



# Cybersecurity and Infrastructure Security Agency (CISA)

---

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating with industry to build more secure and resilient infrastructure for the future. 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.

## WHAT WE DO

CISA is responsible for protecting the Nation's critical infrastructure from physical and cyber threats. This mission requires effective coordination and collaboration among a broad spectrum of government and private sector organizations.

### **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; Information and Communication Technologies Supply Chain Risk Management Task Force; Tri-Sector Executive Working Group; and the Pipeline Cybersecurity Initiative.

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 CISA's 24/7 cyber situational awareness, incident response, and management National Cybersecurity & Communications Integration Center (NCCIC). CISA 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.



---

## 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.



---

## OUR ROLE IN INFRASTRUCTURE SECURITY

CISA is responsible for helping safeguard the Nation's critical infrastructure sectors from threats and vulnerabilities, including security of soft targets and crowded places. As the physical and cyber worlds converge, CISA leverages an integrated cyber-physical approach to security. CISA coordinates the 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.

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.

*For more information visit [www.cisa.gov](http://www.cisa.gov)*