

U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

DEFEND TODAY,
SECURE TOMORROW



CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient
infrastructure for the
American people.

MISSION

CISA partners with industry and
government to understand and
manage risk to our Nation's
critical infrastructure.



OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent
threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

Strengthen critical
infrastructure and
address long-term risks

months | years | decades

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

2023-2025 CISA STRATEGIC PLAN



GOALS

- 1 CYBER DEFENSE**
Lead the National Effort to Ensure Defense and Resilience of Cyberspace
- 2 Risk Reduction & Resilience**
Reduce Risks to, and Strengthen Resilience of, America's Critical Infrastructure
- 3 Operational Collaboration**
Strengthen Whole-of-Nation Operational Collaboration and Information Sharing
- 4 Agency Unification**
Unify as One CISA Through Integrated Functions, Capabilities, and Workforce

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Our Work

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating 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



CORE COMPETENCIES

Partnership Development

CISA fosters innovative and collaborative partnerships that enable stakeholders in the government and the private sector to make informed and voluntary risk management decisions and investments.



Every day, CISA employees: Share information with critical infrastructure partners and serve as the national hub for cybersecurity and communications information data sharing in near-real-time.



Sector outreach: CISA works with government officials and critical infrastructure stakeholders to plan, develop and facilitate exercises that build capacity, improve security and bolster resilience.



CORE COMPETENCIES

Information and Data Sharing

Each and every day, CISA shares information with critical infrastructure partners and serves as the national hub for cybersecurity, critical infrastructure, and communications information and data sharing in near real-time.

CISA performs a suite of functions that provide customers with comprehensive risk management capabilities, products, and services. These functions include:



Information Sharing



Risk & Vulnerability Assessments



Watch Floor Operation



Operational Planning, Training, & Exercises



Data Synthesis & Analysis



Thought Leadership



CORE COMPETENCIES

Capacity Building

Provide capacity-building, technical assistance, tools, exercises, training programs, and awareness efforts that focus on heightening understanding of common risks and possible mitigation strategies for the critical infrastructure community.



Cyber: CISA provides **cyber risk and vulnerability assessments and assists in response to cyber incident coordination.**



Physical: CISA conducts **Infrastructure Survey Tool assessments** in coordination with facility owners and operators to identify and document the overall security and resilience of their facilities.



CISA is a focal point for strategic and customer engagement with critical infrastructure, including small and mid-sized businesses and state, local, tribal, and territorial governments.



CORE COMPETENCIES

Incident Management & Response

Serve as the lead for coordinating activities with the private sector, states, and federal agencies providing an integrated response to incidents impacting critical infrastructure; assess and inform risk management strategies on the consequences of emerging and future risks; and support FEMA led response efforts as the co-lead for Emergency Support Function #2 (Communications) and #14 (Cross-Sector Business and Infrastructure).



Received nearly **106,000** cyber incident reports from federal and critical infrastructure partners. Conducted **23** on-site responses to cyber incidents and identified **129,000** cybersecurity vulnerabilities through scans and vulnerability assessments.



Hunt and Incident Response Team (HIRT) provide free on-site incident response to organizations needing immediate investigation and resolution of cyber attacks.



ESF2, ESF14, and 24/7 operational reporting:

- Coordinates government and industry efforts for the reestablishment and provision of critical communications infrastructure and services.
- Lead Cross-Sector Business and Infrastructure response operations with infrastructure owners and operators, businesses, and their government partners.
- Provide 24/7 operational reporting and situational awareness on incident impacting critical infrastructure.



CORE COMPETENCIES

Risk Assessment and Analysis

Develop and enhance capabilities to support crisis action by identifying and prioritizing infrastructure through the use of analysis and modeling capabilities.



Produces analysis of impacts to critical infrastructure for landfalling hurricanes and other pending disruptions for key partners and stakeholders



Each year CISA conducts more than 1,000 of Hometown Security Initiative activities supporting the needs of small and mid-sized business and local communities.



CORE COMPETENCIES

Network Defense

CISA develops new processes, tools, and technologies to assess cyber and physical threats/vulnerabilities to people and property, as well as the potential consequences that might result.



Share information with critical infrastructure partners and stakeholders across the .gov community and serve as the national hub for cybersecurity and communications information data sharing in near-real-time



Serve as cyber and physical security experts in advancing security operational capabilities by developing processes, tools, and technologies to assess threats and vulnerabilities.



CORE COMPETENCIES

Emergency Communications

CISA enhances public safety interoperable communications at all levels of government.



In FY19, delivered 231 technical assistance engagements across 47 states and territories.



Since 2008, trained more than 10,000 public safety officials on National Incident Management System, Incident Command Structure positions within the Communications Unit.








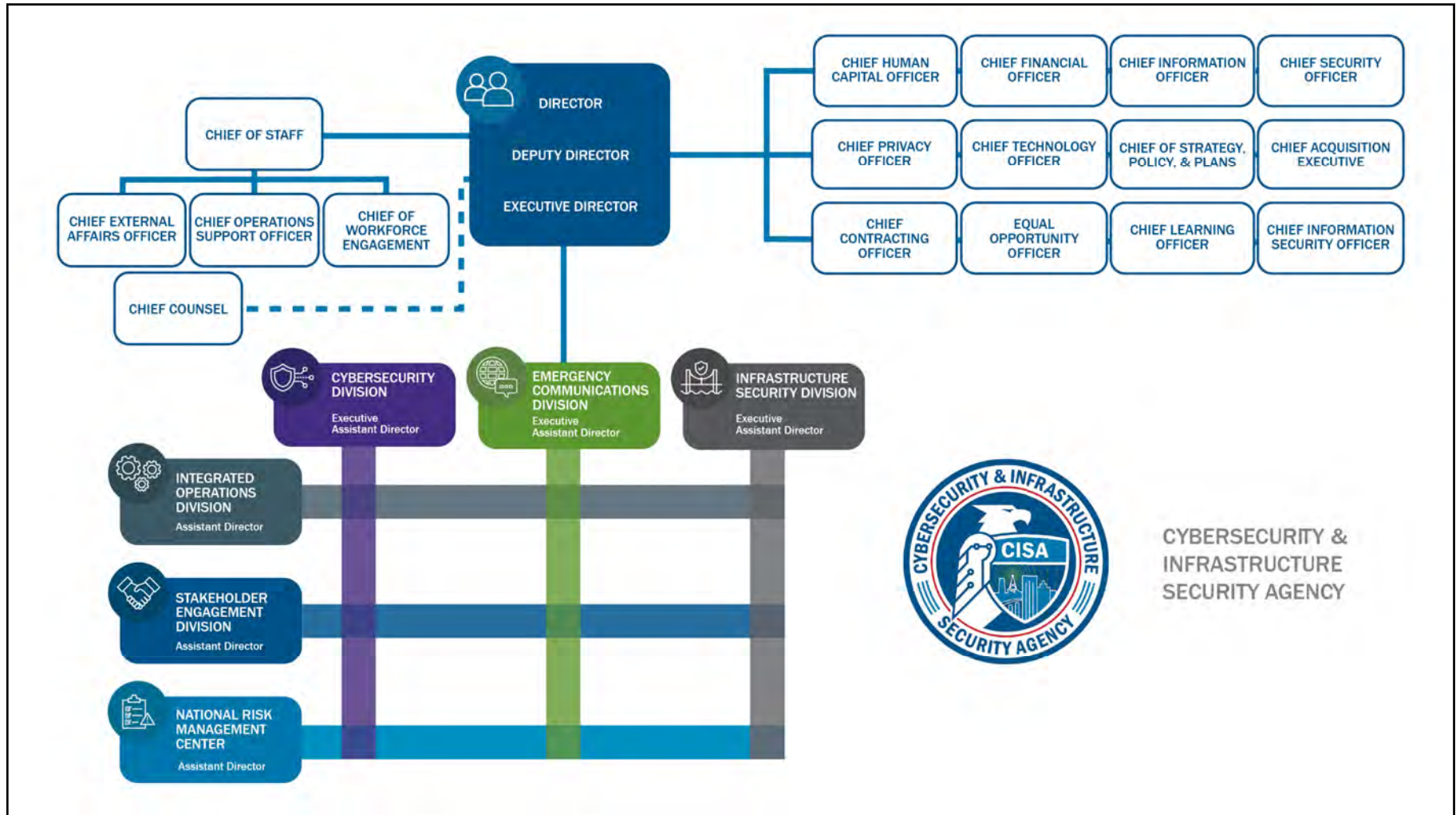
In FY19, partnered with over 3,500 Public Safety representatives to develop and publish the National Emergency Communications Plan update.



GETS call completion rates were over 99% and WPS call completion rates were over 98% for recent hurricanes including Barry and Dorian (commercial grade average is less than 50%).

CISA Operational Priorities

| | | |
|---|-----------------------------------|---|
|  | CYBER SUPPLY CHAIN AND 5G | <p>CISA is focused on supply chain risk management in the context of national security. CISA is looking to reduce the risks of foreign adversary supply chain compromise in 5G and other technologies.</p> |
|  | ELECTION SECURITY | <p>CISA assists state and local governments and the private sector organizations that support them with 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, essential to the conduct of free and fair democratic elections.</p> |
|  | SOFT TARGET SECURITY | <p>As the DHS lead for the soft targets and crowded places security effort, CISA supports partners as they 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.</p> |
|  | FEDERAL CYBERSECURITY | <p>CISA provides technology capabilities, services, and information necessary for agencies across the Federal civilian executive branch to manage sophisticated cybersecurity risks. CISA's authorities enable deployment of robust capabilities to protect Federal civilian unclassified systems, recognizing that continuous improvement is required to combat evolving threats. CISA also works to help State, Local, Tribal and Territorial governments improve cybersecurity and defend against cybersecurity risks.</p> |
|  | INDUSTRIAL CONTROL SYSTEMS | <p>CISA leads the Federal Government's unified effort to work with the Industrial Control Systems (ICS) community to reduce risk to our critical infrastructure by strengthening control systems' security and resilience.</p> |





CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity Division

The Cybersecurity Division (CSD) assures the security, resilience, and reliability of the nation's cyber systems.

MISSION PRIORITIES:



Cyber Defense Operations - CISA detects and prevents cybersecurity risks where possible through information sharing and deployment of detective and preventative technologies and by providing incident response and "hunt" capabilities to minimize impacts of identified incidents.



Federal Networks Governance and Capacity Building - To raise the federal cybersecurity baseline, CISA provides tools, services, expert guidance, and cybersecurity directives to drive cybersecurity risk management within agency defined risk tolerance and CISA's continuous analysis of cyber risks across the Federal enterprise.



Critical Infrastructure/SLTT Governance and Capability Building - CISA provides non-federal entities with cybersecurity information, assessments, and incident response assistance to enable more comprehensive cybersecurity risk management of the critical functions that underpin our national security, public health and safety, and economic security. Support and enable non-federal entities to better manage risk at an acceptable level commensurate with their own defined risk tolerance and national risks of national security, public health and safety, and economic security.



Long-term Cybersecurity - CISA drives national efforts to create a more secure cyber ecosystem through collaboration with the private sector, academia, and government partners to build a diverse cyber workforce, foster development and use of secure technologies, and promote cybersecurity best practices across all organizations.



CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Infrastructure Security Division

The Infrastructure Security Division (ISD) leads the coordinated effort to reduce risks posed to our critical infrastructure, whether from man-made or natural causes.

MISSION PRIORITIES:



Combating Domestic Violent Extremism, including mass shootings and bombing prevention.



Refreshing the National Infrastructure Protection Plan (The National Plan) & Implementing the 2021 NDAA Section 9002.



Increasing External Engagement by focusing on partnership and collaboration, information sharing, and transparency.



Strengthening our work to prevent chemical terrorism, to include securing permanent CFATS Authorization, expanding the voluntary chemical security program, and addressing IED precursors.



CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Emergency Communications Division

The Emergency Communications Division (ECD) ensures Public Safety has the tools needed to communicate during steady state and emergency operations.

MISSION PRIORITIES:



Develop and implement nationwide emergency communications policy and plans, including the National Emergency Communications Plan and 56 Statewide Communications Interoperability Plans.



Manage funding, sustainment, and grant programs to support communications interoperability.



Build capacity with Federal, State, Local, Tribal, and Territorial stakeholders by providing technical assistance, training, resources, and guidance.



Provide priority telecommunications services over commercial networks to enable national security and emergency preparedness personnel to communicate during congestion scenarios across the nation.



Support nationwide sharing of best practices and lessons learned through facilitation of the SAFECOM and Emergency Communications Preparedness Center governance bodies.



CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

National Risk Management Center

The National Risk Management Center (NRMC) is a planning, analysis, and collaboration center. CISA coordinates with the critical infrastructure community to identify; analyze; prioritize; and manage risks to National Critical Functions, which are vital to the United States.

MISSION PRIORITIES:



Analyzes most strategic risks to our Nation's critical infrastructure



Leads public/private partnership initiatives to manage priority areas of national risk



Collaborates with the private sector and other stakeholders to better understand future threats.



CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Integrated Operations Division

The Integrated Operations Division prepares, plans, and coordinates CISA operations and the delivery of CISA capabilities and services to enhance the security of our Nation's infrastructure.

MISSION PRIORITIES:



Regional Service Delivery: Expand and enhance the delivery of CISA programs and services to improve the security and resilience of our Nation's critical infrastructure



Operations: Coordinate and synchronize integrated Agency actions informed by cross-CISA knowledge, insights, and expertise.



Situational Awareness: Consolidate and coordinate timely dissemination of cyber and physical threat information as well as provide incident specific intelligence context and products to support risk acceptance authorities in decision making.



Mission Assurance: Manage business continuity and operational readiness throughout the CISA enterprise.



CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Stakeholder Engagement Division

The Stakeholder Engagement Division (SED) coordinates and integrates stakeholder engagement, fostering collaboration and a culture of shared ownership, and aligns and manages priorities and performance.

MISSION PRIORITIES:



Fosters collaboration and shared stakeholder ownership through the implementation and communication of aligned engagement priorities, governance, processes, standards of practice, feedback loops, performance management, and analytics.



Transforms mission delivery and stakeholder experience by facilitating a consistent and coordinated enterprise stakeholder engagement approach using a customer relationship management platform with interoperability with other Agency systems (e.g., Service Now, CISA Gateway, etc.).



National-level coordination of Sector Risk Management Agency (SRMAs) responsibilities, executing a unified SRMA management approach in collaboration with interagency partners to maximize the value of sector-specific and cross-sector activities.



Management of advisory councils established to provide recommendations to mitigate cyber and physical risks, improve resilience, and protect the Nation's critical infrastructure.

16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

| | | | |
|--|------|--|------------|
|  CHEMICAL | CISA |  FINANCIAL | Treasury |
|  COMMERCIAL FACILITIES | CISA |  FOOD & AGRICULTURE | USDA & HHS |
|  COMMUNICATIONS | CISA |  GOVERNMENT FACILITIES | GSA & FPS |
|  CRITICAL MANUFACTURING | CISA |  HEALTHCARE & PUBLIC HEALTH | HHS |
|  DAMS | CISA |  INFORMATION TECHNOLOGY | CISA |
|  DEFENSE INDUSTRIAL BASE | DOD |  NUCLEAR REACTORS, MATERIALS AND WASTE | CISA |
|  EMERGENCY SERVICES | CISA |  TRANSPORTATIONS SYSTEMS | TSA & USCG |
|  ENERGY | DOE |  WATER | EPA |

CISA Regions

- 1 Boston, MA
- 2 New York, NY
- 3 Philadelphia, PA
- 4 Atlanta, GA
- 5 Chicago, IL
- 6 Irving, TX
- 7 Kansas City, MO
- 8 Lakewood, CO
- 9 Oakland, CA
- 10 Seattle, WA
- CS Pensacola, FL

