In Response To:
DEPARTMENT OF COMMERCE National Institute of Standards and Technology
[Docket No.: 110727437–1433–01]

Title:
"Input on Research and Development Priorities for Desirable Features of a Nationwide Public Safety Broadband Network"

Submitted To:
Mr. Dereck Orr,
Office of Law Enforcement Standards,
National Institute of Standards and Technology,
325 Broadway, Boulder, Colorado 80305,
Telephone number (303) 497–5400.
e-mail address is *dereck.orr@nist.gov*.

Date:
October 12, 2011

Textron Systems | P.O. BOX 91269 | Austin, TX 78709-1269 | USA

POINT OF CONTACT:
Project Manager Name: Evan Corwin
Location: Austin, Texas
Email Address: ccorwin@overwatch.textron.com
Phone Number: 512-484-6996

Table of Contents

1 Introduction 3
1.1 Resiliency in an Emergency 6
1.1.1 Resiliency 6
1.1.2 Self-Organizing 7
1.1.3 Meshing 8
1.1.4 Adaptability 8
1.2 Reliability and Availability 10
1.2.1 Prioritization 10
1.2.2 Quality of Service (QoS) 11
1.3 Security 12
1.3.1 Strong, Dynamic Access Control 12
1.4 Affordability / Commercial Alignment 14
1.4.1 Compatibility with Commercial Infrastructure 14
1.4.2 Network Sharing 14
1.4.3 Scalability 15
1.4.4 Power Awareness 17
1.4.5 Standardized Common Interfaces 18
1.4.6 Uniform, Universal Access 19
2 Further Considerations 21
3 Conclusion 22
Appendix A. The Textron Systems Team Solution 23

Disclosure Policy

This response contains trade secrets and/or privileged or confidential commercial or financial information. This information is maintained in confidence in the course of the Offeror's business and is not otherwise publicly available. The Offeror submits this information in confidence and understands that this information shall not be released or disclosed without the expressed written consent of the Offeror.

1 Introduction

The Textron Systems team is pleased to provide the U.S. Department of Commerce's (DoC) National Institute of Standards and Technology (NIST) inputs on various possible features of a new nationwide interoperable public safety broadband network.

For the past several years, the Textron Systems team, which consists of Textron Systems and xG Technology, has been working on and fielding technology solutions relevant to the Nationwide Public Safety Broadband Network. The commentary in this document is based on the knowledge gained by the team while building, testing and fielding infrastructure and software technology for dynamic broadband networks.

Textron Systems is a world leader in providing integrated, networked information solutions designed for use in tactical environments. The company's spectrum of capabilities includes operational and intelligence systems, multimodal sensor systems, geospatial intelligence, communications systems, airborne platforms, ground vehicles, and terrestrial based platforms.

The Textron Systems team is being led by the Overwatch Systems operating unit of Textron Systems. Overwatch Systems' expertise includes multi-source intelligence (multi-INT), geospatial analysis and custom intelligence solutions provided to the U.S. national agencies, civilian organizations, and the Department of Defense (DoD). The Textron team brings together mature, best of breed COTS/GOTS capabilities designed to operate on any private or commercial cellular network. This includes our partner xG Technologies who provide the secure, cognitive radio links between the handheld smart phone/tablet at the edge and the cellular broadband network backhaul.

Overwatch Systems' handheld, desktop and server-based software solutions improve situational understanding and deliver actionable intelligence in support of counter-terrorism, irregular warfare, civil, military and combined applications. More than 25,000 analysts in various Government agencies and organizations utilize Overwatch solutions. The company has experience delivering mission critical, secure analytic applications to the U.S Government and has fielded applications that have provided critical support to operations in Bosnia, Operation Iraqi Freedom and Operation Enduring Freedom. The company's capabilities were also used for Homeland Security Operations such as the Katrina emergency response (Figure 1).

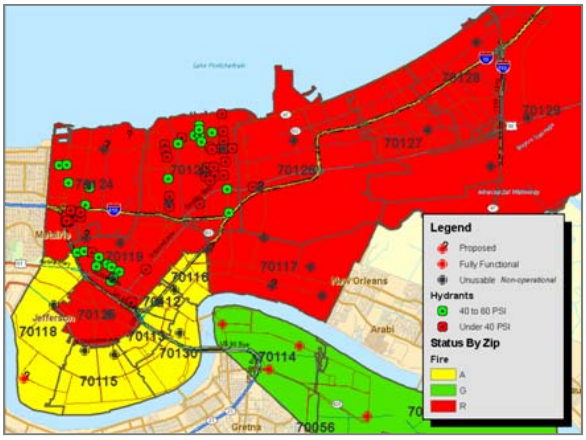

Figure 1. Overwatch analytic tools support Katrina emergency management efforts in 2005.

As a systems integrator, Textron Systems strives to develop open architecture, nonproprietary solutions and is always looking for best of breed partner solutions that share our vision of offering our customers the greatest value at the lowest life cycle cost. One such partner is xG Technology, Inc. xG is the developer of a broad portfolio of technology designed to enhance wired and wireless

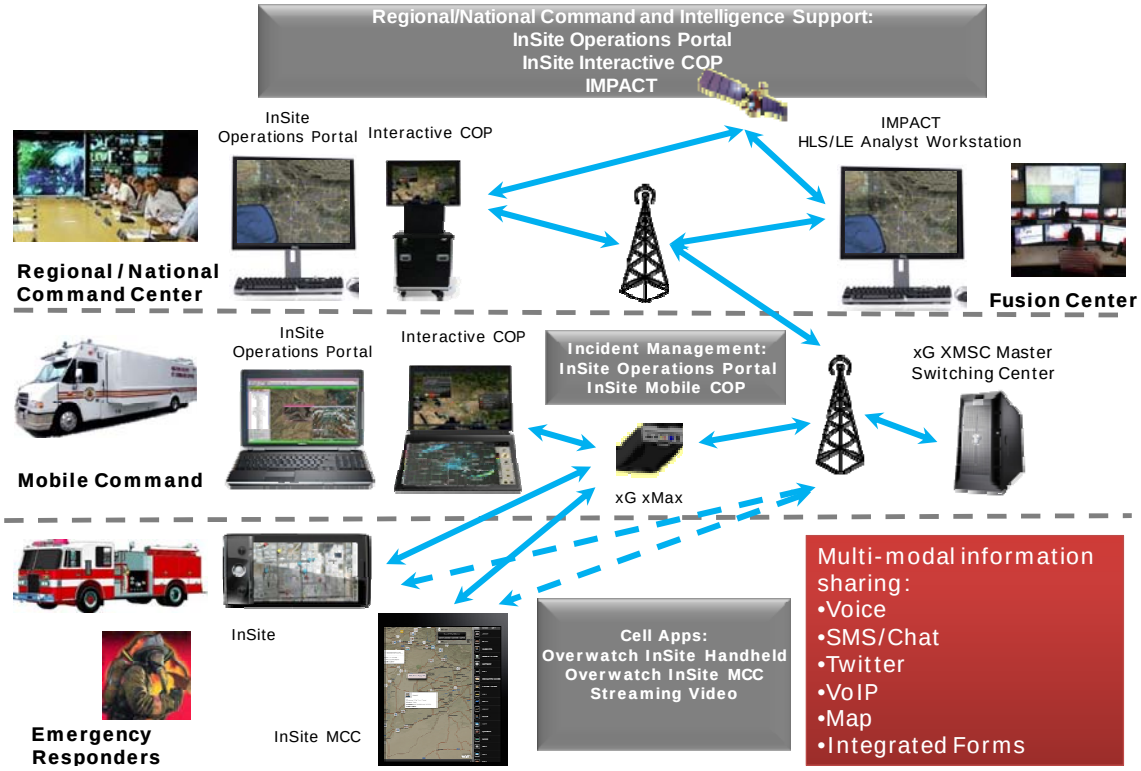

Figure 2. The Textron Systems team solution connects every member of the team with each other, with incident command centers and investigative units at fusion centers.

communications. The technology covers a range of spectrum agnostic, cognitive radio solutions that span numerous industries and applications. These solutions enable communications providers to deliver robust, revenue-generating mobile services using licensed and/or unlicensed spectrum.

xG's initial product release is xMax®, the world's first carrier-class cognitive radio network. Operating within the 902-928 MHz license-free band, xMax is a mobile VoIP and data system that utilizes an end-to-end Internet Protocol (IP) system architecture — an industry first. The xMax product suite includes a line of handsets, base stations, mobile switching centers, network management systems, deployment tools, and customer support. This turnkey solution represents the first commercially available, fully mobile VoIP and broadband network. The xMax system allows mobile operators to utilize free, unlicensed 902-928 MHz ISM band spectrum (available in most of the Americas) instead of purchasing scarce licensed spectrum costing millions of dollars.

The Textron Systems team is focused on delivering a secure, reliable, and collaborative communications system that provides situational awareness combined with the rich analytic capabilities needed to support rapid responses to complex natural and man-made emergencies (Figure 2). The solution supports voice and data communications over commercial or private wireless broadband networks. In addition to chat/SMS, video calls, and email the solution includes:

- Operation specific geospatial overlays delivered to a responder's communication devices. This includes displays such as the

Table 1. The Textron Systems team solution is unique in the industry and provides numerous benefits to the Government.

Textron Systems Team Discriminators	Benefits to Government
• Cloudwave™ Framework with data layer replication and backup. • Flexible Data Model that easily adapts to changes. • A composable, web-based, widget framework that makes adding new tools easy.	• Resilient network solution which recovers from mishap. • Adaptability to changes in missions and environments.
• Cloudwave™ and InSite™ Applications which adapt to various degrees of network connectivity.	• Adaptability to changes in external conditions.
• Overwatch's relevant experience building data prioritization services for large DoD software programs. • Cloudwave™ Framework's ability host application data prioritization services.	• Prioritization of network traffic and application data.
• Quality of Service features specifically designed to enable mobile applications to function on intermittently connected networks.	• Quality of Service control mechanisms to ensure high-quality performance of critical applications.
• Role Based Access Control (RBAC) and federated search of data stores.	• Dynamic access control that is both a protector of data and network resources as well as an enabler of federated access to key data sources and systems.
• Scalable application and data layer solution.	• Scalable network solutions that first rely upon software and then hardware to meet demands.
• Power aware mobile applications that conserve device power and network bandwidth usage.	• Power aware network and applications that actively mitigate power usage.
• Open Cloudwave™ Framework application programming interface (API). • Extensive development experience on open source solutions to include Google™ Android. • Strong proponent of standardized and open interfaces and platforms.	• Standardized Common Interfaces that allow for competitive provisioning.
• An extensive web-services, web client and mobile application framework solution that provides ubiquitous access to applications and data.	• Uniform, Universal access - anywhere, anytime.
• Cognitive radio that searches for and moves to unused frequency “white space” every 30ms • Supports any commercial smart phone	• Nearly impossible to exploit or jam as tested by the US Army. Much more efficient frequency utilization. • Lowers life cycle cost and allows Government to leverage huge annual commercial investment in technology.

current extent of an airborne contaminant plume or the water levels across neighborhoods during a flooding event or the edges of a fire and direction the fire is moving.

- Imagery and voice capture with geospatial and temporal tagging. This allows responders to "leave a message" for others to view and hear as they look at the tag on their devices.
- Augmented reality views of the landscape so responders can quickly orient their own position in relation to the incident and other people and landmarks in the area.
- Support for structured information capture using predefined, operation specific forms. This allows information from databases such as criminal records, motor vehicle license information, etc. to be accessed as needed.
- Interactive analytic products such as personal or organizational networks.
- Automatic publication of operational data to publically available websites based upon predefined releasability criteria. This allows alerting of citizens in affected areas to know the latest information so they can respond accordingly as well as alert responders faster and more efficiently.
- Secure xMax cognitive radio between the appliances at the edge and the Government's broadband cellular infrastructure.

The features and benefits of the Textron Systems team solution are described in Table 1. More detailed information about this system can be found in Appendix A. Features and Comments

In the following sections, the Textron Systems team offers commentary on the features listed in the request for information (RFI). The commentary is based on the team's experience and field tests of relevant technology solutions described in Section 1.

1.1 Resiliency in an Emergency

1.1.1 Resiliency

As defined in the RFI, resiliency is the ability of operable systems to recover from mishap, change, misfortune, or variation in mission or operating requirements. For the Nationwide Public Safety Broadband Network one should consider both the hardware software aspects of system resiliency.

The Textron Systems team recommends addressing hardware resiliency by building underlay networks that support newer interoperable protocols in critical areas.

The Textron Systems team recommends addressing software resiliency in a multi-facetted approach by using proven, robust technologies, flexible data models, widget frameworks, and web based solutions.

Assessment of Importance

For both hardware and software, the Textron Systems team considers it imperative to build resiliency into the Nationwide Public Safety Broadband Network. When using network-stored data, it is critical to utilize a software solution that is resilient to failure or change, but the system must also be scalable. For this reason, resiliency and scalability must be considered in a balanced approach.

Existing Gaps/Possible R&D/Challenges

Two hardware gaps to address are fixed frequency allocation and static channel assignment.

One software challenge to consider is the ability to recover from a mishap or misfortune without losing data. The Nationwide Public Safety Broadband Network should consider technologies that enable automatic system and data recovery with minimal administrator intervention. Research and development should be done on this topic at the same time as the large network architecture is defined. Investigation into how software

virtualization and data replication technologies can facilitate recovery are two specific topics that Textron Systems deems important with respect to the larger system architecture. Though these are largely solved problems in the commercial sector, the gap and impending challenge for the NSPBN will be specifically implementing best practices and technologies into the network's architecture.

Another software challenge is the ability for differing data stores, services, and applications to communicate with each other via the network. This could be managed using a flexible data model with an access layer common to all data stores, services, and applications for the sharing of information. In addition, Standard Interfaces and Platforms, as discussed later, can further reduce these challenges.

Challenging hardware aspects for public safety are that the network requires frequency coordination with large amounts of deployment planning and conditioned shelters. A challenging software aspect of highly flexible and resilient solutions is the management of those solutions. The management of the solutions needs to balance change control with flexibility to accommodate the mission at hand.

Current Offering

For hardware resiliency, the xMax system is designed to be transportable, initialize quickly and adapt to local environments.

Regarding software resiliency, the Textron Systems team has found that it is important to select technologies that allow for the regular backup or replication of data so the system can be recovered from a catastrophic issue without data loss. As explained in Section 1.4.1, "Scalability," the team has made specific design decisions to ensure the resiliency of our solutions such as the Distributed Common Ground Station – Army (DCGS-A), DCGS Standard Cloud, and Cloudwave™.

Not only does a solution need to be resilient to catastrophic events or failures, it also needs to easily accommodate changes in mission and operating requirements. To this end, the team's Cloudwave™ product utilizes a flexible data model. The flexible data model allows for the product to easily be adjusted, responding to changes and variations in operational requirements. For example, if a new data source is added which requires new attributes in the data model, developers or field support personnel can easily extend the data model and the User Interface (UI) will automatically extend itself to display the data. This feature makes adjusting to changed missions easier.

The team has found that providing a web-based widget framework within our Cloudwave™ product enables the user to compose their own workspaces using a variety of widgets and tools that focus on a specific job or scenario. Since it is a web based solution, new or updated widgets to meet new or changed situations can be easily deployed to centralized servers and then immediately made available to users.

1.1.2 Self-Organizing

As defined in the RFI, self-organizing networks dynamically manage their own configuration by automatically making changes to ensure messages reach their destinations.

Research and development should focus on rapidly deployable, self-organizing systems and dynamic spectrum access.

Assessment of Importance

The Textron Systems team believes self-organization to be a very important aspect of the Nationwide Public Safety Broadband Network.

Existing Gaps/Possible R&D/Challenges
Current technology gaps that may prevent the full realization of network self-organization include standards for sensing and priority coordination of frequency.

Research and development to close these gaps should focus on rapidly deployable, self-organizing systems and dynamic spectrum access. This research and development should address the main challenge of today's public safety networks – that they are rigidly channeled. Configuration of these networks is manual and requires extensive planning. Lastly, today's public safety networks are challenged because they do not perform load balancing.

Current Offering
The network enabled by xMax is self organizing. It employs Dynamic Spectrum Access and requires no channel planning. Devices initialize and scan to assess the environment. They select channels to operate on and begin signaling. The subscriber type devices listen to this signaling and determine the "best" channel for operation. Associations are made between devices, but they keep background scanning to determine a better channel.

1.1.3 Meshing

As defined in the RFI, meshing is a type of networking where each node must not only capture and disseminate its own data, but also serve as a relay for other sensor nodes, that is, it must collaborate to propagate the data in the network.

The xMax system uses a TDMA Media Access Control protocol. This TDMA frame is designed to support meshing and each node can become a relay node.

Assessment of Importance
The Textron Systems team believes meshing to be a very important aspect of the Nationwide Public Safety Broadband Network.

Existing Gaps/Possible R&D/Challenges
The most important current technology gap that may prevent the full realization of network meshing is that equipment designs are deficient in supporting the functionality needed for a mesh system. Many research papers have been created that focus on meshing but practical implementations are lacking. Thus, a potential development project is to create new practical implementations of meshing.

A challenge for current public safety in the area of meshing is that the networks are designed to be voice-centric. The networks do not have the concept of individual devices relaying data built into them.

Current Offering
The xMax system uses a TDMA Media Access Control protocol. This TDMA frame is designed to support meshing and each node can become a relay node. This capability allows each unit to hop through other units to find a destination or access a connection to another network. The units utilize an on demand routing protocol that allows discovery of other nodes with low overhead. The complete meshing system is a research topic and should be further pursued.

1.1.4 Adaptability

As defined in the RFI, adaptability is the ability of the network and/or device to

modify/change behavior based upon external conditions. In context of the Nationwide Public Safety Broadband Network one should consider both the hardware software aspects of system adaptability.

The Cloudwave open API is specifically designed to facilitate the rapid development of new applications and rapid integration with existing applications to adapt to changing missions and environments.

Assessment of Importance

Through numerous demonstrations and exercises such as the Army's Empire Challenge (EC) 2011 and Network Integration Evaluation (NIE), the team has learned that a system's ability to adjust behavior based on external conditions such as intermittent and poor network connectivity is a critical concern.

Furthermore, an adaptable application and data layer solution is imperative for a network that must adapt to meet the unexpected situations of national or regional disasters.

Existing Gaps/Possible R&D/Challenges

The major hardware technology gap is the lack of software defined radios. Software technology gaps that should be considered include software issues with intermittent, changing communications quality and data source adaptability.

A hardware research topic that would close existing gaps is in the area of real-time utilization of public safety frequencies in support of software defined radios. Two possible software research and development opportunities are indoor location tracking and adapting to low and intermittent bandwidth conditions. Both of these issues are critical problems that will impact the chosen solution and their research and development in the design and implementation of the network is recommended.

Applications residing on the Nationwide Public Safety Broadband Network will likely face a challenge in adapting to situations where connectivity fluctuates between strong network connectivity and no network connectivity. Some places to look for solutions are technologies such as the BitTorrent™ protocol for transferring large files piece by piece as connections to data providers are available.

Related to the challenge of intermittent connectivity is the ability of the network, middleware and applications to gracefully handle these connectivity fluctuations. It is relatively easy to create a system that relies on constant connectivity and also one that functions well when disconnected. It is a challenge to build one in which applications and devices can gracefully transition between these two modes without seriously degrading the user experience.

Another challenge is data source adaptability. By "adaptability" we mean making the composition of new data sources and the integration of new applications as easy as a few button clicks. A "clicks-not-code" approach to data mashup and integration means a system administrator can add new applications or data sources to the network with a few choice selections from an administration console. Such a capability puts the power to change and adapt to mission needs in the hands of those executing it. Furthermore, it frees up technology providers and technical support personnel to work on the harder problems of implementing and deploying innovative leaps in technology.

Best Practices

In relation to the challenge of operating under limited or intermittent network

connectivity, the use of the BitTorrent protocol for peer to peer data transfer has proven itself to be a best practice.

Current Offering

For network adaptability, xMax utilizes a web configurable rules table. This table allows the system to use or disallow any spectrum block or slice. The rules allow the system to dynamically seize or release spectrum for instant backup of legacy systems should those legacy systems fail or go dark. This action is similar to the way uninterrupted power supply (UPS) systems provide backup power when power mains fail. xMax could be utilized in much the same way to automatically provide backup communications when main systems fail. Simple operational rules make the system extremely flexible.

For network software adaptability, the Textron Systems teams' InSite products' ability to detect and adjust operations based on network connected and network disconnected situations has won great praise in demonstrations and exercises. We have put considerable effort into solving the intermittent connectivity problem for mobile applications.

For application adaptability, the Cloudwave™ Framework's Open Application Programming Interface (API) is specifically designed to enable rapid development and integration of existing or new applications. This approach enables Overwatch to easily partner with technology providers, large and small, to bring new and valuable functionality into the Cloudwave™ Framework. Changing missions may require a new application used on smart phones to track or report key data and it may require new desktop/web-based applications that display the data in a way that's meaningful to incident commanders and decision makers. If the system does not have an open and easily integrated API, brining critical technologies into the Nationwide Public Safety Broadband Network could be slow and cumbersome.

The Cloudwave™ Framework also provides and extensible data model and our applications, both web and smartphone based, can easily be extended to support new types of data and visualization thereof. Such a dynamic capability to adapt to external changes means new data sources can be easily brought into Nationwide Public Safety Broadband Network without expensive development and deployment of new software solutions.

1.2 Reliability and Availability

1.2.1 Prioritization

As stated in the RFI, prioritization is the ability to prioritize network traffic based on assigned priority schemes. For the Nationwide Public Safety Broadband Network one should consider the software aspects of prioritization.

The Nationwide Public Safety Broadband Network should consider prioritization an important part of the solution; both at the network transport layer as well as the application and data layers.

Assessment of Importance

When building a large network to handle enormous amounts of data, prioritization of network traffic becomes imperative. The prioritization must be done at multiple levels, the first being the routing and prioritization of data packets. Above that layer is the prioritization of application data and the data objects that are passed between nodes. The Textron Systems team has learned from experience that building a simple yet powerful prioritization

mechanism for application data is critical to successful data distribution and processing.

Existing Gaps/Possible R&D/Challenges

An existing gap is the ability of the network nodes to automatically recognize prioritized data from node to node. Research could be done on selectively prioritizing individual groups or user for voice and data. This research would move forward in the challenge that although public safety networks have the concept of individual priority, they don't have the concept of classifying users/data to finer degrees.

Another gap can be found at the network edges. The Textron Systems team believes it is likely that the National Public Safety Network will experience bandwidth challenges at the edges of connectivity, where time critical data is most urgent for first responders. The team recommends that consideration is given to both a network layer prioritization scheme as well as an application layer prioritization scheme.

The challenge in implementing such a solution is determining what is important and how to act upon that level of importance. Furthermore, integrating the transport layer prioritization with the application layer prioritization lends itself to research and development efforts to achieve optimal results. As with scalability, general prioritization is in many ways a solved problem. The challenge resides in the specific implementation for the Nationwide Public Safety Broadband Network.

Current Offering

The xMax system is an all IP network. Using local DSCP settings a user or application data can be prioritized for transmission. The ability to prioritize single users (i.e. the Fire Chiefs unit) multiple levels of priority are assignable to end user devices.

The Textron Systems team built the Battlespace Object Prioritization Manager for the Brigade Combat Team Modernization program which prioritized battlespace objects for distribution around the battlespace and within complex data fusion processing services. This technology was matured to a Technology Readiness Level (TRL) 7.

Additionally, in building the Cloudwave™ Framework and deploying it in various military exercises and demonstrations such as the Army's Empire Challenge and NIE, the team has observed a clear need to provide middleware services that prioritize application data. The tactical military networks and experimental expeditionary cellular networks that the team's products have operated on have been bandwidth constrained. This reality has led Textron Systems to take both software and hardware approaches to controlling the use of bandwidth and the priority of application data sent across the network.

1.2.2 Quality of Service (QoS)

According to the RFI, quality of service (QoS) is the set of standards and mechanisms for ensuring high-quality performance for critical applications. In the context of the Nationwide Public Safety Broadband Network one must consider both the hardware and software aspects of QoS.

Server side middleware and the client applications residing on laptops, tablets and smart phones must be designed with intermittent connectivity as an expected condition.

Assessment of Importance

QoS is important for robust and large-bandwidth portions of the network. It is critical for the portions of the network prone to intermittent connectivity or when network resources are highly strained.

Existing Gaps/Possible R&D/Challenges
A first gap to consider is that data services that support system-wide recognition and processing of QoS are not widely deployed in public safety systems. An area of research would be to investigate the feasibility of multi-protocol label switching (MLPS) for handheld devices.

Another gap to consider is that the Nationwide Public Safety Broadband Network architects cannot assume that best of breed commercial software solutions normally residing on networks like Verizon™ or AT&T™ will provide the same QoS on a bandwidth constrained and intermittently available network. In our team's experience with expeditionary cellular networks set up in austere conditions, not unlike a disaster recovery zone, both the server side middleware and the client applications residing on laptops, tablets and smart phones must be designed with intermittent connectivity as an expected condition.

Doing so will increase the overall QoS even when the network cannot provide a quality and robust connected state. The Nationwide Public Safety Broadband Network should consider investing in research and development of this aspect of QoS. It is likely to provide a large return on investment because its benefit is best seen when the network is stressed, degraded and when users are most apt to want the network to "just work."

Best Practices
The Textron Systems team recommends that the Nationwide Public Safety Broadband Network canonize a system that supports a defined QoS regimen and buys only those systems. The Textron Systems team also recommends that the Nationwide Public Safety Broadband Network look to solutions in DoD programs such as the DCGS Standard Cloud, Relevant INTEL to the Edge (RITE) 3G and Connecting Soldier to Digital Applications (CSDA). These programs have had to consider the challenges of providing relatively high QoS in challenging physical and network environments.

Current Offering
The xMax system supports current QoS protocols like 802.1p. A TDMA MAC is employed to give very deterministic packet transmission times. Packets like voice and video that are time sensitive are prioritized over less time sensitive data at every level of the xMax system.

In addition to application data prioritization to deal with limited bandwidth, the Textron Systems team has relevant experience that points to the need to architect both client and server applications, to handle limited bandwidth and intermittent connectivity. The team has found that its InSite mobile application showed solid performance on reliable and robust commercial cellular networks, but initially faltered when deployed on less robust and reliable military tactical networks and experimental expeditionary cellular networks. The root cause of the issue was found to be intermittent connectivity. The system has since been enhanced for QoS capabilities to better handle intermittent connectivity while providing a reliable QoS to the user.

1.3 Security

1.3.1 Strong, Dynamic Access Control

The RFI states that strong, dyanmic access control describes a capability where access control lists can be configured to control both inbound and outbound traffic on networks and authentication/verification of users/devices on the network. For the

Nationwide Public Safety Broadband Network one should consider both the hardware and software aspects of strong, dynamic access control.

Textron Systems recommends users have one user credential to sign into any part of the Nationwide Public Safety Broadband Network.

Assessment of Importance

Based on the Textron Systems team's experience with creating information systems for the DoD and Government agencies, strong, dynamic access control is a ubiquitous element and must be considered critical in similar systems like the Nationwide Public Safety Broadband Network.

Existing Gaps/Possible R&D/Challenges

Authenticating and authorizing disparate groups of users without a central agency is a difficult issue. Many research papers have been written on the subject. Practical procedures for deploying a mixed organization authentication system would be a good topic for further research.

A significant area of research and development, in which the Nationwide Public Safety Broadband Network could leverage commercial advancements is single sign-on technologies. The Textron Systems team recommends users have one user credential to sign into any part of the Nationwide Public Safety Broadband Network and let backend services handle authenticating that user with various databases, applications and networks within the system or its affiliates. Such a single sign on makes the network and its applications much more usable and accessible. It makes users more productive and lets them focus on getting the job done.

Best Practices

Access control best practices for Nationwide Public Safety Broadband Network can be found by examining technologies such as OAuth and OpenID protocols. OAuth is a simple way to publish and interact with protected data. OpenID is an open standard that describes how users can be authenticated in a decentralized manner, obviating the need for services to provide their own ad hoc systems and allowing users to consolidate their digital identities. Though the protocols are in some ways mutually exclusive technologies, they are made to work well together and may solve Nationwide Public Safety Broadband Network specific problems, making the network easier to use.

Current Offering

From a hardware perspective, the xMax network employs AAA functionality to authorize and authenticate network users and infrastructure.

From a software perspective the Textron Systems team recommends the use of a centralized user authentication service with a standardized mechanism for storing and accessing authentication information. An example is the Lightweight Directory Access Protocol (LDAP), for which there are several open source and commercial options. Building upon this foundation, there are two aspects of access control that Nationwide Public Safety Broadband Network should consider: role based access and federated search.

For user role based access to applications and data, middleware services can talk to the LDAP, or similar, servers and then facilitate authentication of users at the application and device layers. Beyond simply authenticating the users, middleware services can facilitate Role Based Access Control (RBAC), which enables administrators to control a user's access to enterprise data and specific

application features based on assigned roles. This capability protects the enterprise's resources from either malicious or accidental insider threats. It also ensures that sensitive data access and very powerful privileges are not granted to users who do not have the technical or organizational knowledge to weld them. The Textron Systems team has built this type of RBAC into its Cloudwave™ Framework and InSite products.

Middleware services can also provide a federated search capability for the myriad law enforcement and public safety databases. Results are obtained from those data sources and shared with users who have authorization to access specific databases. By providing a middleware solution, the system removes the burden from the user remembering credentials and search procedures for every database that is accessed. Instead, one set of user credentials, the one they use each day to log into their work computer or their smart phone, can give them access to any database for which their user account is approved. The Cloudwave™ Framework employs middleware search services that support federation of searches and collection of results to a single user based on his/her one user login to the Cloudwave™ system.

1.4 Affordability / Commercial Alignment

1.4.1 Compatibility with Commercial Infrastructure

With xMod, all of the laptops and smart phones currently in use by the public safety agencies that are equipped with WiFi will be able to work with the xMax network unmodified.

The RFI defines compatibility with commercial infrastructure as the utilization of a variety of commercial services when public safety is in areas not covered by the public safety broadband network.

Assessment of Importance

The Textron Systems team believes compatibility with commercial infrastructure to be a very important aspect of the Nationwide Public Safety Broadband Network.

Existing Gaps/Possible R&D/Challenges

A current technology gap that may prevent the full realization of compatibility with commercial infrastructure is the creation and adoption of devices that support P25, military and cellular protocols is non-existent even though vendors build most of the devices. This topic can be handled via policy and procedure mandates. The technology is currently available.

Current Offering

One of the components of the xMax system is the xMod. The xMod connects WiFi devices to the xMax network. All of the laptops and smart phones currently in use by the public safety agencies that are equipped with WiFi will be able to work with the xMax network unmodified. Different agencies can use the xMax network as long as the devices support WiFi. Since the system is all IP and uses existing smartphones and laptops as subscriber devices, many off the shelf applications like push to talk and position location are already available.

1.4.2 Network Sharing

Different agencies can use the xMax network as long as the devices support WiFi.

According to the RFI, network sharing is the shared use of infrastructure between commercial and public safety users.

Assessment of Importance

The Textron Systems team believes network sharing to be a very important aspect of the Nationwide Public Safety Broadband Network.

Existing Gaps/Possible R&D/Challenges

A current technology gap that may prevent the full realization of network sharing is the bridging of devices that support many-to-many protocols.

Current Offering

One of the components of the xMax system is the xMod. The xMod is a portable or mobile installed device that connects to the xMax wireless network, and then forms a WiFi hotspot in and around the mobile or remote location for access by any and all COTS WiFi enabled devices. All of the laptops and smart phones currently in use by the public safety agencies that are equipped with WiFi will be able to work with the xMax network unmodified. Different agencies can use the xMax network as long as the devices support WiFi. Since the system is all IP and uses existing smartphones and laptops as subscriber devices, many off the shelf applications like push to talk and position location are already available

1.4.3 Scalability

In the context of the RFI, scalability is the ability of a system, network, or process to handle growing amounts of work in a graceful manner or its ability to be enlarged to accommodate that growth. For the Nationwide Public Safety Broadband Network one should consider both the hardware and software aspects of system scalability.

Assessment of Importance

The Textron Systems team considers scalability to be a necessary feature for the Nationwide Public Safety Broadband Network. An essential aspect of a network's scalability is the ability of the application and data layers to meet fluctuations in the demand.

The Textron Systems team's Open API/Cloud based approach is a direct response to the Government's need to have scalable and open solutions that can be quickly adapted to meet the mission needs.

Existing Gaps/Possible R&D/Challenges

Scalability of networks, data layers and applications is typically considered a "solved problem" for many general cases. The challenge is in implementing scalability for a particular system's requirements and expected operating environment. Where the Textron Systems team sees a significant need for research and development is the scalability of networks, data layers and applications in austere communications environments.

Environments at the edges of the network may have intermittent connectivity due to destroyed, impeded, or absent pieces of network infrastructure. It is these types of environments, where the Textron Systems team has exercised and demonstrated its technologies, which have exposed the biggest challenges to scalability and the largest opportunity for innovation.

For example, the following questions must be answered. How does a remote system replicate its data upwards to central data storage and computing warehouses when the bandwidth from the remote site back to those central sites is extremely limited? How should computing and network resources be best deployed down to the network's edge to meet high demands in concentrated areas of disaster response when the network has been negatively impacted by the disaster or was sparse to begin with? These hardware and software scalability issues are not well addressed when one

considers the current landscape of cloud computing and data storage providers.

Lastly, an area of research to consider is the use of cognitive network equipment to increase scalability.

Best Practices

First, a best practice for scalability is to utilize networks that can take advantage of more of the spectrum in a cognitive manner when needed.

Second, the team recommends that the Nationwide Public Safety Broadband Network consider the best practices of scalable solutions providers such as Amazon, Google or Microsoft. Both the data and applications layers of any solution should support scalability and must be deployable in a commercially available environment such as Amazon's EC2 cloud computing offerings or in secure Government owned and operated server farms.

The Nationwide Public Safety Broadband Network should look to DoD programs such as DCGS Standard Cloud, RITE 3G and CSDA for best practices and solutions in bringing network capabilities and computing power to the edge of large networks under austere conditions. These programs have put significant engineering hours into research and development to solve these very real problems for soldiers deployed to today's battlegrounds.

Current Offering

The xMax system has no system limitations on the numbers of users or addresses that can be allocated. The system is self organizing and self healing. With over 135 MHz of spectrum available to xMax, few limitations inhibit growth of the network to meet traffic needs.

Figure 3. An open, extensible architecture hostable in the cloud allows tailoring of the system to meet organizational or mission requirements while reducing investment in new infrastructure.

The Textron Systems team has learned from our experience on large DoD software programs such as DCGS-A and DCGS Standard Cloud (DSC), as well as our own research and development efforts, that addressing application and data layer scalability is just as important as ensuring that the network's transport layer hardware and software scales well.

The Textron Systems team specifically chose non-relational database technologies that have strong data replication capabilities for our Cloudwave™ web framework. The team anticipates the need to replicate data for disaster recovery in the event of a data store failures as well as the need to scale to handle spikes in application access to the data store.

In addition to scaling our data layer, technologies were chosen and implemented to provide a web framework that is deployable in a virtualized environment. Furthermore, we have architected web services such that they can be broken apart and scaled horizontally by adding more virtualized machines running extra instances of specific services needed to meet demands.

This approach of granular virtualization is both a performance optimization and resource saving measure. Instead of always requiring more hardware to meet fluctuations in demand, our services can be scaled virtually on existing hardware.

The team has taken this scalability approach with its Cloudwave™ framework which supports web clients, mobile applications and 3rd Party Services. Both the data and applications layers of the team's solutions support scalability and could be deployed in a commercially available environment such as Amazon's EC2 cloud computing offerings or in secure Government owned and operated server farms. The team recommends that a similarly scalable and flexible solution be considered for the National Public Safety Broadband Network.

1.4.4 Power Awareness

The RFI states that power awareness is the ability of network/devices to control power functions. In context of the Nationwide Public Safety Broadband Network one must consider the software aspects of power awareness.

Recognizing the significant importance of size, weight, and power management, the InSite solution offers numerous settings to assist in optimizing power usage.

Assessment of Importance

In designing the Nationwide Public Safety Broadband Network, making power awareness a primary objective in the design and configuration of the network, and in the design and implementation of the network protocol is important. However, it is equally or more important to consider the power awareness of the mobile devices that will be connected to that network and in the hands of those on the front lines.

Obviously, users of mobile devices are not always near a power source where they can keep their device's battery fully charged and those batteries have a finite amount of energy available. Understanding this fact, it is critical that the software in use on the device be able to make smart decisions in controlling power functions to conserve battery life. On a smart phone, the largest power gluttons are the screen, wireless radio, GPS, WiFi, and Bluetooth. To maximize a device's battery life, you must minimize the power draw without significantly compromising performance.

Existing Gaps/Possible R&D/Challenges

To maximize the power management of the network and applications on devices, the Nationwide Public Safety Broadband Network will need to ensure transmitters and receivers are fully powered when they are actively sending/receiving and are powered appropriately when they are not. Current technologies perform poorly on this task and there is room for improvement.

For devices, the Nationwide Public Safety Broadband Network should investigate Energy-Minimizing Idle Listening (E-MiLi) to reduce the power usage by devices when not actively sending or receiving information.

The Nationwide Public Safety Broadband Network could also face the challenge of quantifying a goal for power awareness. Simply stating that power awareness is considered in the design is easy, but proving design choices were effective in improving the power usage of the device may be difficult.

Current Offering

The xMax network components can change output power based on network situational awareness. Power is reduced and increased for optimum transmission of data and

minimal self interference in changing network conditions.

In the mobile device application InSite, the Textron Systems team has taken steps to encode smart decision-making abilities in the software regarding power consumption. For instance, when the screen is turned off or the application is not in focus, the GPS turns off to conserve battery life. Additionally, the applications make smart decisions regarding the transmission of data over the cellular radio by following a configurable schedule with exceptions built in to accommodate time-critical transmissions.

1.4.5 Standardized Common Interfaces

According to the RFI, standardized common interfaces are the protocols, APIs, application platforms, radio capabilities, etc. that allow for competitive provisioning within the network. In context of the Nationwide Public Safety Broadband Network one must consider the software aspects of standardized common interfaces.

Overwatch recommends Nationwide Public Safety Broadband Network leadership consider adopting commercial standards rather than creating new standards.

Assessment of Importance

The Textron Systems team considers standardized common interfaces and platforms an essential key to the success of the Nationwide Public Safety Broadband Network's initial implementation and its continual innovation.

Existing Gaps/Possible R&D/Challenges

Open and common standards will be a challenge for Nationwide Public Safety Broadband Network in selecting or creating them and in continuing to foster innovation while maintaining standards. The use of standards is an area that deserves substantial up front attention at policy making levels as well as in engineering research and development. Our team recommends the Nationwide Public Safety Broadband Network leadership look to commercial examples and consider outright adoption versus creating specialized Nationwide Public Safety Broadband Network versions. A case in point, Textron Systems has chosen the Google™ Android operating system as our primary mobile application development platform for two reasons. First and foremost was the ease and availability of our engineering teams to implement cutting edge solutions on a variety of hardware platforms on the more open Android development platform versus Apple's iOS and Microsoft's Windows™ Mobile. Second was the surge in momentum of Android in the commercial sector as well as in the DoD research and development community. This is an example of how a more open and available solution has shown its value compared to more controlled and closed competing technologies.

Best Practices

The team recommends that the Nationwide Public Safety Broadband Network look to commercial and open source examples such as Google's™ Android, the LDAP, OAuth and OpenID protocols. Adopting data models such as the National Information Exchange Model (NIEM) will also help because many systems can already exchange data in this format. The Textron Systems team recommends that the Nationwide Public Safety Broadband Network create new standards only when absolutely necessary or when current standards simply will not suffice. Finally, the team recommends that technology vendors be required to provide open standards, APIs and platforms so other vendors can innovate upon current offerings to provide new

features and technology breakthroughs. By doing so the playing field is leveled for large and small providers to bring their ideas to fruition for the benefit of the Nationwide Public Safety Broadband Network end users.

Current Offering

The xMax system is based on many standard interfaces and protocols. The network supports IP communications. WiFi is a supported access protocol. Ethernet and Fiber are defined network interfaces.

The Textron Systems team has developed an open API for the Cloudwave™ Framework and we have experienced the benefits of opening up our API to others for collaboration. By making the API the standard for interfacing to the Cloudwave™ Framework and being willing to share it freely with partners, the ease and success of integration efforts increased dramatically. The team has integrated new applications and technologies in preparation for large demonstrations, such as in the Army exercise Empire Challenge, in a matter of a few weeks from initial discussions to integrated capabilities.

This example shows how important standardized and common interfaces are to the successful and efficient integration of new technologies. The Textron Systems team strongly encourages the Nationwide Public Safety Broadband Network procurement leaders to advocate for, and require, standardized and open interfaces and platforms. Technology providers must be willing to share interface specifications freely and the Nationwide Public Safety Broadband Network leadership needs to encourage new innovation by making those standards available to current and potential technology providers.

1.4.6 Uniform, Universal Access

In the context of the RFI, uniform, universal access is the ability of the system to enable access to the network and data from anywhere at any time through any device. For the Nationwide Public Safety Broadband Network one must consider both the hardware and software aspects of uniform, universal access.

Textron Systems recommends a cloud-based web service approach to access data and services.

Assessment of Importance

When creating a nationwide network intended to be accessed by a wide variety of people, programs, and organizations, it is essential that those clients have uniform and universal access to the network and the services it provides.

Existing Gaps/Possible R&D/Challenges

A large gap is that public safety devices are vendor specific and don't interoperate or provide a method for interoperation.

Another gap that may exist is the ability of the existing systems and data stores to expose web services for others to consume. The creation of web services would make the entire solution more robust and more likely to fulfill its full potential.

The Textron Systems team recommends analyzing the existing systems, applications, and data stores to get an idea of the level of effort required to support a web service approach.

Since the many clients accessing the network will likely have differing end-goals in mind, offering a complete set of web services that will satisfy all customers will

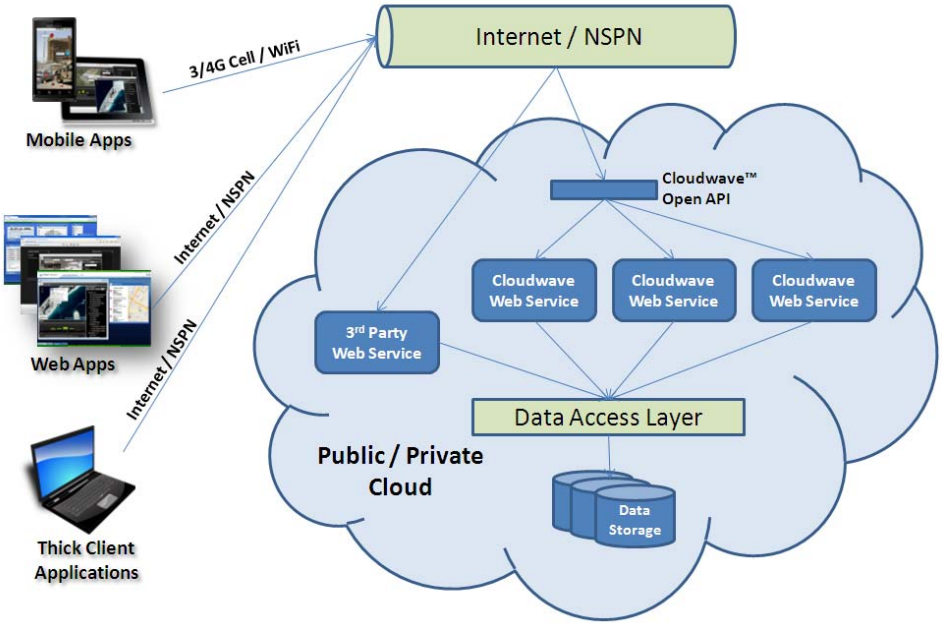

Figure 4. Using web services opens data and services to a variety of client platforms.

be challenging, if not impossible. Therefore, it will be important to identify the core services and features that will appeal to most clients and make those the focus of activity.

The desire to access data anywhere at any time begs for a web services approach (Figure 4). By using web services, the Nationwide Public Safety Broadband Network will reap the benefits of application and data integration, technology flexibility, and code re-use, which all lead to lower cost.

First, web services allow for seamless application and data integration by utilizing a common HTTP or XML protocol. Using a common application data transport protocol allows disparate applications to share data without explicit knowledge of implementation or data format. Additionally, web services have the benefit of loose coupling, allowing those integrated applications to be developed in any chosen technology.

Next, web services expose the functionality of existing code over the network, allowing other applications to access this functionality. Other programs are essentially re-using the code by using the functionality exposed in the web service. This approach results in significant cost savings by removing the need to develop specific interfaces to connect programs and transforming data to share information.

Current Offering

The xMax network was designed to allow off the shelf smartphones, tablets and laptops to be used without modification. This is based on a common WiFi interface. All of these devices can access the network anytime. The xMax network operates in unlicensed bands so can be set up anywhere in North America. What does not exist today is a gateway from legacy P.25 or analog narrowband devices to gate them to an IP network.

The Textron Systems team has taken the web service approach with its Cloudwave™

product and the approach has proven to be highly beneficial for development and integration with other programs and data sources. For example, the team has proven the ability to connect with other programs quickly for demonstrations and exercises like the Army's Empire Challenge and NIE events. Additionally, Cloudwave™ data can be accessed from anywhere on nearly any device with a network connection and when operating in a disconnected environment, the system continues to work seamlessly, re-synching with the server once network connectivity is restored.

2 Further Considerations

What can be done to ensure both short- and long-term affordability of the network for all types of public safety agencies?

The Textron Systems team believes an approach the Government can take to ensure short-term affordability is to emphasize the purchase of Common Off the Shelf (COTS) products and limit custom development to the integration of the COTS products. Based on the description of the Nationwide Public Safety Broadband Network in the RFI, it appears that existing COTS products should be able to meet many of the system requirements. For some COTS products, like the Textron Systems team's InSite product, the Government has already executed tests (e.g. Army Empire Challenge 2011 and the Army NIE) of the COTS products integrated into larger systems and used in simulated environments. The Nationwide Public Safety Broadband Network should take advantage of the information gathered from Government COTS evaluations and emphasize COTS acquisition as a way to reduce risk and drive down costs.

An approach the Government can take to ensure long-term affordability is to require a system architecture that is open and emphasizes standards. This approach increases competition, which benefits Government procurement. It also encourages innovative technology providers to bring the best possible solutions to end users at the lowest possible costs.

An approach the Government can take to ensure both short-termand long-term affordability is to leverage public and private cloud hosting capabilities. Many large cloud hosting providers are making private, secure cloud hosting offerings available to Government agencies. Consider this as an integral part of the larger Nationwide Public Safety Broadband Network architecture to reduce cost and risk.

Cost reductions should be garnered by the lower cost to obtain and use hosting resources versus the cost of a Nationwide Public Safety Broadband Network or Government built solution. Risk reduction with this approach comes in two forms. First, there is lower risk to the Government by not undertaking a massive hosting infrastructure project and instead relying on commercially available products and services. Second, risk is reduced by leveraging commercial techonology and experience regarding security and scalability. Taking advantage of existing robust and reliable hosting services designed to resist cyber attacks and large fluctuations in demand instead of re-creating such a robust and reliable infrastructure from the ground up greatly reduces the Nationwide Public Safety Broadband Network's risk exposure.

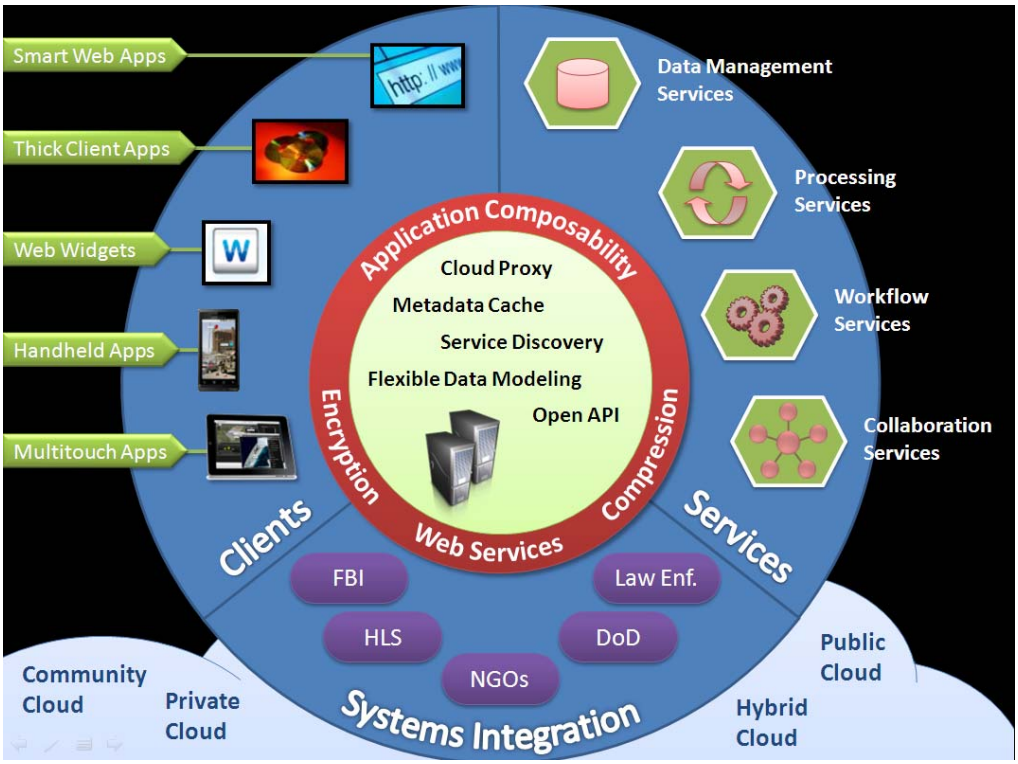

Figure 5. For a highly successful solution, aspects of the system beyond the transport layer, such as the application and data layers, should be emphasized and focused on.

The Textron Systems team recommends that the Government consider building a survivable core of hosting services as a backup risk mitigation measure to reduce or totally prevent the loss of key services in a time of natural disaster or large scale cyber attack.

A smart combination of Government owned and commercially provided solutions should strike the right balance between cost and risk.

What network features or requirements have not been identified above, the lack of which may impair the network's ability to adequately serve the needs of public safety?

Based on the contents of the RFI, Textron Systems recommends greater focus be put on the software application and data layer solutions for the Nationwide Public Safety Broadband Network. From our experience with Government field tests, the application and data layer solutions are as important as the transport layer. Example application and data layer requirements can be derived from the solution described in Appendix A.

3 Conclusion

The Textron Systems team has provided the U.S. DoC NIST a variety of inputs on the possible features of a new nationwide interoperable public safety network. These inputs are based on experience obtained in Government events such as the Army EC 2011 and Army NIE, which included tests of similar network solutions in stressful physical and network environments. The Textron Systems team stands ready to offer further input and solutions to make the Nationwide Public Safety Broadband Network a success.

Appendix A. The Textron Systems Team Solution

The convergence of operations with intelligence (the Ops Intel Convergence Model) is critical to the success of public safety broadband network users.

The system must enable answering the questions, "what now?", "so what?", "what if?", and "now what?"

Based upon our discussions with First Responders, most of the problems they encounter occur in an interrelated environment, whether during an actual emergency or during the preparation and training for the potential emergency. The crisis faced by the first responder never just involves a single discipline. Whether it is a coordinated response of fire, police, and medical aid or the critical response to an active shooter scenario at a school or even a Sheriff's office response to a search and rescue operation…all occur and interact with multiple systems.

Our belief is that if we are dealing with a systems problem, then a systems thinking mindset is required for its solution. A supporting technology that fosters collaboration as its primary importance is needed. If our goal is shared commitment then shared awareness and understanding must be present first. If this is the case, then the formation of shared awareness and understanding must allow for complexity and discovery during analysis. Analysis and understanding must be available via a collaborative framework that further builds relationships to gain future commitment and trust.

Smartphone collection platforms are a crucial first step in gaining the richness of data - or what we call the "what now?"- from all players and in the language that their discipline communicates in. However, more critical is that these technologies do not stop with just the collection that gives us needed situational awareness (SA). SWAT teams, hostage negotiations, ICS Unified commands at disasters, and gang teams figuring out the network, all need this but if one stops there we simply have rich SA. Decision makers need to have the "so what?" answered from the SA; this is the process of analysis. Arguably, a smartphone platform that feeds directly and seamlessly into analytics is a true requirement although even this is still not enough. One's understanding must be communicated to other partners and disciplines that may not speak the same

Figure 6. The Textron team offers a systematic approach to addressing the operations and intelligence convergence model.

language or "cop/fire speak." The ability to view data via multiple visualizations so that the police criminal intelligence officer looking at a nodal depiction is able to then turn around and present his conclusions on a map to the DHS and fire responder on the scene who then in turn uses a timeline to brief a decision maker creates true shared understanding…the critical first step in "Wicked Problem" theory in gaining shared commitment.

Taken further, rich visualization can allow decision makers to try out their "what if?"

questions via their visualization tools, allowing them to move to modeling, much the same way Recognition Primed Decision modeling decision makers work. Ultimately this systems approach allows the decision maker to move to the "now what?" question. The decision can be made in a collaborative environment with ownership and transparency. Textron has adopted a systems approach from the beginning and most importantly sees the smartphone collection platform as a contributor to the process of turning knowledge to action, not an endpoint in and of itself.

The Textron Systems team brings a mature, tested integrated solution in support of the Government's Public Safety network needs.

The Textron Systems team solution is focused on being a secure, reliable, collaborative communications system that provides situational awareness combined with the rich analytic capabilities needed to support rapid responses to complex natural and man-made emergencies.

At the edge of the crisis, handheld and mobile device technologies will enable civil/federal First Responders to more effectively react to and manage missions, tactical emergencies and every day communication needs. The system provides responders and every day user's access to advanced analytical, collaborative and investigative tools via their smartphone devices; greatly enhancing situational awareness and understanding; tactical engagement and the investigative process. Using advanced mobile network technology and application enabled smartphone devices and tablets, users can receive and gather information about a specific mission or emergency as it occurs in real time, respond to events with critical data provided to their mobile devices, and manage the investigative process with command and control centers and other investigative support groups.

The proposed solution connects the emergency responder to other members of their team, to the incident commander and even to investigators and analysts at regional Fusion Centers or other support organizations. From a handheld device or tablet based mobile command application a user has access to unprecedented near real time situational awareness as well as a means to collect and report information which becomes available to any user connected to the system.

The current system includes a cloud-based suite of middleware, operational portals, analytic applications and handheld applications designed to operate on existing server and client hardware and within existing communications infrastructures. It offers an open development API to allow customers and 3rd party developers to rapidly create new applications, facilitating real time information sharing with other information systems and tools, to ensure continued and cost effective relevance as the surrounding mission and system environment evolves.

Considerations included in the solution include the following attributes.

- Distributed Operations
- Data Security
- Secure Cellular Transport Layer
- Middleware Framework
- Smart Phone Common Operating Picture
- Operations Portal
- Full Motion Video
- Analytics and Fusion
- Structured Data Mining

Distributed Operations

The Textron Systems team's solution enhances distributed operations by creating a secure, collaborative, and reliable environment for operation management and understanding.

A key to effective emergency management is information sharing between responders operating at the scene, incident commands and regional or national command centers.

Textron's solution provides access to information anywhere on the network from any device (Figure 1, Figure 7). Synchronization between mobile command centers and fixed sites provides an aggregate, near-real time view of ongoing operations including the ability to manage multiple, concurrent operations. Analysts at Fusion Centers can access this information through a federated search provided by analysis systems. All incident data can be exposed through web based portals, which can be made accessible anywhere on private or public networks.

Data Security

The Textron Systems team's solution offers a highly secure solution that is easily accessible by a large user community.

Textron's mobile, desktop and web service products provide multiple layers of security. Role Based Access Control (RBAC) enables system administrators to control a user's access to enterprise data and specific application features based on his/her assigned role. This protects the enterprise's resources from either malicious or accidental insider threats. It also ensures that sensitive data access and very powerful privileges are not granted to users who do not have the technical or organizational knowledge to wield them.

A second layer of defense is the encryption of data during transmission. Overwatch's products support Secure Sockets Layer

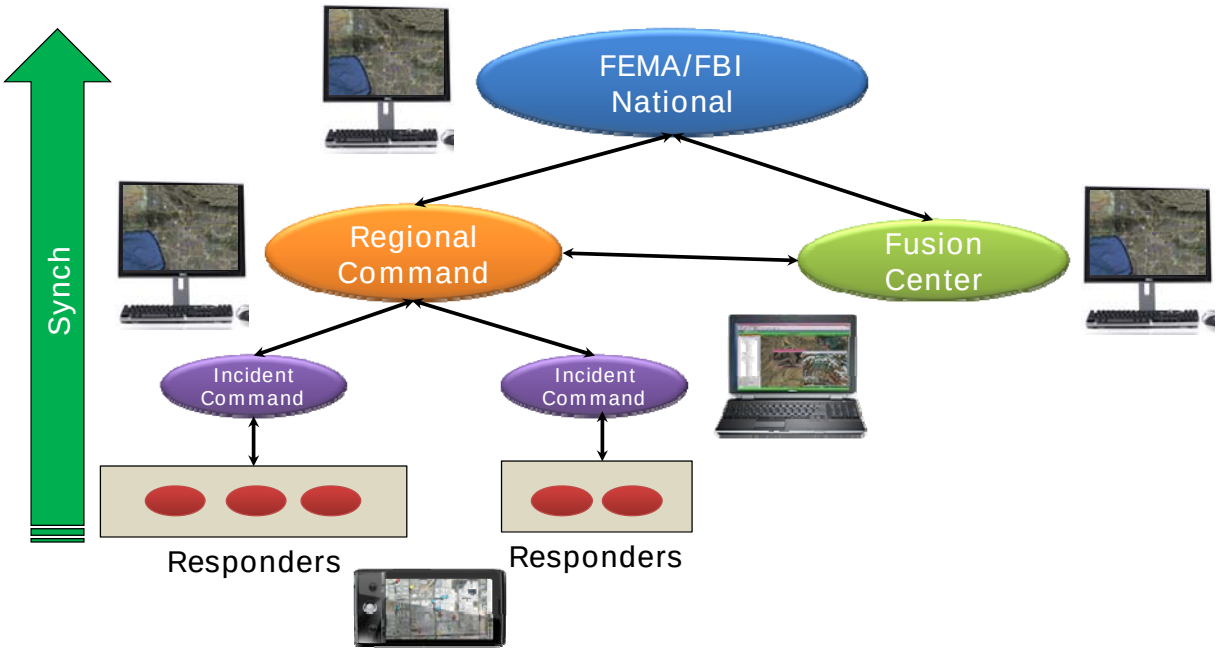

Figure 7. Distributed Common Operating Picture - Information is accessible anywhere on the network.

.

(SSL) encryption of web based traffic. This protects data transmitted between web servers and desktop or mobile clients from being intercepted and used for malicious purposes. A third layer of protection is provided by encrypting data-at-rest. When data is stored to a hard drive on a computer or flash memory on a smart phone, the storage process also encrypts the data. If the device were to fall into the wrong hands, the data would be very hard to retrieve and access. Overwatch is also doing active research and development of sophisticated data-at-rest encryption technologies in which the actual data is aware of its environment and will not allow itself to be accessed in unknown or un-trusted environments or to un-trusted users. The current implementation includes SSL, AES 256 encryption accessed via user log-in on the handhelds and the admin console. InSite can provide higher levels of encryption such as Suite B should that be required.

Secure Cellular Transport Layer: xMax™

xMax affords a deployable, mobile means of operating within existing commercial spectrums, in an unobtrusive manner, without the need of laborious authorizations with an approach that is highly resistant to compromise and jamming.

Developed by xG Technologies, this product provides a low-cost, cellular capability that operates dynamic spectrum access with a cognitive radio capability. This will allow the use of any smart phone or WiFi enabled device (laptop, tablet, etc.) to operate outside the commercial spectrum. The xMax cognitive radio cellular system from xG Technology represents a complete, scalable mobile wideband solution that is capable of supporting a wide range of smartphones, tablets, netbooks and other end-user devices. The coverage and capacity of the network can be tailored to the market and business model at hand and can be rapidly reconfigured to support new or expanded applications or territories. The system has been deployed and demonstrated in disparate settings including a military environment at Fort Bliss and at rural cellular operator sites in Florida and Arkansas. This flexibility to serve disparate markets stems from xG Technology's affordable and rapidly deployable all-IP architecture. While xMax incorporates several state-of-the-art and proprietary technologies such as dynamic spectrum access and multi-spatial interference mitigation, it also leverages COTS end user devices including 3G and 4G smartphones, tablets, netbooks, etc. These advanced features increase operational and deployment flexibility while also improving the utilization of scarce spectrum resources. xMax's cognitive networking technology is frequency agnostic and can be adapted to a wide array of TV white spaces, unlicensed and licensed frequency bands. The xMax system's cognitive networking capability allows it to dynamically access and optimize available spectrum resources, while also enabling it to optimize its own RF plan. Future software releases will enable an automatically self-organizing network (SON) in direct support of xMax's operation as a mobile ad hoc network (MANET and MESH). Finally, its end-to-end IP network architecture supports mobile voice, wideband data, real time video, chat and other apps over a single integrated network, unlike typical 3G and 4G networks which

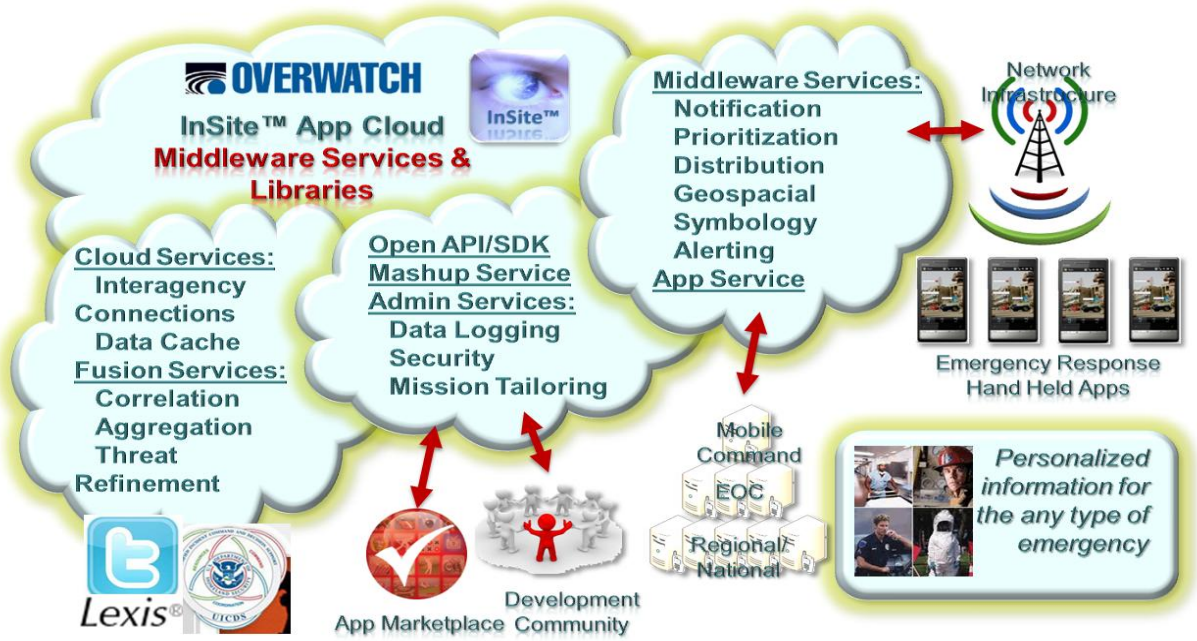

Figure 8. Cloudwave™ Middleware Framework – Provides the middleware services and libraries to necessary to develop, deploy, and maintain relevant hand held applications.

require separate voice and data network equipment and transport layers.

Middleware Framework: Cloudwave ™

The heart of the InSite solution is the Cloudwave™ middleware framework that provides an open, secure, and collaborative environment for application creation and information distribution.

Developed by Overwatch, the Cloudwave™ middleware framework (Figure 8) is a software service, able to reside within spare space on an existing, network connected computer that links mobile devices to capabilities and services such as messaging, image and video services, map services, security and user control services, federated search and notification. These services are exposed via an open API which allows 3rd party developers to build new mobile applications or integrate additional data sources into an existing Cloudwave™ deployment rapidly and at low cost. Because Cloudwave™ relies upon an IP based protocol, it is transport layer and smart phone agnostic. It can operate on any compliant communications system, and with any IP enabled smart phone to include Apple, Android, Windows Mobile, and Symbian based devices. For incident planning, incident debriefs, and system control, Cloudwave™ can be accessed through the Operations Portal application – a thin client which includes interactive mapping and analysis tools. This can be accessed through any network enabled personal computer using a web browser such as Internet Explorer.

Smart Phone Common Operating Picture: InSite™

The InSite Smart Phone COP app provides unequaled situational awareness to the user at the edge in addition to a means for communicating the current situation to the rest of the team.

Developed by Overwatch, the InSite system provides incident responders and

Figure 9. InSite COP Screen Modes – The logical and well thought out screen modes are intuitive and simple to master.

commanders with fused information that is populated to form a critical and more relevant common operating picture (COP). This provides the users greatly enhanced situational awareness and situational understanding whenever needed and wherever they are located. InSite provides handheld capabilities for collecting, reporting and communicating mission critical geo-referenced information (video, reports, photos and more) between the emergency management personnel, incident command centers and existing emergency management systems.

The InSite system provides an open architecture environment that may be rapidly and continuously updated and improved through third party application development and deployment.

InSite supports integration with external data sources and feeds and can provide a single interface to data from existing emergency management systems (such as UCIDS compliant services) as well as live operational data.

The InSite handheld app (Figure 9) is an extremely useful communications, reporting, and assessment tool. This app is intuitive and easy to use by either the experienced smartphone user or the new to smartphone user and offers a number of relevant and critical functions.

- InSite provides a Common Operating Picture through integrated mapping capabilities. The app utilizes a number of sensors on the handheld (e.g. compass, accelerometer, GPS, 3G cell service, and camera) to present the user with existing information within his/her area of interest. Both the user's position and the positions of known other entities and other members of the team are displayed in a geo-rectified manner on the handheld's Map and Augmented Reality modes.
- InSite supports data collection and reporting. The app utilizes the on-board sensors (e.g. the keypad, camera, microphone, GPS, 3G cell service, and video) to collect information the user wishes to report in a simple data input form. All reports are correlated with the author and the physical location of the report and may include attached pictures, audio, and/or video files.
- InSite is a communications tool. InSite continuously reports and displays the position of the handheld and displays that, along with the positions of the rest of the team in near real time. Everyone in the team can "see"

where the rest of the team members are positioned. As reports are generated within the user's operational area, by the team, the Administrator, or users of other emergency management systems; they appear on the team's handhelds. Displayed reports and capabilities on each phone can be adjusted to support security and role requirements, as appropriate to the users and the mission.

InSite presents this information to the user in 4 screen modes:

Screen Modes	Description
Augmented Reality (AR) View	Relevant objects in the user's defined area of interest are overlaid in real time onto the phone's camera video image. The affect is to "augment" the responder's ability to visualize his environment.
Map View	A classic "look down" map view. It is a two dimensional map depiction of entities. The Map view is filtered based each user's defined area of interest and has zoom capability.
List View	The user can see a list of all of the entities within his/her area of interest. The user can sort and filter the list to find specific entities. The user can also select items on the list and drill down into a particular entity to see a compilation or mash-up of data on an object in one easy to read narrative format.
Spot Report	Provides a very simple report capability that allows the user to report on an entity with images and text.

Operations Portal

The InSite Operations Portal provides the command center staff a thin client capable of monitoring the user's location and reports as well as communicating higher level command and intelligence down to the users at the edge.

During an emergency, information surfaces from unexpected sources and circulates organically. This poses a challenge to those who are dealing with the effects of a disaster and trying to stay aware of new developments. These individuals, be they municipal officials or citizens, seek out new sources of information and the innovative capabilities the local population create to address the situation. There is naturally a higher level of information duplication, which drives the need to have the proper context surrounding incoming information. This context is often provided by showing the location of information on maps and providing context of the timeliness of information. The Cloudwave™ portal is a solution that supports the entire lifecycle of information management in emergency situations to include: the collection of information from myriad sources; appropriate visualization of information; correlation of duplicated information; and dissemination to various products, platforms, and types of users.

The key requirement for any system used in an emergency environment is that it must be an open architecture to be extensible and benefit from the future innovations of other vendors and citizens. Additionally, it must use open standards to lower the barriers to information distribution. The Cloudwave portal provides an interactive map indicating regions of interest during a disaster. This feature allows officials to interactively specify regions on a map to communicate evacuation zones, flood damage areas, current active fires, etc. These areas can then be reviewed on InSite mobile devices, as well as on command center COPs such as Ringtail's CTV. When an active region is clicked or tapped, operators can review and update the latest information on that specific region. These regions are stored as a series of coordinates, which can be edited individually or graphically adjusted on the current map. As the disaster evolves, maps are updated based on the latest aerial or satellite imagery. Map layers can be added

to enable users to find all necessary information in one interface. Additional map layers could include current weather radar, rainfall distribution or traffic congestion. This layered imagery can be linked to a dynamically updated source on the Internet (NOAA, for example).

An example of real-world use of social media resources during emergency responses occurred during the recent wildfires in Central Texas:

- Residents of Steiner Ranch near Austin used a Facebook group, Steiner Ranch Social Committee, to disseminate information, pictures, POCs, and coordinate volunteer efforts and donations.
- A citizen created a shared public map in Google Maps which showed the status of various regions based on reports from the fire department/police scanner streaming feed.
- A citizen flew overhead to take pictures of the disaster area and posted them on Facebook. This provided families the confirmation/closure they needed if their homes were destroyed so they could prepare for the next step of their life.
- A citizen posted pictures of houses burning as historical information when there were still active fires. Without the context of time, this can spread misinformation.
- Police were talking with people 1-on-1 to spread information on road access and details of which lanes were open.

Full Motion Video

The InSite application allows instantaneous, real time access to existing video assets affording a large set of eyes that are accessible by the user at the edge.

Cloudwave™ offers access to Full Motion Video (FMV) feeds from multiple application interfaces. Streaming video feeds from Internet Protocol (IP) based video cameras can be accessed from handheld apps (such as InSite), web based applications and desktop applications.

An example of this integrated video capability was demonstrated this year at the Army exercise Empire Challenge 2011 (EC11). In collaboration with AAI, Overwatch provided the capability to view live Unmanned Aerial Vehicle (UAV) FMV streams via Android based smart phones and desktop or web client applications. Soldiers at EC11 found the increased situation understanding provided by real-time overhead aerial video streams a game-changer. By collaborating on what they saw in the video feeds with their command post team members, Soldiers on patrol were able to improve their performance from repeatedly being blindly ambushed in simulated insurgent attacks to routinely outsmarting and routing their opponents.

This same game changing situation awareness can be provided to First Responders via the architecture described in Figure 10. Feeds from law enforcement or national UAVs can be trans-coded and

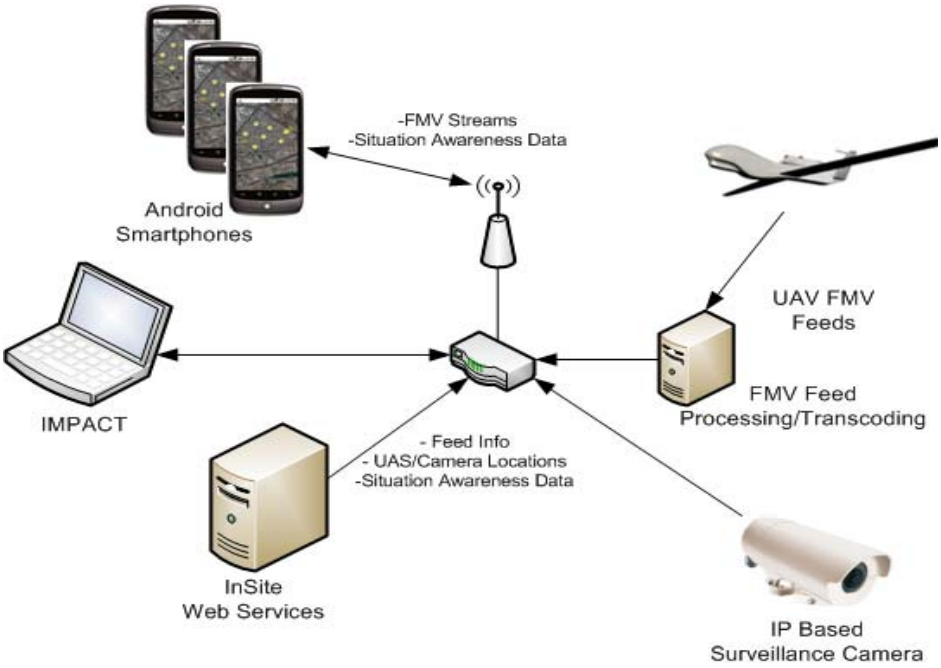

Figure 10. Architecture diagram for InSite Full Motion Video (FMV) ingestion and dissemination.

hosted for smart phone or desktop viewing. The location and video footprints of these assets can be managed by Cloudwave™ services and in turn provided to client smart phones and desktop applications. To the end user it is as simple as selecting an icon on a map depicting the location of a UAV and clicking a hyperlink to view the UAV's real-time feed. Integrating IP based surveillance cameras is even easier. The location information about the camera along with its IP address is automatically captured and this information is provided to desktop and smartphone users. Much like the UAV example above, they select the icon denoting a camera on a map and click a hyperlink to view the camera's real-time video feed.

Analytics and Fusion: IMPACT

Developed by Overwatch, the Intelligence Monitoring, Pattern Analysis and Collection Toolkit, or IMPACT, facilitates analytic investigation, organization, collaboration and contextual understanding of information, in order to create actionable intelligence. Using IMPACT software, investigators and analysts are able to quickly and easily identify and understand complex connections, relationships, patterns and trends that underlie criminal and terrorist activity.

The Textron Systems team recognizes that creating many new sensors (i.e. smart phones) in large applications will result in huge amounts of data. Overwatch is an industry leader in turning volumes of data into understandable information through advanced analytics and data fusion.

IMPACT's field-proven features include advanced search, data discovery and collection, case management, alert and area of interest management, geospatial tools and analytical tools. IMPACT's strengths include searches against multiple disparate data sources, and visualization tools that are intrinsically joined to all underlying data so the user does not have to constantly update views during analysis.

The strengths of IMPACT are:

- Deployed to analyst cells within individual public safety departments or dedicated fusion centers IMPACT can provide Cloudwave™ subscribers with relevant information to support ongoing operations.
- Allows multiple users to collaborate and conduct intelligence functions in Fusion Centers or in dispersed locations in response to national, regional, and local emergencies.
- Data model is compliant with NIEM (National Information Exchange Model) standards and ensures compatibility with multiple databases including the FBI's N-Dex, National Crime Information Center, Lexus Nexus, Clear, and other NIEM compatible databases and applications.
- Includes the 18 components of the Department of Homeland Security's Critical Infrastructure List.
- Facilitates national, regional, and local data sharing over multiple networks to ensure access to raw data and finished intelligence products.
- Provides multi-level access controls for data to be secured and accessed by only those individuals with the authority and need to know.
- Integrates various multimedia formats into its databases, allowing analysts to add and analyze images, documents, videos, and various other recordings.
- Provides mapping capabilities supporting ESRI's ArcGIS and Google Earth.

Structured Data Mining

TAP™ is an application developed by Aptus Technologies, a rapidly growing Veteran Owned Small Business providing tactical data analytics solutions in the Military, Law Enforcement and Corporate Security fields. Their products are currently being used by an Interagency Agency Task Force fighting drug trafficking on the southern border of the United States and integrated into the most advanced C4ISR solutions currently fielded. Their products have been endorsed by the United States Army Special Forces Intelligence School and the United States Army Intelligence Center of Excellence because they address the real requirements of data fusion and analysis at the tactical edge. The Threat Act Program or TAP™ is a massive collaborative intelligence application described as a "threat mining" tool. It is an assistive technology that visualizes "threats" from a variety of data sources (including direct reporting, locally stored files, emails, mIRC chat, etc.).

The Textron Systems team includes the talents of Aptus who are industry experts in tools that allow the command staff to quickly search large, complex unstructured data stores and simply visualize the results in an intuitive, uncomplicated form.

The strengths of TAP™ are:

- Rapid tactical and operational relevance of reporting from Citizen Reporting, incident report, CA Dispatch, fusion center reporting, officer and investigator reporting, social media, RSS and other news feeds and more.
- Capture free text reports and information from the field in real time.
- Intuitive data visualization – dynamic 3D Tag Cloud.
- "Threat Mass" Simple AI algorithms enable rapid info access.
- Back-end brain "learns" from users and gets "smarter."