





The International Forum to Advance First Responder Innovation

Statement of Objectives (SOO) for Technologies Related to: "The Ability to Incorporate Information from Multiple and Nontraditional Sources into Incident Command Operations"

July 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 Incorporate Information from Multiple and Nontraditional Sources into Incident Command Operations"**

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.

IFAFRI has reached consensus on four first responder capability gaps. These gaps represent the highest priority gaps common amongst the first responders represented by the IFAFRI member nations. These gaps are:

- 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 (for example, crowdsourcing and social media) into incident command operations.

To arrive at this initial set of *Common Global Capability Gaps*, IFAFRI participants conducted analyses of first responder capability gaps in their countries.

[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.

IFAFRI is publishing this Statement of Objectives (SOO) to provide a technical overview of the global first responder need and 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 fourth capability gap identified above:

"The ability to incorporate information from multiple and nontraditional sources into incident command operations"

This capability is described as the following: emergency managers and incident commanders "rely on multiple information inputs to make decisions. These inputs include field observations, sensor data, model outputs, images and video, media reports, databases and other sources. With advances in technology, responders are exploring ways to integrate these and other nontraditional sources of valuable data (for example, sensors attached to infrastructure, road cameras, social media data) into decision-making processes. Responders noted the increasing importance of information from nontraditional sources and the need to integrate these information streams into a common operating picture. Although responders see value in systems that could aggregate and analyze nontraditional information sources, they also emphasized the need to verify information. To be actionable, responders need to be confident that data has been validated and obtained from a verified source. At present, nontraditional data are not fully incorporated into incident command common operating pictures for decision-making."[2]

General Description of Operational Capability

There is a significant amount of data available to support incident command and response operations. Often responders are not able to access or use this data. Furthermore, when they are able to access the data, the amount can be overwhelming. During a public order incident (e.g., demonstration, riot), for example, responders would like to have real-time access to municipal and traffic cameras, closed-circuit television feeds from local businesses, social media posts, property ownership records, etc., that will allow them to conduct safer and more effective operations. Information needs differ depending on the type of incident; however, few responders have access to real-time actionable information while in the field.

There are multiple technical difficulties in collecting and integrating data needed by responders. However, the benefits of increased situational awareness and improved responder safety highlight the importance of developing this capability.

Social media presents novel sources of incident-related data that were unavailable only a few years ago. Within minutes of the start of an incident, participants and bystanders begin posting updates to their social media feeds. Much of this information could provide data that is relevant to help responders neutralize a threat, rescue trapped or injured victims, or investigate potential suspects. Responders would like to access this data in real time to support their operations.

Responders have stated that they would like access to public and private data sources. They would like this information seamlessly integrated into a common platform, allowing users to view

[2] *Project Responder 4: 2014 National Technology Plan for Emergency Response to Catastrophic Incidents*, p. 24, https://www.dhs.gov/sites/default/files/publications/Project%20Responder%204_1.pdf

selected data based on user preference. Validation of data sources is a priority to ensure responders are using accurate data; this is especially a concern for social media and other public data repositories.

Existing First Responder Gear

Current capabilities to integrate data feeds include:

- Access to data and applications (apps) via agency or personal smartphones or devices;
- Access to law enforcement and civic records via mobile data terminals located in vehicles;
- Commercially-available data integration and decision-support tools (limited availability due to cost); and
- State and jurisdiction-level data integration and visualization platforms (e.g., Virtual Alabama).[3]

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, to the extent possible, 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;
- Extremely confined spaces;
- Subterranean and underground facilities;
- Wooded areas with dense vegetation;
- Rugged outdoor terrain;
- Areas with limited or no cellular and/or radio connectivity;
- Events with large crowds or numbers of people present;
- Extreme high and low temperatures and humidity;
- Wet conditions;
- Thermal radiation;
- 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. Integrate data from public and private sources into incident command and response operations;
2. Incorporate and validate data; and
3. Display data based on user-configurable preferences and settings.

[3] Additional information on Virtual Alabama can be found at: https://virtual.alabama.gov/

The following section provides responder-identified requirements for potential solutions. 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.

Data Type Requirements

Potential solutions should access, integrate, transmit and display data identified by responders as necessary for incident response.[4] Potential solutions should:

- Ingest data in multiple file formats;
- Access, integrate, transmit and display:
    - Video feeds;
    - Still images;
    - Social media data;
    - Hazard sensor data;
    - Model predictions and forecasts;
    - Digital building blueprints (e.g., building information modeling (BIM));
    - Data from Internet of Things (IoT)-connected devices;
    - Public safety data sources (e.g., law enforcement record systems, license plate readers, computer-aided dispatch (CAD) data);
    - Public data feeds (e.g., traffic, school, municipal video feeds, property tax records);
    - Available private data feeds (e.g., cell phone records and triangulation, bank records);
    - Data from response-related repositories (e.g., Emergency Response Guidebook);[5]
    - Near real-time satellite imagery;
    - Virtual/augmented reality data sources;
- Allow user to easily include new data feeds into the system; and
- Allow user to easily remove data feeds from the system.

Visualization Requirements

Potential solutions should provide a visual display of incident data in real time. Potential solutions should:

- Allow display on common communications and computing devices (e.g., smartphones, tablets, laptops);
- Provide an intuitive graphical user interface (GUI);
- Display data in multiple formats (e.g., text, images);

[4] Data identified as necessary for incident response can include incident-specific data (e.g., protective action guidance) as well as other data not related to the response, but which is still important for decision-making (e.g., weather forecasts, land ownership records).

[5] The Emergency Response Guidebook contains an indexed list of dangerous goods, the general hazards those dangerous goods pose, and recommended safety precautions. Additional information can be found at: https://www.transportation.gov/briefing-room/dot-releases-new-emergency-response-guidebook

- Allow user to customize display settings (e.g., font, icons);
- Allow for the development of customized user profiles (e.g., tags, triggers, searches);
- Provide a 360-degree field of view; and
- Allow user to access first-person point of view video feeds in three dimensions.

Image and Video Feed Requirements

Potential solutions should access, integrate, transmit and display video and images in real time. Potential solutions should:

- Display public and private video feeds from multiple sources:
    - Live video feeds (e.g., body-worn cameras, social media feeds, surveillance camera.);
    - Previously-recorded video;
- Allow for real-time switching between video sources (e.g., to track a suspect as they move from one camera to another);
- Function with facial, object or behavior recognition systems or other biometric data sources;
- Allow user to:
    - Choose or toggle between video feeds and/or images;
    - Bookmark segments of a video feed;
    - Capture, store and tag segments of video;
    - Link image or video to other data sources;
    - Rewind and fast-forward;
- Provide an agency-defined buffer for bookmarked video;
- Automatically store live-streamed video;
- Provide single repository for video (i.e., prevent multiple copies in storage); and
- Encrypt or protect images and video feeds.

Data Usage Requirements

Potential solutions should access, integrate, transmit and display data from multiple data sources in real time. Potential solutions should:

- Disseminate data via role-based permissions;
- Allow prioritized retrieval of data;
- Allow queries of data as defined by agency policy and controls;
- Provide data filter feature;
- Utilize a classification schema to organize data;
- Incorporate metadata into classification schema;
- Allow user to compare data across time (historical and incident-specific);
- Provide user-defined triggers, warnings and alerts;
- Allow user to alter settings in real time;
- Provide confidence measurement to indicate accuracy and reliability of data source;
- Provide visual notification when accessed data feeds have been updated;
- Allow multiple users to access data simultaneously;
- Provide an output summary as defined by the user related to a specific incident;

- Allow the user to create customized reports;
- Convert incident-specific data into common file formats;
- Allow the creation of ad hoc groups to access data sources; and
- Comply with applicable privacy laws.

Data Analysis Requirements

Potential solutions should perform basic analysis using data from integrated sources. Potential solutions should:

- Perform data quality analysis (e.g., validation of data sources);
- Perform data analysis in real time (e.g., trend and pattern, link, sentiment);
- Alert user to anomalies or results that need further attention;
- Perform analysis to determine the sentiment of social media data;
- Provide confidence measurement to indicate accuracy and reliability of analysis;
- Utilize prioritized parameters to assess confidence in analysis (i.e., data from trusted sources increases confidence); and
- Provide a visual indication of confidence level.

Transmission Requirements

Potential solutions should transmit threat and hazard data to authorized personnel (e.g., emergency managers, commanders, responders). Potential solutions should:

- Encrypt responder geolocation data prior to transmission;
- Transmit data to intended destination;
- Transmit data in real time;
- Transmit location of video and images using geographic information system (GIS) coordinates;
- 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; and
- Store incident-related threat and hazard data for post-incident analysis.

Compatibility Requirements

Potential solutions should integrate with current emergency response software systems and applications. Potential solutions should:

- Comply with exchange standards for data transmission (e.g., National Information Exchange Model (NIEM));
- Bi-directionally integrate with:
    - Existing communications devices;
    - Electronic situational awareness tools;
    - Electronic incident command systems;
    - Dispatch systems;
    - Social media feeds;

- Model prediction and forecast systems;
- Responder geolocation systems;
- Incident-specific maps;
- Existing digital maps, blueprints and floorplans; and
- Other incident-specific data sources (e.g., traffic cameras, weather projections).

Maintenance Requirements

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

- Maintain backwards compatibility after upgrade;
- Be designed to reduce the time to repair;
- Be designed to minimize skills needed for maintenance;
- Perform automated periodic virus detection and cybersecurity screening of software components;
- Utilize a simple, automated upgrade process;
- Allow for remote maintenance;
- Allow for remote upgrades;
- Provide live notification of a fault; and
- Maintain a fault log.

Cost Requirements

Potential solutions should be designed to minimize the price of systems and maintenance. Potential solutions should be priced to be affordable to all response agencies.

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;
- Specification to guide the development of viable commercial system(s);
- Standards, guidelines, other legal requirements; and
- Stakeholder oversight/interaction, to ensure the developed system meets the requirements identified by the first responder community.