2016 Public Safety Analytics R&D Summit

Executive Summary for Summit Attendees

Purpose of the Analytics Summit

The Public Safety Communications Research Program (PSCR) convened over 75 stakeholders at the Department of Commerce Boulder, CO campus to build on the findings presented in the 2016 Public Safety Analytics R&D Roadmap Report. The Public Safety Analytics Summit – held August 3-4, 2016 – served to socialize the Roadmap with a broader stakeholder base and determine the core technology challenges inhibiting Public Safety's effective and expanded use of Analytics in daily operations.

The Summit resulted in a list of clearly defined Analytics technology gaps prioritized against criteria, specific problem statements relating to the highest priority Analytics challenges, and a list of Analytics capabilities that could arise as a result of the application of NIST R&D funds.

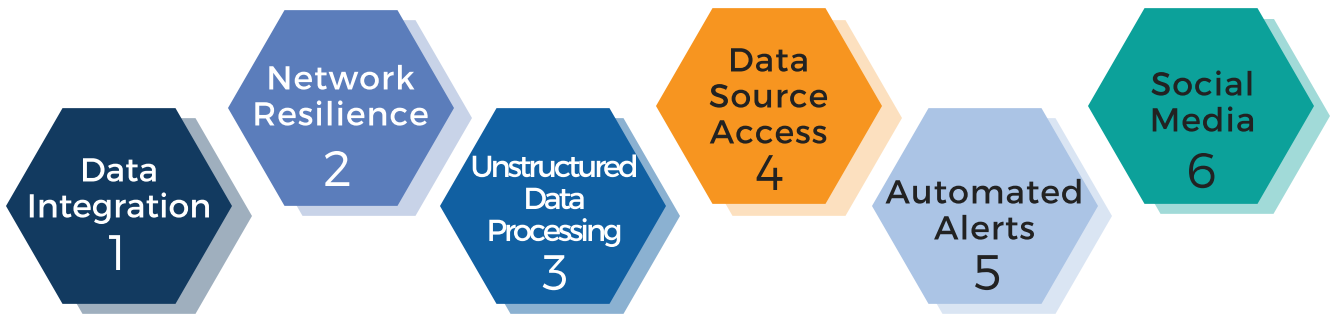
PSCR R&D Investment Criteria

Leverage | Feasibility | Impact on PS | Rewards/Results | Unique to PS

Attendees were instructed to identify the most pressing technology gaps limiting the use of Analytics in Public Safety today, and then prioritize these challenges based on PSCR's investment criteria. The above criteria were developed in close collaboration with FirstNet and the Public Safety Advisory Committee (PSAC).

Workshop Results

Using the investment criteria outlined above, Summit attendees identified the following six gaps as the highest priority Analytics R&D investment areas for PSCR to consider as it transitions into Analytics R&D Program planning and execution:



Prioritized Gap Problem Statements

Data Integration

- Data analytics cannot make cross-agency, cross-jurisdictional, or cross-application decisions preventing first responders from having the right information at the right time.
- Inconsistent data formats & values prevent real-time information analysis and normalization preventing first responders from using analytics.
- Data exchange standards don't operate effectively across disciplines preventing first responder analytics from aggregating, ingesting, and processing information.
- Current reporting technologies cannot do effective comparisons across agencies preventing agencies from accurately comparing performance data and continuously improving service delivery.
- Data collection & storage cannot remove unnecessary redundancies preventing public safety from having efficient decision support systems.

Network Resilience

- Public safety communications do not self-recover from network faults preventing analytics engines from collecting appropriate information from components to meet operational requirements (components, harmful interferences, capabilities, and other forms of network degradation)
- Public safety communications architecture cannot optimize/prioritize available communications resources preventing users from seamlessly accessing multiple data access technologies.
- Public safety communications do not provide predictive analysis of cyber intrusions preventing operators from protecting the network, users, and information.
- Public safety communications resources do not inform end users of their current capabilities preventing users from communicating accurately and effectively.
- LTE is limited in proximity preventing end users from supporting the mission 'at-the-edge' of coverage or with degraded coverage.

Unstructured Data Processing

- Unstructured data processing algorithms cannot accurately identify combinations of words, objects, and activities from multiple unstructured data sources preventing efficient and timely response to critical events.
- Cameras cannot automatically notify dispatchers preventing timely situational awareness for first responders
- Public safety analytics decision engines cannot correlate and contextualize incoming data from listening devices/sensors with other data sources because relevant and like data attributes are not easily identifiable.
- Data processing algorithms do not have the capability to extract spatial, textual, video, audio or any other form of unstructured data in a time-bound and merged fashion that is contextually relevant to the incident, preventing public safety response based on the available set of data/information.
- Public safety analytics cannot do efficient and cost effective filtering of video data preventing public safety from processing and gaining insights, leading to backlog and decreased effectiveness of collection devices and associated investments.
- Public safety lacks ability to effectively predict events or prioritize response based on historical evidence due to inability to digest free-form text & 'narrative' reports currently on record.

Data Source Access

- Unifying data analytics and dynamic filters cannot be performed in real time preventing public safety from obtaining real time situational and contextual awareness.
- Public safety applications cannot access jurisdiction and external data preventing first responders from using data to improve public safety operations.
- Public safety data systems cannot exchange private or sensitive data which impedes the sharing of information in real time keeping public safety from improved decision making.
- Public safety data repositories cannot share historical data preventing public safety from discovering potential trends and making improved predictions.
- Internet-of-Things (IoT) sensor data cannot be seamlessly integrated preventing public safety from utilizing available data for improved decision making.

Prioritized Gap Problem Statements

Automated Alerts

- Video analytics can not generate automated alerts based on enhanced detection data (ie., linger detection, gesture detection, known object detection), preventing public safety from making actionable decisions informed by video capabilities.
- Public safety is not equipped with algorithms that adapt or accept new information preventing existing analytics capabilities from being truly transformative.
- Cognitive engines can not create deep learning models causing first responders to rely on memory, intuition, and personal experience, preventing them from receiving the right information at the right time in the right format.

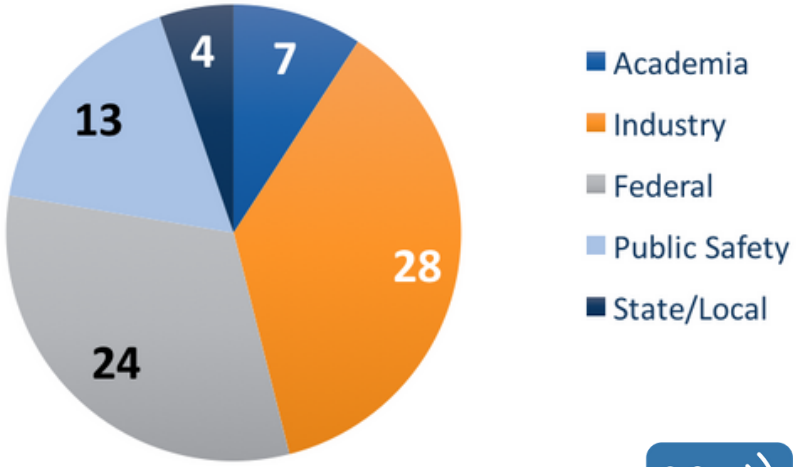
Social Media

- Public safety software can not conduct timely and automated analysis of social media data preventing public safety (dispatchers, incident command, etc.) from timely and informed decision making and response.
- Public safety-specific algorithms for prediction and hypothesis testing do not exist to integrate social media data with: data models, physics-based models (weather, flood, traffic), criminal records
- Public safety-specific algorithms/software don't exist to sort, filter, prioritize social media data.
- Public safety-specific algorithms/software don't exist to quantify truthfulness/assess validity/quality of social media data preventing public safety from having confidence in data.
- Public safety-specific integration with social media platforms does not exist to send data directly from social media platform to/from relevant public safety agency/entity (like 911 for social media)
- Public safety-specific user interface does not exist to direct analytics/run analysis on specific data sets.

Additional Information

This document represents the consensus views that were expressed by the working group over the course of the two-day summit. The conclusions represented here should not be considered an official NIST technical approach but will serve to inform the PSCR R&D process.

Breakout of Summit Attendees



PSCR

Gap: Data Integration

Problem Statements:

- Data analytics cannot make cross-agency, cross-jurisdictional, or cross-application decisions which keeps all first responders from having the right information at the right time.
- Inconsistent data formats & values prevent real-time information analysis and normalization which keeps first responders from using analytics.
- Data exchange standards don't operate effectively across disciplines which keeps first responder analytics from aggregating, ingesting, and processing information.
- Current reporting technologies cannot do effective comparisons across agencies which keeps agencies from accurately comparing performance data and continuously improving service delivery.
- Data collection & storage cannot remove unnecessary redundancies which keeps public safety from having efficient decision support systems.

Development Enablers

Requirements to Collect:	**Data Dictionary / Taxonomy**	Lack of agreed upon data dictionary prevents recognition of duplicate data
	Data Accessibility	Transparent and consistent parameters for data access rules enable efficient data access business process
	Data Types	Data entities requirements developed across public safety (PS) disciplines to define cross-leverageable sources and attributes
Standards to Develop:	**Data Architecture**	Standard practice on data entry, structure, normalization, anonymization, aggregation, etc. to enable integration and consistent query language
	Data Modeling	Baseline / core data models for public safety enterprise to ensure consistent response across agencies
	PS Data Taxonomy	Common data taxonomy to form a PS data exchange language and interchange document
Technological Capabilities to Build:	**Data Conversion Middleware**	Applications needed to aggregate disparate formats and transfer legacy to modern systems using machine learning and metadata generation
	Data Sharing Verification Middleware	Method for establishing trust or 'handshake' between agencies when exchanging and integrating data
Measurement Capabilities to Deploy:	**SLA Performance Dashboard**	Query dashboard to monitor and manage Service Level Agreements (SLAs)

Gap: Network Resilience

Problem Statements

- Public safety communications do not self-recover from network faults preventing analytics engines from collecting appropriate information from components to meet operational requirements (components, harmful interferences, capabilities, and other forms of network degradation)
- Public safety communications architecture cannot optimize/prioritize available communications resources preventing users from seamlessly accessing multiple data access technologies.
- Public safety communications do not provide predictive analysis of cyber intrusions preventing operators from protecting the network, users, and information.
- Public safety communications resources do not inform end users of their current capabilities preventing users from communicating accurately and effectively.
- LTE is limited in proximity preventing end users from supporting the mission 'at-the-edge' of coverage or with degraded coverage.

Development Enablers

Requirements to Collect:	**Public Safety LTE Intrusion Model**	Model the specifications of a network intrusion on Public Safety LTE spectrum relative to commercial carrier network
	Cyber Threat Assessment	Uniform threat assessment across Public Safety LTE spectrum including testing and reporting metrics
Standards to Develop:	**Data Architecture & Format**	Architecture to incorporate interoperable lanes (LTE, Satcom, Mesh network, LMR); Format for metadata description (priority, permissions, urgency)
	Network Status Alert	Consistent alerting to communicate available bandwidth, on/off-service, network congestion, etc.
	Secure Routing Protocols	Data routing protocols across PS networks based on user and type of network traffic; predictive cyber threat protocols
Technological Capabilities to Build:	**Network Management Hub**	Central network management tool to connect, prioritize, and assign network resources, accounting for congestion and prioritization protocols
	Offline Data Access	Network elements ability to access data & analytics absent and with degraded network connectivity including live data 'push' when connection restored
	Network Self-Opimizatiion	Utilization of self-organizing LTE network (SON) that optimizes performance within network coverage and roams between networks for best UX
	Heterogenous Wireless Network	Persistent simultaneous access to multiple Radio Access Technologies (RAT) increasing reliability, coverage, and spectrum efficiency through load balancing across RATs
	Persistent Data Delivery Indicator	Indication of communications delivery to enable awareness of team member connectivity & real-time status
Measurement Capabilities to Deploy:	**Quality Metrics**	Connection reliability; LTE network coverage measurement; accessibility & retainability; Load balancing
	Performance Metrics	Uptime; Ontime; Failure rate (call setup, connection setup, handover); Uplink throughput; Downlink throughput

Gap: Unstructured Data Processing

Problem Statements

- Data processing algorithms cannot accurately identify combinations of words, objects, and activities from multiple unstructured data sources preventing efficient and timely response to critical events
- Cameras cannot automatically notify dispatchers preventing timely situational awareness for PS
- Public safety analytics decision engines cannot correlate incoming data from listening devices/sensors with other data sources because relevant and like data attributes are not easily identifiable
- Data processing algorithms do not extract spatial, textual, video, audio or any other form of unstructured data in a time-bound and merged fashion that is contextually relevant to the incident, preventing public safety response based on the available set of data/information.
- Public safety analytics cannot do efficient and cost effective filtering of video data, leading to backlog and decreased effectiveness of collection devices and associated investments
- Public safety lacks ability to effectively predict events or prioritize response based on historical evidence due to inability to digest free-form text & 'narrative' reports currently on record.

Development Enablers

Requirements to Collect:

PS Use Case Definition	Includes common situations for unstructured data collection (fire, crowd, persons in masks, wanted persons) as well as common objects for recognition (gun, bolt cutters, etc)
Processing / Response Time	Define processing time required for various mission response so processing can be scheduled and managed effectively

Standards to Develop:

Data Tagging & Format	Coding to be applied to data attributes (time, geo, subject, event, decibel level, etc) across all unstructured data
Sample Data Set / Test Bed	PS data sets (video, audio, text) labeled for algorithm developers to conduct training and testing
Semantic Language	Language for extracting semantics; consistent data taxonomy & ontology

Technological Capabilities to Build:

Integration Middleware	Engine to integrate various data source feeds into single access point for analytics
Data Processing Algorithms	Algorithmic processing engine to derive actionable information from unstructured video (objects, activities), text (events, relationships), and audio (speech, sound)
Open Data Capture Platform	Massive, highly extensible open platform for capture and cognition of audio and video data with ability to ingest broad set of formats
Analytic-enabled Devices	Embedded analytic capability on-device to process image/audio/video and enable filtration & aggregation

Measurement Capabilities to Deploy:

Quality Metrics	Accuracy scores for correlation of ingested data
Algorithm Latency	Average and variance of algorithm latency (in seconds)

Gap: Data Source Access

Problem Statements

- Unifying data analytics and dynamic filters cannot be performed in real time preventing public safety from obtaining real time situational and contextual awareness.
- Public safety applications cannot access jurisdiction and external data preventing first responders from using data to improve public safety operations.
- Public safety data systems cannot exchange potentially private data which impedes the sharing of information in real time keeping public safety from improved decision making.
- Public safety data repositories cannot share historical data preventing public safety from discovering potential trends and making improved predictions.
- Internet-of-Things (IoT) sensor data cannot be seamlessly integrated preventing public safety from utilizing available data for improved decision making.

Development Enablers

Requirements to Collect:

Security / Access Protocols	Parameters to access and retrieve data in accordance with privacy and property standards specific to public safety data sets (PII, sensitive crime data, etc.)
Specific Data Types	Identification of discrete closed-source data types and owners for utilization by PS analytics supported by quantitative justification

Standards to Develop:

Data Architecture & Format	Consistent object architecture, digital object identifiers, IoT indexing, file formats, and data formats will enable wider access to existing data stores
Public Safety API	Common Application Program Interface (API), language and message bus for IoT data will allow streamlined integration with emerging data sources / apps
Data Sharing & Governance	Nation-spanning data exchange allowing general sharing agreements in place of jurisdiction-to-jurisdiction sharing
Mobile Plug-in	Standard plug-in sensor interface for mobile devices (IEEE 1451)

Technological Capabilities to Build:

Data Integration Middleware	Software engine to translate, merge, and distill common data elements from disparate systems and unstructured sources
Anonymized Data Ingest	Privacy masking technology for data extraction and tracking of privacy attributes on sensitive data or PII
Secure Access Model	Trustmark-style system to ensure data is accessed by cleared / allowed individuals; application of GSA's ICAM to PS space
Data Query Engine	Interface to query and access datasets / resources from multiple agencies based on specific inquiry requirements and mission
Predictive Analytics	Aggregated analytic engine that processes and leverages data access (historical and current) for actionable insights

Measurement Capabilities to Deploy:

Exchange Rate	Amount of data exchanged per time unit (Kbps)
Data Effectiveness	Predictive algorithm performance in providing actionable insights / intelligence from each data source, type, and overall
Data Frequency	Frequency of availability to new and/or updated data sources (recency)

Gap: Automated Alerts

Problem Statements

- Video analytics can not generate automated alerts based on enhanced detection data (ie., linger detection, gesture detection, known object detection), preventing public safety from making actionable decisions informed by video capabilities.
- Public safety is not equipped with algorithms that adapt or accept new information preventing existing analytics capabilities from being truly transformative.
- Cognitive engines can not create deep learning models causing first responders to rely on memory, intuition, and personal experience, preventing them from receiving the right information at the right time in the right format.

Development Enablers

Requirements to Collect:

Processes for Automation	Analysis to determine business processes requiring automation and automation levels

Standards to Develop:

Database & Access	Shared database to populate algorithms across national and local jurisdictions
Core Algorithms	Set of base algorithms used to generate alerts that can be locally tailored
Alerting Business Rules	Baseline set of alerting rules to automate alert post 'trigger' event

Technological Capabilities to Build:

Data Processing Algorithms	Algorithmic processing engine to derive actionable information from unstructured video (objects, activities), text (events, relationships), and audio (speech, sound)
Predictive Alerting	Predictive Incident progression algorithm based on live analysis of historical and cross-source integrated data
Location-based Alerting	Automated alerting based on location or incident history
Context-aware Alerts	Intelligent alert and notification handling to avoid overwhelming / desensitizing recipient

Measurement Capabilities to Deploy:

Reliability / Performance Ratings:	To calculate missed alerts, false alarms, response time reductions, improvements in resource allocation; used to inform machine learning

Gap: Social Media

Problem Statements

- Software can not conduct timely and automated analysis of social media data preventing public safety (dispatchers, Incident Command, etc.) from timely and informed decision making and response
- PS-specific algorithms for prediction and hypothesis testing do not exist to integrate social media data with: data models, physics-based models (weather, flood, traffic), criminal records
- PS-specific algorithms/software don't exist to sort, filter, prioritize social media data
- PS-specific algorithms/software don't exist to quantify truthfulness/assess validity/quality of social media data preventing public safety from having confidence in data
- PS-specific integration with social media platforms does not exist to send data directly from social media platform to/from relevant public safety agency/entity (like 911 for social media)
- PS-specific user interface does not exist to direct analytics/run analysis on specific data sets

Development Enablers

Requirements to Collect:

Specific Social Media Data Sets	Define the priority / actionable data sets emerging from the social media-sphere for use by PS
Triggers & Flags	Definition of 'actionable intelligence' derived from social media to inform development of algorithms and response procedures

Standards to Develop:

Data Architecture & Format	Structure for storing social media inputs allowing for consistent sorting, filtering and prioritization of various social media data types
Public Safety API	API for commercial Social Media companies to communicate to PS systems (at national, regional, and local levels)
Sample Data Set	Uniform mock data set for tool testing and comparison across agencies
Mobile Plug-in	Standard plug-in sensor interface for mobile devices (IEEE 1451)

Technological Capabilities to Build:

Data Integration Middleware	Real-time integration between social media data sets and integration with existing PS databases
Algorithmic Processing	Bayesian analytic capability to extract relevant social media content in real-time to obtain view of emerging trends & events
Verified Access Model	Verification filter for publicly generated data targeting false data & misinformation; verify IP and geolocation data
Social Lexicon Analytics	Analysis of emoticons and current slang / commonly used abbreviations
Social Media Response	Support for two-way communications between first responders and social media users to acknowledge and/or coordinate response

Measurement Capabilities to Deploy:

Data-Event Correlation	Evaluate the utility and performance of social media data as a predictor for PS activity across data type / source
Validity	Calculate percentage of data triggers that are genuine in source to increase efficiency of processing model

Acronyms Used

API	Application Program Interface
GSA	General Services Administration
ICAM	Identity, Credentials, and Access Management
IEEE	Institute of Electrical and Electronics Engineers
IP	Intellectual Property
Kbps	Kilobits per second
LMR	Land Mobile Radio
LTE	Long-term Evolution
PII	Personally Identifiable Information
R&D	Research & Development
RAT	Radio Access Technology
SLA	Service Level Agreement
SON	Self-organizing Network
UX	User Experience