

U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Glenn Moore

Protective Security Advisor

Oklahoma District



CISA
CYBER+INFRASTRUCTURE

The Significance of Critical Infrastructure

Critical infrastructure refers to the assets, systems, and networks, whether physical or cyber, so vital to the Nation that their incapacitation or destruction would have a debilitating effect on **national security, the economy, public health or safety, and our way of life.**



CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY



Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient
infrastructure for the
American people.

MISSION

Lead the Nation's efforts to
understand and manage risk to our
critical infrastructure.

Who We Are

CISA works with public sector, private sector, and government partners to share information, build greater trust, and lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.



FEDERAL NETWORK
PROTECTION



PROACTIVE CYBER
PROTECTION



INFRASTRUCTURE
RESILIENCE &
FIELD OPERATIONS



EMERGENCY
COMMUNICATIONS



CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Infrastructure Security Division

Infrastructure Security Division leads the coordinated effort to reduce the risks posed to our critical infrastructure by acts of terrorism. Infrastructure Security Division also leads the nation's preparedness efforts for these attacks.

MISSION PRIORITIES:



Securing critical infrastructure from terrorist attacks.



Advancing integrated cyber and physical risk management.



Developing products and mitigation measures, with a focus on the cascading effects across sectors and lifeline functions.



Promoting security and resilience in infrastructure planning and investment.



Managing regulatory compliance of securing chemical facilities through the Chemical Facility Anti-Terrorism Standards program.



CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity Division

Cybersecurity Division assures the security, resilience, and reliability of the nation's cyber and telecommunications systems.

MISSION PRIORITIES:



Enhance the security of the information and information systems of the federal civilian executive branch departments and agencies.



Collaborate with the private sector (the dot-com domain) to increase the security of critical networks.



Work with Federal, State, Local, Tribal, and Territorial stakeholders to support interoperable communications. Provide priority telecommunications services over commercial networks to enable national security and emergency preparedness personnel to communicate during congestion scenarios across the nation.



Apply unique analytic perspectives, ensure shared situational awareness, and coordinate synchronized response efforts while still protecting American's privacy in cybersecurity and communications.



CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Emergency Communications Division

The Emergency Communications Division 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 ECPC governance bodies.



CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

DHS National Risk Management Center

The Center will be a government and industry partnership to coordinate risk management efforts, initially by leading a series of activities that will help define what is truly critical; create the frameworks by which government and industry collectively manage risk; and initiate specific cross-sector activities to address known threats.

MISSION PRIORITIES:



Identify, assess, and prioritize risks to national critical functions



Collaborate on the development of risk management strategies and approaches to manage risks to national critical functions



Coordinate integrated cross-sector risk management activities



CISA
CYBER+INFRASTRUCTURE