CISA
CYBER+INFRASTRUCTURE

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Programs and Capabilities

MARCH 2019

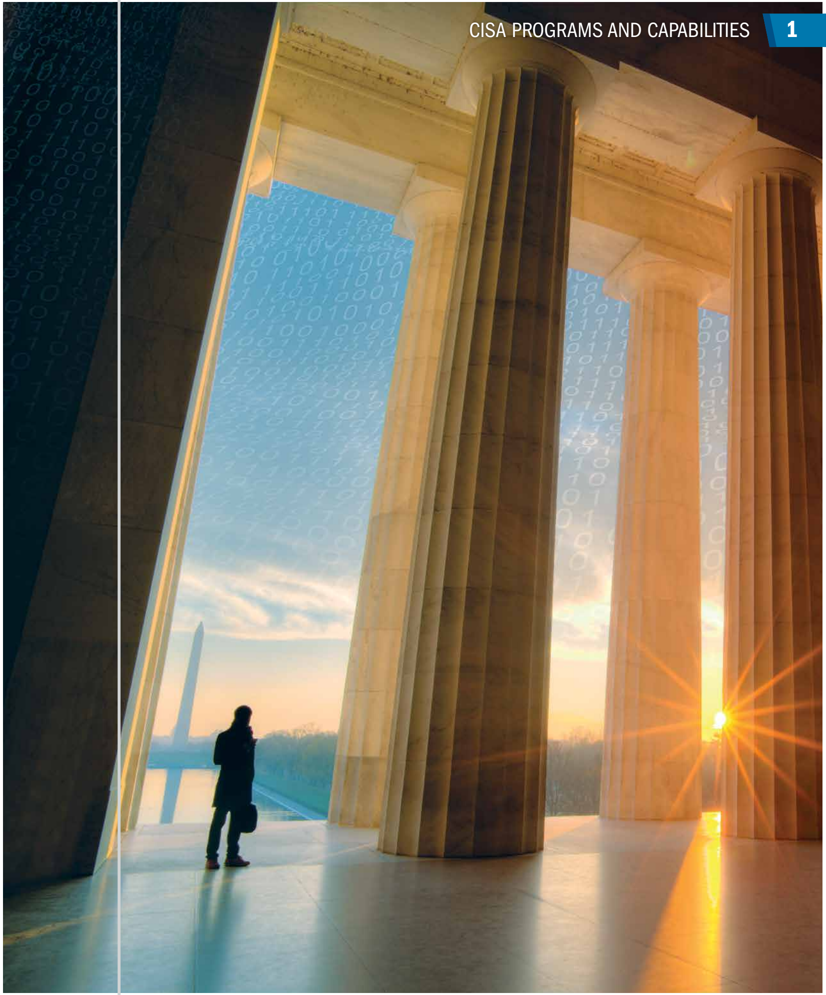
THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

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.

The threats we face—digital and physical, man-made, technological, and natural—are more complex, and the threat actors more diverse, than at any point in our history. CISA is at the heart of mobilizing a collective defense as we lead the Nation's efforts to understand and manage risk to our critical infrastructure.

Our partners in this mission span the public and private sectors. Programs and services we provide are driven by our comprehensive understanding of the risk environment and the corresponding needs identified by our stakeholders. We seek to help organizations better manage risk and increase resilience using all available resources, whether provided by the Federal Government, commercial vendors, or their own capabilities.

Come partner with us!



WHAT WE DO

- **National Infrastructure Risk Management:** CISA monitors, assesses, and prioritizes catastrophic and systemic national risk across critical infrastructure sectors and develops guiding strategies for corresponding risk management activities with public and private sector partners.

- **Infrastructure and Cybersecurity Operations:** CISA rapidly notifies relevant critical infrastructure stakeholders of elevated risk exposure, conducts incident management operations, provides vulnerability assessments, and directly deploys risk management information, tools, and technical services to mitigate risk, including regulatory enforcement where authorized.

- **Critical Infrastructure Capacity-building:** CISA builds national critical infrastructure security and resilience capacity through information sharing, advisory services, training, best practice/standards/regulation development, exercise design and facilitation, evaluation, and planning assistance services for public and private sector stakeholders.

- **Federal Information Security:** CISA ensures the security and resilience of federal civilian enterprise networks and the ".gov" domain by providing defensive technologies and monitoring capabilities, as well as conducting cyber response operations and providing capacity-building services for partner departments and agencies.

- **Interoperable Emergency Communications:** CISA enhances public safety interoperable communications at all levels of government and conducts extensive, nationwide outreach to support and promote the ability of emergency response providers and relevant government officials to communicate in the event of natural disasters, acts of terrorism, and other hazards.

NATIONAL RISK ASSESSMENT

CISA conducts planning, analysis, and collaboration to identify and address the most significant risks to the Nation's critical infrastructure. Initiatives include:

- **Election Security and Resilience:** As the sector-specific agency for the elections infrastructure subsector, CISA collaborates with state and local election officials, law enforcement, and the intelligence community, to increase information sharing with election officials, provide technical assistance and vulnerability assessments, strengthen communications channels, and build trust.

- **Information and Communication Technologies Supply Chain Risk Management Task Force**, with members from government and the IT and Communications Sectors, is a federal focal point to examine and develop consensus recommendations to identify and manage risk to the global technology supply chain.

- **Tri-Sector Executive Working Group**, senior representatives from the Financial Services Sector, Communications Sector, and Electricity Sub-Sector and the Departments of Homeland Security, Treasury, and Energy, help direct intelligence collection requirements, build cross-sector risk management playbooks, and better understand system risk.

- **Pipeline Cybersecurity Initiative**, with Transportation Security Administration expertise, CISA works with asset owners and operators on in-depth review and evaluation of the control system's network design, configuration, and interdependencies.

CISA also conducts risk management initiatives on electromagnetic pulse; position, navigation and timing; and securing unmanned aircraft systems.

OUR ROLE IN CYBERSECURITY

CISA leads efforts to protect the federal ".gov" domain of civilian government networks and to collaborate with the private sector in the ".com" domain to increase the security of critical networks.

Federal response to cyber threats is managed through the **National Cybersecurity & Communications Integration Center (NCCIC)**, CISA's 24/7 cyber situational awareness, incident response, and management center. NCCIC works in close coordination with public, private sector, and international partners through technical assistance, information security, and outreach to defend federal networks, help the private sector defend its own networks, and build awareness of the current cyber and communications risk landscape.

CISA works with partners to prepare for, prevent, and respond to catastrophic cyber incidents. In addition to the NCCIC, CISA maintains situational awareness of the Nation's critical infrastructure for the Federal Government from a physical threat perspective through the National Infrastructure Coordinating Center.

Cybersecurity Capabilities

- **Hunt and Incident Response Teams (HIRT)** provide free, onsite incident response to organizations needing immediate investigation and resolution of cyber attacks. Services include frontline response to cyber incidents and proactive hunts for malicious cyber activity. HIRT can perform a preliminary diagnosis to determine the extent of the compromise. At the customer's request, a team will visit the affected organization to review network topology, identify infected systems, and collect other data as needed to perform thorough follow-on analysis. HIRT provides mitigation strategies, assists in restoring service, and provides recommendations to improve overall network and control systems security.

- **Industrial control systems** are attractive targets for cyber attacks. CISA reduces risks in and across all critical infrastructure sectors by partnering with law enforcement agencies and the intelligence community and coordinating efforts among federal, state, local, and tribal governments and control systems owners, operators, and vendors. CISA collaborates with international and domestic sector Computer Emergency Response Teams to share control systems-related security incidents and mitigation measures.

- The **Advanced Analytic Lab** performs digital media and malware analysis on samples from infected systems. The lab hosts a representative sample of vendor equipment onsite so analysts can test malware capabilities in controlled system environments, letting CISA assess possible effects of malicious software and consequences a vulnerability may have on critical infrastructure.

- The **Advanced Malware Analysis Center** collects, analyzes, and exchanges malware information 24 hours a day. Malware artifacts can be submitted electronically to CISA.

OUR ROLE IN NETWORK DEFENSE

CISA works with chief information officers and chief information security officers at all levels of government to protect networks, ensure continuity of services, and protect the personal information of millions of Americans.

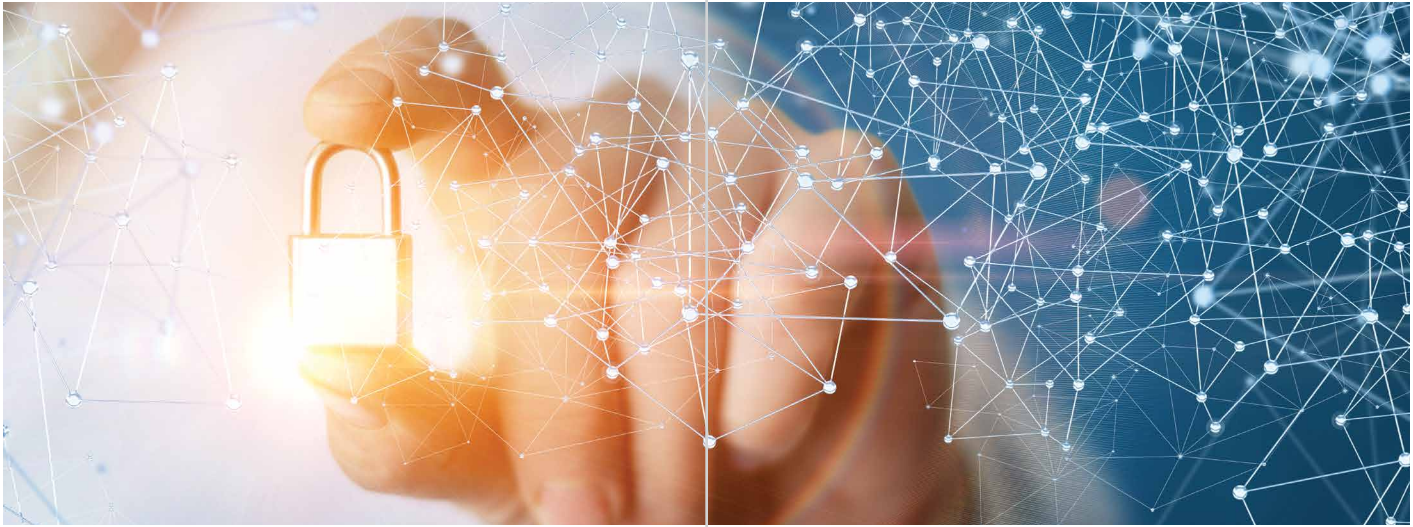
The **National Cybersecurity Protection System's EINSTEIN** program provides active network defense and the **Continuous Diagnostics and Mitigation** program informs network administrators about the state of their networks at any given time. Together, they help provide real-time protection against malicious activities on federal networks and systems.

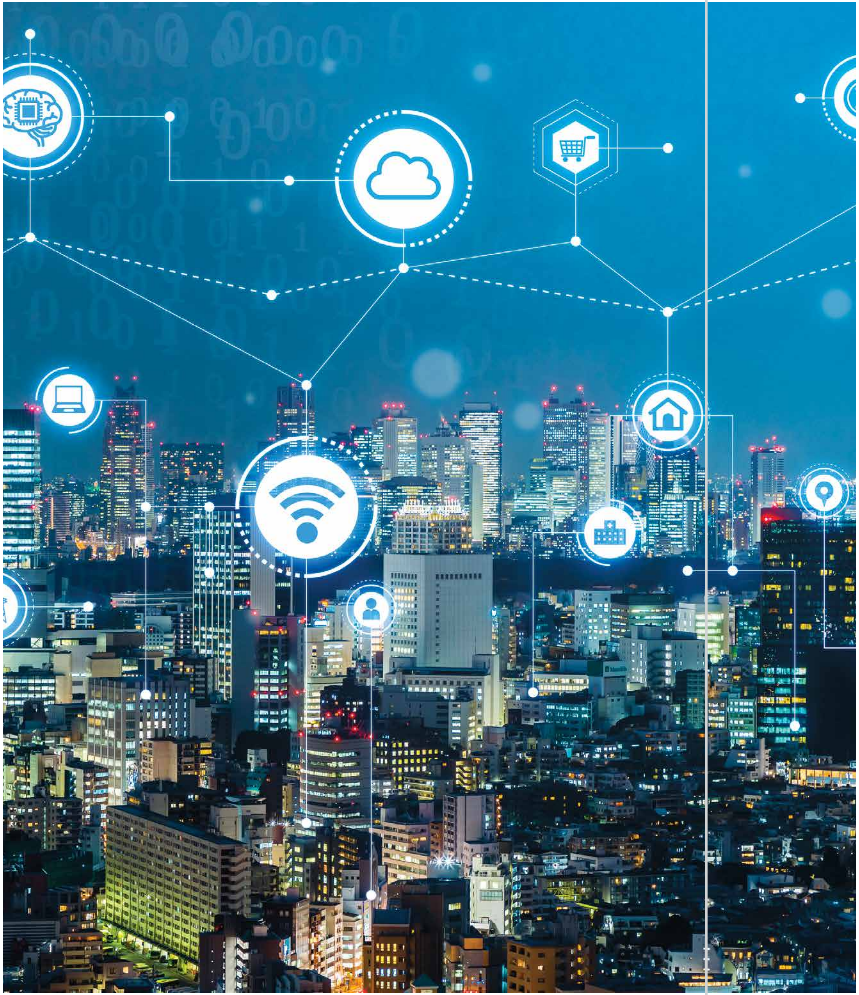
Helping Protect Industry and State and Local Government Networks

CISA's **Enhanced Cybersecurity Services (ECS)** program, like EINSTEIN, provides near real-time intrusion prevention and analysis capability services to help U.S.-based companies and state and local governments protect their computer systems against unauthorized access, exploitation, and data exfiltration. ECS works by sharing sensitive and classified cyber threat information with accredited Commercial Service Providers (CSPs) who use the information to block certain types of malicious traffic from entering customer networks. ECS is meant to augment, not replace, existing cybersecurity capabilities.

State, Local, Tribal, and Territorial Government Cybersecurity Support

The **Multi-State Information Sharing and Analysis Center (MS-ISAC)** is the key resource for cyber threat prevention, protection, response, and recovery for state, local, tribal, and territorial governments. The MS-ISAC provides advisories, cybersecurity guides, toolkits, and other services at no cost to members. The MS-ISAC operates the **Elections Infrastructure Sharing and Analysis Center (EI-ISAC)**, a dedicated, free venue to receive assistance and share information on election system cyber threats and vulnerabilities. The EI-ISAC provides 24/7 network monitoring and election threat intelligence.





OUR ROLE IN INFORMATION SHARING

Threat information sharing is key to preparing for and preventing incidents. CISA consolidates and shares threat and compromise indicators; alerts and warnings; adversary tactics, techniques, and procedures; best practices, recommendations, and countermeasures for cybersecurity improvements; and other critical technical information with its stakeholders and partners.

The **Cybersecurity Act of 2015** clarified DHS's (and now CISA's) role as the key civilian information-sharing portal between the government and the private sector. The Act encourages companies to share cyber threat indicators and defensive measures with each other and the Federal Government, while ensuring strong protections for the privacy and civil liberties of all Americans.

Created by law, the **Protected Critical Infrastructure Information (PCII) Program** protects private sector and non-Federal Government infrastructure information voluntarily given to DHS for homeland security use. PCII is not subject to public disclosure through Freedom of Information Act requests; state, local, tribal, and territorial disclosure laws; regulatory actions; or civil litigation. PCII protections give partners confidence that sensitive or proprietary data will not be exposed.

CISA's **Automated Information Sharing (AIS)** capability enables two-way exchange of cyber threat indicators between the Federal Government and the private sector at machine speed. The goal of AIS is to create an ecosystem enabling a company or federal agency to share cyber threat indicators in real time with partners via a confidential and secure format, helping to protect them from the threat. As a result, adversaries are only able to use an attack once, which increases their costs and ultimately reduces the prevalence of cyber attacks.

We Want You! The Federal Government shares indicators with trusted partners through AIS—but we always need more private sector companies to join AIS to receive and to share indicators back with us!

The **Homeland Security Information Network – Critical Infrastructure (HSIN-CI)** is the trusted network for the critical infrastructure community to share sensitive but unclassified information. HSIN-CI enables free and secure collaboration by industry and government organizations responsible for the security and resilience of the Nation's critical infrastructure.

CISA's **Cyber Information Sharing and Collaboration Program** is a voluntary information sharing program among critical infrastructure partners and the Federal Government. The program builds a community of trust and enhances collaboration between participants.

Information Sharing and Analysis Centers (ISACs) are infrastructure-sector-specific organizations formed by owners and operators to help protect their facilities, personnel, and customers from cyber and physical security threats and other hazards. ISACs collect, analyze and disseminate actionable threat information and provide members with tools to mitigate risks and enhance resiliency.

Information Sharing and Analysis Organizations (ISAOs) are a flexible approach to self-organized information sharing activities among communities of interest, such as businesses across critical infrastructure sectors. Like ISACs, ISAOs collect, analyze, and share cyber threat information pertinent to their stakeholders' needs.

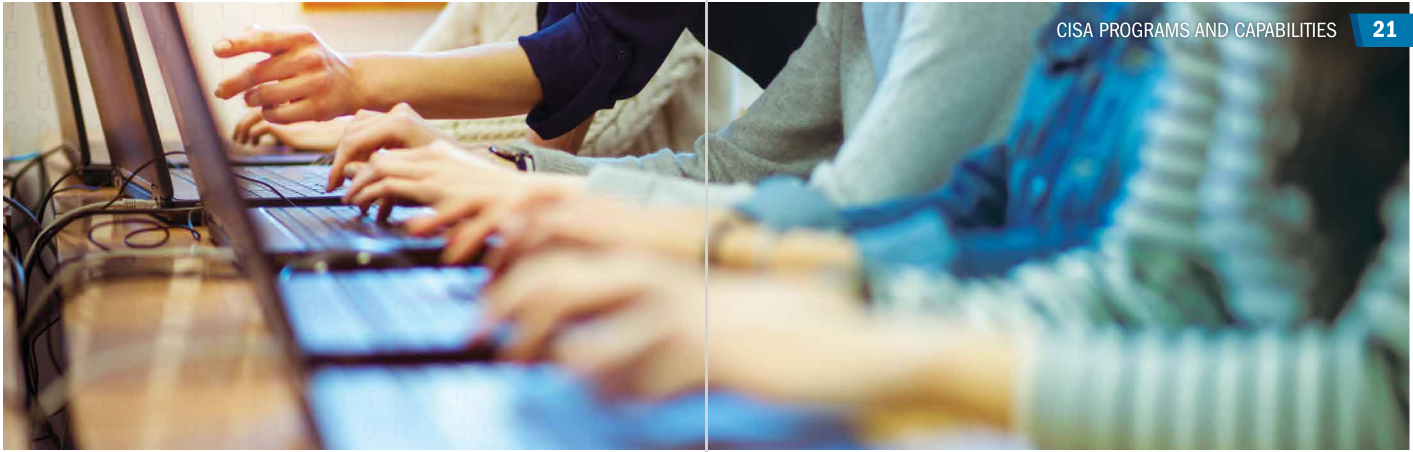
TRAINING

The **Federal Virtual Training Environment (FedVTE)** is a free online, on-demand cybersecurity training system for veterans and government personnel (and some government contractors). Managed by CISA, FedVTE contains more than 800 hours of training on topics such as ethical hacking and surveillance, risk management, and malware analysis. Course proficiency ranges from beginner to advanced levels.

CISA hosts a collaborative **Critical Infrastructure Security and Resilience Training Portal** for members of the Homeland Security Information Network – Critical Infrastructure (HSIN-CI) community. This depository of links and documents serves as a central location for training courses and other resources to support critical infrastructure security and resilience activities.

Active shooter incidents are unpredictable and evolve quickly. In the midst of the chaos, anyone can help mitigate the impacts of an active shooter incident. CISA aims to enhance preparedness through a "whole community" approach by providing products, tools, and resources tailored to first responders, human resources or security personnel, and private citizens to help prepare for and respond to an active shooter incident.

CISA offers **Counter-Improvised Explosive Device (C-IED) Training**, free-of-charge to build nationwide counter-IED capabilities and increase awareness of IED threats. Trainings are available in various formats.



CISA provides access to a range of free training opportunities for the critical infrastructure community. Courses and training materials provide government officials and private sector owners and operators with vital information to enhance the security and resilience of their respective organizations. **Online Critical Infrastructure Independent Study Courses** include security awareness, as well as foundational, topic-specific, and sector-specific online courses.

Direct Delivery In-Person Training

Coordinated through CISA protective security advisors, state homeland security officials, and training offices, bombing-prevention courses educate federal, state, local, tribal, and territorial participants, critical infrastructure owners and operators, and security staff—on strategies to prevent, protect against, respond to, and mitigate bombing incidents. Unless indicated, many courses are instructor-led and designed for a small groups of 25 participants.

Virtual Instructor Led Training

Web-based courses provide general awareness-level C-IED information at no cost to a broad audience via an online virtual training experience with a live instructor, through the Homeland Security Information Network. Courses are designed for up to 50 participants.

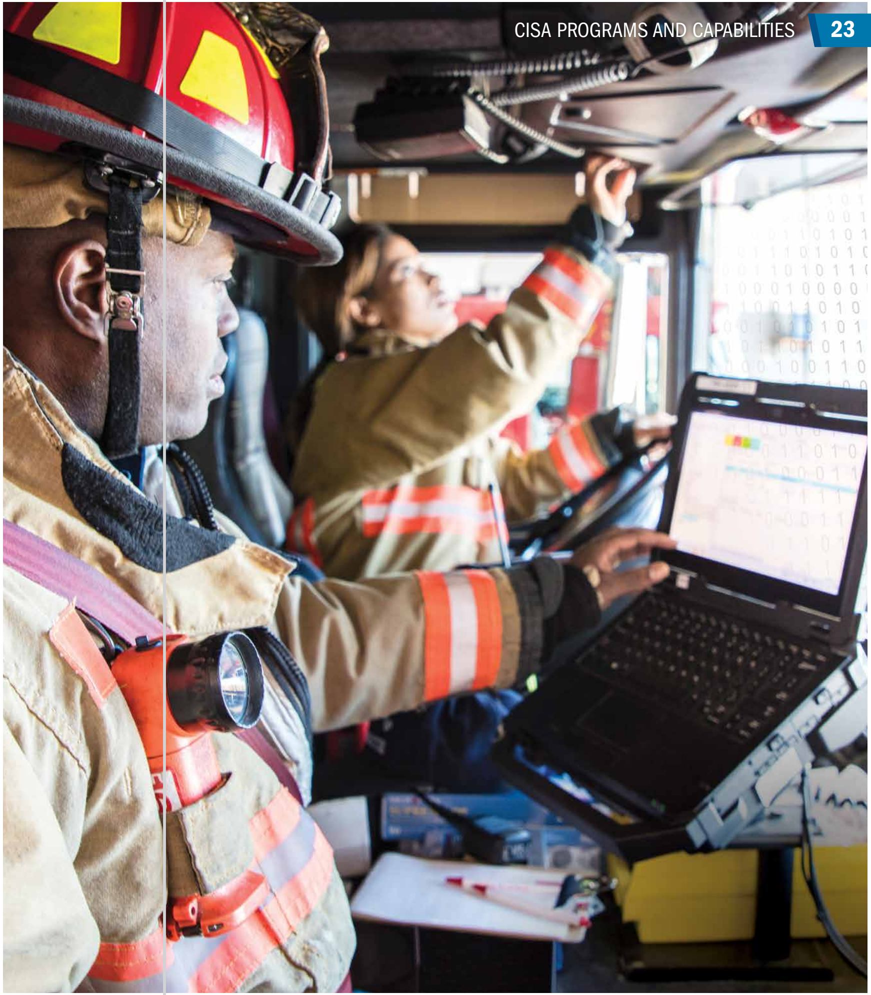
Independent Studies

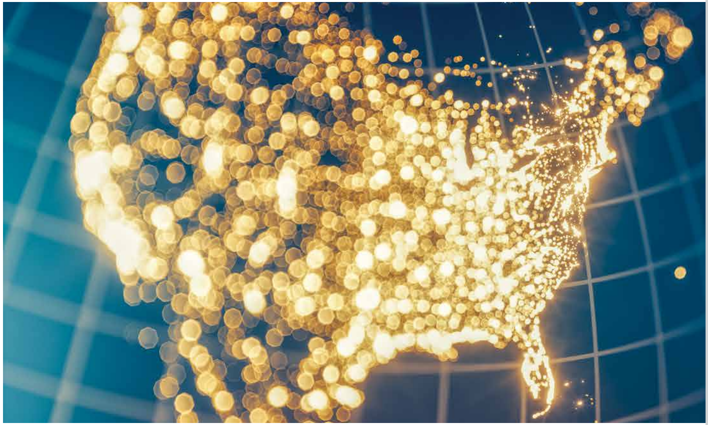
Web-based courses are self-paced and designed for a broad audience to provide general awareness-level, C-IED information at no cost to general public and private sector partners to enhance awareness and response to IED threats.

OUR ROLE IN EMERGENCY COMMUNICATIONS

CISA supports and promotes communications used by emergency responders and government officials to keep America safe, secure, and resilient.

CISA leads the Nation's operable and interoperable public safety and national security and emergency preparedness (NS/EP) communications efforts. CISA provides training, coordination, tools, and guidance to help its federal, state, local, tribal, territorial (FSLTT) and industry partners develop their emergency communications capabilities. CISA's programs and services coordinate emergency communications planning, preparation and evaluation, to ensure safer, better-prepared communities nationwide.





National Emergency Communications Plan

CISA develops and updates a **National Emergency Communications Plan (NECP)** in coordination with FSLTT and private sector stakeholders. The NECP provides information and guidance to those who plan for, coordinate, invest in, and use operable and interoperable communications for response and recovery operations. The NECP seeks to optimize the communications capabilities available to emergency responders—voice, video, and data—to ensure the secure data and information exchange.

Stakeholder Engagement

Formed after the terrorist attacks of September 11, 2001, **SAFECOM** works to improve public safety interoperability, allowing emergency responders to communicate effectively before, during, and after emergencies and disasters in collaboration with responder organizations across FSLTT government and international borders.

SAFECOM works with other federal communications programs and key emergency response stakeholders to address the need for better technologies and processes for coordinating current communications systems and future networks.

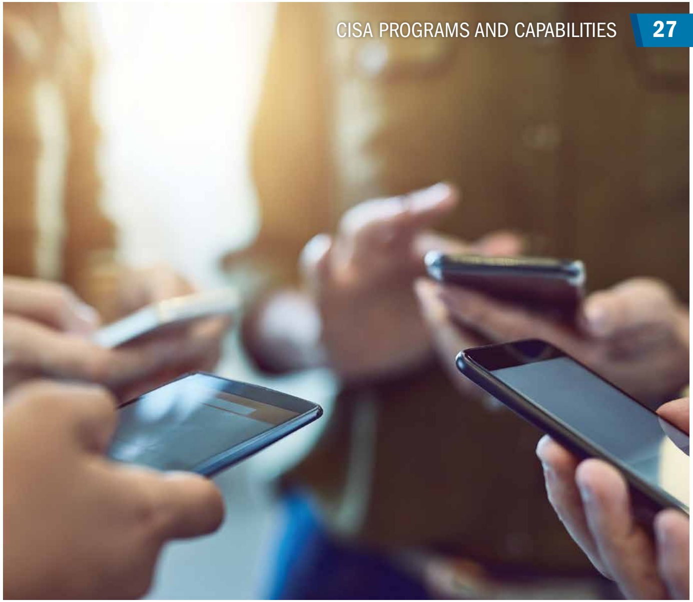
National Council of Statewide Interoperability Coordinators (NCSWIC) supports coordinators from the 56 states and territories with products and services to help them leverage their relationships, professional knowledge, and experience with other public safety partners involved in interoperable communications at all levels of government.

CISA’s **Emergency Communications Preparedness Center (ECPC)** is the federal interagency focal point for interoperable and operable communications coordination. Its members represent the federal government's broad role in emergency communications, including regulation, policy, operations, grants, and technical assistance. The ECPC is a clearinghouse for sharing intergovernmental information on emergency communications.

Priority Telecommunications Services

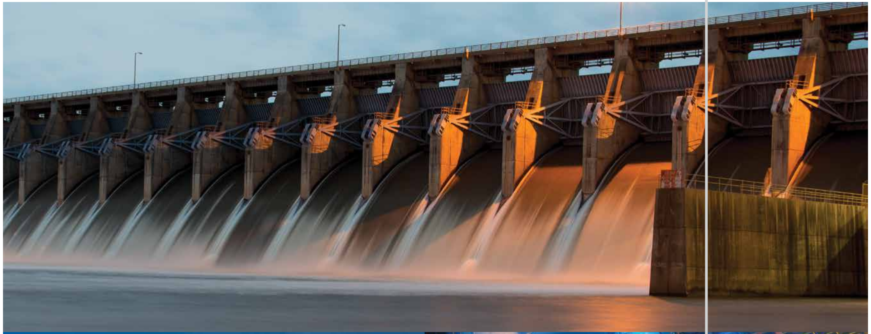
Priority Telecommunications Services provides National Security and Emergency Preparedness (NS/EP) communications under all circumstances, when network congestion or damage renders conventional communications ineffective. CISA manages four programs supporting restoration, and works to ensure all DHS programs continue to support NS/EP communications.

- **Government Emergency Telecommunications Service (GETS)** gives users end-to-end priority on the landline network, historically offering users more than a 95th percentile call completion rate during periods of network congestion. As of February 4, 2019, GETS is offered to more than 375,728 users.
- **Wireless Priority Service** complements GETS, providing users with priority communication over wireless networks and offering users more than a 90 percent call completion rate during higher call volumes. As of February 4, 2019, it is offered to more than 219,355 users.
- **Telecommunications Service Priority** program authorizes NS/EP organizations to receive priority repair and installation of vital voice and data circuits and other telecommunications services, letting telecommunications carriers prioritize restoration, recovery and reconstitution of critical circuits and voice capabilities following a disaster.
- **Next Generation Network Priority Services** is a DHS acquisition program that enables users to obtain priority voice, data, and video communications as the communications networks evolve. CISA leads development of priority services for voice over Internet Protocol-based networks and plans for data and video priority.



Interoperable Communications Technical Assistance Program

CISA's **Interoperable Communications Technical Assistance Program** provides all 56 states and territories with training tools and onsite technical assistance at no cost to advance public safety interoperable communications capabilities. CISA also has emergency communications coordinators in the regions to strengthen emergency communications and response capabilities.



OUR ROLE IN INFRASTRUCTURE SECURITY

CISA is responsible for helping safeguard the Nation's critical infrastructure sectors from physical threats and vulnerabilities. CISA leads the coordinated national effort to manage physical risks to critical infrastructure and collaborates across government and private sector stakeholders that own or operate the majority of critical infrastructure in the Nation.

CISA gathers and manages vital physical information on the Nation's critical infrastructure to help ensure needed infrastructure data is available to homeland security partners, identifying information sources and developing applications to use and analyze critical infrastructure data.

Sector-Specific Agency Responsibilities

CISA is the Sector-Specific Agency (SSA) for 8 of the 16 critical infrastructure sectors, and the Election Infrastructure Subsector under the Government Facilities Sector, which has CISA and the General Services Administration as co-SSAs.

CISA SSA Sectors:

- Chemical
- Commercial Facilities
- Communications
- Critical Manufacturing
- Dams
- Emergency Services
- Information Technology
- Nuclear Reactors, Materials & Waste

Each sector has unique characteristics, operating models, and risk profiles. As their SSA, CISA brings its specific knowledge and expertise to individual sectors and serves as a day-to-day federal interface for the dynamic prioritization, collaboration, and coordination of sector-specific and cross-sector activities.

Chemical Facility Anti-Terrorism Standards Program

The Chemical Facility Anti-Terrorism Standards Program (CFATS) focuses on security at high-risk chemical facilities. CISA works with facilities to ensure they have security measures in place to reduce the risks associated with certain hazardous chemicals and prevent them from being exploited in a terrorist attack.

Assessments and Advisors

CISA provides **cybersecurity and physical risk and vulnerability assessments and technical assistance** to identify operational risks and analyze data to help stakeholders secure networks and facilities, and manage risk. Assessments can determine how susceptible organizations are to phishing attacks, or reveal network vulnerabilities. Our assessments teams can also conduct on-request, remote penetration testing of stakeholders' data repositories and online-accessible assets, such as voter registration databases and web portals.

CISA conducts specialized field **security and resilience assessments** to identify vulnerabilities, interdependencies, capabilities, and cascading effects of impacts on the Nation's critical infrastructure. Assessments span facilities, systems, and regional networks of interconnected infrastructure across all sectors.

Cybersecurity and protective security advisors work with FSLTT government and private sector stakeholders to protect critical infrastructure by identifying and evaluating what is at risk and how to protect it. Advisors conduct assessments and perform outreach activities.

Bombing Prevention

CISA leads efforts to implement the **National Policy for Countering Improvised Explosive Devices** and enhance the Nation's ability to prevent, protect against, respond to, and mitigate the use of explosives against critical infrastructure; the private sector; and federal, state, local, tribal, and territorial (FSLTT) entities.

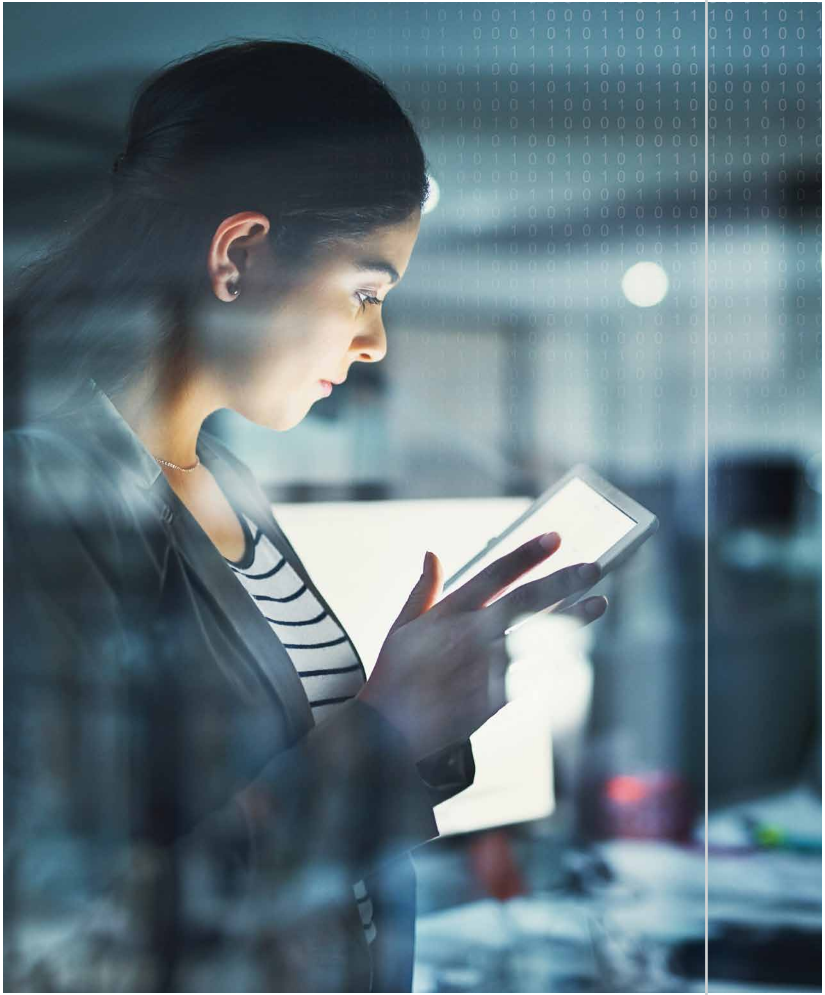
To reduce physical risk to critical infrastructure, CISA develops and delivers a diverse curriculum of training and awareness products on bombing prevention to build nationwide counter-IED core capabilities and enhance awareness of terrorist threats. CISA courses educate FSLTT participants, critical infrastructure owners, operators, and security staff on strategies to prevent, protect against, respond to, and mitigate bombing incidents.

CISA also offers the **Bomb-Making Materials Awareness Program (BMAP)**, a national outreach initiative to promote private sector point-of-sale awareness and suspicious activity reporting to prevent misuse of common household items as explosive precursor chemicals and IEDs components.

CISA's **Multi-Jurisdiction Improvised Explosive Device Security Planning (MJIEDSP) Program** is a systematic process that fuses counter-IED capability analysis, training, and planning to enhance urban area IED prevention, protection, mitigation, and response capabilities. CISA works closely with communities to provide expertise on planning and operational requirements for IED incident.

The **Technical Resource for Incident Prevention (TRIPwire)** is CISA's online, collaborative information and resource-sharing portal for the Nation's security and emergency services professionals across the FSLTT sectors to increase awareness of evolving IED tactics, techniques, and procedures as well as incident lessons learned and counter-IED preparedness information.

CISA's **National Counter-IED Capabilities Analysis Database (NCCAD)** assessment program is the single, authoritative data source on counter-IED capabilities and readiness throughout the United States. NCCAD uses a consistent and repeatable analytical methodology to assess and analyze the counter-IED capabilities of bomb squads, explosives detection canine teams, public safety dive teams, and special weapons and tactics teams.



INCREASING SECURITY AWARENESS

CISA sponsors a wide range of educational information. Key initiatives and partnerships include:

Stop.Think.Connect™ is a national public awareness campaign aimed at increasing the understanding of cyber threats and empowering Americans to be safer and more secure online.

National Cybersecurity Awareness Month, recognized annually in October, is a collaborative effort between DHS and public and private partners to raise awareness on the importance of cybersecurity.

Critical Infrastructure Security and Resilience Month, observed annually in November, builds awareness and appreciation of the importance of critical infrastructure and reaffirms the nationwide commitment to keep our critical infrastructure and our communities safe and secure.

"If You See Something, Say Something®" is a national campaign to raise awareness of the indicators of terrorism and terrorism-related crime, and importance of reporting suspicious activity to state and local law enforcement.

What You Can Do When There Is a Bomb Threat educates the public on steps that citizens should take in the event of a bomb threat.

Securing Soft Targets and Crowded Places

CISA is **prioritizing soft target and crowded places security**. The government, law enforcement, owners and operators of public venues and events, and the public all share responsibility for securing soft targets and crowded places. Together, CISA and its partners have the power to stop attacks before they occur by investing in security, sharing information, enhancing preparedness, and staying vigilant. While not every attack may be prevented, many attacks can be prevented from succeeding through focused security and preparedness efforts.

CISA has developed programs and resources for public venue owners and others to use to help increase their security. These include active shooter preparedness training and exercises, bombing prevention programs, commercial facilities best practices guides, and our Hometown Security Initiative. CISA's soft target security resource guide provides an easy reference for the range of trainings, tools, and other resources that are available.

CISA is leading a cultural shift in which:

- Enhanced security is seen as good business and worthy of investment and public support.
- Facility owners, individual and communities have an understanding of the threats and their roles in helping to prevent attacks.
- Communities and individuals feel empowered to be part of the solution, and know how to identify and report or avert a threat.

Hometown Security

CISA is committed to working in partnership with local governments and venue owners to enhance security and reduce risk. CISA fosters collaboration between the private and public sectors to secure even the most vulnerable parts of society, such as K-12 schools, institutes of higher education, houses of worship, and special events. CISA encourages businesses to apply the four tenets of the Hometown Security Initiative—**Connect**, **Plan**, **Train**, and **Report**—to help enhance their safety and security posture. Applying these steps in advance of an incident or attack can help better prepare community members to think proactively about the role they play in the safety and security of their businesses and communities.

CONNECT WITH US

cisa.gov

Report Incidents, Phishing, Malware, or Vulnerabilities

(888) 282-0870 | info@us-cert.gov
us-cert.gov/report

NCCIC Resources

(888) 282-0870 | ncciccustomerservice@hq.dhs.gov

Twitter

@cisagov | @cyber | @uscert_gov

LinkedIn

linkedin.com/company/cybersecurity-and-infrastructure-security-agency

U.S. DEPARTMENT OF HOMELAND SECURITY

CISA
CYBER+INFRASTRUCTURE