





The International Forum to Advance First Responder Innovation

Statement of Objectives (SOO) for Technologies Related to: "The Ability to Maintain Interoperable Communications with Responders in Any Environmental Conditions"

December 2018

International Forum to Advance
FIRST RESPONDER INNOVATION

Sponsorship:
Effort sponsored in whole or in part by the Department of Homeland Security (DHS) Science and Technology Directorate (S&T) and the Air Force Research Laboratory (AFRL), under Memorandum of Understanding/Partnership Intermediary Agreement No. FA8650-09-3-9400. The U.S. government is authorized to reproduce and distribute reprints for governmental purposes notwithstanding any copyright notation thereon.

Endorsement:
This document has been checked for accuracy by the International Forum to Advance First Responder Innovation (IFAFRI) and accords with its aim to inform and guide industry and provide unbiased information on first responder technologies.

International Forum to Advance
FIRST RESPONDER INNOVATION

Statement of Objectives (SOO) for Technologies Related to: **"The ability to maintain interoperable communications with responders in any environmental conditions"**

Background

The International Forum to Advance First Responder Innovation (IFAFRI) is an organization of international government leaders from 13 countries and the European Commission, focused on enhancing and expanding the development of new technology for first responders worldwide.[1] IFAFRI does this by:

1. Working with the global first responder community to define a list of common, high priority capability gaps;
2. Providing a platform for international collaboration on innovative research and development (R&D) initiatives and solutions;
3. Characterizing global first responder markets to inform and guide industry and academia to develop and produce innovative technology solutions at affordable prices; and
4. Providing information about relevant and available first responder technologies to the first responder community.

To arrive at a set of *Common Global Capability Gaps*, IFAFRI members conducted analyses of first responder capability gaps in their respective countries. IFAFRI then assessed those gaps to identify those that were common across multiple member nations. The gaps with the highest commonality amongst member nations were presented to all IFAFRI members for consensus. IFAFRI has reached consensus on six first responder capability gaps:

- The ability to know the location of responders and their proximity to risks and hazards in real time;
- The ability to detect, monitor, and analyze passive and active threats and hazards at incident scenes in real time;
- The ability to rapidly identify hazardous agents and contaminants; and
- The ability to incorporate information from multiple and nontraditional sources into incident command operations.

[1] For the purpose of this document, the term "first responder" refers to those individuals who, in the early stages of an incident, are responsible for the protection and preservation of life, property, evidence and the environment, including fire service, law enforcement and emergency medical services.

- The ability to maintain interoperable communications with responders in any environmental conditions.
- The ability to obtain critical information remotely about the extent, perimeter, or interior of the incident.

IFAFRI is publishing this Statement of Objectives (SOO) to provide a technical overview of the global first responder need and to direct researchers who may be interested in pursuing development of a solution. IFAFRI will assist with facilitating interactions between first responders and organizations pursuing development toward this capability gap. This particular SOO is focused on the 5th bulleted capability gap identified above:

"The ability to maintain interoperable communications with responders in any environmental conditions"

This capability gap is described as follows: "[s]ome environments are conducive to sending and receiving communications, however, others pose significant challenges. For example, communications can be difficult inside buildings, tunnels or underground spaces. Communications may also be degraded if equipment and infrastructure have been damaged by the incident or overwhelmed by call volume. Regardless of the operating environment, emergency responders must be able to seamlessly send or receive orders and information, provide tactical updates, request help and receive warnings about hazardous or changing conditions. Therefore, the need to ensure verbal and digital communication through all physical and electronic environments is essential."[2]

General Description of Operational Capability

The ability to communicate with responders in any environmental condition is crucial because communications enable safe and effective incident response. Coordinating the efforts of responders, commanders, emergency managers, civic leaders, and the public depends on timely, reliable and effective modes of communication. During incident response operations, communications may involve a significant number of responders, jurisdictions and systems across a vast geographic area. Deficiencies in communications capacity, interoperability or infrastructure can strain or overwhelm steady-state capabilities; all of these deficiencies can be exacerbated during larger incidents. Responders' ability to communicate with each other has a significant impact on operational efficiency and safety. Message transmission or clarity can be substantially reduced when operating in certain environments, particularly inside buildings, tunnels, underground spaces or over long distances.[3]

Despite a high level of public and private funding to advance technology for interoperable communications, the lack thereof continues to remain a significant factor hindering emergency response operations across IFAFRI member nations. Elements such as country size and degree of

[2] *Project Responder 4: 2014 National Technology Plan for Emergency Response to Catastrophic Incidents*, p. 58, https://www.dhs.gov/sites/default/files/publications/Project%20Responder%204_1.pdf

[3] *Project Responder 4: 2014 National Technology Plan for Emergency Response to Catastrophic Incidents*, p. 23, https://www.dhs.gov/sites/default/files/publications/Project%20Responder%204_1.pdf

centralization of response functions impact on this capability. However, a comprehensive, affordable solution is not yet available.

Many responders currently use push-to-talk land mobile radio (LMR) devices, many which are only capable of transmitting and receiving voice communications on specific frequencies. Commercially available smart phones provide additional access to video and data. However, most are not ruggedized to withstand austere environments on the incident scene. In addition, existing networks are often overwhelmed by the volume of message traffic and incident operations often hamper the ability to communicate intelligibly. Responders report the need for devices that allow clear, successful, and secure bi-directional communications, and that provide data needed for situational awareness and the conduct of incident operations.

Addressing this capability gap may involve a system of devices, network software, and infrastructure equipment that can provide interoperable communications during incident response operations.

Existing First Responder Gear

Current capabilities to communicate on the incident scene include:

- Push-to-talk land mobile radio (LMR) systems;
- Smart cellular phones;
- Satellite phones;
- Tablets and other mobile devices (vehicle-mounted and man-portable);
- Radio frequency (RF)-based communications (e.g., very high frequency (VHF), ultra high frequency (UHF));
- Television signal datacasting;
- Deployable/mobile cell sites (e.g., cell-on-wheels (COWs), cell-on-light-trucks (COLTs));
- Mesh networks;
- Interoperability gateway devices;
- Repeater networks;
- Dedicated public safety broadband networks; and
- Face-to-face communications.

Operational Environment

The following list provides examples of operational environments that *may* be encountered by first responders on a daily basis. Tools and systems developed to address this capability gap should be able to be used during routine operations.

- Single and multi-level buildings;
- Structures of varied construction materials (e.g., steel, concrete, wood frame, masonry, synthetic materials);
- Collapsed or threatened buildings;
- Confined spaces;
- Subterranean and underground facilities;
- Wooded areas with dense vegetation;
- Rugged outdoor terrain;

- Areas with limited or no cellular and/or radio connectivity;
- Extreme high and low temperatures and humidity;
- Wet conditions;
- Thermal radiation[4];
- Direct flame contact or exposure;
- Excessively noisy and smoky conditions in outdoor, indoor and/or subterranean areas;
- Lack of line-of-sight vision between commanders and deployed personnel; and
- Underwater and maritime environments.

Target Objectives

1. Interoperable communication of voice, audio, video and data among authorized responders and command, regardless of agency, service, and/or jurisdiction;
2. Communication through all environments, including inside buildings, underground, and through physical barriers; and
3. Disaster-resilient or rapidly-deployable communications systems to support incident operations regardless of location or incident effects.

The following section provides responder-identified requirements for potential solutions. It is understood that not all requirements may be currently technically feasible. Responders would prefer incremental, continuous advancement of solutions instead of waiting for equipment that meets all of the requirements at the same time. As such, these requirements do not represent a minimum set of requirements that must be met before new tools, devices, platforms or systems can be released.

Device Requirements

Communications devices should provide voice, text, image, and video communications. Potential solutions should:

- Transmit and receive regardless of physical environment:
  - Voice communications;
  - Data communications (e.g., text, documents, sensor data, images, video);
- Record and transmit:
  - Streaming audio;
  - Streaming video;
- Associate devices with specific users (e.g., persons, roles);
- Allow proximity-based communications;
- Allow device-to-device (D2D) links, forming a chain of nodes to create or extend a network;
- Allow D2D synchronization of data;
- Minimize mouth-to-ear (M2E) latency;

[4] Thermal radiation, one of three methods of heat transfer, causes increase in temperature from electromagnetic waves. Thermal radiation can cause flashover within a room, causing all contents to raise to their ignition temperature and engulf the room from floor to ceiling. Thermal radiation can also increase the temperature of firefighter garments, damaging the gear and causing potential harm to the responder.

- Enhance fidelity of voice communication and incorporate mechanisms to ensure that spoken communication is intelligible;
- Selectively neutralize the effects of ambient sound, regardless of proximity, decibel, or frequency;
- Provide multi-sensory (e.g., visual, haptic) communications;
- Integrate or be compatible with personal protective equipment (PPE) and/or provide hands free functionality;
- Convert voice to text;
- Convert text to voice;
- Translate among languages;
- Assign channels automatically, based on role and user;
- Allow authorized over-the-air programming of new channels; and
- Communicate with other public safety devices, regardless of frequency or waveform.

Network Requirements

The communications network relies on software to encode, transmit, and decode voice, audio, video, and data from the sender to the intended destination. Potential solutions should:

- Support all required devices for communication of:
    - Voice;
    - Audio;
    - Video;
    - Images;
    - Text;
    - Computer-aided dispatch (CAD) data;
    - Sensor (e.g., chemical, radiological) data;
    - Geographic information system (GIS) data;
    - Application data;
    - Other incident-related data (e.g., building blueprints, model outputs);
- Provide continuous connectivity to all devices on the incident scene;
- Integrate with existing LMR systems that may be using multiple frequency bands;
- Allow multiple independent networks to interoperate without impact on user;
- Share location and RF transmission parameters to avoid or minimize interference;
- Allow D2D communications when user equipment is in proximity without reliance on network connectivity;
- Allow authorized users to elevate or reduce the priority of operations or user transmissions;
- Allow preemption for emergency message traffic and critical alerts (e.g., Personal Alert Safety System (PASS));
- Allow user-configurable prioritization of users or devices;
- Automate data routing, storage, and processing;
- Deployable systems should be ad-hoc, reliable, self-forming, and self-healing;
- Self-organize to maximize coverage area and resource distribution;

- Support "edge" computing to identify, ingest, process, and transmit most relevant data[5];
- Continuously assess network health and reliability; and
- Report on network health and availability.

Infrastructure Requirements

Communications infrastructure (permanent and temporary) includes transmitters, servers, gateways, routers, etc. These hardware components are necessary to encode and transmit the voice, audio, data, and video essential for incident response. Potential solutions should:

- Utilize the existing infrastructure to enhance or amplify signals or clarity of communications;
- Be scalable based on incident size and scope;
- Be rapidly deployable to meet mission requirements; and
- Be deployable in remote environments and rugged terrain.

Security Requirements

It is critical to ensure the authenticity, integrity, and confidentiality of communications on the incident scene. Potential solutions should:

- Encrypt voice, audio, video and data prior to transmission[6];
- Offer provision access based on user or device;
- Incorporate identity, credential, and access management (ICAM) functionality;
- ICAM should function in online and offline modes;
- Dynamically authenticate users on network;
- Allow agency to control access to data;
- Be resistant to jamming and other denial of service attacks; and
- Be compliant with internationally-recognized standards for network security and identity management.

Transmission Requirements

Potential solutions should provide real-time transmission of voice, audio, video and data among responders, command, dispatch, and other intended destinations. Potential solutions should:

- Transmit voice, audio, video and data:
    - To the intended destination;
    - In real time;
    - With metadata indication of source (e.g., user, device, role); and
    - With metadata indication of GIS coordinates;

[5] Edge computing allows processing of data to be conducted by devices instead of at centralized nodes.
[6] Responders recognize that it may not be possible to encrypt solutions that rely on analog technologies.

- Function in a communications-degraded environment:
    - Securely cache data intended for recipients when connection to a communication network cannot be made;
    - Securely transmit cached data to recipients when connection to a communications network is restored without affecting live data streaming;
- Store voice, audio, video and data traffic for post-incident analysis;
- Prioritize transmission of responder safety-related data (e.g., distress, hazard proximity) and related images and video to agency-configured destination; and
- Comply with exchange standards for data transmission (e.g., National Information Exchange Model (NIEM)).

Power Source Requirements

Potential solutions should use a non-proprietary power source that provides sufficient power for the duration of the incident response and recovery operations. Potential solutions should:

- Be able to be powered using multiple sources including those on the incident scene;
- Be self-optimizing to reduce power consumption of communications equipment;
- Be able to replenish power supply using non-proprietary technology;
- Utilize an easy-to-replenish power source;
- Device power source should:
    - Operate for a minimum of 24 hours;
    - Be replaceable with gloved hands and wearing protective clothing in a manner that reduces the potential for erroneous installation without interruption to operations, to extend operational life;
- Be compatible with renewable or sustainable energy sources; and
- Incorporate power systems that can be safely and compliantly carried on commercial aircraft.

Maintenance Requirements

Potential solutions should be easy to operate, calibrate and maintain throughout the service life. Potential solutions should:

- Self-initialize in less than one minute;
- Be modular to allow for upgrade and replacement of components;
- Maintain backwards compatibility after upgrade;
- Be rated for a service life of no less than five years;
- Be designed to reduce the time to repair;
- Be designed to minimize skills needed for maintenance (e.g., calibration, cleaning);
- Perform automated periodic malware detection and cybersecurity screening of software and firmware components;
- Allow for remote maintenance;
- Allow for remote upgrades;
- Provide live notification of a fault; and
- Maintain a fault log.

Robustness Requirements

Potential solutions should operate within multiple environments (e.g., smoke, humidity, temperature extremes, precipitation). Potential solutions should:

- Operate at temperature ranges typical of international climate (e.g., -30 degrees C to 50 degrees C);[7,8]
- Operate at temperature ranges typical of response activities (e.g., -100 degrees C to 500 degrees C);[9,10]
- Be ruggedized;
- Resistant to effects of electromagnetic pulse (EMP);
- Function after immersion in water;[11]
- Function at humidity of 100%;
- Function properly after exposure for five minutes at a maximum thermal radiation threshold of 500 degrees C;
- Resist air pollutants, dust, smoke, ash and sand;[12]
- Match the laundry life of garment or textile if components are integrated into garments or textiles;
- Have recyclable components;
- Be easy to decontaminate;[13]
- Be non-degradable due to wear or hazard;
- Not cause injury to the user if damaged;
- Comply with existing federal and/or international standards and guidelines; and
- Function underwater.

Cost Requirements

Potential solutions should be designed to minimize price of system, consumables, training, and maintenance. Potential solutions should be priced to be affordable to all response agencies and should be designed for daily use.

---

[7] Average minimum temperature in Sweden was used to provide a minimum figure for international climate, https://www.weatheronline.co.uk/reports/climate/Sweden.htm

[8] Historic summer temperature in Phoenix, Arizona, was used to provide a maximum figure for international climate, http://www.12news.com/article/weather/heat/hottest-day-ever-122-and-other-cool-phoenix-is-really-hot-facts/448964915

[9] *NIST Technical Note 1474: Thermal Environment for Electronic Equipment Used by First Responders*, p. 7 http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=101375

[10] First responder participants of the SOO Validation Meeting (January 23-25, 2018, in Stockholm, Sweden) stated that operations may involve temperatures of -100 degrees C to 500 degrees C.

[11] Refer to IP68 of IEC 60529: Degrees of Protection Provided by Enclosures, https://webstore.iec.ch/publication/2452

[12] Refer to IP68 of IEC 60529: Degrees of Protection Provided by Enclosures, https://webstore.iec.ch/publication/2452

[13] Refer to NFPA 1841: Standard on Selection, Care, and Maintenance of Protective Ensembles for Structural Fire Fighting and Proximity Fire Fighting, https://www.nfpa.org/codes-and-standards/all-codes-and-standards/list-of-codes-and-standards/detail?code=1851

Additional Considerations

As in other research and development endeavors, additional considerations should be evaluated by organizations wishing to pursue innovation toward this gap:

- Detailed test and evaluation strategy for the viability of system(s);
- Transition strategy to guide the prototype(s) into commercialization;
- Specifications to guide the development of viable commercial system(s);
- Standards, guidelines, other legal requirements; and
- Stakeholder oversight/interaction, to ensure that the developed system meets the requirements identified by the first responder community.