



EMERGENCY COMMUNICATIONS DIVISION NATIONWIDE INTEROPERABILITY SERVICES

EMERGING & ADVANCED TECHNOLOGY BRANCH FACTSHEET



BACKGROUND

For those who appreciate technology and look to embrace it, the opportunities for public safety communications are almost limitless. Citizens today are equipped with the latest technology. They expect their public safety providers to be equipped with the same capabilities and be prepared to take advantage of the data they can provide from smartphones and Internet of Things (IoT) devices. However, public safety must be cautious and deliberate in their approach to adoption. The public safety operating environment is unique and the consequences of adopting something “less than ideal” may be the difference between life and death. New or enhanced technology may not be appropriate for every public safety organization’s mission, nor can new or advanced technology be adopted without consideration of impacts to governance, standard operating procedures, use, training, and exercises.

PURPOSE

Emerging & Advanced Technology (E-AT) Branch’s mission is to explore and assess the impact of emerging and advanced technology on the operability, interoperability, cybersecurity, and resiliency of public safety communications. E-AT addresses technology-based challenges and requirements in collaboration with partners across the Emergency Communications Ecosystem.



EMERGING TECHNOLOGY

The rapid rate of technology advancement continues to outpace the public safety community’s acquisition cycle

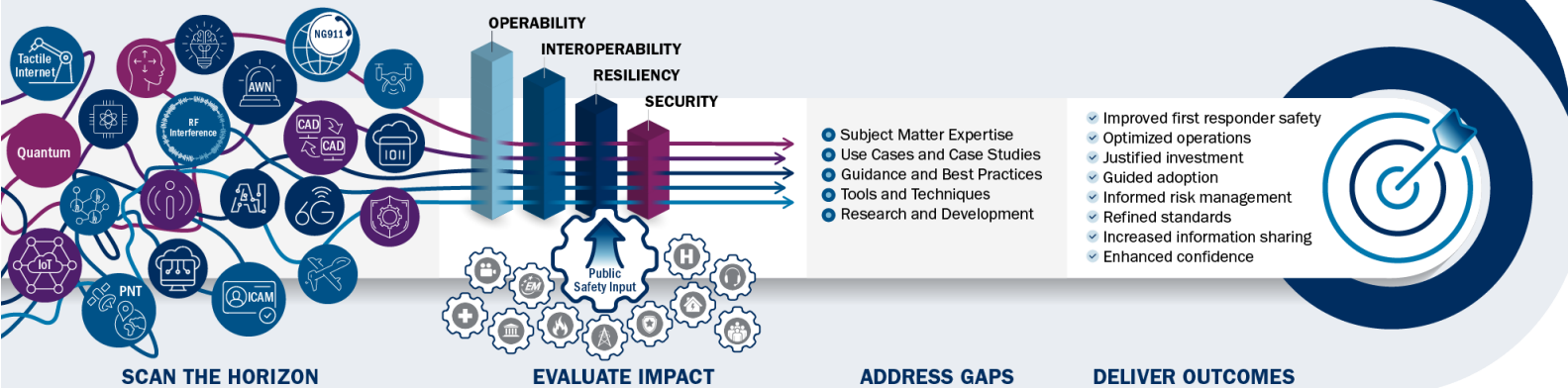
New technologies have the potential to be expensive and disrupt mission-critical operations, but emerging technologies can offer advanced capabilities to enhance command and control and situational awareness for emergency responders.

E-AT helps the public safety community harness the promise of technology.

E-AT BRANCH PROCESS

E-AT **scans the horizon** for technologies that may impact public safety communications, such as artificial intelligence (AI), cloud, IoT, and quantum communications. In conjunction with public safety practitioners, subject matter experts **evaluate the impact** of technology on the operability, interoperability, cybersecurity, and resiliency of public safety communications. Solutions often must be tailored to public safety’s unique requirements. Off-the-shelf or commercial-oriented solutions may not adequately protect systems and may limit interoperability and mission-critical capabilities. **Gaps are addressed** by various methods, including information sharing by early adopters and the creation of best practices, techniques, and tools to guide adoption. In some cases, the gaps require investment in research and development in conjunction with industry, academia, the public safety community, and other government partners.

CISA ECD NIS EMERGING & ADVANCED TECHNOLOGY BRANCH PROCESS



PRODUCTS AND RESOURCES



cisa.gov/public-safety-cybersecurity

Public Safety Cybersecurity Website: This page compiles resources developed by CISA for public safety communications practitioners, as well as anyone looking to gain further knowledge about cybersecurity for public safety communications. This page provides resources to public safety practitioners regarding common questions related to public safety cybersecurity.



Public Safety Cyber Resiliency Toolkit: CISA developed this interactive graphic to assist public safety agencies and others responsible for communications networks in evaluating current resiliency capabilities, identifying ways to improve resiliency, and developing plans for mitigating the effects of potential resiliency threats. Topic-specific systems-based resources appear as building shapes (blue); threats are cloud shapes (red). Clicking on a topic reveals a list of resources accompanied by a brief description.



cisa.gov/communications-resiliency

COMMUNITY COLLABORATION

E-AT addresses technology-based challenges and requirements in collaboration with partners in the Emergency Communications Ecosystem:

- Industry
- Associations
- Academia
- Policy, Research, and Development Entities
- Standards Development Organizations (SDOs)
- Non-Governmental Organizations (NGOs)
 - Voluntary Organizations Active in Disasters (VOADs)
 - Non-profit Organizations
- Other Government Partners

E-AT identifies technology-based requirements and gaps from throughout the public safety community and actively works to resolve them.

CONTACT INFORMATION

David J. Nolan
 Emerging & Advanced Technology Branch Chief
 Cybersecurity and Infrastructure Security Agency
 U.S. Department of Homeland Security
david.nolan@mail.cisa.dhs.gov

BENEFIT NOW!

| | |
|--|--|
|  Review Guidance |  Ask Questions |
|  Share requirements and gaps |  Participate in research & development efforts |

CONTACT: publicsafetycomms@mail.cisa.dhs.gov

For more information or additional help, contact ecd@mail.cisa.dhs.gov or visit cisa.gov/topics/emergency-communications.