



Cybersecurity and Infrastructure Security Agency

On November 16, 2018, President Trump signed into law the Cybersecurity and Infrastructure Security Agency Act of 2018. This landmark legislation elevates the mission of the former National Protection and Programs Directorate (NPPD) within DHS and establishes the Cybersecurity and Infrastructure Security Agency (CISA).

- CISA leads the national effort to *defend* critical infrastructure against the threats of *today*, while working with partners across all levels of government and in the private sector to *secure* against the evolving risks of *tomorrow*.
- The name CISA brings recognition to the work being done, improving its ability to engage with partners and stakeholders, and recruit top cybersecurity talent.



What Does CISA 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.

Proactive Cyber Protection:

- CISA's National Cybersecurity and Communications Integration Center (NCCIC) provides 24x7 cyber situational awareness, analysis, incident response and cyber defense capabilities to the Federal government; state, local, tribal and territorial governments; the private sector and international partners.
- CISA provides cybersecurity tools, incident response services and assessment capabilities to safeguard the '.gov' networks that support the essential operations of partner departments and agencies.

Infrastructure Resilience:

- CISA coordinates security and resilience efforts using trusted partnerships across the private and public sectors, and delivers training, technical assistance, and assessments to federal stakeholders as well as to infrastructure owners and operators nationwide.
- CISA provides consolidated all-hazards risk analysis for U.S. critical infrastructure through the National Risk Management Center.

Emergency Communications:

- CISA enhances public safety interoperable communications at all levels of government, providing training, coordination, tools and guidance to help partners across the country develop their emergency communications capabilities.
- Working with stakeholders across the country, CISA conducts extensive, nationwide outreach to support and promote the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters.



Organizational Changes Related to the CISA Act

The CISA Act establishes three divisions in the new agency: Cybersecurity, Infrastructure Security and Emergency Communications.

- The Act transfers the Office of Biometrics Identity Management (OBIM) to DHS's Management Directorate. Placement within the DHS Headquarters supports expanded collaboration and ensures OBIM's capabilities are available across the DHS enterprise and the interagency.
- The bill provides the Secretary of Homeland Security the flexibility to determine an alignment of the Federal Protective Service (FPS) that best supports its critical role of protecting federal employees and securing federal facilities across the nation and territories.