to stakeholders and the Nation. Without successful collaboration with our partners, we cannot achieve our mission. Our approach will drive conversation about the problem and potential solutions and will require new models of partnership. We will be humble, we will listen, and we will solve problems together. In many cases, we will "lead, follow, or get out of the way."

2 RISK-PRIORITIZATION.

The foremost responsibility of CISA is to safeguard the American people and we prioritize our efforts at all levels to focus on the greatest threats and vulnerabilities facing the homeland. We will organize our risk management efforts around securing the national critical functions that underpin national security, economic security, public health and safety, and government continuity of operations. Our efforts must be data-driven, threat-informed, and validated by our stakeholders.

3 RESULTS-ORIENTED.

We must focus our efforts on having the greatest impact for the investment made. Our services must demonstrably reduce risk, respond to requirements put forward by our partners, and work toward defined common outcomes. We will leverage, rather than duplicate, services offered by the private sector and other agencies. Our solutions must be innovative, agile, and responsive to the evolving threat. Wherever possible, our solutions should be highly scalable, where the benefits far outweigh the costs.

4 RESPECT FOR NATIONAL VALUES.

Our work to protect national critical functions must reflect their ultimate purpose of enabling an open and prosperous society. Security is not an end unto itself, and efforts to mitigate risks must be appropriately balanced with civil liberties, free expression, commerce, and innovation. We are an ally to civil society and we must uphold privacy, civil rights, and civil liberties in accordance with applicable law and policy. We are partners in commerce and innovation and must find ways to play a productive role.

5 UNIFIED MISSION AND AGENCY.

We are one mission and one agency. We fundamentally focus on risk management, however it presents itself—cyber, physical, human factors, or supply-chain. Through our transformation, we will execute our mission in a coordinated, cross-agency manner that uses the right mix of capabilities tailored to the task at hand. We will ensure strong regional service delivery that is fully integrated with headquarters operations. We will ensure the right team for the right mission through maximizing our hiring flexibilities and incentivizing commitment to the mission and innovation to address the complex problems we face.

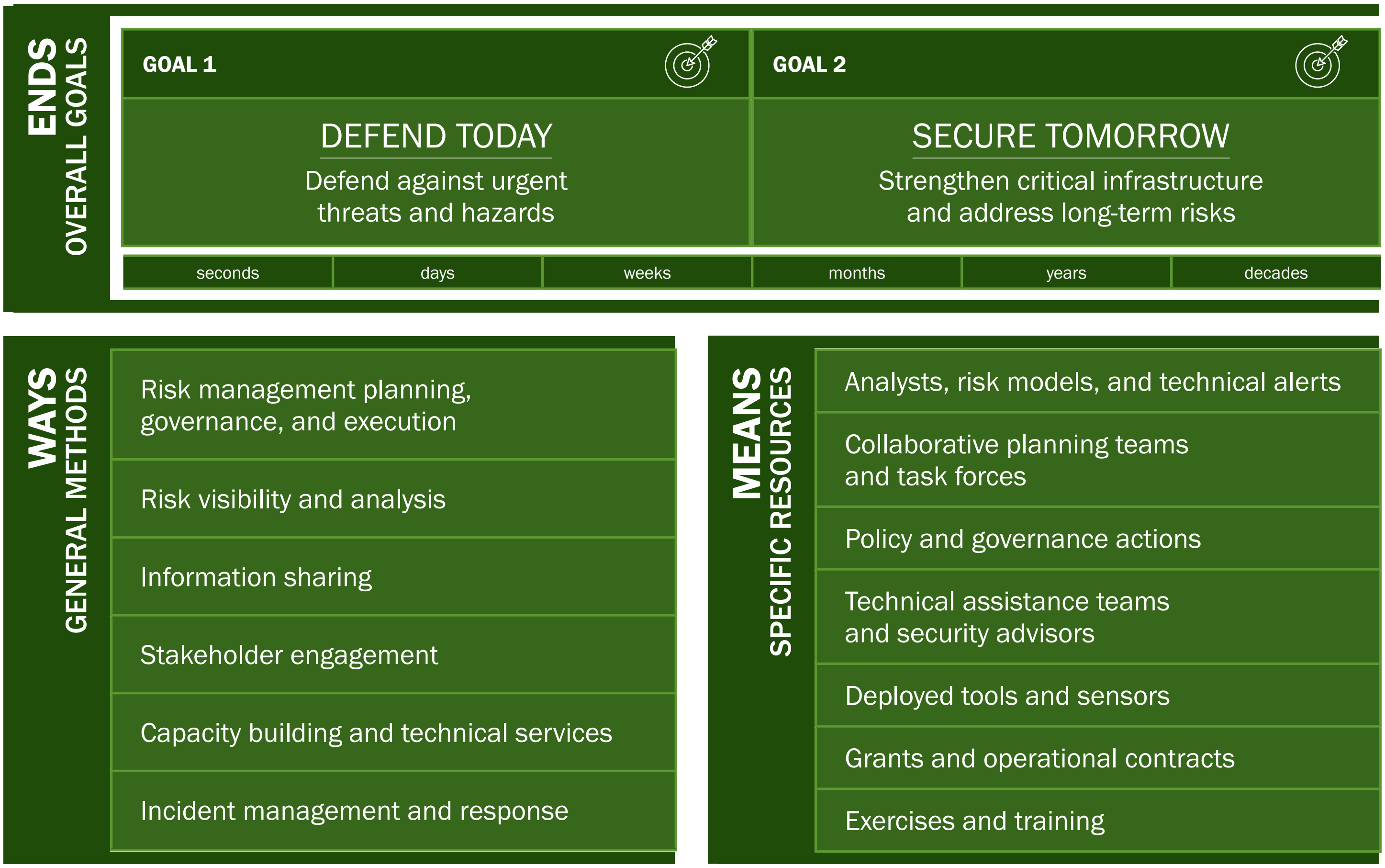
“DEFEND TODAY, SECURE TOMORROW.”

APPROACH

The heart of CISA’s purpose is to mobilize a collective defense of our nation’s critical infrastructure. We lead the Nation’s risk management efforts by bringing together diverse stakeholders to collaboratively identify risks, prioritize them, develop solutions, and drive those solutions to ensure the stability of our national critical functions. As the nation’s risk advisor, CISA is unique in its position to partner with private industry, researchers, international governments, emergency responders, intelligence, defense, and other communities.

As a single, unified agency, CISA seeks to achieve two strategic goals across all of our mission space. First, CISA defends today by addressing the imminent risks facing our national critical functions. For example, we deploy intrusion prevention technologies in federal networks and support emergency communication during the response to wildfires that threaten lives and critical infrastructure.

Second, CISA secures tomorrow by helping organizations manage their own risk during steady-state conditions.



ENDS
OVERALL GOALS

GOAL 1

DEFEND TODAY
Defend against urgent threats and hazards

GOAL 2

SECURE TOMORROW
Strengthen critical infrastructure and address long-term risks

seconds | days | weeks | months | years | decades

WAYS
GENERAL METHODS

- Risk management planning, governance, and execution
- Risk visibility and analysis
- Information sharing
- Stakeholder engagement
- Capacity building and technical services
- Incident management and response

MEANS
SPECIFIC RESOURCES

- Analysts, risk models, and technical alerts
- Collaborative planning teams and task forces
- Policy and governance actions
- Technical assistance teams and security advisors
- Deployed tools and sensors
- Grants and operational contracts
- Exercises and training

For example, we help soft targets and crowded places plan and secure themselves in advance of an attack. We also drive high-impact, long-term solutions to support our partners. For example, CISA drives the creation of new technical standards to further automate cybersecurity operations.

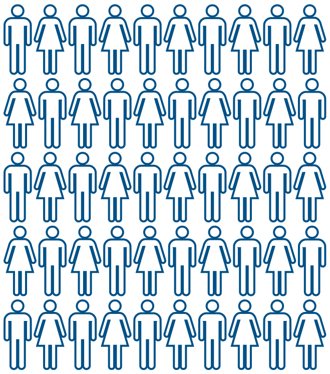
We achieve these ends through a variety of ways that are common across our goals and mission domains. These include risk analysis, risk management planning, information sharing, capacity building, and incident response. For both goals, functional teams from across CISA work together in a matrixed fashion with a national field presence. These ways are all reliant on successful partnerships with other stakeholders.

ELECTION SECURITY:

A model for collaborative risk management

CISA's work on election security is a model for how the agency can rally its resources and bring together a variety of stakeholders to address a common risk.

One of the highest-profile threats we face today is attempts by nation-state actors to maliciously interfere in our democratic elections. Leading up to the 2018 midterm elections, CISA worked hand-in-hand with federal partners, state and local election officials, and private sector vendors to provide them with information and capabilities to enable them to better defend their infrastructure. Some examples of CISA's efforts include the following:



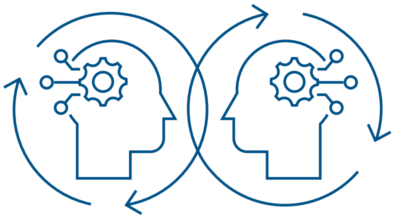
OVER 500 CISA EMPLOYEES SUPPORTED ELECTION SECURITY PREPAREDNESS NATIONWIDE,

including providing free technical cybersecurity assistance, information sharing, and expertise to election offices, campaigns, and technology vendors.

One person equals 10 employees.

HOSTED THE NATIONAL-LEVEL "TABLETOP THE VOTE"

exercise, a three-day, first-of-its-kind event to assist federal partners, state and local election officials, and private sector vendors to assist in incident planning, preparedness, identification, response, and recovery.

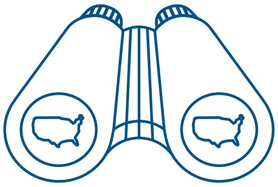


COLLABORATIVELY DEVELOPED & PUBLISHED GUIDANCE ON CRITICAL CYBERSECURITY

actions that should be implemented in counties and political campaigns.

ESTABLISHED A NATION-WIDE VIRTUAL WATCH FLOOR

CISA field staff were co-located with election officials in their own security operations centers.



These efforts exemplify CISA's model for addressing national-level risks: agile in how we pivot toward emerging threats; collaborative in identifying strategies and solutions; and results-oriented in how we respond and follow through.

DIRECTOR'S OPERATIONAL PRIORITIES

While the goals and outcomes within of the *Strategic Intent* create a common framework across our entire mission space and activities, the Director has five specific operational areas of focus that, in some cases, span across several goals and objectives.

1 CHINA, SUPPLY CHAIN, AND 5G

China presents the most pressing long-term strategic risk to the United States. The persistent threat posed by China compels CISA's focus on supply chain risk management in the context of national security. CISA is looking to reduce the risks of Chinese supply chain compromise, whether that is through 5G or any other technologies.

2 ELECTION SECURITY

CISA is responsible for assisting state and local governments, and the private sector organizations that support them, with their efforts to enhance the security and resilience of election infrastructure. CISA's objective is to reduce the likelihood of compromises to election infrastructure confidentiality, integrity, and availability, which are essential to the conduct of free and fair democratic elections. We will pivot off the trust, expertise, and relationships developed through our election security work to broaden our State and Local cybersecurity risk management efforts.

3 SOFT TARGET SECURITY

Intentional targeting of soft targets and crowded places presents a daunting security challenge—undermining traditional risk management and physical security practices by deliberately exploiting vulnerabilities. As the DHS lead for the soft targets and crowded places security effort, CISA supports partners to identify, develop, and implement innovative and scalable measures to mitigate risks to these venues; many of which serve an integral role in the country's economy.

4 FEDERAL CYBERSECURITY

The speed of change in the cyber world is outpacing the current federal "policy to implementation" process. CISA leads the Federal Government in confronting this challenge with a unity of purpose that drives federal agencies to make risk-informed cybersecurity decisions. CISA's authorities present the capability and opportunity to create federal cybersecurity approaches that address the speed of change. We will also use our insight, expertise, capabilities and reach to assist our State and Local government partners in improving their cybersecurity posture and defending against the outbreak of ransomware.

5 INDUSTRIAL CONTROL SYSTEMS

Much of critical infrastructure shares a common characteristic: a dependence on industrial control systems (ICS). ICS control, monitor, and manage essential functions for a wide array of critical infrastructure, including transportation systems, telecommunications networks, industrial manufacturing plants, electric power generators, oil and natural gas pipelines, and more recently, the Internet of Things. CISA leads the Federal Government's unified effort to work with the ICS community to reduce risk to our critical infrastructure by strengthening control systems' security and resilience.

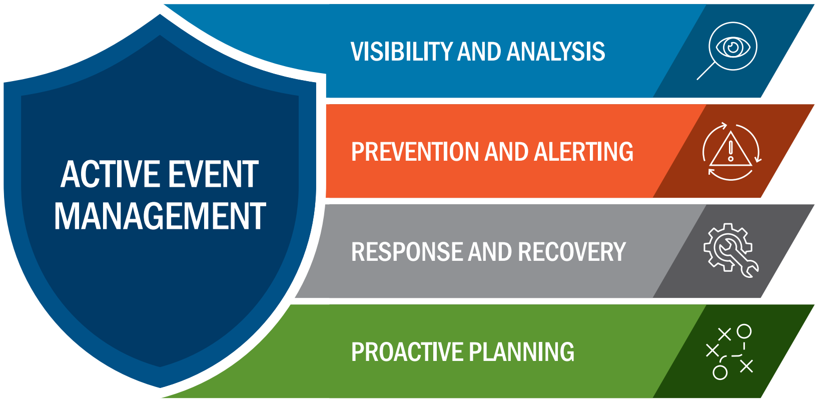
Defend against urgent threats and hazards.

With the right preparations and partnerships, CISA can ensure:

- the prevention or mitigation of most of the significant threats in federal networks and critical infrastructure;
- the mitigation of impacts of all-hazards events to the greatest extent possible;
- the seamless flow of voice, video, and data communications during incident response; and
- the appropriate mitigation of significant hybrid, supply chain, and emerging threats.

A national, coordinated effort is necessary to meet these ends. This requires proactive, collaborative, and creative planning of the best ways to respond. Through data sharing and deployed technologies, we have a unique national position to gain risk visibility. We prevent, mitigate, and respond through alerts and risk reporting, technical assistance, deployed technologies, and collaboration with operational partners. We stand shoulder-to-shoulder with our partners in defending the homeland and each other.

> **Desired end-state:** Incidents with a potentially significant impact on national security, public health and safety, and economic security are prevented or mitigated.



ACTIVE EVENT MANAGEMENT

VISIBILITY AND ANALYSIS

PREVENTION AND ALERTING

RESPONSE AND RECOVERY

PROACTIVE PLANNING

OBJECTIVE 1.1
CYBER DEFENSE

Significant cyber threats are unable to achieve their objectives in CISA mission space.

SUB-OBJECTIVE 1.1.1
VISIBILITY

CISA knows current threat activity and strategic interests of every major threat group and has timely access to available data on the risk posture of key information systems.

SUB-OBJECTIVE 1.1.2
ANALYSIS AND EVENT MANAGEMENT

CISA prioritizes the most urgent risks and coordinates response actions within CISA and with its partners.

SUB-OBJECTIVE 1.1.3
PREVENTION AND RESPONSE ACTIONS

Prevention and response actions from CISA and its partners prevent or mitigate significant threat activity and vulnerabilities.

OBJECTIVE 1.2
PHYSICAL HAZARDS

Impacts from physical hazards are minimized through coordinated incident preparation and response.

SUB-OBJECTIVE 1.2.1
VISIBILITY AND ANALYSIS

CISA will have awareness of imminent threats to critical infrastructure with an accuracy and fidelity commensurate with risk to the national security, public health and safety, and economic security of the Nation.

SUB-OBJECTIVE 1.2.2
PLANNING AND PREPAREDNESS SERVICES

Stakeholders are prepared in advance for specific natural hazards and special events and mass gatherings.

SUB-OBJECTIVE 1.2.3
EVENT MANAGEMENT AND RECOVERY

Impacts are minimized to the greatest extent possible through coordination with partners during an incident, including through Emergency Support Function #14.

OBJECTIVE 1.3
INCIDENT COMMUNICATIONS

Voice, video, and data communications are available and interoperable during daily operations and incident response.

SUB-OBJECTIVE 1.3.1
EMERGENCY SUPPORT FUNCTION #2

During times of emergency and declared disasters, communications are protected, restored, and reconstituted effectively.

SUB-OBJECTIVE 1.3.2
PRIORITY TELECOMMUNICATIONS SERVICES

National security and emergency preparedness communications are available and prioritized on commercial networks under all circumstances when network congestion or damage renders conventional communications ineffective.

SUB-OBJECTIVE 1.3.3
INCIDENT COMMUNICATIONS SUPPORT

Emergency communications are operable, interoperable, and resilient during natural disasters, acts of terrorism, or planned events.

OBJECTIVE 1.4
HYBRID, SUPPLY CHAIN, AND EMERGING THREATS

Hybrid, supply chain, and emerging threats are unable to achieve their objectives in CISA mission space.

SUB-OBJECTIVE 1.4.1
VISIBILITY AND ANALYSIS

CISA has awareness of imminent hybrid, supply chain, and emerging threats and their potential impacts on society.

SUB-OBJECTIVE 1.4.2
RESPONSE PLANNING AND PREPAREDNESS

Through collaborative planning, stakeholders are prepared in advance of incidents.

SUB-OBJECTIVE 1.4.3
RESPONSE ACTIONS AND MANAGEMENT

Impacts are minimized to the greatest extent possible through response actions and coordination with partners during an incident.

RISK MANAGEMENT IN ACTION

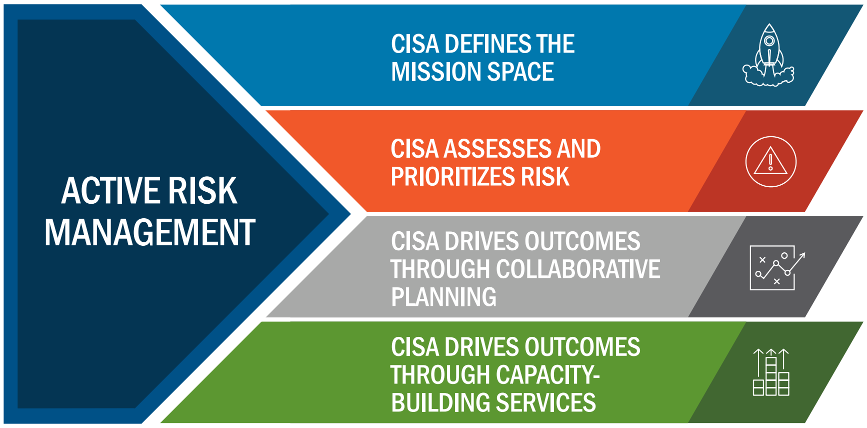
In January 2019, CISA issued its first Emergency Directive to address ongoing incidents associated with global Domain Name System (DNS) infrastructure tampering. CISA had visibility on this threat from several cybersecurity service provider partners. In rapid order, CISA collaboratively planned and executed a response that included preventive actions across the Federal Government. Several private sector organizations followed CISA's leadership within in the .gov domain and took decisive actions on their own in line with CISA's recommended procedures.

Strengthen critical infrastructure and address long-term risks.

To manage significant medium-term risks, CISA will assess and prioritize strategic risk, drive planning and policy efforts, and build the capacity of our stakeholders. As the Nation’s risk advisor, CISA must ensure that growing risks to critical infrastructure and other entities are managed at an acceptable level. That means identifying the serious risks to critical infrastructure and evaluating whether they are being managed appropriately. If there is a gap, CISA must act as the backstop and bring options for technical assistance, help to drive policy changes, or find other creative solutions for mitigation. CISA must support critical infrastructure and other stakeholders so that they have the capabilities to manage national-level risks.

For long-term risks, we need to sow the seeds of change today to make a difference in the years to come. CISA will make a concerted effort to anticipate and address long-term risks, including building systems secure by design and ensuring a national workforce supply to support critical infrastructure.

> **Desired end-state:** The community successfully manages medium- and long-term risks with a significant impact on national security, public health and safety, and economic security.


ACTIVE RISK MANAGEMENT
CISA DEFINES THE MISSION SPACE
CISA ASSESSES AND PRIORITIZES RISK
CISA DRIVES OUTCOMES THROUGH COLLABORATIVE PLANNING
CISA DRIVES OUTCOMES THROUGH CAPACITY-BUILDING SERVICES

OBJECTIVE 2.1 CRITICAL INFRASTRUCTURE RESILIENCE AND CAPACITY BUILDING

The community maintains an appropriate level of security and resilience through risk management and capacity building.

SUB-OBJECTIVE 2.1.1 STRATEGIC RISK POSTURE AWARENESS

CISA knows the risk postures of critical infrastructure and other entities with an accuracy and fidelity commensurate with risk to the national security, public health and safety, and economic security of the Nation.

SUB-OBJECTIVE 2.1.2 PLANNING, POLICY, AND GOVERNANCE

CISA effectively uses all available levers, including statutorily required regulatory programs, to drive risk management and ensure appropriate security at critical infrastructure and other entities.

SUB-OBJECTIVE 2.1.3 CAPACITY BUILDING AND MITIGATION SERVICES

CISA provides tools and services that fill key gaps in the security of critical infrastructure and other entities, establish relationships to help with defense operations, and increase our visibility into the risk posture of the nation.

OBJECTIVE 2.2

FEDERAL CYBERSECURITY GOVERNANCE AND CAPACITY BUILDING

Cybersecurity risk in federal civilian executive branch agencies is managed at an acceptable level, commensurate with each agency's own risk and that of the broader federal enterprise.

SUB-OBJECTIVE 2.2.1

STRATEGIC RISK POSTURE AWARENESS

CISA knows the risk postures of agencies with an accuracy and fidelity commensurate with risk to the critical functions of the federal enterprise.

SUB-OBJECTIVE 2.2.2

PLANNING, POLICY, AND GOVERNANCE

CISA effectively uses all available governance levers to drive appropriate security within the federal enterprise.

SUB-OBJECTIVE 2.2.3

CAPACITY BUILDING TOOLS AND SERVICES

CISA provides tools and services that fill critical gaps in the cybersecurity of federal entities, establish relationships to help with cyber defense operations, and increase our visibility into the risk posture of the federal enterprise.

OBJECTIVE 2.3

EMERGENCY COMMUNICATIONS GOVERNANCE AND CAPACITY BUILDING

Responders at all levels of government have the ability to seamlessly share voice, video, and data communications during daily operations and major incidents and events.

SUB-OBJECTIVE 2.3.1

CAPACITY BUILDING SERVICES AND GRANTS

CISA provides grants guidance, technical assistance, training, standard operating procedures, and services to ensure that all levels of government can manage their communications resources, strengthen response, and prepare for emerging technologies.

SUB-OBJECTIVE 2.3.2

GOVERNANCE

CISA effectively facilitates national governance bodies and partners with standards development organizations to share best practices, develop tools and resources, and drive policies and standards to improve interoperability.

SUB-OBJECTIVE 2.3.3

ANALYSIS, PLANNING, AND POLICY

CISA knows the effectiveness of emergency communications across the country and uses the National Emergency Communications Plan and other policy and planning sources to ensure that public safety agencies are effectively managing current and future communications resources.

OBJECTIVE 2.4

LONG-TERM RISK MANAGEMENT

Long-term risks are addressed through collaborative risk management across the community.

SUB-OBJECTIVE 2.4.1

ANALYSIS, PLANNING, AND INNOVATIONS

CISA anticipates, understands, and responds to long-term risks.

SUB-OBJECTIVE 2.4.2

SECURE BY DESIGN

Systems, assets, and services are designed with the security and resilience of national critical functions in mind.

SUB-OBJECTIVE 2.4.3

NATIONAL WORKFORCE

There is an appropriate supply of security professionals for the national demand.

RISK MANAGEMENT IN ACTION

CISA worked with industry and government partners to establish the Tri-Sector Executive Working Group. Senior leaders from the financial services, communications, and electricity communities are working together to manage risks to the Nation. Activities are underway to help direct intelligence collection requirements, build cross-sector risk management playbooks, and better understand and address systemic risk.

GOAL 3: MISSION SUPPORT

Become a 21st Century Agency

CISA's internal services support mission execution.

To address the advanced threats and hazards of today, we need excellent mission support. CISA mission and business support functions must deliver customer-focused support in order for CISA operations to secure and enhance the resilience of the Nation's infrastructure. Across all of our mission support elements—workforce development, CISA transformation, capability delivery, and other business support—CISA must identify and apply lessons learned from across the Federal Government and private industry. We will create a culture that fosters and rewards effective innovation. Effective mission support is an essential element to defending today and securing tomorrow.

> **Desired outcome:** CISA exceeds Federal Government averages on overall mission support performance.

OBJECTIVE 3.1 WORKFORCE DEVELOPMENT AND RETENTION

Missions and mission support are fully staffed with the appropriate skills, competencies, and performance. The CISA workforce directly reflects the strengths and vibrancy of a diverse and inclusive Nation and, to a person, is provided an equal opportunity to thrive.

OBJECTIVE 3.2 TRANSFORMATION

CISA successfully designs, validates, and implements the *CISA 2020* internal change management campaign to unify the agency, enhance mission effectiveness, and improve the overall CISA employee experience.

OBJECTIVE 3.3 CAPABILITY DELIVERY

Mission operators and partners receive new capabilities in a timely and effective manner to address evolving threats.

OBJECTIVE 3.4 MISSION SUPPORT MANAGEMENT

CISA exceeds Federal Government averages on mission support performance.

U.S. DEPARTMENT OF HOMELAND SECURITY

CISA

CYBER+INFRASTRUCTURE