Mark Cleverley
Don Dejewski
John Hogan
Richard McDonald

An IBM Academy of Technology Perspective about FirstNet, a Public Safety Network

Preface

This IBM® Redpaper™ describes the middleware infrastructure that is required to ensure the successful implementation of a public safety network for first responders. In the United States, this network is called the First Responders Network Authority *(FirstNet*) or the 700 MHz network. It is our goal to communicate what we believe are the necessary functionalities, products, and next steps to achieve the successful implementation of a collaborative public safety network for first responders. We make the assumption (and therefore do not address) that the telecommunications infrastructure is in place. We focus on the need for various public safety agencies to collaborate and share information, data, and processes.

This paper has multiple sections. The first section, *Background*, defines the FirstNet-enabled environment and the problems that we believe the middleware infrastructure is designed to solve. We make the assumption that there are two aspects for a public safety broadband implementation:

- The first aspect is the wireless network (which in the US is planned to be 4G LTE). Long-Term Evolution® (LTE), commonly marketed as 4G LTE, is a standard for wireless communication of high-speed data for mobile phones.
- The second aspect is the middleware that provides the applications, integration, and data services required.

The authors of this paper assume that telecommunications providers handle the first aspect mentioned. Therefore, this paper focuses on the second aspect mentioned.

The second section of this paper, *Solution overview,* begins with a generic description of the capabilities we believe are required to be implemented to meet the requirements of a collaborative First Responder network. We describe a possible reference architecture and the use of IBM technologies that can be used to build out the reference architecture to become a functional implementation.

We conclude with a brief description of the next steps that an agency, city, or state might start with as they embark on considering solutions for their locale.

This paper is the product of the sponsorship and collaborative efforts of members of the *IBM Academy of Technology* (http://www.ibm.com/ibm/academy/index.html), a society of IBM technical leaders organized to advance the understanding of key technical areas, to improve communications in and the development of the IBM global technical community, and to engage clients in technical pursuits of common value.

We extend our thanks to the members of the *IBM Academy of Technology* who sponsored this paper, which describes how the nation's first public safety network, FirstNet, can be implemented.

Background

After the events of September 2001 in the United States, first responders rallied the United States government to dedicate a portion of the 700 MHz radio frequency in North America to emergency first responders. The 9/11 Commission[1] recommended the establishment of a nationwide, interoperable public safety communications network to resolve the communication challenges that are faced by first responders nationwide. In the United States, this network is called *FirstNet*.

In this paper, the term FirstNet refers to a FirstNet-enabled environment, agency, or agencies. This paper is meant for those who are involved in understanding or designing solutions for a public safety broadband network. This could be those who are involved in FirstNet (in the US) or other, similar networks being deployed around the world. Those who would benefit the most would be IT C-suite decision makers and their solution architects. Additionally, contacts at the State level who are responsible for FirstNet would benefit from this paper.

This IBM Redpaper describes the middleware infrastructure that is required to ensure the successful implementation of a collaborative public safety network for first responders. This paper also focuses on the efforts required by multiple public safety agencies to collaborate and to share information, data, and processes. To do this, we first need to understand the following:

- *Define what the FirstNet infrastructure is and can be,* and then highlight the challenges that this middleware infrastructure is designed to solve. The wireless infrastructure that is required for implementing FirstNet is described briefly in this paper. See "What is the FirstNet infrastructure?" on page 3.
- *Understand the IBM solutions* that can be evaluated for suitability in your city, state, or federal environment. See "Solution overview" on page 7 for a generic description of the capabilities to be implemented to meet the requirements of a collaborative first responder network.

  This section also provides a reference architecture and the IBM technologies that can be used to build out the reference architecture into a functional implementation.
- *Determine the next steps and considerations* for agencies, cities, and states to use when embarking on a solution for their locale. See "Next steps" on page 20.

[1] *Public Safety Broadband: Fulfilling a 9/11 Commission Recommendation*
https://www.dhs.gov/public-safety-broadband-fulfilling-911-commission-recommendation

What is the FirstNet infrastructure?

The Federal Communications Commission (FCC) helped to design and promote a program to produce a nationally interoperable broadband network for public safety. A FirstNet-enabled environment requires a collaborative public safety network that provides emergency responders and their supporting agencies with the first nationwide, high-speed, wireless broadband network dedicated to public safety.

The goal of FirstNet is to ensure that emergency responders can communicate with each other to optimize emergency responses and reduce the risks taken during emergency situations. There are two distinct aspects to implementing a FirstNet-enabled environment:

- The wireless network (which in the United States is planned to be 4G Long-Term Evolution (or 4G LTE). LTE is the standard for wireless communication of high-speed data for mobile phones.
- The evolution from voice (radio) to rich content and applications that will be embodied in the middleware that provides the applications, integration, and data.

Figure 1 depicts the complexity of the evolution.

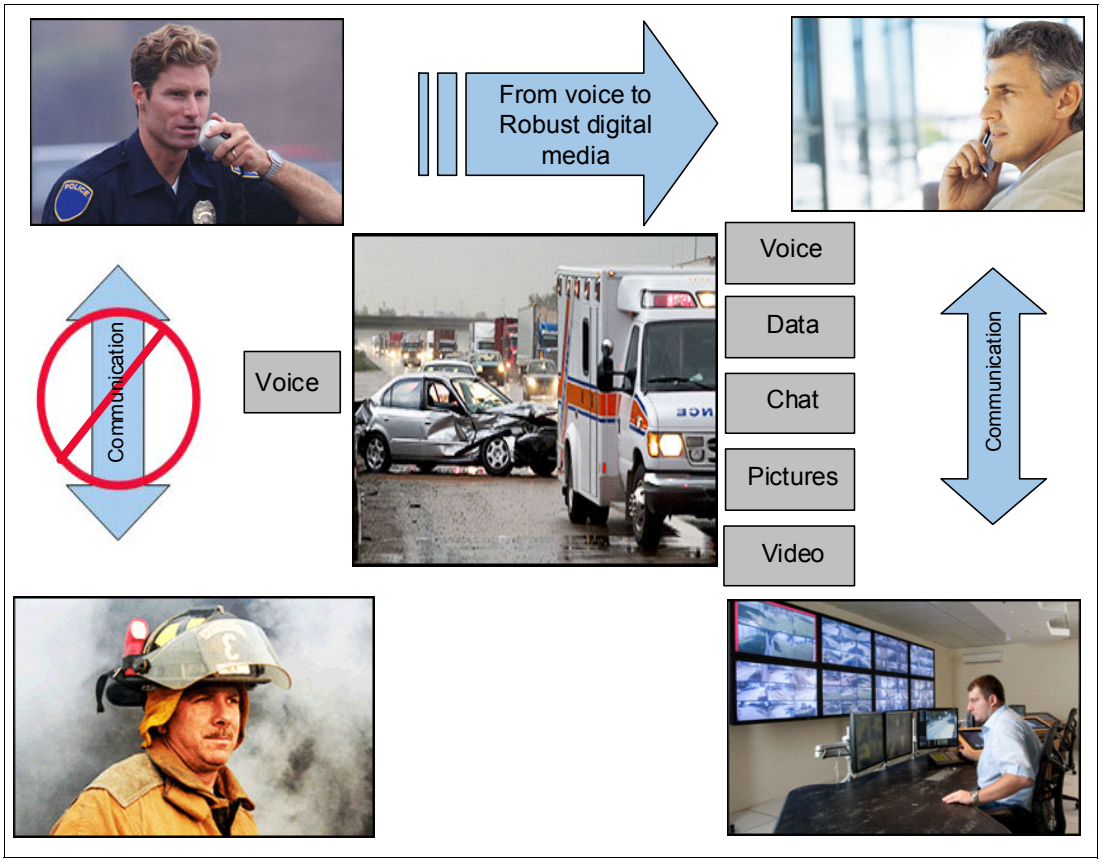

Figure 1 First responder communications, today, and tomorrow

Wireless communications

The evolution of FirstNet demands not only that its members be on the same network, but also that first responders can share relevant data and collaborate to meet the needs of the emergency. FirstNet board member, Sue Swenson,[2] provided an update on the FirstNet work effort, which highlights several scenarios to be supported using FirstNet. When discussing the data aspect of FirstNet, Ms. Swenson states:

- *"Emergency responders have also been walled off from accessing the latest technology. Essentially, the pipe is too small and the pressure is too weak to pump data through. ... Many emergency personnel resort to using their own smartphones to get the benefit of higher bandwidth and faster speeds."*
- *"What they need, and can get with LTE technology, is the ability to*
  - *Download aerial videos of an incident to enable more effective planning and strategy before responders enter the scene*
  - *Stream video of a patient from a remote location to get medical assistance during a long ambulance journey to the nearest hospital*
  - *Review architectural drawings before entering a burning building."*

A wireless communication infrastructure is developed and managed by wireless providers and their partners. It consists of the antenna, the 4G LTE network, modems, and other components of the telecommunications infrastructure. This configuration can use the dedicated bands in the 700 MHz spectrum for voice and applications in a secure fashion. This is an important aspect because it lays the required foundation for inter-agency and intra-agency first responders to communicate over a secure, high-bandwidth network in the future. Network security falls within the domain of the telecommunications providers, but it is likely that other middleware and application security capabilities will be required to achieve the various end-to-end security profiles.

The shift from voice to rich content

The sharing of data, the integration of applications, and the processes that support the public safety applications all necessitate the evolution from voice (radio) to rich content and applications, as depicted in Figure 1 on page 3. Communication has progressed from voice-only to digital electronic content that is transmitted over a network. This enables the first responders to more clearly interact with each other.

IBM has valuable perspectives and solutions in this space. IBM has strengths in mobile, analytics, and cloud technologies. In addition, IBM is regarded as a leader in middleware technologies. IBM has maximized these competencies with multiple public safety agencies and with cities as part of our IBM Smarter Cities® solutions. (See http://www.ibm.com/innovation/us/thesmartercity for information.) Because of our proven technologies and skills, IBM is considered as a key partner with many organizations that develop public safety broadband solutions.

The need for middleware infrastructure

The goal of FirstNet is to have a collaborative solution implemented for first responders in multiple agencies and cities. This is a tremendous undertaking.

[2] *FirstNet Board Member Sue Swenson Delivers Remarks to CCA Conference* http://www.ntia.doc.gov/press-release/2013/firstnet-board-member-sue-swenson-delivers-remarks-cca-conference

How does an agency or group of agencies create the infrastructure required to meet this need for collaborative communications? Any one agency starts their communications process with their own mobile and voice applications. They can use radios or telephony that run on an existing network. Enabling first responders with mobility and mobile applications is a strong starting point, but more is needed.

For the FirstNet-enabled environment to succeed, first responders from multiple agencies in a city or region must have access to applications, not only for their own agency, but for communications with multiple agencies. For this to happen, middleware infrastructure that is beyond the telecommunications infrastructure is required.

Broader context

The implications for a national, interoperable, high-speed broadband network (or set of networks) specifically for public safety personnel are not just for first responders. There are increasingly large numbers of *second responders* and related participants in the process of preparation, mitigation, response, and recovery to crime and man-made or natural disasters. Next generation technologies relevant to FirstNet, including LTE cellular, change the nature of operations within our public safety community. Social analytics technologies can provide:

- Current crowd-based information to first responders during an emergency, and possibly even before an emergency call is placed.
- Cognitive content and traditional analytics to equip a first responder with an appropriate best action and next best action.
- Video analytics for providing current live information about the emergency and surrounding areas.

These are just a few examples of the *art of the possible* with high-speed broadband and the appropriate infrastructure.

The real power of the FirstNet infrastructure is not just in the national, interoperable, high-speed, broadband network. The long-term impact of FirstNet has more to do with the applications and information that will be newly accessible, and with the cultural, behavioral, and generational changes across the organizations that use it.

For any authorized participant (traditional first responders or related responders, such as electrical crews or public health officials or public work agencies), there are many benefits of implementing FirstNet. Not only will the FirstNet-enabled environment include high-speed wireless communications, but the data that is collected can be used for collaboration, sharing, and presentation of information and actionable analytics. Working together in this manner will become the norm.

For example, when responding to an emergency, responders will have various rich applications that are tailored for their differing roles and on rugged handheld devices. These devices can provide them with context, background, and historical information about the location and the people involved. It is planned that first responders will have access to building blueprints. As the technology matures, responders will be able to open three-dimensional (3D) visualizations of the premises, based on existing building or floor plans that are drawn from both public and private sources. These responders will be able to send ad hoc requests for real-time analytics directly from their devices. It is anticipated that the devices will receive streaming audio from 911 centers and streaming video from nearby cameras. Maximizing these rich applications reduces potential risks, such as the possibility of firearms, dangerous animals, or associates that might be in potential danger.

These applications will provide notifications (or alerts) to first responders about potential dangers. These notifications can be related to the location of other first responders or to a change in the emergency itself. It will also be possible to use photographs, audio, video, and multi-media text locally, perhaps during a victim interview, to create a crime signature and compare it with suspect signatures, generating lead lists perhaps minutes after arrival.

For this example to be fulfilled, it requires FirstNet to deliver a robust, secure, high speed dedicated set of networks that enable seamless operations across the country.

Participating agencies, and in some cases FirstNet as well, must do more than address the issue of new pipes and new ways of preparing and managing what flows through them. A metaphor for this is that "*the pipe is too small and the pressure is too weak to pump data through*" (see "Wireless communications" on page 4). They must also develop the information infrastructure that these scenarios need. The country needs both; one without the other is suboptimal, and does not allow for newly developed support to be deployed with the impact wanted. Seamless, cloud-based access to different and diverse sources of information (from government databases, to private sector cameras, and citizen-based social media proximity to an incident) requires a scalable, robust, secure approach to information management and mobility. Regardless of the Information and Communications Technology (ICT) infrastructure, agencies are required to plan ahead about the governance that is needed to operate FirstNet. These areas include decision rights, accountability, and so on, to enable information sharing, integration, analysis, and distribution.

The FirstNet mission is focused on the United States. Canada is addressing the same need and aims for interoperability with the United States. Many other countries have similar concerns, such as:

- The inability to interoperate between adjacent agencies
- Difficulty with making best use of the most important resources apart from people
- Burgeoning amounts of relevant data from which to draw and deliver timely, actionable insight

Hence, this document is written for all projects globally that aim to achieve objectives similar to FirstNet.

Making real the currently fictional capabilities of popular TV crime dramas will be several steps closer to possible when FirstNet has achieved its mission. These shows depict inter-agency collaboration and demonstrate technology such as sophisticated video/voice analytics and 3D vision. To achieve these capabilities, FirstNet and its participating public safety agencies must design and implement the "I" within "ICT" to levels of sophistication that are not widely available today.

Solution overview

Figure 2 shows the evolution from a single agency with private applications, data, and processes to multiple agencies in a city to the eventual end state of multiple first responders from multiple cities (and federal) all collaborating in an emergency.

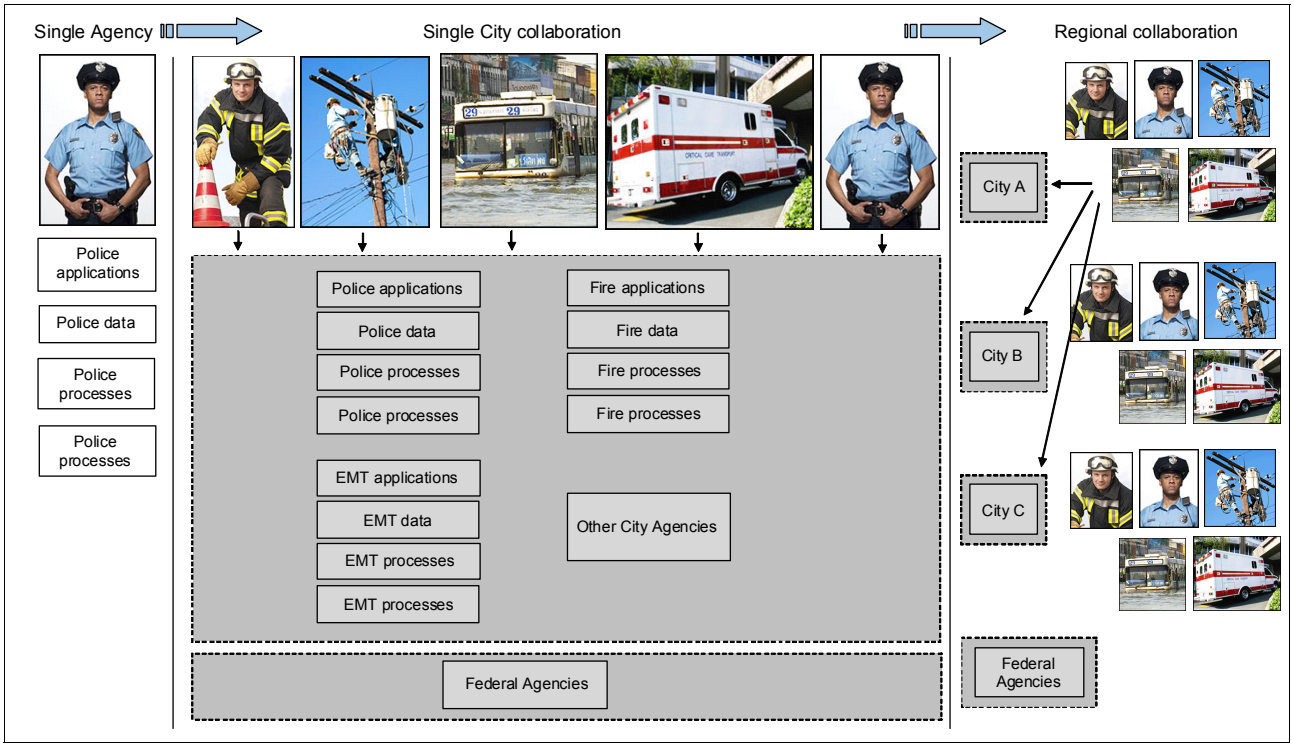

Figure 2 Vision of the FirstNet-enabled environment

The model depicted in Figure 2 is evolutionary. An organization, looking to migrate to FirstNet, starts with existing mobile applications running on an existing public or private wireless network and evolves to applications adhering to FirstNet requirements on the private FirstNet network. To prepare, agencies with existing mobile applications start to make those applications more robust and allow use by multiple agencies. For example, if the police have an existing 911 application, can that same application be shared with other agencies that also receive 911 calls? The infrastructure is modified to allow for the appropriate level of sharing (such as 911 call information, pictures, and videos). One possible path is for an agency to host a collaborative environment for their city in a private cloud or to have an infrastructure hosted for them (public cloud). Ultimately, as FirstNet matures, all new development and runtimes will reside in private, hybrid, or perhaps public clouds.

Capabilities required

For FirstNet to be successful, applications must be developed which use and share data and processes across jurisdictions and interoperate to form a complete solution. To meet these requirements, any solution must have the following capabilities:

- The integration and sharing of appropriate data (such as a 911 call or video/images from the emergency), processes, and events
- Integrated collaboration services
- A common command and control environment, also known as C&C, or C2

- Analytics
- A catalog of applications and services
- Security and privacy
- Standard operating procedures
- A development environment or platform

Overview of the required capabilities of FirstNet

The capabilities that are required beyond the network are expanded as follows:

- Integration and sharing of appropriate data, processes, and events

  Agencies need to have the same information, follow a common set of processes, and be alerted to a common set of ongoing events regardless of the jurisdiction or organization. For example, consider a large incident that has information coming from Twitter, 911 calls, first responder radio calls, and crowd sourced solutions (such as the non-U.S. based company, Usahidi). This incident also includes areas such as the New York metropolitan area, which comprises three states. From a process and event standpoint, it is clear that all first responders need to be alerted if a particular new event occurs, or if a coordinated response is required where each set of first responders (and agencies) must react to the new event. 911 or 311 systems become overloaded. As occurred with Hurricane Sandy, responders still needed to communicate regionally even though cell coverage was out.

  The success of emergency responses often hinges on obscure details, and detailed information is abundant in today's public safety organizations. Everything from criminal bookings and prior addresses, to traffic patterns and security breaches are recorded in systems and data repositories and are made potentially available for investigations. Achieving the mission at hand requires a smart approach to managing all available information, no matter its format.

  With the explosion of email and social media, public safety agencies need the ability to analyze unstructured content from the web, combining and comparing it with structured data from traditional sources to detect critical connections and develop rapid insight.

- Integrated Collaborative Services

  FirstNet was established to help with collaboration. All of the necessary services (voice, phone, and radio, but also social media) must be integrated. Radios must be able to communicate to all other modes such as phone and instant message, and there must be a return path for those communications. These modes of communications must be highly available, easy to use, and secure. These modes of communications must also be network aware if the private 4G LTE network becomes unavailable and the device needs to switch to another network (public 4G LTE, public or private WiFi) or operate without a network in a disconnected mode. The applications need to be aware of the network connection and behave differently depending on the connection or lack of connection.

- Command and control environment (C&C, or C2)

  First responders need to be alerted to and act upon new events and incidents that subsequently invoke standard operating procedures (see "Capabilities required" on page 7). Because of the complexity of coordinating first responder activities across jurisdictional boundaries, a real-time C&C environment with common operating procedures must be deployed upon incident initiation. Within this environment, common events, processes, resources, and statuses are displayed real time with supporting data such as maps. This C&C dashboard allows the leaders to have an understanding and coordination of the emergency across all first responders. For example, the office of emergency management needs to have insight into all aspects of each emergency incident. After the incident, all of the data about the incident can be analyzed against key performance indicators (KPIs) to understand and improve team performance.

- Analytics (next best action, social media, and more)

  A first responder is required to make quick decisions. Sometimes there are documented procedures for the responder to follow; sometimes a responder must use a gut feeling. FirstNet, along with current and emerging technologies, can make this decision less dependent on a person's gut feeling. It might be possible to provide the top three probable actions, along with the probability of which one might be the most appropriate action. The technology might identify the need for additional information as well. If the first responder has the information and insight necessary to make the next best decision, as they are personally involved in the emergency, outcomes can improve. A FirstNet-enabled environment can provide these types of recommendations.

  Traditional analytics from structured content are required in FirstNet-enabled environments. FirstNet takes this requirement to the next level to include cognitive analytics and therefore an understanding of a situation in real-time, using contextual information from non-traditional sources of unstructured data, including social media and voice. Cognitive analytic systems use natural language and machine learning and interact naturally with people. They help human experts make better decisions by penetrating the complexity of big data to surface new actionable insights leveraging the context of the situation. The corpus of big data can include law enforcement databases, geospatial information, incident histories, or unstructured information found in documents, reports, email, web content, and much more.

  - Next best action

    A cognitive solution provides information pre-determined to be applicable to the response based on best practices. However, machine learning will allow for real-time changes to the next best action and to predictions of possible developments to the situation. Of course, all of this can be viewed in the Common Command and Control environment solution or on a mobile device for analysis by the response team.

    Advanced natural language processing of radio, social media, and 911 calls can be used with cognitive computing to recommend a list of optimal responses. Cognitive computing has the advantage of being able to process massive amounts of data instantly, accurately, and without bias to assist human responders.

  - Social media

    Another critical area is Social Media Analytics. In an emergency, social media feeds can be critical for obtaining real-time citizen feedback as to what is happening. This feedback allows teams to be more responsive as the situation develops. An emergency vehicle might have to be diverted to a more critical area, or possibly to the original area but with more locational accuracy. Another use can be identifying the real nature of an emergency and dispatching other organizations. For example, perhaps a police vehicle is originally dispatched, but twitter feeds indicate an ambulance is now also required.

    Today's world requires comprehensive surveillance to protect airports, railways, bridges, and ports from sabotage, terrorism, theft, or vandalism. But video surveillance alone has not improved site security nor sufficiently reduced its safety risks (even with an increased number of cameras). Magnetic tapes take storage space, eventually wear out, and are not easily shared between security centers. Reviewing an event can take hours or even weeks to find evidence. Digital technology and video analytics provide the opportunity to get more value out of the video content captured and stored.

- Catalog of applications and services

  Many agencies have a set of mobile applications that are intended to run in a FirstNet-enabled environment. But having differing applications for each agency's first responders becomes counterproductive. Imagine that two counties are working together on an emergency, and each county has their own 911 mobile applications. How can they coordinate their efforts? How can they know that their efforts are coordinated? With a

common catalog of applications, the first responders from each agency can quickly obtain, install, and use applications that can interoperate. Further, applications running as services on a cloud that might be hosted by the FirstNet-enabled environment provide immediate access and interoperability to participating agencies. The catalog can include a set of common applications that are bundled and targeted for specific uses. For example, paramedics can have a range of medical services, and the hazardous materials (hazmat) team can have chemical incident applications readily available. The catalog can also contain application programming interface (API) functional primitives so that developers can tie these services together.

- Security and privacy

  Because the FirstNet-enabled environment deals with personal and sensitive situations, the data and applications must be secure and the privacy of those involved ensured. The security of the FirstNet environment needs to use a layered approach, such as:

  a. First, the ICT environment must be secure from unauthorized access, both internal and external. This can be accomplished with standard ICT security tools, which provide role-based entitlements and authentication and access services.

  b. Second, the data must be secure. In a FirstNet-enabled world, the data produced by jurisdictions can be used locally, or it may be provided to a central authority for use by others for analysis. These types of data sets will need to follow an approval and curation process to ensure that only the correct and non-personally identifiable data is released.

  c. Third, applications that operate on data must be secure. Entitlement to application usage and their data output must be governed.

  d. Fourth, devices in the field must be secured from unauthorized usage by both physical and cyber entities. This is made more complex by the bring-your-own-device movement, which introduces various user devices that are not directly owned by the enterprise. Physical security can be implemented based on guidelines from FirstNet, which provide a base. Cyber security for mobile devices can prevent unauthorized takeover of the device and uses, such as phishing. Mobile device policies can be managed from a central authority.

- Development environment or platform

  To encourage the creation of applications in FirstNet by developers and to maintain high quality, a common development Platform as a Service (PaaS) will be needed. This platform facilitates common tools, sharing, testing, and lifecycle governance of the applications.

  The existing development tools need to be pre-integrated and customized to FirstNet capability. A pallet of tools can also be provided so pre-existing functions can simply be joined to create new capabilities dynamically. This results in minimal technical training needed to be fluent in creating new applications. By lowering the skill entry point, FirstNet subject matter experts can create and release simple applications to the catalog data quickly and easily. For more complex applications, the environment supports rapid net new development of applications by providing a well thought out application lifecycle process to test for performance, security and integrity, gain approvals, and perform maintenance.

  Especially important is the availability of APIs for integration. APIs facilitate access to function within an application and data. Using APIs, new applications can be easily created and maintained without changing the underlying code. APIs enable mobile apps and offer a programmatic way to integrate systems. This makes mobile and API integration essential, and is a major driver for the API economy (the term *API Economy* or *API Marketplace* suggests primarily a new business model more so than a new technology). APIs are an old technical construct, used now in a new business model context. APIs are not about (new) technology in itself, but rather, an architectural approach revolving around

providing reusable interfaces. In the implementation of FirstNet, there must be a discipline of creating, documenting, and managing interfaces for exposing them to many different and unknown sets of users and ultimately establishing a platform. APIs need to be considered a priority in the design of mobile apps. This entails the need for API management, and that, too, is a priority.

FirstNet could define the architecture and catalog of the APIs and govern their extension by both FirstNet members and third parties.

Figure 3 depicts the necessary components for the capability requirements that are listed in “Capabilities required” on page 7.

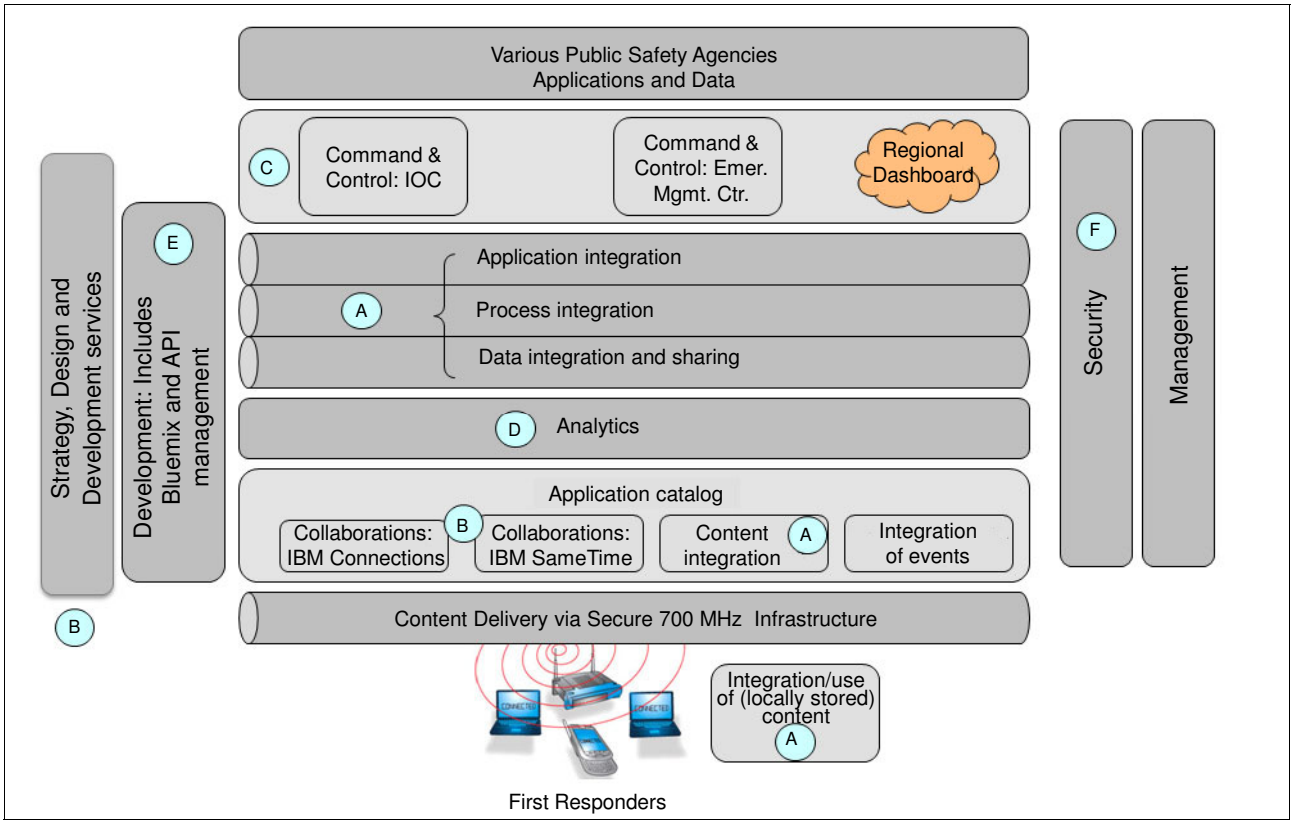

Figure 3 FirstNet reference architecture

As you can see, the FirstNet-enabled environment requires a middleware infrastructure and a way to collaborate across agencies, and regions. The fact that the middleware infrastructure must be accessible to all agencies in an emergency denotes that a cloud solution infrastructure is required. This can be an environment hosted by a third party or hosted (as a private cloud) by a significant regional authority (such as a police department). If this were hosted by a regional authority, it is possible that the infrastructure costs can be shared by the regional subscribers.

IBM solutions and integration

IBM has various capabilities to support FirstNet, including services, software, server hardware, and, on the cloud, Platform as a Service (PaaS) and Solution as a Service (SLaaS). The following section focuses on the key IBM solutions.

These solutions are noted in the following list and refer to the labeled areas in Figure 3 on page 11:

A Integration
B Collaboration
C Command and Control
D Analytics
E Development
F Security

An integral component of the FirstNet-enabled environment is to connect applications and business processes data and content across the various first responder organizations. IBM has solutions across the entire integration spectrum to enable this cross agency collaboration.

A Integration

An integral component of the FirstNet-enabled environment is to connect applications and business processes data and content across the various first responder organizations. IBM has solutions across the entire integration spectrum to enable this cross agency collaboration.

– Application integration

The IBM Integration Bus, formerly known as the IBM WebSphere® Message Broker, provides various options for implementing a universal integration foundation based on an enterprise service bus (ESB). This ESB provides connectivity and universal data transformation for service-oriented architecture (SOA) and non-SOA environments. Some of the functions included are noted in the following list:

- The ability to address diverse integration requirements that FirstNet requires.
- Connect an array of heterogeneous FirstNet applications and web services, removing the need for complex point-to-point connectivity.
- Deliver a standardized, simplified, and flexible integration foundation.

– Process integration

IBM Business Process Manager is a comprehensive Business Process Management Platform (BPM), providing full visibility and insight to managing business processes (including the processes that are required to respond effectively to an emergency). It provides tooling and run time for process design, execution, monitoring, and optimization, along with basic system integration support. IBM Business Process Manager focuses on workflow and productivity and includes the abilities noted in the following list:

- Instant collaboration and real-time visibility through analytics to reinvent business processes
- Seamless integration of business processes
- Infuse insightful context from mobile engagements into the processes to drive better interactions among first responders

– Data integration and sharing

Application and process integration is one area to explore with a FirstNet application. There are times when you might need direct access to another agency's data (such as 911 information). This capability is accomplished through the data integration layer with the integration capabilities of IBM InfoSphere® Information Server. This enables you to understand the data and to cleanse, monitor, transform, and deliver data.

Four key requirements are needed for trusted information integration:

i. Understand your information and foster collaboration between business and IT

   Encourage a standardized approach to sharing the data among first responder agencies to establish a common business language.

ii. Cleanse data and monitor data quality

   By analyzing, cleansing, monitoring, and managing data, you can turn data into trusted information. This enables the first responders to get the correct data that they need to respond.

iii. Transform data in any style and deliver it to any system

iv. Integrate data on demand across multiple agencies

– Content integration

In a FirstNet-enabled environment, first responders can now have the ability to share rich, unstructured data. This data comes in many forms including building blueprints, streaming voice (a 911 call), images and videos, and possibly even social media. A solution is needed to store and retrieve that content. This is achieved with the content management layer provided by IBM Enterprise Content Management. This layer delivers the capabilities for combined analysis of both structured and unstructured content, enabling agencies to enhance crime-fighting, emergency planning, and incident response.

IBM Enterprise Content Manager software, including IBM Content Analytics and IBM Case Manager, together with the IBM Intelligent Operations Center for Smarter Cities, provide unparalleled capabilities to help ensure public safety. The following list notes several of the ways that IBM can support public safety:

- IBM Content Analytics uncovers investigative insights and identifies patterns and trends trapped in the many forms of unstructured content available today to improve public safety analysis.
- IBM Intelligent Operations Center, integrated with IBM Content Analytics and IBM Shared Content, enables highly efficient, centralized public safety management by bringing together and analyzing information from multiple sources and providing the tools for optimal deployment of resources.
- IBM Case Manager and advanced case management technologies support collaborative investigation of public safety matters, integrating with content analytics and leading law enforcement software to help drive positive outcomes.

– Integration and use of locally stored content

FirstNet needs to access data when the network is unavailable. The IBM GAIAN database is a secure, dynamic, distributed, federated database (DDFD) consisting of multiple nodes. The nodes can be anywhere in the network and connected so that traffic and resource consumption is minimized. Each GAIAN node can process data from other GAIAN nodes, federated data from existing data sources (such as relational database management systems (RDBMSs), files, big data, web services) and its own data to provide a live, single view of all the relevant data in the network. This is required with enforcing security and a filtering policy at every node. Data stored on the GAIAN database on the device can be federated with other databases even when other GAIAN nodes change IP addresses. This provides a simple *no-management required* data virtualization layer. This means that data in each local database can be accessed even if the FirstNet network is unavailable.

The GAIAN database establishes the concept of a secure DDFD. This is a self-organizing distributed database that combines ideas from distributed database technology, database federation, network topology, and the semantics of data. The

GAIAN database makes it possible for a set of heterogeneous data sources to be accessed as a single federated database (including sources as diverse as databases, document repositories, spreadsheets, and text files). Applications can transparently perform database queries across a multiplicity of data sources in a single operation. Access to data and the flow of data can both be controlled using formal policy-based mechanisms that provide fine-grained management of security constraints.

– Integration of events and event management

First responders generally have processes that they follow. Sometimes specific *events* happen that can alter the process. IBM Operational Decision Manager provides a way to automate these processes and events. IBM Operational Decision Manager provides an elegant development environment, along with dedicated, business user interfaces, for automating and governing frequently occurring, repeatable business decisions across processes and applications. This solution also allows for the ability to handle complex event processing. Complex event processing detects the opportunity for an action that is based on events that are happening in combination over time.

The IBM Operational Decision Manager helps to support the *smart* in Smarter Process, supporting decision automation inside business processes, mobile applications, and cloud environments.

IBM Operational Decision Manager, built on the success of IBM ILOG® JRules, consists of two components, which form a platform for managing and executing business rules and business events. The following list notes those two components:

- *IBM Decision Center* provides an integrated repository and management components, allowing subject matter experts to maintain and govern their business decisions.
- *IBM Decision Server* provides the runtime components to automate decision logic, enabling the detection of business situations and precise response based on the context of the interaction.

B Collaboration

Two of the IBM tools currently in use can augment the FirstNet framework. These tools are IBM Connections and IBM Sametime®:

– Integrated collaborative services with IBM Connections

IBM Connections is one of the leaders of integrated, secure, social software platforms that can assist first responders in collaborating during an emergency. With IBM Connections in use in the event of an emergency, first responders will be able to do the following functions:

- Share and store relevant information in any format, including video
- View and update critical information about mobile devices
- Communicate using point-to-point instant messaging and situationally defined collaboration communities

When coupled with third party solutions (which integrate streaming video, phone, and radio), Connections provides the collaborative platform for FirstNet.

– Secure chat and instant messaging with IBM Sametime

IBM Sametime provides the secure chat capabilities that are required for FirstNet, in addition to secure instant messaging integrated with voice, video, and data. IBM Sametime supports communications features required for collaboration, including:

- Enterprise instant messaging

- Online presence indicators
- Community collaboration for instant connection to other first responders, including mobile device support (connecting you from anywhere on a smartphone or tablet) and voice and video integration

C Command and Control (C&C, or C2)

Complementary products in the FirstNet framework are the Intelligent Operations Centers (IOCs) for Smarter Cities and the IBM Emergency Management Center. Each provides important services:

– IOCs for Smarter Cities

Intelligent Operations Centers for Smarter Cities can provide a C&C to the FirstNet-enabled environment and to participating agencies, above the level of computer-aided dispatch. This helps first responders and city leaders to gain insight into a situation in real time. The executive dashboard spans agencies and enables drill-down capabilities into each underlying agency such as emergency management or public safety. The following list details the activities of the Intelligent Operations Center:

- Provides a common operating picture maximizing information across all city agencies and departments to make smarter decisions
- Anticipates problems to minimize the impact of disruptions to city services and operations
- Coordinates cross-agency resources to respond to issues rapidly and effectively
- Provides an integration point for information generated during an incident for KPI analysis and process improvement

The following list notes what the Intelligent Operations Center is designed to do:

- Monitor everyday agency and citywide operations and incidents
- Involve citizens and businesses in incident reporting and resolution
- Gather and analyze citizen feedback using social media
- Manage a broad range of government and commercial operations
- Deploy rapidly with minimal IT resources

– IBM Emergency Management Center

The IBM Emergency Management Center is a geospatial and analytical software solution that enables decision-makers to aggregate information from disparate sources, identify adverse conditions, quickly determine and assess different responsive actions, and monitor the implementation and effectiveness of those actions. The solution fuses knowledge of *current operational status* with a powerful *consequence analysis* functionality, delivering a *real-time* geospatial framework that provides unparalleled command and control functionality. The integrated solution is the “only” situational awareness/decision support software solution that provides robust support across all elements of “Situational Awareness” and provides 90% situational awareness in 30 seconds of less.

The solution enables the user to perform the following functions:

- Establish a geospatial common operating picture (COP)
- Integrate disparate sources of information into the COP environment in real time
- Understand the data and project, and evaluate the possible consequences that may flow from them using various tools provided as part of the integrated product

- Collaborate with stakeholders by sharing the COP and by interactively planning and implementing incident responses
- Evaluate the potential impacts of man-made or natural events by transitioning seamlessly, back and forth, from a comprehensive *live state COP* to a *what if COP* that is capable of integrating multiple third-party simulations

The functionality designed into the solution addresses all four elements of situational awareness (SA), assisting the decision-maker in the following tasks:

- Perceiving the status, attributes, and dynamics of relevant elements in the environment
- Understanding the significance of those elements in light of the goals of the decision-maker
- Projecting the future actions of the relevant elements in the environment
- Sharing SA, its components, and the decision-making process with those who need it

That functionality thus provides to the decision-maker all of the situational elements needed to make decisions in an evolving environment, serving as a foundation upon the overall decision-making process.

D Analytics

First responders make decisions all the time. These decisions can be based in a document procedure or based on gut feel. It is now possible to document these procedures (as discussed previously in process management). It is also possible to make decisions based on past history (what worked or did not work prior) and even make some future predictive decisions. IBM calls this new process of analytics *Next Best Action*. The Next Best Action solution has the following major parts (some of which have been mentioned previously):

Decision management This subsystem is responsible for developing the decision models for the solution. It is supplied with information about the emergency and the steps that can be followed. This includes historical information about similar emergencies or procedures to follow. Additionally, information gathered by first responders and citizen activity (such as through social media) are included.

Real-time decisions This subsystem contains the execution of the decision loop of the solution. The subsystem is where the action is calculated and delivered to the first responder.

State-of-the-art analytics, information management, and service-oriented technology sit in each subsystem of the solution as noted in the following scenarios.

– Decision management

Decision management supports the information pattern discovery process and information decision definition process in the decision management subsystem. It also supports the decision loop in the real-time decisions subsystem and event-driven activity. It has the following components:

- Business rules, which are used to capture the policies, regulations, best practices, and know-how of an organization. An example is that, by policy, there must be a minimum number of paramedics or ambulances on duty at any given time.
- Business events, which support the ongoing process of monitoring events that can impact the situation. An example is that when hazardous materials are detected, special teams and equipment are dispatched.

- Predictive analytics, which uses an analytical model that is derived from historical data to determine the likelihood of certain events that might occur in the future. An example is predictive policing, which attempts to forecast area and times where there might be an increase in crime.
- Natural Language Processing, from Watson, to understand radio traffic, 911 calls, and social media. With this understanding, it invokes a cognitive computing platform from advanced capabilities, such as IBM Watson, to recommend a course of action.
- Optimization, which is the process of determining the best recommendation of many possible recommendations.

– Big data platform

  The big data platform is the platform for managing the information that is used by the IBM next best action solution. It includes the following capabilities:

  - Stream computing analyzes various types of data in motion in its native format. This process is done in massive volume and scale (terabytes per second). You can process new information about the emergency that was not viable before.
  - Distributed MapReduce, which analyzes large volumes of data at rest to gain insights that were not previously possible. Sources include social media data, emails, web-click logs, and other document collections. It analyzes data in its native format, without imposing a schema or structure, to enable fast ad hoc analysis.
  - Data warehouse based on Hadoop and Hive enables high performance analytics on a large volume of historical data that is structured for control, consistency, and integrity. This historical data can be from past emergencies, situations, or people.
  - Master data management (MDM) provides a single view of (previously mentioned) information integration, which moves, transforms, and remediates information as it flows between the other components, ensuring the appropriate level of quality.
  - Application Integration (ESB) can host the decision loop and offer it as a common service for the IBM Next Best Action solution to real-time systems.
  - Cognitive computing from Watson integrates to a corpus of varied information, processes questions from natural language processing and scores response hypothesis instantaneously. Watson then can present these answers to the responder in a human consumable way in the field through a mobile client.

– Video analytics

  IBM Intelligent Video Analytics identifies events, attributes, or patterns of behavior through video analysis of monitored environments. This video analysis software monitors video streams in near real time and automatically creates current security alerts or analyzes historical data to identify specific incidents and patterns. It helps city agencies to organize, analyze, and share the insight gained from data to make smarter decisions and enable enhanced coordination within or across municipal agencies. The following list notes actions that are available in video analytics:

  - Rich content-based indexing and advanced search capability to quickly find specific near real time or historic events.
  - Expansive security, intelligence, and investigative capabilities that can provide fast security alerts.
  - Integration with IBM Intelligent Operations Center for extended data analysis and collaborative response across the city and multiple first responders.

– Social Media Analytics

  IBM Social Media Analytics is a powerful tool for discovering a citizen's perspective of a situation. First responders can use the power of social media to gain a better

understanding of an emergency. In order to accomplish this, they need deep analytics expertise to transform this *big data* into actionable insight. IBM Social Media Analytics can help you harness social data and take decisive action.

E Development

These tools represent the applications that deliver all of the components listed in “IBM solutions and integration” on page 11. These tools are developed for multiple, secure platforms and adhere to FirstNet specifications as they are defined. With the new emerging FirstNet, first responders need mobile applications that enable them to respond to emergencies. This is transforming the interaction among first responders, citizens, and city leaders. To accomplish this, the FirstNet board will write and deploy these applications, and they will define the requirements for managing and securing the applications across various devices.

IBM Worklight® is an open mobile solution for Smartphones and tablets that helps organizations of all sizes to efficiently develop, run, and manage HTML5, hybrid, and native apps. IBM Worklight makes the most of standards-based technologies and does not employ automatic code translators, proprietary interpreters, or unpopular scripting languages. IBM Worklight helps reduce time to market, manages the cost and complexity of development, and enables a rich user experience throughout multiple devices. Using this technology, developers can maximize the reusability of the code base, and can optimize the app for the unique design and functional requirements of its intended environment. The following list notes what can be achieved with IBM Worklight:

- Develop rich mobile apps using standards-based technologies
- Maximize the growing ecosystem of third-party libraries and frameworks
- Connect to various back-end enterprise systems and cloud-based services
- Control and manage a catalog of mobile apps from one central interface

A unique requirement in the FirstNet-enabled environment might be the need for an application to behave differently depending upon the network (FirstNet or commercial) that the device is connected to. Worklight provides that capability.

Other tools include BlueMix and API management:

- BlueMix and other applications

  BlueMix (CloudOE) is an advanced PaaS for development of interactive applications. BlueMix incorporates mobile, social, and analytical functions pre-packaged and tailored to the clients technical requirements. Because it is in the cloud, BlueMix is cost effective and easily accessible. As a whole, BlueMix embraces creation of new applications as it lowers risk by running on a self-healing infrastructure in an environment where the mechanics of development are automatically provisioned. Functioning this way dramatically shortens development time sometimes to hours instead of days or weeks.

  Advanced development frameworks and hosted runtimes for Java, PHP, NodeJS, Rails, and more are available for use without configuration. Using the development environment with pre-packaged services for common applications such as Mongo DB, Postgresql, or *get location*, the developer merely must provision instead of writing from scratch. The developer community also benefits by having continuous availability and continuous code delivery enabled automatically. A framework for mobile development through Worklight is available along with analytics tools including those for social media. All of this combines to simplify development so that developers can focus on the capability of the FirstNet-related applications and not the underlying IT infrastructure.

  BlueMix therefore is necessary for FirstNet to achieve its vision of a rich environment of engagement applications built by the development community and then shared with

selected members or universally. Over time, a rich store of applications customized to FirstNet will be built and used in the field.

– API management

FirstNet APIs can be internal or external to a particular organization. An example of an internal set of APIs can be those needed for a mobile application to access back-end systems. External APIs can be needed to access other systems that might be provided by other organizations and possibly FirstNet itself. The WebSphere IBM DataPower® appliances can be used as an application gateway and for API management.

F Security

The topic of security encompasses a number of aspects to consider:

– Mobile security

There are many aspects of mobile security. These include securing the device itself, securing the data, and ensuring that the right users have access.

– Mobile device management

MaaS360 is an enterprise mobility platform that enables IT to deliver end-to-end security and management for applications, documents, email, and devices. Businesses use MaaS360 to provide their employees with secure access to corporate resources and information from personal mobile devices. MaaS360 does not compromise the user experience, data security, or privacy. MaaS360 delivers maximum flexibility for bring your own device (BYOD) environments with a dual persona approach, multi-platform support, self-service enrollment, customized over-the-air configuration, automated policy enforcement, and secure distribution of applications and documents. The following lists notes the range of product modules and bundles from MaaS360 that handle various mobility requirements:

- MaaS360 Mobile Device Management
- MaaS360 Mobile Application Management
- MaaS360 Secure Document Sharing
- MaaS360 Secure Mail
- MaaS360 Secure Browser

– Secure mobile browser

IBM provides end users with a secure mobile browser that ensures safe web access. Fake websites and Man-in-the-Middle attacks are detected by the secure mobile browser, and end users are prevented from accessing the fraudulent site.

– Mobile device risk

Trusteer Mobile SDK protects organizations' native mobile apps by performing device risk factors analysis and providing a persistent mobile device ID. Trusteer Mobile SDK collects multiple mobile device risk factors and provides them to the mobile app, enabling organizations to restrict mobile app functionality based on risk levels. Trusteer Mobile SDK capabilities include those noted in the following list:

- Detection of high risk access from compromised or vulnerable devices
- Generation of a persistent mobile device ID for unique device identification

– Access and authentication services

The Trusteer out-of-band authentication enables secure transaction authorization and self-service account lockdown. Organizations can push transaction authorization requests to end users' mobile devices to validate account login and online transactions. End users can lock down their online accounts to disable criminal access. Multiple layers of security ensure that out-of-band controls are not compromised by malware on the mobile device.

IBM Security Access Manager for Mobile is an appliance-based solution combining web access management and web application protection in a modular package. It is specifically designed to help safeguard mobile, cloud, and social interactions across the enterprise. Available as either a virtual or hardware-based appliance, IBM Security Access Manager for Mobile helps secure access points into the corporate network and enforce context- based access policies that define who and what can access protected resources. Highly scalable and configurable, the solution is designed to provide a policy-based user authentication and authorization system that helps defend against the latest web-based security threats. With IBM Security Access Manager for Mobile, enterprises can now address their mobile security challenges by the actions noted in the following list:

- Helping enable user access to mobile and web applications through single sign-on and session management.
- Enforcing context-aware authorization through mobile device finger printing, geographic location awareness, and IP reputation.
- Helping improve identity assurance for the mobile users with built-in and flexible, strong authentication schemes including many one-time password options. These are often used in mobile transactions (for example, email, counter-based, RSA, SMS, and time-based one-time passwords).
- Providing mobile security intelligence and demonstrating compliance through built-in integration with IBM QRadar® Security Intelligence Platform.

Next steps

There is significant work underway around the country within the FirstNet organization. This work is ongoing through the State Single Points of Contact (state, local, federal, and tribal agencies concerned) to ensure that the first responder community is best served by the program. FirstNet outreach and consultation continues to inform its network program and the positions of the individual states in their own plans.

Nevertheless, it is helpful to present what one industry participant sees as some of the activities that will be important as groundwork for the new environment. The perspective of this paper is that which the authors see as the area in which they can best support FirstNet efforts. These areas are beyond the network itself, into the information management, integration, and presentation areas of the FirstNet-enabled applications, and the governance that supports them.

The agency perspective and the mobile strategy development perspective

This paper describes the next steps from three perspectives:

- Tasks carried out at the level of the single agency
- Tasks carried out at the level of a cross-agency perspective
- Developing and implementing a mobile strategy

For each of these perspectives, typically an assessment of current and required states is followed by a plan to close any gaps. More specifically:

1. At the level of the agency (or group of agencies sharing a) technology infrastructure, consider the following:
   - *Understand the role of your organization:* In the FirstNet-enabled environment, there are both leader and participant roles. A leader might be a large policing agency that is

the initial focal point to receive emergency calls from citizens. A participant might be a second responder that is called in to assist during an emergency or one that is initially called in to assist, but then need to take over (such as the Federal Emergency Management Agency (FEMA)).

– *Identify gaps:* Here, we summarize some of the action items and identify a few next steps, but you must balance these with the role of your agency role in FirstNet.

  Let us start with the assumption that the telecommunications infrastructure is already in place or in the process of being established. The next focus is on the middleware and infrastructure. What do you have, what do you require, and what will you provide? Consider these questions from a gap analysis perspective, from both your current situation and future state. Then, craft a strategy to fill any gaps. The following questions should all be addressed:

  - Are you a provider of FirstNet services (for example, the police department) or are you a participating agency (for example, a hospital)?
  - What information needs to be shared with other first responders?
  - What information do you need to consume from other first responders?
  - Do you want to build the infrastructure for collaboration sharing, or do you want to subscribe to the infrastructure of another agency to obtain the information?

With these considerations finalized, tackle the middleware component. Of the different components this document addresses the following questions:

– Which ones do you need?
– Which ones do you have?
– Which ones can you maximize from other organizations?

2. At the level of the cross-agency (regional or state-wide) planning and governance functions, review information sources and needs. Interoperability is at the core of the FirstNet-enabled environment. By definition, interoperability means that more information, of one form or another, crosses boundaries. Interoperability is happening and must increase:

   – Are the relevant organizations ready for interoperability?
   – Are there regulatory or other legal restrictions to consider?
   – Review the capabilities of systems in other agencies in the region you are serving

   FirstNet intends to provide significant bandwidth increases. So, the systems that supply the bandwidth might need attention over time to provide information in forms and quantities that make the most of the communications capabilities. Consider the following areas:

   – Assess stakeholder involvement and define who is already at the table, who is missing, and who needs to be there?

   – Review and (if necessary) adapt the governance that will operate within the jurisdiction. This can involve several levels of governance as local rolls up to statewide.

   – Are there reasons to invite representation from beyond government and the volunteer community? What about from other community groups, industries, homeowners, or business associations?

   – Assimilate plans for education, training, skills assessment, and gap analyses. Prepare specific training programs that are part of any transformation project. Appropriate training increases and builds upon each user's abilities and efficiencies with the application environment.

- Explore locally relevant partnerships. The various FirstNet build out options are likely to involve multiple consortia, probably based on geography, working to deploy not only FirstNet, but supporting programs as well. Such programs can span a spectrum of types, from agency-performed, in-house development, to the provision of a managed service with a telecommunications service and a set of applications behind it. These can be designed, built, owned, and operated (or any combination thereof) by a vendor consortium. In each case, there are different financial models, different participants from the private sector, and so on. Initial assessments might include the following questions:
  - Who in your domain is interested and capable?
  - What resources can these interested parties bring into the project?
  - What business model might work best? Consider those models that are being discussed in the broader community.

3. Development of a mobile strategy

   Because FirstNet is all about mobile, let us look at the middleware component a little deeper.

   A good beginning is to establish a mobile framework. This step-by-step process guides an organization through the mobile development and deployment processes. The framework helps to answer the question of how mobile technology supports the organizations' mission by using the following listed considerations:

   - Review and consider who, what data, and where
   - Balanced by security, economics, and risk (financial, policy, legal, technical, operational, privacy, and security)
   - Define the required infrastructure (using architectural decisions)
     - Supported platforms and devices
     - Supported technologies
     - Applications

Your strategy and gap analysis must also include aspects of the data and the capabilities around them. Shared inter-agency collaboration relies on quality, accessible data. Questions to ask include:

- Is the data accessible? If so, by whom?
- Is the data secure? Can it be shared?
- Is the data current?
- How would this data relate to other data and information?
- Is there critical data that you must retain (using what method, for what length of time, and where is the archived data retained)?

Infrastructure

After you have identified the gaps and decided how to address them, you might also require an infrastructure on which the middleware will be deployed. This document focuses more on the middleware perspective, but there are areas to consider for infrastructure as well. Some questions to ask are about the use of cloud technologies. Because the FirstNet-enabled environment is about collaboration, the cloud must be part of the solution. Your organization might decide to host a cloud that other participating agencies can subscribe to. You can also be a subscriber to other FirstNet cloud providers or choose to use some public cloud services. IBM can assist in all of these cloud areas.

For information, visit the following websites:

http://www.ibm.com/cloud
http://www.FirstNet.gov
http://www.ibm.com/analytics
http://www.ibm.com/mobilefirst

Another infrastructure item to consider is the use of a portable mobile data center (PMDC). A PMDC is a transport container with a self-contained cell tower, application servers, and pre-populated databases. These can be *dropped* in situations where the normal infrastructure is totally inaccessible (as was the case with Superstorm Sandy). This will allow first responders to continue to communicate and collaborate.

If you decide to deploy the middleware on-premises (either as a private cloud or as part of the infrastructure that you require for FirstNet), you need to decide on the systems required. One platform choice can be the use of an expert integrated system which includes the software and the hardware to create an easily deployable PaaS.

With your role determined, your considerations addressed, and decisions made, all of these can be applied to the infrastructure. Your decisions about middleware cannot be made in a vacuum.

Standards

An important area to consider is that of standards. To share data successfully, each agency must ensure that standards are followed. As the Information Sharing Environment team suggests, “Structured, standards-driven approaches to technology and enterprise data management are the foundation for responsible information sharing that protects privacy, civil rights, and civil liberties. Standards provide a common lexicon to enable information exchanges.”[3]

Examples of highly relevant standards in the United States (various countries have their standards as well) include:

- The National Information Exchange Model

  https://www.niem.gov/Pages/default.aspx
- Select areas under the aegis of the Law Enforcement Standards Office of NIST

  http://www.nist.gov/oles

Summary

In addition to the technology objectives of implementing a FirstNet-enabled environment, the set of business models through which agencies acquire and deliver capabilities must transform. FirstNet allows a broad range of new models of acquisition, build, and delivery. For example, a local police department, for security or financial reasons, might not immediately adapt to FirstNet public cloud-based intermediation and delivery. However, other agencies might be quick to do so. Some agencies might decide to build a private or hybrid cloud and offer their FirstNet middleware infrastructure for use to other sharing agencies, cities, and counties. In addition, FirstNet (or its constituent projects) can implement such mechanisms. Whatever the jurisdiction’s preference, FirstNet must help to determine the method of funding.

[3] *A Standards-Based Approach,* Information Sharing Environment, http://www.ise.gov/standards-based-approach

Public safety organizations that are interested in FirstNet capabilities need to start considering now how they will structure creation of these information management, analysis, delivery, and presentation capabilities. These considerations are important for their organizations and those they work with today and tomorrow.

In this paper, we argue that, beyond the raw telecommunications innovation for public safety that FirstNet represents, FirstNet also offers the chance to accelerate the momentum for transforming the way public safety agencies collaborate. This paper describes the infrastructure and middleware to allow for this collaboration.

The recognition and promotion of relevant standards for information sharing within the public safety community, while not explicitly a mandated role for the FirstNet organization, is an example of the *soft power* that FirstNet can put to good use for the benefit of the community as a whole.

Authors

This paper was produced by a team of specialists from around the world working at the IBM International Technical Support Organization, Poughkeepsie Center.

Mark Cleverley is a member of the IBM Industry Academy and the Director of Public Safety Solutions for the IBM Global Government Industry. He has worked with many levels of government around the world, since the original conception of e-government. He was a member of the original team that developed IBM Smarter Cities initiatives, specializing in the application of these initiatives to law enforcement and emergency services. He holds a degree in Psychology and Philosophy from the University of Oxford.

Don Dejewski is a member of the IBM Academy of Technology and an IBM Executive Architect and Technical Advisor for a large public sector client. Don has been an architect since 2001 and has designed many solutions for State and Local and Public Safety clients.

John Hogan is a Senior Technical Staff Member in the Watson Group. Previously, he was the chief architect for the Smart City program and for Government solutions. In this capacity, he initiated the Intelligent Operations Center project and various solutions that manage cities and governments. In prior positions, John has designed and deployed complex enterprise systems management solutions for companies such as Nissan, Honeywell, Avaya, American Express, and Northrop Grumman. He received a M.S. degree in Management Information Systems from the University of Arizona in 1996.

Richard McDonald is a member of the IBM Academy of Technology and an IBM Distinguished Engineer based in Canada. He has 33 years of experience in product development and technical sales. He holds a BSc degree in Computer Sciences from the University of Toronto. His clients include telecommunications companies in North America and Canadian clients who operate in public safety.

Thanks to the following people and groups for their contributions to this project:

- The IBM Academy of Technology

We extend our thanks to the **IBM Academy of Technology** for sponsoring this paper. The Academy is a group of IBM technical leaders, clients, Business Partners, and network affiliates who host creative and investigational ideas for application across a wide business spectrum. Because of this sponsorship and the collaboration of select Academy members, this paper describes how the nation's first public safety network, FirstNet, can be implemented. Engage with the Academy at http://www-03.ibm.com/ibm/academy/index.html.

- Peter Bahrs, Member, IBM Academy of Technology, and CTO and Distinguished Engineer, IBM WebSphere and Software Services
- Ian Baker, Global Industry Leader, GBS Government IBM Command Center® and Digital Front Office
- Roland Barcia, Distinguished Engineer, AIM Client Success CTO Mobile and WebSphere Foundation
- Patrick Dantressangle, IM Architect, Senior Technical Staff member and Master Inventor, Advanced Engagement Team and Emerging Technology
- Romelia Flores, Distinguished Engineer, Master Inventor and Academy of Technology Core Operations Team
- Gary Nestler, Global Public Safety subject matter expert, Emergency and Crisis Management, Command and Control
- Mike Reade, Public Safety and Law Enforcement Consultant, Industry Smarter Solutions Team
- Sandipan Sarkar, Executive Architect, Global Government Centre of Competence, IBM Distinguished Chief Architect, The Open Group Member, IBM Academy of Technology

Now you can become a published author, too!

Here's an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an ITSO residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Stay connected to IBM Redbooks

- Find us on Facebook:

  http://www.facebook.com/IBMRedbooks

- Follow us on Twitter:

  http://twitter.com/ibmredbooks

- Look for us on LinkedIn:

  http://www.linkedin.com/groups?home=&gid=2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/Redbooks.nsf/subscribe?OpenForm

- Stay current on recent Redbooks publications with RSS Feeds:

  http://www.redbooks.ibm.com/rss.html

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document REDP-5105-00 was created or updated on November 14, 2014.

Send us your comments in one of the following ways:
- Use the online **Contact us** review Redbooks form found at:
  ibm.com/redbooks
- Send your comments in an email to:
  redbooks@us.ibm.com
- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

Trademarks