Toolbox Study

Televate

Broadband Mobile Toolbox: Mapping Services Tool

The Mapping Services Tool is a broad category of tools focused on location and geographical mapping. These tools range from high-end geographic information systems (GIS) to automatic vehicle location (AVL) to route navigation systems. Many of the tools serve as standalone applications, especially GIS applications, but many, if not all, can also be a component or feature of another tool (i.e. computer aided dispatch (CAD), situational awareness, etc.). Because of this, mapping tools can be found throughout the public safety mobile environment.

The purpose of this document is to focus on the considerations and requirements regarding the remote field interactions with mobile applications, we will explore the mobile mapping environment and not the system as a whole.

Use Cases

Some mapping tools are used by nearly all public safety agencies, i.e. map-based calls for service and navigation, but, there are discipline specific use cases. For example, law enforcement may utilize location based incident data for predictive policing, patrol area boundaries, asset location, and area statistics. The fire service may utilize GIS for locating available hydrants, building inspection data, location of hazardous material, floorplan of the structure, and evacuation routes. EMS may utilize GIS data in a similar manner to both the fire service and law enforcement, but, draw upon predictive road traffic data to reduce response times and transportation to medical centers.

Nontraditional or forward-thinking uses of map data can include the active geographic mapping of personnel that could include biometric data, map-based hyperlinks to active body cameras, map-based weapon holster status, and map-based availability of assets; coupled with more traditional information, such as vehicle location and status GIS based information is helping to provide powerful situational awareness that can be updated in real-time and available for further analysis.

Features

A GIS system will typically have many layers of mapped data accessible to end users. The quantity of map data is truly limitless in terms of scope, as nearly all data can be mapped. GIS systems generally have a built-in query tool for recalling pertinent data. These systems provide secure access through a user interface where authorized users can select data layers to map.

A location based services platform (LBS) will typically be tracking personnel, vehicles, and other assets providing status for each. The LBS system can integrate location with other data to inform end users of data relevant to their location and display other pertinent datasets such as high crime areas, incident and event history, or the nearest public safety facility.

Typical Features
• **Map retrieval with requested layers and updates** • **Overlay event and incident data on maps** • **Asset Location and Information** • **Orthophotography**

- **Pictometry**
- **Crime/Data Analysis**
- **Live or near real time AVL and personnel location mapping**
- **Vehicle and personnel location history**
- **Simple user interface, web based**

Adoption Considerations

There are numerous considerations when adopting a new technology or in this case, mobile access to mapping information. The following subsections explore considerations that a decision maker should address when looking to implement a specific mobile application in a toolbox category. This is focused on the mobile client application, such as in records management systems (RMS) or computer aided dispatch (CAD) applications, and not the core product if there is one.

Usage

How mapping tools and its data will be used in a mobile environment is critical to understanding your wireless needs. Depending on the data requirements, network bandwidth could be a major factor in performance and overall usefulness of the tool. For example, displaying orthophotography or an urban building layer, with tens of thousands of structures, may require downloading an incredibly large data file over your wireless connection. If needed bandwidth is not available, this simple task could bring your local computing environment (MDT, command vehicle, smartphone, etc.) to a standstill. Here are some other considerations to take into account for adopting mobile mapping:

- Understand what data is required to be accessed in your mobile environment and have a strategy for large data files
- Ensure the end user mobile device (i.e. smartphone, tablet, PC) is capable/suitable to host the client software and robust enough to display the potentially data intensive interface
- Select LBS devices that have sufficient battery life and dual WIFI/cellular connectivity
- Secure access for remote viewing of data with session persistence
- Select devices with low user interaction or hands-free operation
- Improve connectivity by using external vehicle antennas where possible

Wireless Connection

Mapping services are potentially major data users looking for an “always on” connection for position updates and map updates. With this in mind, access to the services can be through WIFI or cellular broadband, here are some items that should be taken into consideration.

- Coverage and Priority: Mapping tools have become a vital tool used by public safety. Likewise, the coverage afforded by the wireless carrier needs to match the service area and expectations of the agency. When selecting a wireless carrier, coverage should not be the only criteria considered but also include quality of service, priority, and preemption (QPP). “Quality of service” means that public safety personnel maintain appropriate access to critical communication resources at all times. “Priority” means that public safety personnel/application

receive access to those resources first, ahead of other users. "Preemption" means that higher priority personnel/applications can utilize all available resources within the network, even if services to lower priority personnel are denied. Special consideration should be given to the wireless carrier who can provide the most robust QPP for mobile mapping access and other important public safety applications.

- Bandwidth: Geospatial data files tend to be large and LBS shares data continuously, consider the unlimited data plan for those users (i.e. GIS users). It is important to assess the bandwidth requirement for the selected features and testing these features in the field to ensure useful operations.
- Session Persistence: Wireless coverage is not ubiquitous and there may exist areas of insufficient coverage in your jurisdiction. Therefore, the mapping solutions may need to have a strategy for handling session discontinuity.

Security

Certain data, such as LBS data, could be considered sensitive if the system is tracking high value assets or personnel. Making sure the data is controlled and secure is a top priority. From the field perspective, ease of use and high security have to go hand in hand. Credentialing and a secure sign on process are points to consider along with:

- FIPS 140-2[1] required for all federal inquiries
- Virtual Private Network (VPN), for local network access and end-to-end security
- Strong authentication and authorization mechanisms that take privacy, session management, identity management and device security features into account
- Multi-factor authentication
- Using technologies such as the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol
- Compliance with local security requirements
    - Credentialing: Support for Single Sign-On (SSO) if implemented locally
        - Ability to leverage identity, credential, and access management (ICAM),[2] or State Identity, Credential, and Access Management (SICAM)[3] credentialing

Interoperability

Intra- and Interagency interoperability is another important factor to consider for coordinating multiple agency resources at a major incident or event, such as a wildfire or major planned event. Mapping

[1] Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules.
[2] Federated identity, credential, and access management (ICAM) solutions are intended to help the public safety community overcome information sharing challenges and provide public safety personnel with the ability to securely gain access to critical information from a wide variety of systems.
[3] The SICAM architecture enables states and their partners to share and audit identification, authentication, and authorization across state enterprise boundaries.

services, such as GIS and AVL, are mature technologies that have established standards that could and should be used.

Interoperability considerations include:

- Ensure that geospatial data used and produced is made available in a nonproprietary format and use industry standards
- Ensure that data is accessible/sharable and not "locked" within a native application
- Consider utilizing web based viewers to avoid proprietary clients installs
- Are there robust methods (i.e. API, SDK, web service) that allow the application to receive and send data to 3rd Party applications?
- Are resources available, either in-house or contracted, who are capable of performing the necessary technical work for required integrations?
- Will the mobile environment require a secure connection to access additional information (i.e. NCIC, warrants, offenders, etc.)[4]?

System Architecture

Mobile mapping service tools will supply and draw data from services that are in place at the agency. Assuring smooth data transfers, resulting in good user experiences, means that the GIS application must interact with other applications seamlessly. Observing the daily operations of an application, which has installed GIS components, is a way to learn about the effectiveness of the tool. The agency should note the lessons learned from current users and establish the pros and cons as well as document the best practices for other agencies to consider and investigate. Other issues to consider are:

- Hardware considerations are based on the computing needs of the mobile GIS or LBS client or application.
    - Is the mobile application a thick client[5] requiring a robust computing environment?
    - Is the client/app meant for a smartphone or tablet only?
- Software considerations include the client and required operating system(s)
    - Does your current GIS software offer a mobile GIS interface?
    - What operating systems does the client support (i.e. iOS, Android, Windows)?
    - Is the mobile client a browser-based interface only?
- Backend architecture knowledge is critical to any mobile deployment
    - Is the core application a cloud-based or an on-premise application?
    - For an on-premise architecture, is the core application (server) accessible outside of the local network?
    - What resources are required for both initial implementation and the operational upkeep of the mobile environment?

[4] Please note that access to various federal and state databases may require an additional VPN credential.
[5] A computer (client), in client-server architecture or networks, that typically provides rich functionality independent of the central server.

Cost

A Rough Order of Magnitude (ROM) cost estimate should be conducted on an individual and volume discount basis. Prospective mapping service solution providers should provide standard product list pricing. The preliminary cost analysis will facilitate executive management decision making, and address budgetary considerations.

A cost/benefit analysis should be conducted to make sure that implementing these applications is worth doing, and support the decision process throughout the organization. Cost considerations can include:

- Justification of the need
- The cost benefit statement
- ROM pricing
- Resource requirements for implementation and operation (in-house or contract staff)
- Delivery schedule
- Impact on agency department budget

Broadband Mobile Toolbox: Push-to-Talk Tool

Push-to-Talk, or PTT, is a well-known communications tool in the public safety arena. PTT is a means of instantaneous communications that uses a button to switch a device from voice reception mode to voice transmission mode. Public safety PTT systems adhere to widely known national standards (i.e., P25) deployed on networks with levels of redundancy to ensure mission-critical communications. Mission Critical PTT is defined as a Land Mobile Radio (LMR) communications network with extremely high reliability and resiliency, assuring the communications across the network with a high degree of certainty. Public safety agencies use their PTT networks for voice and data communications on a daily basis. With the advent of the FirstNet network, there is a potential to take advantage of the cellular 4G LTE functionality to augment public safety PTT communications.

There are several commercial PTT applications available in the marketplace today, some more common than others. In fact, FirstNet offers two separate PTT applications to support different implementation scenarios. Concurrently, FirstNet is also heavily involved in the Mission Critical Push-to-Talk (MC-PTT) standards process. The MC-PTT 3GPP[1] standard is designed to provide the same level of reliability and similar functionality as today's public safety networks. The work on the MC-PTT standard has been ongoing since 2015. Early releases of a PTT baseline solution, that is compliant with the MC-PTT standard's framework, are available today.

This document addresses the use cases, features and considerations for today's PTT baseline solution, and the known features of the MC-PTT solution that will be available in the future.

Use Cases

LMR P25 radios are built to a standard that is rarely available with commercial devices. Radios are generally built to what is referred to as an "ingress protection" standard. The ingress protection standard is a manufacturing standard designed to protect the device from the ingress of particles and liquids. The most common ingress standard in the marketplace is IP67.[2] In addition, these same radios are also built to be compliant with various U.S. military specifications[3] that are designed to ensure that the device remains functional in very harsh environments. Collectively, these devices are known as "ruggedized" devices , which, built to a high IP standard or military spec, tend to be significantly more expensive.

In the public safety world there are some users that do not require an expensive dedicated radio for voice communications. Some agencies or users may be able to take advantage of a commercial PTT baseline solution to augment their communications with personnel that do not have a need for a ruggedized radio. Infrequent users may also be excellent candidates for a commercial PTT baseline

[1] http://www.3gpp.org/
[2] IP67 – IP Code, Ingress Protection Marking IEC standard 60529
[3] Typical US military specification 810C, 810D, 810E, 810F etc.

solution such as a smartphone app that operates on the cellular network. Another advantage of the commercial PTT baseline solution would be communications availabilities for users who travel outside of their home LMR networks. These use cases may reduce costs for maintaining the LMR P25 system by offloading some users that do not require ruggedized radios to a commercial PTT baseline solution without impacting their ability to access the LMR P25 network.

Features

A commercial PTT baseline application has a set of standard features that most products offer; these are listed in the table below. The list is not meant to be all-inclusive and does not include add-ons and additional modules that may be vendor specific. To ensure user requirements are met, your specific functionality and feature requirements should be gathered during the software assessment phase and then compared carefully to what the commercial PTT baseline application offers.

Typical Features
• **Access to talk groups or specific channels for reaching specific user groups** • **High reliability systems with virtually no downtime** • **High quality audio for clear reception** • **Man Down/Emergency Alert button** • **Peer to peer local connectivity, without access to the network**
Integration with a 4G LTE system desired features:

• **Seamless integration between the end user device and the LMR system**
• **Access to talk groups/channels**
• **High reliability with virtually no downtime**
• **High quality audio**
• **Man Down/Emergency Alert with location**
• **Peer to peer local connectivity, without access to the network**
• **Multiple accessory options for end user interface**
  ○ **Hands free/Voice Control**
  ○ **Bluetooth headset and microphone**
  ○ **Dedicated PTT button on device or accessories**

Adoption Considerations

There are numerous considerations when adopting a new technology, such as a commercial PTT baseline solution. The following subsections explore core considerations that a decision maker should address when looking to implement a specific mobile application in a toolbox category. This is focused on the mobile client application and some of the basic requirements for the core product platform.

Usage

How the commercial PTT baseline application will be used in a mobile environment is critical to understanding your wireless needs. The bandwidth requirement to support a commercial PTT application for voice communications is relatively small, a few Kilobytes per second, on average. However, commercial PTT applications can be installed on smartphones, tablets and potentially mobile data computers. Since these devices will likely be running several applications concurrently, the data usage by all applications should be used to assess the usage requirements and wireless services plan.

The following list highlights some general information on data usage that should be taken into consideration.

- Data Transmissions: Bi-directional data
    - Digitized voice communications on both uplink (send) and downlink (receive).
- Throughput Requirements: Variable, simplex, digitized voice requires very little bandwidth. However, some devices may be sending and receiving data from other applications concurrent with the operation of the commercial PTT baseline application.
    - Digitized voice data: Requires minimal bandwidth

Wireless Connection

This section outlines some of the network related concerns that may need to be considered when evaluating a commercial PTT solution. PTT/MC-PTT is highly dependent on connectivity between the devices, the commercial wireless network, and P25 network. For most users of the P25 network, it is easy to identify coverage areas, good, moderate, and bad. Most end users are familiar with dead spots or poor coverage areas and either avoid them, or know where to go to get a signal. When using a commercial PTT solution over cellular system, the dead spots can be harder to identify, and using multiple ways to connect (e.g., Wi-Fi, cellular, DAS) adds to the complexity of maintaining signal integrity and data integrity. In addition, the cellular signal may be present, but the system may not have the capacity to carry data; this is known as congestion. Some packets may be lost to congestion, garbling the transmission or causing connectivity problems.

- Coverage and Priority: PTT voice communications remains one of the most vital tools used by public safety. Likewise, the coverage afforded by the wireless carrier needs to match, and if possible, exceed the service area of the P25 system. The coverage should meet expectations of the agency. When selecting a wireless carrier, coverage should not be the only decision factor; quality of service, priority, and preemption (QPP) should also be considered. “Quality of service” means that public safety personnel maintain appropriate access to critical communication resources at all times. “Priority” means that public safety personnel receive access to those resources first, ahead of other users. “Preemption” means that higher priority personnel can utilize all available resources within the network, even if services to lower priority personnel are denied. Special consideration should be given to the wireless carrier who can provide the most robust QPP for mobile RMS access and other important public safety applications.

- Bandwidth: The amount of data exchanged between a mobile user and the centralized P25 network can be relatively small. However, commercial PTT solution may, over time, come with more data intensive features. Therefore, it is important to assess present and future bandwidth requirements to ensure useful operations.
- Session Persistence: If a user is on the move, session persistence is a factor. The system should not drop a user who switches to a roaming partner or an indoor system. Choose the carrier for coverage, capacity, and priority, if offered.
- Proximity Services: Another consideration is that users may be clustered together, and only need to talk to each other. With the advent of Proximity Services (ProSe), direct communication between devices within range of each other can be possible.

Security

Voice transmissions over the PTT system are sensitive and are likewise encrypted. Encryption is a consideration; security requirements vary by agency and application. The following list includes security features that should be considered.

- Compatible end to end encryption AES 256 (if required)
- FIPS 140-2[4] (if required)
- Virtual Private Network (VPN), for local network access and end-to-end security
- Strong authentication and authorization mechanisms that take privacy, session management, identity management and device security features into account
- Multi-factor authentication
- Technologies such as the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol (browser access)
- Compliance with local security requirements
    - Credentialing: Support for Single Sign-On (SSO) if implemented locally
        - Ability to leverage identity, credential, and access management (ICAM),[5] or State Identity, Credential, and Access Management (SICAM)[6] credentialing

[4] Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules.
[5] Federated identity, credential, and access management (ICAM) solutions are intended to help the public safety community overcome information sharing challenges and provide public safety personnel with the ability to securely access critical information from a wide variety of systems.
[6] The SICAM architecture enables states and their partners to share and audit identification, authentication, and authorization across state enterprise boundaries.

Interoperability

Bi-directional communications, or interoperability, is essential to a commercial PTT solution. The main goal of the PTT/MC-PTT solution is to integrate seamlessly with the existing P25 network to allow easy integration of talk-groups. The connection of the commercial PTT solution with the P25 network will likely be through a specialized IP gateway. The commercial PTT solution should ensure full interoperability with users on the P25 network.

- Commercial PTT solution should ensure full interoperability with the P25 system and third-party devices used on the network
- Commercial PTT solution shall ensure seamless integration with LMR system and talk groups/channel assignments

System Architecture

The general system architecture is an on-premise client-server gateway connected to the P25 system through an ISSI[7] IP network connection. In addition to the gateway, the commercial PTT solution should provide an application to manage the PTT users on that system.

- Network considerations will be dependent upon the network requirements of the resident P25 system
    - High reliability and high resiliency are important for all network components and gateways
- Hardware:
    - Smartphone with dedicated PTT button, man down/emergency alert button
    - Accessories for users to utilize with gloves or hands free
- Software considerations:
    - Does your commercial PTT software offer a suitable interface?
    - What operating systems does the mobile application support (i.e., iOS, Android, Windows)?
- Backend architecture:
    - Is the commercial PTT software a cloud-based or an on-premise application?
    - For an off-premise architecture, how reliable will the connection be to the IP gateway connected to the P25 system?

Cost

A Rough Order of Magnitude (ROM) cost estimate should be conducted on an individual and volume discount basis. Prospective PTT providers should provide standard product list pricing. The preliminary

[7] Inter-RF Subsystem Interface (ISSI) that provides communications interoperability

cost analysis will facilitate executive management decision making, and address budgetary considerations. The vendor should also estimate the transition costs to MC-PTT as well to determine if it is feasible to implement their solution cost-effectively.

Pricing should be extended to capture the hardware and software solution costs, installation and integration, annual maintenance, along with other special pricing considerations.

Cost considerations can include:

- Justification of the need
- The cost-benefit statement
- ROM pricing
- Resource requirements for implementation and operation (in-house or contract staff)
- New hardware requirements for field deployment
- Cost of application per end user
- Cost to install server or cloud connection host for application
- Cost of technical support to implement the application/server/host
- Cost for maintenance of the program

Broadband Mobile Toolbox: Computer Aided Dispatch

Computer Aided Dispatch (CAD) systems are specifically designed and engineered for multi-disciplinary, and occasional multi-jurisdictional dispatching capabilities. Public safety agencies use CAD to facilitate incident response and communications in the field. Traditional CAD systems manage responder dispatch based on the transfer of 911 calls from the 911 call management system. Modern CAD systems that support Next Generation 9-1-1 can handle calls for service from multiple points of origin to include alarm systems, E911 systems, direct calls (7- or 10-digit numbers), walk-ins, CAD-to-CAD interfaces or Internet Web-based systems. The CAD system can also support the documentation of service and support requests from first responders in the field.

CAD systems have matured over the years and can be more than just a way to dispatch emergency personnel. Typical CAD system functions may include resource management, call taking, location verification, dispatching, unit status management, and call disposition. Additionally, systems frequently provide mapping functionality, support an optional mobile CAD application to interface with mobile data computers (MDC) and other wireless devices, and they interface with external local, state, and federal database systems or records management systems. Call takers, dispatchers, and their supervisors are the primary users of CAD. Public safety field units interact with the CAD through a specially designed module installed on mobile data computers, tablets or smartphones. Many CAD systems support tracking the location of first responder units to better dispatch emergency units based on distance to the scene of the incident and can also provide directions based on the fastest route.

The purpose of this document is to focus on the considerations and requirements regarding the remote field interactions with mobile applications, we will explore the mobile CAD environment and not the system as a whole.

Use Cases

The mobile CAD module, used by the first responder, supplements the radio dispatch call for service, or is the primary service dispatch for some jurisdictions, and provides valuable data and content to facilitate the emergency response. The CAD systems are designed to push relevant information to the field, in a near real-time basis, and can provide a manner for first responders to query information from local, state and federal sources. For example, in the case of law enforcement, CAD modules may provide field units access to agency records management systems with the ability to search names, vehicles, incidents, property, or wanted persons.

Features

Mobile CAD applications have a set of standard features that most products offer; these are listed in the below table. The list is not all-inclusive and does not include add-ons and additional modules that may be offered by the CAD vendor. To ensure user requirements are met, your specific functionality and

feature requirements should be gathered during the software assessment phase and then compared carefully to what the mobile CAD client/application offers.

Typical Features
• **Dispatch Status and updates** • **Event viewing and creation** • **Field Reporting with Field Interview** • **Location History** • **Accident / Crash Reporting** • **Mobile Arrest Form** • **AVL Mapping** • **Mobile Records Search** • **State and National Records Search** • **Messaging, Alerting & Notification** • **Rip and Run (call information hardcopy)**

Adoption Considerations

There are numerous considerations when adopting a new technology or in this case, mobile access to a CAD. The following subsections explore considerations that a decision maker should address when looking to implement a specific mobile application in a toolbox category. This is focused on the mobile client application, such as in records management systems (RMS) or computer aided dispatch (CAD) applications, and not the core product if there is one.

Usage

How the CAD data will be used in a mobile environment is critical to understanding your wireless needs. The data usage for a field-based/mobile CAD module is highly dependent on the data sent and received. Data from some services, such as automatic vehicle location (AVL) based on GPS location information, is constantly streamed back to the main system from active units. Most other data is event driven, or communicated on demand.

How are you using your mobile CAD? Identifying the information you are receiving and sending is very important to understanding your wireless needs. The following list highlights some general information on data usage that should be taken into consideration:

- Understand what data is required to be accessed in your mobile environment and have a strategy for large data files
- Ensure the end user mobile device (i.e. smartphone, tablet, PC) is capable/suitable to host the client software and robust enough to display the potentially data intensive interface
- Secure access for remote viewing of data with session persistence
- Select devices with low user interaction or hands-free operation
- Improve connectivity by using external vehicle antennas where possible

- Data Transmissions: Bi-directional data
  - Record queries, record creation, and AVL data are sent on the uplink (send)
  - Records are sent both on the uplink (send) and downlink (receive)
- Throughput Requirements: Variable depending on the information type
  - Textual data: Requires minimal bandwidth
  - AVL data: Requires minimal bandwidth
  - Situational Awareness Map Data: Highly dependent upon the amount of data in the map layer. This can vary considerably from minimal to very large.
  - Multimedia Files: Some CAD systems can send and receive multimedia data to include video, images, audio, and documents. Multimedia files tend to be large and will require higher bandwidth.

Wireless Connection

The following section outlines some of network related concerns that may need to be considered when evaluating a mobile CAD system used over a wireless network.

- Coverage and Priority: CAD remains one of the most vital tools used by public safety. Likewise, the coverage afforded by the wireless carrier needs to match the service area and expectations of the agency. When selecting a wireless carrier, coverage should not be the only criteria considered but also include quality of service, priority, and preemption (QPP). "Quality of service" means that public safety personnel maintain appropriate access to critical communication resources at all times. "Priority" means that public safety personnel/application receive access to those resources first, ahead of other users. "Preemption" means that higher priority personnel/applications can utilize all available resources within the network, even if services to lower priority personnel are denied. Special consideration should be given to the wireless carrier who can provide the most robust QPP for mobile CAD access and other important public safety applications.
- Session Persistence: Wireless coverage is not ubiquitous and there may be areas of insufficient coverage. Therefore, the CAD module needs to have a strategy for handling session discontinuity.
- The choice of the wireless carrier should correspond with the minimum coverage and throughput requirements necessary for the operations of the mobile CAD throughout the jurisdiction. Special consideration should be given to wireless carriers that can provide a higher priority on the network for public safety than the general subscriber.

Security

Due to the sensitivity of dispatch data and possible records management system access, an encrypted connection is required as standard for a mobile CAD connection. Exact security requirements will depend on accessed information but common policy would include:

- FIPS 140-2[1] required for all federal inquiries
- Virtual Private Network (VPN), for local network access and end-to-end security
- Strong authentication and authorization mechanisms that take privacy, session management, identity management and device security features into account
- Multi-factor authentication
- Using technologies such as the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol
- Compliance with local security requirements
    - Credentialing: Support for Single Sign-On (SSO) if implemented locally
        - Ability to leverage identity, credential, and access management (ICAM),[2] or State Identity, Credential, and Access Management (SICAM)[3] credentialing

Interoperability

Interagency or interjurisdictional interoperability is accomplished through the central CAD system. Many CAD systems offer an application programming interface (API) and software development kits (SDKs), or common interfaces for data exchange that use an Extensible Markup Language (XML)[4] framework. The sharing of data is evaluated on an agency-by-agency/jurisdiction-by-jurisdiction basis. Information stored within the CAD system is extremely useful and access to that data should be of the utmost importance and be a leading consideration.

Interoperability considerations include:

- If requirements dictate that field personnel shall be able to query various internal and external data sources, the mobile client should:
    - Provide a secure access to required data sources
    - Provide a graphical user interface to query/look up required records
- If requirements dictate that field personnel shall be able to create and/or update records to internal and external data sources, the mobile client should:
    - Provide a secure access to required data sources
    - Provide a graphical user interface to create and/or update required records
- Agency Records Management Systems

[1] Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules.
[2] Federated identity, credential, and access management (ICAM) solutions are intended to help the public safety community overcome information sharing challenges and provide public safety personnel with the ability to securely gain access to critical information from a wide variety of systems.
[3] The SICAM architecture enables states and their partners to share and audit identification, authentication, and authorization across state enterprise boundaries.
[4] Extensible Markup Language (XML) is a markup language that defines a set of rules for encoding documents in a format which is both human-readable and machine-readable.

    - For Law Enforcement, it would include query access to State and National Records (NCIC, Warrants, Offenders, etc.)[5]
- Communication systems (land mobile radio [LMR] systems, message and alerting platforms, etc.)
- Are there robust methods (i.e. API, SDK, web service) that allow the application to receive and send data to 3rd Party applications?
- Are resources available, either in-house or contracted, who are capable of performing the necessary technical work for required integrations?

System Architecture

Understanding the architecture of your existing CAD system, even at a high level, is a critical consideration for mobile adoption. This can and most likely will, dictate how you are able to deploy the mobile CAD system into field operations.

- Hardware considerations are based on the computing needs of the mobile CAD client or application.
    - Is the mobile CAD a thick client[6] requiring a robust computing environment?
    - Is the client/app meant for a smartphone or tablet only?
- Software considerations include the client and required operating system(s)
    - Does your current CAD software offer a mobile CAD interface?
    - What operating systems does the client support (i.e. iOS, Android, Windows)?
    - Is the mobile client a browser-based interface only?
- Backend architecture knowledge is critical to any mobile CAD deployment
    - Is the core CAD application a cloud-based or an on-premise application?
    - For an on-premise architecture, is the core CAD application (server) accessible outside of the local network?
    - What resources are required for both initial implementation and the operational upkeep of the mobile CAD environment?

Cost

A Rough Order of Magnitude (ROM) cost estimate should be conducted on an individual and volume discount basis. Prospective CAD and mobile CAD solution providers should provide standard product list pricing. The preliminary cost analysis will facilitate executive management decision making, and address budgetary considerations.

If the requirement is to add a mobile CAD capability, first determine if the legacy CAD system version supports a mobile CAD application. If not, the legacy CAD system may need to be replaced, or upgraded

[5] Please note that access to various federal and state databases may additionally require a VPN credential.
[6] A computer (client), in client-server architecture or networks, that typically provides rich functionality independent of the central server.

to a new version. Pricing should be extended to capture the hardware and software solution costs, installation and integration, annual maintenance, along with other special pricing considerations.

Cost considerations can include:

- Justification of the need
- The cost benefit statement
- ROM pricing
- Resource requirements for implementation and operation (in-house or contract staff)
- Delivery schedule
- Impact on agency department budget

Broadband Mobile Toolbox: Mass Notification Tool

Mass notification systems are multi-modal communications platforms designed to send emergency and non-emergency notifications to the general public or internally within large companies. For the public safety sector, mass notification systems are built on robust platforms and are designed to provide location based notifications to a targeted group of recipients. Many platforms offer support for multi-language notifications as well. Many large platforms have built-in administrative functionality including: data analytics, group management, contact list management, and secure access control. To improve the efficiency of notifications, the mass notification system integrates multiple communications platforms to include some, or all, of the following:

- Short Message Service (SMS) Text Messages
- E-Mail
- Voice messages: either pre-recorded or text-to-voice conversions
- Broadcast Text Telephony (TTY)
- Rich Site Summary (RSS) feed updates or web widget (JavaScript)
- Social Media: Facebook and Twitter
- Digital Signage: traffic signage or informational stanchions
- In-building systems: alert beacons, fire alarms, loudspeaker paging systems, IP televisions, third-party applications

The purpose of this document is to focus on the considerations and requirements regarding the remote field interactions with mobile applications, we will explore the mobile mass notification platform environment and not the system as a whole.

Use Cases

The sole use case of a mass notification system is communications; it is the ability to inform a group of people of a specific event or provide information for their benefit. Weather events and infrastructure issues (i.e. transportation, utility, etc.) tend to be the most common uses of the mass notification system. The system works well and efficiently when dealing with a large number of receipts requiring a consistent and informative message. Be it a weather watch, or warning, road closure, a shelter in-place, or a full-blown evacuation order, most modern mass notification systems can send the information through multiple channels better ensuring users or general public can receive the information. The mass notification platform is used to ensure an efficient and effective communications across all consumer platforms and devices.

Features

Mass notification systems are platforms specifically designed to enhance communications between an organization and the general public or internally to itself. Although these platforms can receive

information from other systems, such as the National Weather Service, the platforms specialize in outbound communications across multiple communication modes or formats. The typical features found in these systems are as follows.

Typical Features

• Message sending channels:
  ○ Short Message Service (SMS) Text Messages either through email or short code
  ○ E-Mail
  ○ Voice messages: either pre-recorded or text-to-voice conversions as well as multi-language support
  ○ Rich Site Summary (RSS) feed updates or web widget (JavaScript)
  ○ Social Media: Facebook and Twitter
  ○ Broadcast Text Telephony (TTY)
  ○ Inbound Hotline with pre-recorded messages
  ○ Digital Signage: traffic signage or informational stanchions
  ○ Integration with third-party systems such as In-building alert beacons, fire alarms, loudspeaker paging systems, IP televisions, and independent applications
• Public opt-in capabilities
• Geo-targeted messages
• Integration with the FEMA Wireless Emergency Alerts (WEA) program
• Contact management
• Analytics and reporting
• Access control
• Data interoperability

Adoption Considerations

There are numerous considerations when adopting a new technology or in this case, mobile access to a mass notification system. The following subsections explore considerations that a decision maker should address when looking to implement a specific mobile application in a toolbox category. This is focused on the mobile client application, such as in records management systems (RMS) or computer aided dispatch (CAD) applications, and not the core product if there is one.

Usage

Mass notification system software can either be a hosted cloud-based solution or an on-premise client-server solution. The mobile access to the mass notification system has historically been through a web interface but many systems today offer mobile applications running on the iOS, Android, and Window mobile operating systems.

The mobile usage experience, from a message sending perspective, should be very similar to that back in the office or command center. There are a few mobile usage considerations to take into account:

- Although a high bandwidth connection is not necessarily required, a consistent one is and session persistence is important to maintain
- Secure access for remote viewing of data with session persistence
- Ensure the end user mobile device (i.e. smartphone, tablet, PC) is capable/suitable to host the client software and robust enough to display the potentially data intensive interface
- Due to the potential for public notifications, properly trained personnel on the system is critical, especially if the mobile interface differs from office usage.
- Throughput Requirements: Variable depending similar to web browsing
    - Textual data: bi-directional communications, minimal on uplink
    - Multimedia Files: Uplink of multimedia files likely to be rarely used.

Wireless Connection

It is highly recommended that the mass notification system uses a secure connection with the hosted cloud-based solution or a client-server solution to operate. Offline operations are generally not an option.

- Coverage and Priority: The mass notification system is a vital tool used by public safety to notify and alert the public and internally. Likewise, the coverage afforded by the wireless carrier needs to match the service area and expectations of the agency. When selecting a wireless carrier, coverage should not be the only criteria considered but also include quality of service, priority, and preemption (QPP). “Quality of service” means that public safety personnel maintain appropriate access to critical communication resources at all times. “Priority” means that public safety personnel/application receive access to those resources first, ahead of other users. “Preemption” means that higher priority personnel/applications can utilize all available resources within the network, even if services to lower priority personnel are denied. Special consideration should be given to the wireless carrier who can provide the most robust QPP for mobile mass notification system access and other important public safety applications.
- Session Persistence: Wireless coverage is not ubiquitous and there may exist areas of insufficient coverage in your jurisdiction. The mass notification system needs to have a strategy for handling session discontinuity.
- If the platform is to be used in the field, then the choice of the wireless carrier should correspond with the minimum service area required at all likely emergency response staging areas. Special consideration should be given to wireless carriers that can provide a higher priority on the network for public safety than the general subscriber.

Security

Emergency notifications sent to the general public are inherently vital to preservation of life and property. Unauthorized access or worse, an unauthorized public message, can have catastrophic outcomes. Secure, authorized access to the system is a top priority.

The security should adhere to the following minimum requirements:

- FIPS 140-2[1] may be a consideration
- Virtual Private Network (VPN), security end-to-end may be a requirement
- Strong authentication and authorization mechanisms that take privacy, session management, identity management and device security features into account
- Multi-factor authentication
- Using technologies such as the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol
- Compliance with local security requirements
    - Credentialing: Support for Single Sign-On (SSO) if implemented locally
        - Ability to leverage identity, credential, and access management (ICAM),[2] or State Identity, Credential, and Access Management (SICAM)[3] credentialing

Interoperability

Interoperability between regional mass notification systems is not generally a requirement but is becoming more appealing for both a coordination and resource considerations. The mass notification systems are locally managed and operated. Additional considerations may include:

- Are there robust methods (i.e. API, SDK, web service) that allow the application to receive and send data to 3rd Party applications?
- Are resources available, either in-house or contracted, who are capable of performing the necessary technical work for any required integration (i.e. CAD or human resource software)?
- Data export and import tools

System Architecture

Mass notification systems can either be a hosted cloud-based solution or an on-premise client-server solution. Remote access to the hosted or client-server solution is through an internet browser or mobile application.

- Hardware considerations are based on the computing needs of the mobile client or application.
    - Is the client/app meant for a smartphone or tablet only?
- Software considerations include the client and required operating system(s).

[1] Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules.
[2] Federated identity, credential, and access management (ICAM) solutions are intended to help the public safety community overcome information sharing challenges and provide public safety personnel with the ability to securely gain access to critical information from a wide variety of systems.
[3] The SICAM architecture enables states and their partners to share and audit identification, authentication, and authorization across state enterprise boundaries.

  - Does the software support all browsers?
  - What mobile operating system are supported (i.e. iOS, Android, Windows)?
  - Is the mobile client a web browser-based interface only?
- Backend architecture knowledge is critical to any deployment
  - Is the system a cloud-based hosted solution or an on-premise client-server application?
  - For an on-premise architecture, is the application (server) accessible outside of the local area network?
  - What resources are required for both initial implementation and the operational upkeep of the devices that access the mass notification system?

Cost

A Rough Order of Magnitude (ROM) cost estimate should be made for each communications end-point. Prospective mass notification system vendors should provide standard product list pricing and identify all communication end-point that are and are not native to their system. All customized integration services will require the vendor to provide a reliable estimate. The preliminary cost analysis should help to address budgetary considerations and facilitate effective management decision.

Pricing should be extended to capture any non-standard hardware required, the total software solution costs, installation and integration, annual maintenance, training, warrantee, along with other special pricing considerations. Cost considerations can include:

- Justification of the need
- The cost benefit statement
- ROM pricing
- Resource requirements for implementation and operation (in-house or contract staff)
- Delivery and implementation schedule
- Impact on agency department budget

Multi-Agency Collaboration Software

Multi-agency collaboration software is frequently used at emergency operations centers (EOCs) and watch centers across the country. The software is commonly built to support the mission of crisis management involving public safety emergency response personnel, utility companies, volunteer organizations, charities, and the private sector. The software is designed to help coordinate activities by creating a collaborative environment and attempts to establish a clear operating picture during emergency events. It improves situational awareness, intelligent incident response, and promotes business resiliency. Many software solutions support daily operations to help ensure an easy transition to EOC activations during an incident escalation.

Most software solutions are designed to create a common repository of information. Personnel can keep track of incident logs, files, contact information, plans, procedures, and compliance reports. The software solutions provide position-specific activity logging and significant events tracking for real-time situational awareness during the lifecycle of an incident. The software is commonly designed to produce critical outputs such as situational reports (SITREPs) and a variety of Incident Command System (ICS) forms and reports. The software is also used to generate after-action reports allowing users to document comments and recommendations, and track the resolution of action items.

The purpose of this document is to focus on the considerations and requirements regarding the remote field interactions with mobile applications; thus, this document will explore the mobile crisis management environment and not the system as a whole.

Use Cases

The multi-agency collaboration software can either be a hosted or client-server solution. Most software solutions come with a mobile application to allow for bi-directional communications with personnel in the field. The software is used to support multiple activities and can include the following typical use case:

- Field Operations: Incident or event field operations is the most common mobile use of the collaboration software. Onsite field coordination, reporting back, and maintaining constant situational awareness with a command center is typical usage. This can be accomplished from a formal mobile command or to something as simple as a single emergency responder on foot. Depending on specific requirements and standard operating procedures of an agency or department, field operations may be used for large or small incidents such as the following:
    - Large planned event
    - Man-made disaster
    - Severe weather response
    - Forest fires
    - Transportation incident

Features

Multi-agency collaboration software solutions are platforms specifically designed to enhance information management. These solutions consume information from an assortment of different data sources and then disseminate it out to all users. The data can be generated by the personnel in the field or by agencies centrally. The typical features available are as follows.

Typical Features
• **Incident activity logging** • **Field reporting** • **Situational awareness** • **Incident and asset mapping** • **Asset, device, and logistics management** • **Notifications and alerts** • **Task and work order management** • **Email, text and multimedia messaging and alerts** • **GIS mapping and geographical visualization** • **Evacuation and patient tracking**

Adoption Considerations

There are numerous considerations when adopting a new technology, such as multi-agency collaboration software. The following subsections explore core considerations that a decision maker should address when looking to implement a specific mobile application in a toolbox category. This focuses on the mobile client application and a few of the relevant features of the core product.

Usage

Multi-agency collaboration software is a one-to-many communications product; information sent by one individual is usually posted for a group of users. By distributing the information, emergency managers and response units can build a clear operating picture. The following list highlights common mobile usage considerations.

- Understand what data is required to be accessed in your mobile environment and have a strategy for large data files
- Ensure the end user mobile device (i.e., smartphone, tablet, PC) is capable/suitable to host the client software and robust enough to display the potentially data intensive interface
- Secure access for remote viewing of data with session persistence
- Improve connectivity by using external vehicle antennas where possible
- Data Transmissions: Bi-directional data
    - Incident data
    - Record queries

  - Record creation
  - Map data
  - Multimedia files
  - AVL data
- Throughput Requirements: Variable depending on the information type
  - Textual data: Requires minimal bandwidth
  - AVL data: Requires minimal bandwidth
  - Situational Awareness or Map Data: Highly dependent upon the amount of data in the map layer. This can vary considerably from minimal to very large.
  - Multimedia Files: Some collaboration software can send and receive multimedia data to include video, images, audio, and documents. Multimedia files tend to be large and require higher bandwidth.

Wireless Connection

The following section outlines some network-related concerns that should be considered when evaluating a multi-agency collaboration software product for mobile devices used over a wireless network.

- Coverage and Priority: Multi-agency collaboration tools are critical when coordinating an incident response. Likewise, the coverage afforded by the wireless carrier needs to match the service area and expectations of the responding agencies. When selecting a wireless carrier, coverage should not be the only decision factor; quality of service, priority, and preemption (QPP) should also be considered. “Quality of service” means that public safety personnel maintain appropriate access to critical communication resources at all times. “Priority” means that public safety personnel/application receive access to those resources first, ahead of other users. “Preemption” means that higher priority personnel/applications can utilize all available resources within the network, even if services to lower priority personnel are denied. Special consideration should be given to the wireless carrier that can provide the most robust QPP for mobile collaboration tool access and other important public safety applications.
- Session Persistence: During an emergency, there may be significant areas without wireless service; therefore, all devices operating multi-agency collaboration software need to have an automated ability to store entered data and to reinitiate the session wherever possible.
- The choice of the wireless carrier should correspond with the minimum coverage and throughput requirements necessary for the multi-agency collaboration software enabled devices throughout the jurisdiction. Special consideration should be given to wireless carriers that can provide a higher priority on the network for public safety than the general subscriber.

Security

Certain data, such as law enforcement sensitive data, requires certain security protocols. Making sure the data is controlled and secure is a top priority. From the perspective of users in the field, ease of use and high security must go hand in hand. Credentialing and a secure sign on process are points to consider along with:

- Strong authentication and authorization mechanisms that take privacy, session management, identity management and device security features into account
- Multi-factor authentication
- Using technologies such as the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol
- Virtual Private Network (VPN), for local network access and end-to-end security
- Compliance with local security requirements
    - Credentialing: Support for Single Sign-On (SSO) if implemented locally
        - Ability to leverage identity, credential, and access management (ICAM),[1] or State Identity, Credential, and Access Management (SICAM)[2] credentialing

Interoperability

Interagency or interjurisdictional interoperability is accomplished through the central multi-agency collaboration system. Many collaboration systems offer an application programming interface (API) and software development kits (SDKs). In addition, multi-agency collaboration software tends to be both an information producer and consumer. This results in a requirement to ingest disparate system information as well as provide information to those same systems.

Interoperability considerations include:

- Whether there are robust methods (i.e., API, SDK, web service) that allow the application to receive and send data to 3rd Party applications
- Ensuring that data is accessible/sharable and not "locked" within a native application
- Utilizing web-based viewers to avoid proprietary clients installs
- The availability of resources, either in-house or contracted, to perform the necessary technical work for required integrations
- Ensuring that geospatial data used and produced is made available in a nonproprietary format and uses industry standards

[1] Federated identity, credential, and access management (ICAM) solutions are intended to help the public safety community overcome information sharing challenges and provide public safety personnel with the ability to securely gain access to critical information from a wide variety of systems.

[2] The SICAM architecture enables states and their partners to share and audit identification, authentication, and authorization across state enterprise boundaries.

System Architecture

Multi-agency collaboration software can either be a hosted cloud-based solution or a client-server solution. Access to the hosted or the client-server solution is generally through an internet browser or a mobile application.

- Hardware considerations:
  - Can the multi-agency collaboration software run equally well through an internet browser and mobile application, providing maximum flexibility?
- Software considerations include the client and required operating system(s)
  - What operating systems does the mobile client support (i.e., iOS, Android, Windows)?
  - Is the mobile client a browser-based interface only?
- Backend architecture knowledge is critical to any deployment
  - Is the multi-agency collaboration software a cloud-based hosted solution or an on-premise client-server application?
  - For an on-premise architecture, is the application (server) accessible outside of the local area network?
  - What resources are required for both initial implementation and the operational upkeep of the devices that access the emergency management software?

Cost

A Rough Order of Magnitude (ROM) cost estimate should be conducted on an individual and volume discount basis. Prospective multi-agency collaboration software vendors should provide standard product list pricing. The preliminary cost analysis will facilitate executive management decision making, and address budgetary considerations.

Pricing should be extended to capture the hardware and software solution costs, installation and integration, annual maintenance, training, warrantee, along with other special pricing considerations. Cost considerations can include:

- Justification of the need
- The cost-benefit statement
- ROM pricing
- Resource requirements for implementation and operation (in-house or contract staff)
- Delivery schedule
- Impact on agency department budget

Broadband Mobile Toolbox: Records Management System

The public safety records management system (RMS) is generally a system of separate databases for various public safety records. At its core, an RMS provides a method for the agency to record and manage the data associated with its activities. RMS covers the entire lifecycle of records development—from the initial generation to its completion. An effective RMS allows single entry of data, while supporting multiple reporting mechanisms; for example, automated reporting to the State and Federal agencies. The RMS should also provide the capability to electronically forward or query data from external data sources, either automatically or upon the user's request.

The RMS application either resides within the agency's internal network (on-premise) or hosted remotely (cloud service). Users (i.e. police, fire, EMS) access the mobile RMS remotely, typically through a secure, encrypted connection.

The purpose of this document is to focus on the considerations and requirements regarding the remote field interactions with mobile applications; thus, this document will explore the mobile RMS environment and not the system as a whole.

Use Cases

Records Managements Systems record data from a multitude of activities. Generally, an RMS uses purpose-built software modules for each distinct user activity; for example, electronic citations is usually a separate module from the incident report. An agency's RMS should provide the capabilities for mobile users to make inquiries to both internal and external data sources—such as the Department of Motor Vehicles, criminal history files, or data from the National Crime Information Center (NCIC). Use cases can include, accident reporting, arrests, field contact reporting, and citations.

Features

Mobile RMS applications have a set of standard features that most products offer; these are listed in the below table. The list is not all-inclusive and does not include add-ons and additional modules that may be offered by the RMS vendor. To ensure user requirements are met, your specific functionality and feature requirements should be gathered during the software assessment phase and then compared carefully to what the mobile RMS client/application offers.

The following is a list of common features available in RMS. Each feature is purpose-driven supporting a particular activity.

Typical Features	
• **Record Creation** • **Report Generation** • **Data Analysis**	• **Citations, Parking Tickets** • **Juvenile Referral List Mapping** • **Protection Orders**

• **Data Querying** • **Warrants / NCIC / Triple I[1]** • **Incident / Accident Reports** • **Case Reporting, Investigations, Intelligence & Leads** • **Master Record Notes** • **Vehicle Registrations**	• **Sex Offenders** • **Warnings** • **Gun Permits** • **Pawn Property** • **Bar Coding** • **Integrated Mug Shots** • **Notifications**

Examples of some of the external reporting and data exchange systems are listed below.

Law Enforcement - External Reports & Exchanges	Fire and EMS – External Reports
• **N-DEx (National Data Exchange System)** • **UCR[2]** • **NIBR[3]** • **LEOKA[4]**	• **NIFRS[5]** • **NEMSIS[6]** • **Computer Aided Dispatch**

Adoption Considerations

There are numerous considerations when adopting a new technology, such as mobile access to a records management system(s). The following subsections explore core considerations that a decision maker should address when looking to implement a specific mobile application in a toolbox category. This is focused on the mobile client application and not the core product, such as in RMS and computer aided dispatch (CAD) applications.

Usage

The RMS usage will be highly dependent upon the type of information sent or received by the end users. Multimedia files are quickly becoming part of the digital records systems, for example audio files are

[1] Interstate Identification Index, known by the acronym III and informally as "Triple I," is an "index-pointer" system for the interstate and Federal/State exchange of criminal history record information.
[2] The Uniform Crime Reporting (UCR) Program is a nationwide cooperative statistical effort (voluntary) of over 18,000 cities, university/college, county, state, tribal, and federal law enforcement agencies. The crime data is submitted either through a state UCR Program or directly to the FBI's UCR Program.
[3] National Incident-Based Reporting System (NIBRS), unlike UCR—an aggregate monthly tally of crimes—NIBRS goes deeper to provide circumstances and context for crimes including all offenses within a single incident, location, time of day, and whether the incident was cleared.
[4] Law Enforcement Officers Killed and Assaulted Program (LEOKA)
[5] https://www.nfirs.fema.gov/ national reporting system used by U.S. fire departments to report fires and other incidents to which they respond
[6] https://nemsis.org/ via a state EMS information system

being saved for witness statements, and images are being appended to accident reports, just to name a few.

How are you using your mobile RMS? Identifying the information you are receiving and sending is very important to understanding your wireless needs. The following list highlights some general information on data usage that should be taken into consideration.

- Understand what data is required to be accessed in your mobile environment and have a strategy for large data files
- Ensure the end user mobile device (i.e. smartphone, tablet, PC) is capable/suitable to host the client software and robust enough to display the potentially data intensive interface
- Secure access for remote viewing of data with session persistence
- Select devices with low user interaction or hands-free operation
- Improve connectivity by using external vehicle antennas where possible
- Data Transmissions: Bi-directional data
    - Record queries and report creation are sent on the uplink (send)
    - Records are sent both on the uplink (send) and downlink (receive).
- Throughput Requirements: Variable, textual information requires very little bandwidth. However, RMS systems generally provide an option to send and receive multimedia (audio, images and video) which will require higher bandwidth.
    - Textual data: Requires minimal bandwidth
    - Map Data: Highly dependent upon the amount of data in the map layer. This can vary considerably from minimal to very large.
    - Multimedia Files: Multimedia files tend to be large and will require higher bandwidth.

Wireless Connection

The following section outlines wireless network concerns that should be considered when evaluating a mobile RMS system.

- Coverage and Priority: RMS remains one of the most vital tools used by public safety. Likewise, the coverage afforded by the wireless carrier needs to match the service area and expectations of the agency. When selecting a wireless carrier, coverage should not be the only decision factor; quality of service, priority, and preemption (QPP) should also be considered. “Quality of service” means that public safety personnel maintain appropriate access to critical communication resources at all times. “Priority” means that public safety personnel receive access to those resources first, ahead of other users. “Preemption” means that higher priority personnel can utilize all available resources within the network, even if services to lower priority personnel are denied. Special consideration should be given to the wireless carrier who can provide the most robust QPP for mobile RMS access and other important public safety applications.

- Bandwidth: Excluding multimedia files, the amount of data exchanged between a mobile user and the centralized RMS can be relatively small. However, many RMS systems come with more data intensive features such as graphical map interfaces and GIS data layers. Multimedia data too, can drive bandwidth requirements. Therefore, it is important to assess the bandwidth requirement for the selected features and testing these feature in the field to ensure useful operations.
- Session Persistence: Wireless coverage is not ubiquitous and therefore there may exist areas of insufficient coverage in your jurisdiction. Therefore, the RMS system needs to have a strategy for handling session discontinuity.

Security

RMS systems transmit and receive some of the most sensitive data handled by public safety agencies. The security should adhere to the following minimum requirements.

- FIPS 140-2[7] required for all federal inquiries
- Virtual Private Network (VPN), security is required end-to-end
- Strong authentication and authorization mechanisms that take privacy, session management, identity management and device security features into account
- Multi-factor authentication
- Using technologies such as the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol
- Compliance with local security requirements
    - Credentialing: Support for Single Sign-On (SSO) if implemented locally
        - Ability to leverage identity, credential, and access management (ICAM),[8] or State Identity, Credential, and Access Management (SICAM)[9] credentialing

Interoperability

Bi-directional communications or interoperability is essential with an RMS solution in today's public safety environment. The RMS, in many installations, communicates with the local CAD system to automatically retrieve call information or it may push information out into State or Federal systems. Many RMSs offer interoperability through an application programming interface (API), software development kits (SDK), or web services that allow for various levels of interoperability. Information

[7] Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules.
[8] Federated identity, credential, and access management (ICAM) solutions are intended to help the public safety community overcome information sharing challenges and provide public safety personnel with the ability to securely gain access to critical information from a wide variety of systems.
[9] The SICAM architecture enables states and their partners to share and audit identification, authentication, and authorization across state enterprise boundaries.

stored within the RMS and externally in other systems is extremely useful and access to that data should be of the utmost importance and a leading consideration.

Interoperability considerations include:

- If requirements dictate that field personnel shall be able to query various internal and external data sources, the mobile client should:
    - Provide a secure access to required data sources
    - Provide a graphical user interface to query/look up required records
- If requirements dictate that field personnel shall be able to create and/or update records to internal and external data sources, the mobile client should:
    - Provide a secure access to required data sources
    - Provide a graphical user interface to create and/or update required records
- Are there robust methods (i.e. API, SDK, web service) that allow the application to receive and send data to 3rd Party applications?
- Are resources available, either in-house or contracted, who are capable of performing the necessary technical work for required integrations?
- Will the mobile environment require a secure connection to access additional information (i.e. NCIC, warrants, offenders, etc.)[10]?
- Will accessing additional data sources require an updated graphical user interface on the mobile client?

System Architecture

The general system architecture is an on-premise client-server scenario with many software platforms now offering a cloud based architecture. For those RMS platforms that reside inside the agency, network policies will require updating to allow for remote field access.

- Hardware considerations are based on the computing needs of the mobile RMS client or application.
    - Is the mobile RMS a thick client[11] requiring a robust computing environment?
    - Is the client/app meant for a smartphone or tablet only?
    - Are the Mobile RMS user device requirements in-line with what is currently deployed in the field?
- Software considerations include the client and required operating system(s)
    - Does your current RMS software offer a mobile RMS interface?
    - What operating systems does the client support (i.e. iOS, Android, Windows)?
    - Is the mobile client a web browser-based interface only?

[10] Please note that access to various federal and state databases may additionally require a VPN credential.
[11] A computer (client), in client-server architecture or networks, that typically provides rich functionality independent of the central server.

- Backend architecture knowledge is critical to any mobile RMS deployment
    - Is the core RMS application a cloud-based or an on-premise application?
    - For an on-premise architecture, is the core RMS application (server) accessible outside of the local network?
    - What resources are required for both initial implementation and the operational upkeep of the mobile RMS environment

Cost

A Rough Order of Magnitude (ROM) cost estimate should be conducted on an individual and volume discount basis. Prospective RMS and mobile RMS solution providers should provide standard product list pricing. The preliminary cost analysis will facilitate executive management decision making, and address budgetary considerations.

If the requirement is to add a mobile RMS capability, first determine if the legacy RMS system version supports a mobile RMS application. If not, the legacy RMS system may need to be replaced, or upgraded to a new version. Pricing should be extended to capture the hardware and software solution costs, installation and integration, annual maintenance, along with other special pricing considerations.

Cost considerations can include:

- Justification of the need
- The cost-benefit statement
- ROM pricing
- Resource requirements for implementation and operation (in-house or contract staff)
- Cost for maintenance of the program
- New hardware requirements for field deployment

Broadband Mobile Toolbox: Situational Awareness Tool

Situational awareness means many things to many people and can be applied to any situation; from an emergency event to the general status of public safety personnel. Regardless of the environment, situational awareness involves being aware of what is happening in the vicinity of the incident to understand how information, events, and one's own actions will impact goals and objectives, both immediately and in the near future.[1] For public safety to achieve this awareness – or at least some part of it – public safety and the vendor community have, for many years, attempted to automate an otherwise potentially time intensive and chaotic process. There are many applications on the market today that claim to improve or even solve situational awareness issues. The truthfulness of these claims, depends on the user, their requirements and most importantly, the incident at hand.

Is a user more aware in a situation if they can track their assets on a map in real-time? If an asset was responding to a call for service, would displaying dispatch information also be useful? What if the situation was an active shooter in a government building, would floor plans help in a time-sensitive event such as this? Maybe even building security cameras would assist in situational awareness. What about; recent geo-tagged social media posts, building evacuation plans, nearby critical infrastructure, dash cameras, land mobile radio communications, crime data, or evacuation routes? The point is, potential sources of information that contribute to situational awareness can be endless.

The amount of information the incident commander requires in a situation, depends on the situation. Too much information can become a burden and can hinder the response, unless there are rules (analysis) and automation employed to relieve the users of the tedious task of sifting through information to get what they need. Successful situational awareness tools strike a balance on the amount of information sent to the end user, so that they receive what is needed – when they need it – without being distracted from the emergency response.

The purpose of this document is to focus on the considerations and requirements regarding the remote field interactions with mobile applications; thus, this document will explore the mobile situational awareness environment and not the system as a whole, but some aspects of interaction with the system must be discussed for context reasons.

Use Cases

Having access to and sorting through the information of many disparate sources (i.e. data, video, and voice), can be the biggest challenges for situational awareness. The ability to "filter out the noise" and have the relative or important information stand out could and should be a key feature of any situational awareness tool. There are endless use cases for public safety for situational awareness

[1] https://en.wikipedia.org/wiki/Situation_awareness

applications. For the purposes of this document, we will identify three common uses in today's mobile public safety environment.

Daily Operations: Public safety agencies, at many state and local levels, use situational awareness tools to monitor the overall "health" of their state/jurisdiction. This can be as simple as a mapping interface displaying traffic and weather events to something more complex that involves analyzing CAD events and more sensitive federal databases. Resulting real-time information can be pushed out to appropriate field personnel or executive staff, via mobile device or mobile data terminal (MDT).

Incident Response: As noted in the beginning of this document, situation awareness for any incident response is dependent on the specific incident, the information available, and user requirements. In our example of an active shooter type scenario, which tends to be a relatively short timeframe incident, predetermined data sources will be necessary to achieve any type of acceptable situational awareness. Field command staff would ideally have access to this information (data, video, and voice) through their mobile devices and MDTs.

Long-term Incident Response: Incidents such as forest fires or search and rescue that have the potential to last multiple days or weeks can make use of predetermined data sources as well as ad-hoc and real-time information sources (i.e. drone video, satellite imagery, predictive modeling, and areas of concern). In this scenario, the potential for more or all field personnel having access to and making use of situational awareness, increases dramatically.

Features

Situational Awareness tools have a set of standard features that most products offer; these are listed in the below table. The list is not all-inclusive and does not include add-ons and additional modules that may be offered by a certain vendor. To ensure user requirements are met, your specific functionality and feature requirements should be gathered during the software assessment phase and then compared carefully to what the application offers.

Typical Features
• Asset location personnel/vehicles/tools mapping • Asset status personnel/vehicles/tools • Data and video integration features • Data analytics • Geospatial analytics • Rule based decision making • What-if scenarios • Threat assessment • Reporting • Messaging, Alerting & Notification

Adoption Considerations

There are numerous considerations when adopting a new technology, such as mobile access to a situational awareness tool. The following subsections explore core considerations that a decision maker should address when looking to implement a specific mobile application in a toolbox category. This is focused on the mobile client application and not the core product if there is one, such as in records management systems (RMS) and computer aided dispatch (CAD) applications.

Usage

How the data will be used in a mobile environment is critical to understanding your wireless needs. The data usage for a field-based situational awareness tool is highly dependent on the data sent and received. Data from some services, such as automatic vehicle location (AVL) or streaming video, is constantly streamed down to the application. Most other data requirements are event driven, or communicated on demand.

How are you using situational awareness? Identifying the information are you receiving and sending is very important to understanding your wireless needs. The following list highlights some general information on data usage that should be taken into consideration.

- Understand what data is required to be accessed in your mobile environment and have a strategy for large data files
- Ensure the end user mobile device (i.e. smartphone, tablet, PC) is capable/suitable to host the client software and robust enough to display the potentially data intensive interface
- Secure access for remote viewing of data with session persistence
- Improve connectivity by using external vehicle antennas where possible
- Data Transmissions: Bi-directional data
    - Record queries, record creation, and AVL data are sent on the uplink (send)
    - Records are sent both on the uplink (send) and downlink (receive)
- Throughput Requirements: Variable depending on the information type
    - Textual data: Requires minimal bandwidth
    - AVL data: Requires minimal bandwidth
    - Situational Awareness Map Data: Highly dependent upon the amount of data in the map layer. This can vary considerably from minimal to very large.
    - Multimedia Files: Send and receive multimedia data to include video, images, audio, and documents. Multimedia files tend to be large and will require higher bandwidth.

Wireless Connection

The following section outlines some of network related concerns that may need to be considered when evaluating a situational awareness tool used over a wireless network.

- Coverage and Priority: Once used, situational awareness quickly becomes a vital tool for public safety. Likewise, the coverage afforded by the wireless carrier needs to match the service area and expectations of the agency. When selecting a wireless carrier, coverage should not be the

only decision factor; quality of service, priority, and preemption (QPP) should also be considered. "Quality of service" means that public safety personnel maintain appropriate access to critical communication resources at all times. "Priority" means that public safety personnel receive access to those resources first, ahead of other users. "Preemption" means that higher priority personnel can utilize all available resources within the network, even if services to lower priority personnel are denied. Special consideration should be given to the wireless carrier who can provide the most robust QPP for mobile situational awareness access and other important public safety applications.

- Session Persistence: Wireless coverage is not ubiquitous and therefore there may be areas of insufficient coverage. If the situational awareness tool is deemed mission critical, a strategy for handling session discontinuity requires a solution.
- The choice of the wireless carrier should correspond with the minimum coverage and throughput requirements necessary for the operations of the situational awareness tool throughout the jurisdiction. Special consideration should be given to wireless carriers who can provide a higher priority on the network for public safety than the general subscriber.

Security

Due to the possible sensitivity of the ingested data sources, an encrypted connection should be required as standard. Exact security requirements will depend on accessed information but the following list includes security features that should be considered.

- FIPS 140-2[2] required for all federal inquiries
- Virtual Private Network (VPN), for local network access and end-to-end security
- Strong authentication and authorization mechanisms that take privacy, session management, identity management and device security features into account
- Multi-factor authentication
- Technologies such as the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol
- Compliance with local security requirements
    - Credentialing: Support for Single Sign-On (SSO) if implemented locally
        - Ability to leverage identity, credential, and access management (ICAM),[3] or State Identity, Credential, and Access Management (SICAM)[4] credentialing

[2] Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules.
[3] Federated identity, credential, and access management (ICAM) solutions are intended to help the public safety community overcome information sharing challenges and provide public safety personnel with the ability to securely gain access to critical information from a wide variety of systems.
[4] The SICAM architecture enables states and their partners to share and audit identification, authentication, and authorization across state enterprise boundaries.

Interoperability

Interagency or interjurisdictional interoperability is accomplished through the central situational awareness system. Many situational awareness systems offer an application programming interface (API) and software development kits (SDKs). In addition, situational awareness applications tend to be more of an information consumer rather than an information producer. With that said, analytical products could and should be produced which could require results to be sharable with other systems/applications. The sharing of data is evaluated on an agency-by-agency/jurisdiction-by-jurisdiction basis.

Interoperability considerations include:

- Are there robust methods (i.e. API, SDK, web service) that allow the application to receive and send data to 3rd Party applications?
- Are resources available, either in-house or contracted, who are capable of performing the necessary technical work for required integrations?
- If requirements dictate that field personnel shall be able to query various internal and external data sources, the mobile client should:
    - Provide secure access to required data sources
    - Provide a graphical user interface to query/look up required records
- If requirements dictate that field personnel shall be able to create and/or update records to internal and external data sources, the mobile client should:
    - Provide secure access to required data sources
    - Provide a graphical user interface to create and/or update required records
- Agency Records Management Systems
    - For Law Enforcement, it would include query access to State and National Records (NCIC, Warrants, Offenders, etc.)[5]
- Communication systems (land mobile radio [LMR] systems, message and alerting platforms, etc.)

System Architecture

The architecture of the situational awareness itself may be fairly simplistic, probably an on-premise client-server environment. Due to the probability of a requirement to ingest multiple data sources, internal and external, this could very quickly complicate the overall system architecture.

- Hardware considerations are based on the computing needs of the mobile situational awareness client or application.
    - Is the mobile situational awareness application a thick client[6] requiring a robust computing environment?

[5] Please note that access to various federal and state databases may require an additional VPN credential.
[6] A computer (client), in client-server architecture or networks, that typically provides rich functionality independent of the central server.

    - Is the client/app meant for a smartphone or tablet only?
- Software considerations include the client and required operating system(s)
    - Does your current situational awareness software offer a mobile situational awareness interface?
    - What operating systems does the client support (i.e. iOS, Android, Windows)?
    - Is the mobile client a browser-based interface only?
- Backend architecture knowledge is critical to any mobile situational awareness deployment
    - Is the core situational awareness application a cloud-based or an on-premise application?
    - For an on-premise architecture, is the core situational awareness application (server) accessible outside of the local network?
    - What resources are required for both initial implementation and the operational upkeep of the mobile situational awareness environment?

Cost

A Rough Order of Magnitude (ROM) cost estimate should be conducted on an individual and volume discount basis. Perspective situational awareness and mobile situational awareness solution providers should provide standard product list pricing. The preliminary cost analysis will facilitate executive management decision making, and address budgetary considerations.

If the requirement is to add a mobile situational awareness capability, first determine if the legacy situational awareness system version supports a mobile situational awareness application. If not, the legacy situational awareness system may need to be replaced, or upgraded to a new version. Pricing should be extended to capture the hardware and software solution costs, installation and integration, annual maintenance, along with other special pricing considerations.

Cost considerations can include:

- Justification of the need
- The cost-benefit statement
- ROM pricing (to take into account any and all data source integration)
- Cost for maintenance of the program
- Resource requirements for implementation and operation (in-house or contract staff)
- Delivery schedule
- Impact on agency department budget

Broadband Mobile Toolbox: Telemedicine and Telemetry

The focus of this document is on emergency care mobile telemedicine, and not telemedicine as a whole. Telemedicine is far reaching and goes beyond the public safety realm into all aspects of healthcare, outpatient care, inpatient care, nursing home care, workplace, and consumer homes. Emergency care telemedicine or telemedicine for the remainder of the document, is an important group of technologies designed to better treat the injured. Telemedicine extends emergency patient care beyond the emergency room – or more directly – it is designed to bring highly specialized medical care directly to the patient at the scene of the incident or while in transport.

Using the tools of telemedicine, doctors and specialists can be brought to the incident scene where they can better speed the triage of patients, direct more complex treatments sooner, and help to improve medical outcome thus resulting in more successful emergency treatments. This can be especially true in rural areas, where access to specialized medical care can be limited and distances to advanced care centers can be large.

One of the most important tools for telemedicine is telemetry. Telemetry is defined as an automated communications process by which measurements and other data are collected and then transmitted to a central location for monitoring. The most common example of telemetry is cardiac monitoring. Today, cardiac monitoring is coupled with other vital sign data for a clearer picture of patient's health status. In addition to vital sign monitoring, streaming video is an important component for telemedicine. With real-time video, a health care specialist can get a better grasp of the severity of an incident and better consult with on-site paramedics.

The purpose of this document is to focus on the considerations and requirements regarding the remote public safety field interactions with mobile applications; thus, this document will explore the mobile telemedicine environment and not the system as a whole.

Use Cases

Telemedicine and telemetry solutions, used by public safety, are generally referred to as point-to-point connections; it is a link between the patient and central health facility via a high-speed wireless connection. This type of telemedicine creates a digital connection between the patient and a remote monitoring facility, so that a patient's medical data is measured and then transmitted electronically to a distant medical monitoring facility. If additional medical consultation is required, the medical facility can forward the medical data to a specialist at yet another location. The most common telemetry use cases are for the monitoring of pulmonary, cardiac, and prenatal medical data.

Features

Mobile telemedicine and telemetry solutions are specialty devices designed to monitor specific vital signs and to transmit the information to a specific medical center. The features are built into the device selection and are chosen at the point of purchase. A robust wireless broadband connection is critical to the successful use of mobile telemedicine and telemetry.

Typical Features
• **Cardiac Monitoring** • **Pulmonary Monitoring** • **Prenatal Monitoring** • **Point-to-Point Video and Audio**

In addition, telemedicine Common Objectives[1] are provided as a source of reference.

Common Objectives
• **Improving patient outcomes** • **Increasing patient engagement and satisfaction** • **Improving patient convenience** • **Providing remote and rural patients with access to care** • **Improving leverage of limited physician resources** • **Reducing cost of care delivery** • **Reducing hospital readmissions** • **Improving specialist efficiency** • **Providing access to new specialties** • **Providing 24/7 access to specialists**

Adoption Considerations

There are numerous considerations when adopting a new technology, such as mobile access to telemedicine and telemetry solutions. The following subsections explore considerations that a decision maker should address when looking to implement a specific mobile application in a toolbox category. This is focused on the mobile client application and not the core product if there is one, such as in records management systems (RMS) and computer aided dispatch (CAD) applications.

[1] 2017 industry survey: http://reachhealth.com/resources/telemedicine-industry-survey/

Usage

Telemedicine is a point-to-point communications link for medical data (telemetry equipped devices) and, where possible, streaming video. The following list highlights some general information on typical data usage:

- Telemetry Equipped Devices: Bi-directional data
  - Data Transmissions:
    - Due to the importance of the data, it is must be received in near real-time with very little latency
  - Throughput requirements:
    - Overall, the data throughput requirements are minimal (a few tens of kbps) and almost all the data is sent on the uplink connection
- Stream Video: Can be uplink only or Bi-directional data
  - Data Transmissions:
    - The purpose of the video connection is to give medical practitioners a better idea of the severity of the injury. Therefore, video sent from the scene to the medical center is of a primary concern.
    - The video can be sent from a hand-held camera or one that is fixed inside the ambulance.
    - In some applications, such as mental health checkups, the video is two-way so the patient and physician can see and talk to each other.
  - Throughput requirements:
    - The throughput requirement is highly dependent on the quality of the video sent. Typical network throughput requirements for streaming video is given below.

Video Quality	Resolution	Frame Rate	Video Bitrate
240p	426-240	30	0.3-0.7 Mbps
360p	640x360	30	0.4-1 Mbps
480p	853x480	30	0.5-2 Mbps
HD 720p	1280x720	30	1.5-4 Mbps
Full HD 1080p	1920x1080	30	3-6 Mbps

Wireless Connection

The following section outlines some network related concerns that should be considered when evaluating a telemedicine and telemetry equipped device for use over a wireless network.

- Coverage and Priority: telemedicine is one of the most vital tools used by public safety. Likewise, the coverage afforded by the wireless carrier needs to match the service area and expectations of the agency. When selecting a wireless carrier, coverage should not be the only decision factor; quality of service, priority, and preemption (QPP) should also be considered. "Quality of service" means that public safety personnel maintain appropriate access to critical communication resources at all times. "Priority" means that public safety personnel receive access to those resources first, ahead of other users. "Preemption" means that higher priority personnel can utilize all available resources within the network, even if services to lower priority personnel are denied. Special consideration should be given to the wireless carrier who can provide the most robust QPP for mobile telemedicine access and other important public safety applications.
- Session Persistence: Wireless coverage is not ubiquitous and therefore there may be areas of insufficient coverage. All telemetric enabled devices need to have an automated ability to reinitiate the session wherever possible.
- The choice of the wireless carrier should correspond with the minimum coverage and throughput requirements necessary for the telemedicine operations and telemetric enabled devices throughout the jurisdiction. Special consideration should be given to wireless carriers who can provide a higher priority on the network for public safety than the general subscriber.

Security

Medical health care data transmitted by telemetric enabled devices falls under the Health Insurance Portability and Accountability Act (HIPAA[2]) definition of privileged data. Due to the sensitivity of medical data an encrypted connection is required. Exact security requirements will depend on local IT requirements the following list includes security features that should be considered.

- Virtual Private Network (VPN), for local network access and end-to-end security
- FIPS 140-2[3] encryption compliance
- Strong authentication and authorization mechanisms that take privacy, session management, identity management and device security features into account
- Multi-factor authentication
- Using technologies such as the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol

[2] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996. Sections 261 through 264 of HIPAA require the Secretary of HHS to publicize standards for the electronic exchange, privacy and security of health information

[3] Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules.

Interoperability

Telemedicine is a point-to-point communications link for medical data between the parametric unit and the medical center. The transmission specifications for telemetry data varies greatly from Group 3 Facsimile standard[4] to IP enabled standards connected via Bluetooth, Wi-Fi or carrier based internet. Each telemetric enabled device should utilize a standardized medical data format so that if necessary, the data can be sent to an alternate medical center.

System Architecture

Telemetric enabled devices either connect directly to the medical center through a built in wireless modem or establish a connection through a wireless hotspot or mobile router. The ultimate system architecture will be dependent upon the selected enabled capabilities of the telemetric medical device.

- Hardware considerations.
  - Does the telemetric enabled device connect to the medical center?
  - Does the telemetric enabled device require a client/app on a smartphone or tablet to operate?
- Software considerations include the client and required operating system(s)
  - What operating systems does the client support (i.e. iOS, Android, Windows)?
  - Is the mobile client a browser-based interface only?
- Backend architecture knowledge is critical to any deployment
  - Is the telemetric application a cloud-based or an on-premise application?
  - For an on-premise architecture, is the telemetric application (server) accessible outside of the local network?
  - What resources are required for both initial implementation and the operational upkeep of the telemetric devices?

Cost

A Rough Order of Magnitude (ROM) cost estimate should be conducted on an individual and volume discount basis. Prospective telemetric medical device vendors should provide standard product list pricing. The preliminary cost analysis will facilitate executive management decision making, and address budgetary considerations.

Pricing should be extended to capture the hardware and software solution costs, installation and integration, annual maintenance, training, warrantee, along with other special pricing considerations.

Cost considerations can include:

- Justification of the need
- The cost-benefit statement

[4] Example: http://www.zoll.com/uploadedFiles/Public_Site/Products/E_Series/ESeries-SpecLo.pdf

- ROM pricing
- Resource requirements for implementation and operation (in-house or contract staff)
- Cost for maintenance of the program
- Delivery schedule
- Impact on agency department budget

Broadband Mobile Toolbox: Video

First responders have come to rely on video technology to increase their onsite situational awareness, to remotely monitor an incident, and to enhance day-to-day operations. Mobile video provides many important benefits for public safety, including: increased citizen safety, improved transparency, and better public safety response. Mobile video can enhance public safety efficiency and improve the command center awareness of an incident, allowing decisions to be made faster and assets dispatched more efficiently, providing a better overall emergency response.

Recent years have seen a significant increase in the use of video in the mobile environment. High resolution/high quality video is a large consumer of bandwidth. Sustaining a high level of throughput is difficult over current commercial wireless networks. In many instances, high throughput levels are not sustained. Video data rates can vary dramatically depending on the resolution, frame rate and video compression quality. Careful consideration must be given to video usage, specifically on how it will be transported both to and from the field.

The purpose of this document is to focus on the considerations and requirements that affect remote field interactions with mobile applications, this document will explore the mobile video environment and not the system as a whole.

Use Cases

There are a great many use cases for public safety video. For the purposes of this document, we will concentrate on common uses in today's mobile public safety environment.

In-Vehicle Cameras: In-vehicle cameras, or dashcams can be a simple single front facing vehicle mounted camera or more complex with 2, 3, or 4 fixed cameras. Vehicle cameras are versatile and have many applications from law enforcement evidentiary benefits, to fire situational awareness, to EMS telemedicine. Vehicle camera deployment is typically designed with an onboard storage system. The video stored on the unit storage device is either manually removed or uploaded to the public safety entity's local network. Live streaming of video back to a command center has become more common recently.

Bodycam: The use of body-worn cameras (BWCs) within the law enforcement community has drastically increased over the past several years. The suggested benefits of BWCs include improved civility of police-citizen encounters and enhances citizen perceptions of police transparency and legitimacy. The BWCs typically stores the video locally on the device, and most devices are designed to be available for an entire shift. User requirements will dictate video quality and storage capacity, with lower resolution and quality increasing the allowable recording time. BWCs commonly upload the video content via a networked docking station. Live streaming of video back to a command center has also become more common recently.

Transportation Cameras: Transportation cameras are designed for continuous observation and general public safety. Transportation cameras are fixed on buildings, alongside roads, at intersections, in public places, and mounted inside public transportation. Mobile access to street level cameras are typically used for situational awareness and are a common method for quickly assessing an area or situation. These cameras typically fall into two categories, those that stream their feeds to a central location and those that store their video on onboard storage systems. The cameras that stream their feeds to a central location may or may not record the video on a central video management system.

Drone Cameras: The use of drones has grown exponentially in the commercial sector over the last few years, however, use by public safety agencies has only begun. 2016 saw less than 400 agencies adopt drone technology nationwide[1]. But growth is expected to rise as technology and applications improve. Use in search and rescue and wildfire tracking are the most common applications for drones. A Drone camera can be deployed with or without a local storage device. Most drones have the option to stream video back to the remote user or incident command center. These drones generally use unlicensed WiFi spectrum for both telemetry and video transport; however, licensed 4.9GHz spectrum is also an option.

Features

Mobile video applications have a set of standard features that most products offer; these are listed in the below table. The list is not all-inclusive and does not include add-ons and additional modules that may be offered by the mobile video vendor. To ensure user requirements are met, your specific functionality and feature requirements should be gathered during the software assessment phase and then compared carefully to what the mobile video application offers.

Typical Features	
• **Viewing of live streaming video** • **Recording of live video** • **Automatic Event Triggering (for recording)** • **Pre-event recording (ex. automatic buffering 30 to 60 seconds)** • **Smartphone, Tablet, or PC accessible**	• **Thermal Imaging** • **Telemedicine** • **Real time analytics** • **License plate reader (Optical character recognition-OCR)** • **Video conferencing**

Adoption Considerations

There are numerous considerations when adopting a new technology, such as mobile access to video. The following subsections explore core considerations that a decision maker should address when looking to implement a specific mobile application in a toolbox category. This is focused on the mobile client application and not the core product if there is one, such as in a centralized video management platform.

[1] http://dronecenter.bard.edu/files/2017/04/CSD-Public-Safety-Drones-Web.pdf

Usage

There are two specific use cases for video: prerecorded video or live video streaming. In the prerecorded use case, the main issue here is the size of the data file requested. For example, one minute of HD quality video recorded at 30 frames/second and using H.264[2] compression will likely generate a data file of 45MB. The compression standard, resolution, frame rate and recording time are all variables that define the data file size.

Streaming video has similar constraints. Here the video quality is directly correlated to the amount of data transmitted or received over the network connection. Most video players are adaptive and adjust to the quality of the data and the available throughput of the network connection. For adaptive players, as the throughput of the network connection degrades, so too will the video quality. Typical network throughput requirements for streaming video is given below.

Video Quality	Resolution	Frame Rate	Video Bitrate
240p	426-240	30	0.3-0.7 Mbps
360p	640x360	30	0.4-1 Mbps
480p	853x480	30	0.5-2 Mbps
HD 720p	1280x720	30	1.5-4 Mbps
Full HD 1080p	1920x1080	30	3-6 Mbps

- Data Transmissions:
  - The quality of the streaming video is latency intolerant and highly dependent on the quality of the network connection
  - The ability to send or receive recorded video will depend upon the available bandwidth and the amount of video (file size).
- Throughput Requirements: Variable depending on compression standard, resolution, frame rate, and for recorded video, the length of time.
- Understand what data is required to be accessed in your mobile environment and have a strategy for large data files
- Ensure the end user mobile device (i.e. smartphone, tablet, PC) is capable/suitable to host the client software and robust enough to display the potentially data intensive interface
- Improve connectivity by using external vehicle antennas where possible

[2] H.264 is a block-oriented motion-compensation-based video compression standard used for the recording, compression, and distribution of video content.

Wireless Connection

Video is a data intensive form of communications. The streaming of high resolution video can easily consume most of the bandwidth available on the wireless network. It is not uncommon to see a single camera stream 2-4Mbps of data and generate more than 100GB of data per month. Therefore, careful management techniques need to be deployed in order to balance the availability of the bandwidth with the desired image quality. Secondly, video data files can be quite large, likewise, if commercial networks are used for transport, then the rate plan needs to match the likely monthly usage.

- Wireless Plan:
  - The choice of the wireless carrier and the network plan should correspond to the likely amount of data you plan to transmit or receive.
  - Video quality is highly dependent on the amount of bandwidth available on the network, if your expectation is to have the best video quality available, then you will need to consider prioritizing video over other less important applications.
  - Assigning a higher priority[3] to video, more network resources can be allocated and thus quality can improve.
- Uplink vs. Downlink Capacity:
  - Wireless networks are not perfectly symmetrical, there is not an equal amount of capacity on both the uplink (the connection from the mobile device to the wireless network) versus the downlink (from the wireless network to the mobile device).
  - Uplink capacity is generally less than downlink capacity resulting in better performance viewing streaming video than sending streaming video.
- Coverage and Priority: Video has become a vital tool used by public safety. Therefore, the coverage afforded by the wireless carrier needs to match the service area and expectations of the agency. When selecting a wireless carrier, coverage should not be the only decision factor; quality of service, priority, and preemption (QPP) should also be considered. “Quality of service” means that public safety personnel maintain appropriate access to critical communication resources at all times. “Priority” means that public safety personnel receive access to those resources first, ahead of other users. “Preemption” means that higher priority personnel can utilize all available resources within the network, even if services to lower priority personnel are denied. Special consideration should be given to the wireless carrier who can provide the most robust QPP for mobile video access and other important public safety applications.
- Session Persistence: Wireless coverage is not ubiquitous, there may be areas of insufficient coverage. Therefore, the video module needs to have a strategy for handling session discontinuity.
- The choice of the wireless carrier should correspond with the minimum coverage and throughput requirements necessary for use of mobile video throughout the jurisdiction. Special consideration should be given to wireless carriers who can provide a higher priority on the network for public safety than the general subscriber.

[3] https://firstnet.gov/newsroom/blog/priority-pre-emption-and-quality-service-tutorial-lte-key-concepts

Security

Video source data can be made available to the general public; an example can include traffic or weather cameras. However, due to the sensitivity of most video sources, an encrypted connection is required. Exact security requirements will depend the local regulations and common policy regarding the data. If security is required, then the following items may need to be taken into consideration.

- FIPS 140-2[4] required for all federal inquiries
- Virtual Private Network (VPN), for local network access and end-to-end security
- Strong authentication and authorization mechanisms that take privacy, session management, identity management and device security features into account
- Multi-factor authentication
- Technologies such as the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol
- Compliance with local security requirements
    - Credentialing: Support for Single Sign-On (SSO) if implemented locally
        - Ability to leverage identity, credential, and access management (ICAM),[5] or State Identity, Credential, and Access Management (SICAM)[6] credentialing

Interoperability

Video cameras support multiple standardized video compression technologies. However, not all cameras are fully interoperable and may require proprietary drivers/software to view resulting video. As a consequence, cameras come with drivers and generally with an associated API or SDK to aid developers with the integration into the video management platforms. When reviewing the interoperability of a video system, the agency should:

- Ensure that all video sources have available APIs or SDKs to allow greater integration with applications.
- If integration is required, ensure you have the necessary resources to accomplish the technical task.
- Develop standards or guidelines for video management platforms or video sources that require credentialed access

[4] Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules.
[5] Federated identity, credential, and access management (ICAM) solutions are intended to help the public safety community overcome information sharing challenges and provide public safety personnel with the ability to securely gain access to critical information from a wide variety of systems.
[6] The SICAM architecture enables states and their partners to share and audit identification, authentication, and authorization across state enterprise boundaries.

- Develop compression and resolution standards based on the likely use cases. For example, poor-quality resolution can severely limit the video for evidentiary purposes.

System Architecture

Video management systems are used to manage, view and store data. The storage of the video data can be done locally or sent to a central storage system. Both systems generally overwrite stored video data after a preset period; however, some systems can keep video data for years, or indefinitely, if required.

- Hardware considerations are based on the computing needs of the mobile video client or application.
    - Is the mobile video a thick client[7] requiring a robust computing environment?
    - Is the client/app meant for a smartphone or tablet only?
- Software considerations include the client and required operating system(s)
    - Does your current video software offer a mobile video interface?
    - What operating systems does the client support (i.e. iOS, Android, Windows)?
    - Is the mobile client a browser-based interface only?
- Backend architecture knowledge is critical to any mobile video deployment
    - Is the centralized video management platform a cloud-based or an on-premise application?
    - For an on-premise architecture, is the video management platform (server) accessible outside of the local network?
    - What resources are required for both initial implementation and the operational upkeep of the mobile video environment?

Cost

A Rough Order of Magnitude (ROM) cost estimate should be conducted on an individual and volume discount basis. Vendors should provide standard product list pricing for both the devices as well as the video management software. The preliminary cost analysis should help to address budgetary considerations and facilitate effective management decisions.

Pricing should be extended to capture the hardware and software solution costs, installation and integration, annual maintenance, training, warrantee, along with other special pricing considerations. Cost considerations can include:

- Does the cost include an API or SDK?
- What will it cost – and what is the level of effort if integration with other systems is required?
- Justification of the need

[7] A computer (client), in client-server architecture or networks, that typically provides rich functionality independent of the central server.

- The cost benefit statement
- ROM pricing
- Resource requirements for implementation and operation (in-house or contract staff)
- Cost for maintenance of the program
- Delivery schedule
- Impact on agency department budget

Broadband Mobile Toolbox: Wearable Devices and Sensors

With technology moving rapidly and recent advances in the Internet of Things (IoT), the field of wearable devices and sensors is beginning to grow in areas once only imagined. Presently, the commercially available technologies are constrained to a few law enforcement and emergency medical applications. New application and technology offerings, across all public safety disciplines, are expected in the near future.

A wearable device can act as an alert or an alarm based on a specific event or series of events. It may monitor a specific activity, such as medical vital signs or the status of a weapon in a holster, and then send that data for analysis. Wearable devices may be in constant communication, updated on a near real-time basis with the host application, or have little to no communications until it receives some event or trigger. Wearables depend on a wireless network connection to communicate back to their corresponding systems.

Some of the more common wearable devices or sensors are:

- Body Armor Sensors – Generally a passive device unless triggered
- Holster Sensor – Generally a passive device unless triggered
- Ankle Monitor – Active device designed to actively transmit location
- Vital Sign Monitor – Active device designed to actively transmit specific vital signs

There is a potential for significant growth in the wearable device marketplace as newer technologies are developed and as networks that support machine-to-machine[1] communications expand. This document provides an outline of the basic requirements and considerations for the most common device form factors and is not intended to detail the system as a whole.

Use Cases

The use case for wearable devices and sensors are very specific. For example, body armor sensors can alert the network in the case of damage to the body armor or a man-down scenario. Body armor sensors use accelerometers and a mesh circuit integrated into the vest for this purpose. Active devices, such as ankle monitors actively transmit the location of the wearer. Ankle monitors derive the location through a GPS receiver and/or through the location-based services embedded within the wireless networks. Use cases for a few known devices are:

- Body Armor Sensors
    - Can detect damage to the body armor
    - Can detect lack of motion (man-down)
- Holster or Firearm Sensor

[1] This refers to direct automated data transmission and measurement between mechanical or electronic devices using any communications channel.

  - Can detect removal of firearm from holster
  - Can detect firearm recoil
- Ankle Monitor
  - Can detect removal of device or device tampering
  - Can detect motion or lack of motion
  - Can detect active location
- Vital Sign Monitor
  - Can detect external sensorial inputs: heart rate, respiratory activity, etc.
  - Can detect location

Features

The features found with wearable devices or sensors are specific to the device application. Some typical features found in these devices are as follows.

Typical Features
• **Motion Detection or Movement** • **Event triggering, break of circuit, damage, device tampering** • **External Sensorial Input: heart rate, respiratory activity, etc.** • **Location through GPS or wireless network location based services**

Adoption Considerations

There are numerous considerations when adopting a new technology such as a field-worn device. The following subsections explore considerations that a decision maker should address when looking to implement a specific mobile application in a toolbox category. This is focused on the mobile client application, such as in records management systems (RMS) or computer aided dispatch (CAD) applications, and not the core product if there is one.

Usage

The data transmitted by wearable devices is relatively minimal. The communications between the device and the network is specifically tailored to the purpose of the device, therefore the amount of data sent is minimized by design to conserve power and make the device more resilient on a wireless network.

Software applications that manage and report the status of wearable devices can be cloud-based or a client-server solution. The software application receives the inputs from the wearable device and can retransmit status or notifications to a user or a group of users through a web interface, email, SMS messaging or a client application. For active wearables, the required bandwidth will be a small, continuous stream of data that would be like the loading of a typical web page. Bandwidth requirements from a passive device would be considerably smaller as these devices would only transmit when

triggered. Access to the data from the sensors is either from an interface supplied with the software, or through a web browser.

Communications between the wearable device and the software application is generally on the uplink; from the wearable device to the software application. Some software applications have the ability to communicate directly with the wearable device; however, in many situations, this is limited to firmware upgrades or software updates.

- Throughput Requirements: minimal on uplink, similar to web browsing

Wireless Connection

As stated above, data is usually sent from the device to a wireless network. The devices are use-case-specific, meaning that the communications will be limited to the purpose the device serves. The network connection can be direct; from the wearable device to the software application over a public or commercial wireless network or the wearable device can communicate through a secondary device, such as a smartphone, Wi-Fi hotspot, or mobile router.

The connection requirements for a wearable device can run the full gamut of options, from devices that require active connections and session persistence, to devices that can operate offline and store event data until retrieved. At a minimum, the following should be considered:

- Coverage and Priority: Wearable devices are becoming more important as their portfolio expands for public safety. Likewise, the coverage afforded by the wireless carrier needs to match the service area and expectations of the agency. When selecting a wireless carrier, coverage should not be the only decision factor; quality of service, priority, and preemption (QPP) should also be considered. “Quality of service” means that public safety personnel maintain appropriate access to critical communication resources at all times. “Priority” means that public safety personnel/application receive access to those resources first, ahead of other users. “Preemption” means that higher priority personnel/applications can utilize all available resources within the network, even if services to lower priority personnel are denied. Special consideration should be given to the wireless carrier that can provide the most robust QPP for wearable devices and other important public safety applications.
- Session Persistence: Wireless coverage is not ubiquitous and there may be areas of insufficient coverage. Therefore, the device and/or application needs to have a strategy for handling session discontinuity.
- The choice of the wireless carrier should correspond with the minimum coverage and throughput requirements necessary for the operation of the wearable device throughout the jurisdiction. Special consideration should be given to wireless carriers that can provide a higher priority on the network for public safety than the general subscriber.

Security

The security requirement can vary greatly due to the sensitivity of the data transmitted. The security requirements will be driven by local, state and federal laws and regulations. If the data is deemed sensitive or protected, then the minimum requirements are as follows:

- Network encryption of the data; FIPS 140-2[2]
- Using technologies such as the Secure Sockets Layer (SSL) or Transport Layer Security (TLS) protocol
- Medical health care data transmitted by wearable devices generally falls under the Health Insurance Portability and Accountability Act (HIPAA[3]) definition of privileged data.

Interoperability

Communications between wearable devices is envisioned for the future; however, most devices limit their communications to the software application that reports their status. Interoperability between software applications can be achieved through common APIs and SDKs provided by the vendor.

System Architecture

The software application that manages the wearable device can either be a hosted cloud-based solution or a client-server solution. The wearable devices generally transmit their data only on the uplink.

- Hardware considerations for the wearable device: Generally, none, the devices are purpose-built. Some wearable devices communicate through secondary devices such as smartphones, hotspots, or mobile routers. Pairing or communication credentials may be required.
- Software considerations for the remote user: None, dependent upon the wearable solution
- Backend architecture
    - Is the software application a cloud-based hosted solution or, an on-premise client-server application?
    - For an on-premise architecture, is the application (server) accessible outside of the local area network?
    - What resources are required for both initial implementation and the operational upkeep of the devices and the software application?

[2] Federal Information Processing Standard (FIPS) Publication 140-2, (FIPS PUB 140-2), is a U.S. government computer security standard used to approve cryptographic modules.
[3] Health Insurance Portability and Accountability Act of 1996 (HIPAA), Public Law 104-191, was enacted on August 21, 1996. Sections 261 through 264 of HIPAA require the Secretary of HHS to publicize standards for the electronic exchange, privacy and security of health information.

Cost

A Rough Order of Magnitude (ROM) cost estimate should be conducted on an individual and volume discount basis. Prospective wearable device vendors should provide standard product list pricing. The preliminary cost analysis will facilitate executive management decision making, and address budgetary considerations.

Pricing should be extended to capture the hardware and software solution costs, installation and integration, annual maintenance, training, warrantee, along with other special pricing considerations.

Cost considerations can include:

- Justification of the need
- The cost benefit statement
- ROM pricing
- Resource requirements for implementation and operation (in-house or contract staff)
- Delivery schedule
- Impact on agency/department budget