

Cybersecurity

- **Mission Area:** Protection
- **Description:** Protect (and if needed, restore) electronic communications systems, information, and services from damage, unauthorized use, and exploitation.

Intelligence and Information Sharing

- **Mission Areas:** Prevention, Protection
- **Description:** Provide timely, accurate, and actionable information resulting from the planning, direction, collection, exploitation, processing, analysis, production, dissemination, evaluation, and feedback of available information concerning physical and cyber threats to the United States, its people, property, or interests; the development, proliferation, or use of WMDs; or any other matter bearing on U.S. national or homeland security by local, state, tribal, territorial, Federal, and other stakeholders. Information sharing is the ability to exchange intelligence, information, data, or knowledge among government or private sector entities, as appropriate.

Public Information and Warning

- **Mission Areas:** All
- **Description:** Deliver coordinated, prompt, reliable, and actionable information to the whole community through the use of clear, consistent, accessible, and culturally and linguistically appropriate methods to effectively relay information regarding any threat or hazard, as well as the actions being taken and the assistance being made available, as appropriate.

Operational Coordination

- **Mission Areas:** All
- **Description:** Establish and maintain a unified and coordinated operational structure and process that appropriately integrates all critical stakeholders and supports the execution of core capabilities.

Operational Communications

- **Mission Area:** Response
- **Description:** Ensure the capacity for timely communications in support of security, situational awareness, and operations by any and all means Core Capabilities available, among and between affected communities in the impact area and all response forces.