Overview

U.S. consumers and businesses are rapidly adopting new communications products and services that are increasingly mobile, data-centric, and bandwidth-intensive. These trends are driving innovations in areas like 5G Mobility, Internet-of-Things (IoT), and Cloud Computing. These advanced capabilities, along with Next Generation 911, will yield benefits for public safety. Unfortunately, government agencies face budget constraints that often make it difficult to adopt new technologies. As a result, they are forced to use and maintain aging equipment that imposes significant risks including operational malfunctions, vulnerability to hacking, and service outages.

Policy Goal: Advocate for State and Federal policies that promote widespread adoption of advanced technologies that improve emergency response and increase public safety.

iCERT seeks to achieve this goal by supporting policies that address funding challenges, create incentives to invest in new technology, and promote an open, interoperable environment that enables public safety agencies to fully leverage technological innovation.

1. Increase Technology Investments. iCERT supports increased investments in advanced communications technologies that will improve network resiliency and enable public safety agencies to leverage data to improve situational awareness and emergency response.

2. Establish Sustainable Funding Policies. iCERT supports policies that ensure a stable and sufficient level of funding for emergency response systems including direct Federal funding for NG911 systems and services.

3. Conform to Open Standards. iCERT supports the utilization of open standards for all components of the emergency response ecosystem and works with its member companies to promote standards compliance.

4. Promote Interoperability. iCERT supports the utilization of standards, best practices, and policies that promote interoperability and effective data sharing across the emergency response ecosystem.

5. Protect Against Cyber Threats. iCERT supports public policies that anticipate cyber-based threats and promote effective protection of public safety networks, services, equipment, applications, and information.