Public Safety Messaging

A New Frontier for Collaboration and Interoperability

Broadband Applications and Information Sharing Strategic Advisory Group

July, 2019

SWIC
Texas Statewide Interoperability Coordinator

Texas Public Safety Broadband Program

Table of Contents

1. Introduction 2
2. Purpose of Document 2
3. Defining Messaging 2
4. Messaging Trends 3
5. The Benefits of Messaging for Public Safety 3
6. Emergencies and Special Events 4
7. Messaging as a Platform for Collaboration 4
8. Lessons Learned from the Military and from Harris County 5
9. Public Safety Drivers 6
10. The Need for Interoperability 7
11. Approaches to Interoperability 7
12. Public Safety Messaging Requirements List 8
13. Core Requirements 9
14. Desirable Requirements 12
15. Next Steps 15
16. Strategic Advisory Group Members 16
17. References 17

1. Introduction

The evolution of mobile broadband and the creation of FirstNet have spurred a new market for devices, services, and applications for the public safety community. Interoperability efforts, which have traditionally focused on land mobile radio, are beginning to incorporate the growing field of broadband-enabled data. The Texas Interoperable Communications Coalition (TXICC) has made interoperable public safety broadband applications one of the long-term goals of its Texas Statewide Communications Interoperability Plan[1].

Recognizing that interoperability is a broad and complex topic, the TXICC chose to approach different types of applications one at a time. Based on emerging national trends and observations of public safety broadband deployments in Texas, the group chose to focus initially on messaging applications.

In February 2019, the Texas Broadband Applications and Information Sharing strategic advisory group (Texas Broadband SAG) formed to develop this position paper on the need to identify standards and requirements for public safety messaging.

2. Purpose of Document

This paper has four primary objectives:

1. Provide an overview of the value of messaging applications in public safety communications
2. Highlight the fragmented nature of the existing messaging landscape and the problems it will present to future interoperability efforts
3. Present a list of preliminary requirements for effective messaging solutions
4. Recommend next steps toward the sustainable adoption of secure public safety messaging

3. Defining Messaging

The term "messaging" has different meanings for different people. In this paper, the term is used as shorthand for over-the-top (OTT) applications with the following characteristics:

1. Optimized for real-time, synchronous text communication in both one-to-one and group formats
2. Group communication can take place in rooms or channels
3. Usable in both desktop and mobile environments

[1] Texas Interoperable Communications Coalition, *Texas Statewide Interoperable Communications Plan*, 20.

Depending on the provider, applications with these characteristics are alternatively referred to as chat, messengers, team communication, or team collaboration. Terminology aside, it is important to emphasize that OTT messaging is very different from standard SMS/MMS text messaging on cellular devices.

4. Messaging Trends

The usage of OTT messaging is increasingly popular for private communications. Traditional SMS text messaging started to peak in 2011, with users gradually shifting toward social media and OTT messaging applications like Facebook Messenger and WhatsApp[2].

At the same time, messaging and team collaboration applications like Slack and Microsoft Teams are also trending for business. These types of applications are popular because they help reduce the volume of email and the number of in-person meetings[3] for an organization, while also improving communication for geographically dispersed teams.

Taken together, these trends have implications for the first responder community. After all, the generation that grew up texting in the 2000s and messaging in the early 2010s as teenagers are the new police, fire, and emergency medical services recruits of today. These users will increasingly look to apply modern tools when communicating at work.

5. The Benefits of Messaging for Public Safety

Messaging potentially fills a gap in the public safety toolbox by providing a real-time, one-to-many communication tool, often accompanied by support for attached files and rich media. Messaging thus combines many of the strengths of both email and push-to-talk voice. Consider the following parallels with email:

- Text-based, which allows for the use of copy/paste actions. This is both faster to transmit and less prone to transcription error than alternative voice methods of communication. For example, it takes time to accurately convey an email address, a long name, or a set of coordinates over the phone or the radio.
- The ability to share multimedia, such as documents, images, video files, or audio clips.
- Easily searched, sorted, or filtered, making it easy to quickly find and digest information in a chronological and organized way.

In addition, messaging shares some key similarities with radio:

- Communication can take place in channels or rooms, which allows for proactive planning. In the event of an incident, pre-designated chat/message rooms can act as

[2] Brian Chen, "Text Messaging Is in Decline in Some Countries," *The New York Times,* January 1, 2012.
[3] IDC Research, "The Business Value of Slack," 2017, 3.

rallying points for interested stakeholders to go to in order to receive relevant updates. This is a big contrast to email or group text messaging, which is either ad-hoc or inflexible in accommodating new recipients on the fly.

- Fast, one-to-many operation. Email requires addressing, formatting, and carries more data overhead to convey something than messaging, making it slower for both the sender and the recipient of the email. Messaging can be thought of as "radio for data" because of its speed and channelized one-to-many structure.

6. Emergencies and Special Events

During large events and emergencies, it is a constant struggle to keep stakeholders on the same page. Phone calls, emails, and text messages do not scale well during these events because they rely upon the sender not only knowing who the recipients need to be, but also having their contact information easily accessible. This is difficult when there are multiple agencies and units working in shifts during a dynamic event. Inevitably, there will be many people with a need to know who are left out of the primary communication methods.

Operations center staff spend a significant amount of time answering redundant phone calls and emails asking the same common questions and requesting the same repeated updates. In a message/chat room, everyone has the ability to receive information in real-time. New users coming on shift benefit from the ability to quickly scan the messages received during the previous shift. Follow-up questions and answers are likewise available for the benefit of everyone in the room. This cuts down drastically on the number of point-to-point emails and phone calls asking for clarification, allowing overloaded staff to focus on their core tasks. At the conclusion of an event, message/chat rooms facilitate the creation of comprehensive logs and after action reports.

7. Messaging as a Platform for Collaboration

For data communications beyond email, many public safety agencies use enterprise computer-aided dispatch (CAD), records management systems (RMS), and incident management systems (IMS). These tools are often highly-tailored to agency-specific structures and workflows. When an incident grows in complexity and begins to involve multiple agencies, these systems are not as flexible.

Messaging can act as a more unstructured tool that can adapt and scale according to operational needs. When combined with appropriate security precautions, synchronous group text can act as a glue between siloed systems. Power users can place themselves in multiple chat/message rooms that cross functional and jurisdictional boundaries, quickly transferring information from an isolated RMS into a potentially large and diverse group of recipients in a message room. By adding some basic features like file-sharing and task management/checklist capabilities, messaging becomes a lightweight but powerful tool for collaboration.

8. Lessons Learned from the Military and from Harris County

The benefits of messaging for homeland security or public safety are not hypothetical; they are substantiated by decades of real-world operational usage. The military has been using Internet Relay Chat (IRC) since the 1990s to coordinate everything from medical evacuations to air strikes. IRC usage exploded during Operation Enduring Freedom and Operation Iraqi Freedom, with organic user adoption often outpacing official Department of Defense support and sponsorship[4].

The benefits are increasingly apparent for public safety organizations as well. As an approved early builder of the public safety broadband network, Harris County, Texas was a testbed for the deployment of many broadband devices and applications. For Super Bowl 51 in Houston, the Harris County team invested considerable time in fielding the collaboration and messaging platform Moxtra. The deployment was successful on a number of fronts, with seven of eight operational benefits highlighted in the official after action report substantially attributable to messaging:

1) Significantly reduced radio traffic
2) Provided a secured mechanism for sharing sensitive information not broadcast on the radio
3) Provided improved information sharing across agencies and different units within those agencies
4) Group messaging allowed for the immediate redistribution of information
5) Redistribution of original content and sharing of pictures and videos reduced the amount of misinformation that happens automatically as information is passed to numerous individuals
6) Incident Commander (IC) could monitor events in real-time from any location
7) Reduced the noise and chaos in the Forward Command Post[5]

After Super Bowl 51, agencies in Harris County went on to use messaging during subsequent events like the response to flooding in the aftermath of Hurricane Harvey. With no integrated CAD systems between Harris County and the City of Houston, Harris County Constable Precinct 5 utilized Moxtra's task management features to dispatch Houston Police Department (HPD) resources by copying call-for-service information from county CAD and pasting it as a "to-do" item in Moxtra. Upon completing the rescue, HPD personnel would check the to-do item as complete in the app and Precinct 5 would update the call in the county CAD system.

See figure 1 below for screenshots of the Harris County deployment.

[4] Brian Eovito, "An Assessment of Joint Chat Requirements from Current Usage Patterns," Naval Postgraduate School, 2006, 2-3.
[5] Harris County Central Technology Services, *Super Bowl LI: FirstNet After Action Report*, 2017, 6.

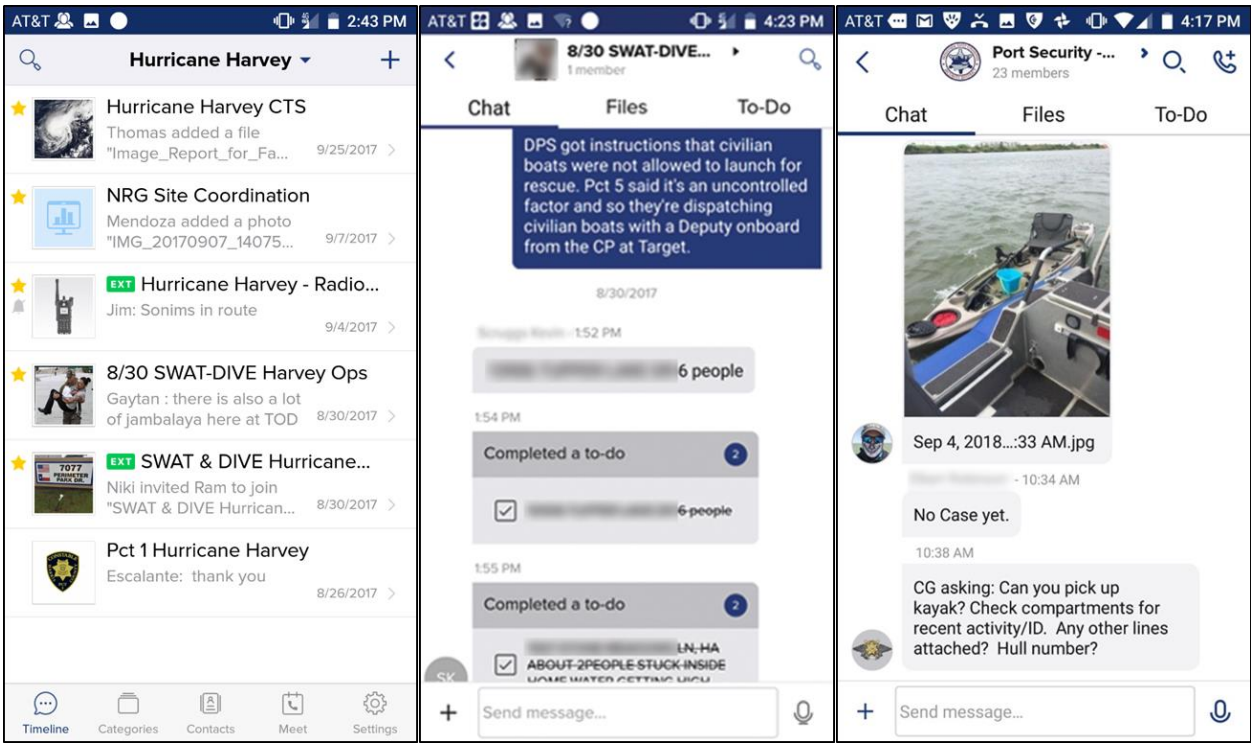

Fig. 1: Application screenshots from Harris County showing, from left, functional rooms during the Hurricane Harvey response, to-do lists organized for water rescues, and port security coordination concerning an abandoned kayak

9. Public Safety Drivers

In addition to the tactical and operational benefits of messaging, public safety users could also benefit from the better retention and safeguarding of official communication. Almost all governments have existing records retention rules governing the period of time in which data must be stored, though the exact rules and safeguards may vary by jurisdiction and data type. They also have rules about the discovery of said information, whether it be related to a criminal trial or a Freedom of Information Act (FOIA) request.

Currently, the primary means for obtaining information from texts and non-sanctioned OTT messaging apps for discovery or FOIA requests is to commandeer the smartphone or to subpoena the cellular network carrier. This poses obvious problems for public safety personnel who are using personal phones for official purposes.

The shift toward messaging in public safety is already taking place unofficially across the country. First responders will use their smartphones, whether privately owned or agency-issued, to text or use OTT messaging applications if it helps them to communicate or do their jobs more effectively. In the absence of official agency solutions, users often gravitate toward unsanctioned solutions that are free and easy. This represents potential security and liability risks for the agency, especially for protected forms of information such as criminal justice and patient health information.

A better solution would be to provide official, secure applications that meet the users' clear need for messaging. These OTT applications allow far more flexibility in information storage and reporting, and they help obviate the need to store sensitive information on the end user's device.

10. The Need for Interoperability

While the usage of messaging is certainly increasing, walled gardens of communication are proliferating. Unlike email, where Simple Mail Transport Protocol (SMTP) allows users to communicate regardless of their email client, messaging has no such standard. Common messaging protocols like Extensible Messaging and Presence Protocol (XMPP) have largely been abandoned in favor of proprietary implementations[6].

The big messaging and chat companies seem to have little incentive to promote interoperability, preferring to lock users into isolated islands of communication[7]. This is an inconvenience for private users, who often maintain a whole suite of different messaging applications in order to communicate with their friends, family, co-workers, or social groups. For public safety however, this fragmentation is untenable and potentially dangerous.

The enormous potential of broadband applications will be wasted if first responders are digitally isolated from one another, unable to share the information and insights that these tools provide. It is a common concern among public safety communications stakeholders that without intervention, the community is likely to relive the same issues with broadband that it has experienced for decades with land mobile radio and CAD.

11. Approaches to Interoperability

Interoperability is a longstanding challenge facing the public safety community, the result of evolving technology and market forces combined with the federated government structure of the United States. For years, organizations like SAFECOM have produced tools to help address the problem, chief among them being the Interoperability Continuum[8], pictured below. In the technology lane of the Interoperability Continuum, data sharing processes vary from manual file sharing to two-way, standards-based data flow.

Standards generally represent the best-case solution to the data interoperability problem. However, the process of creating standards and seeing them gain traction in the marketplace is an uncertain one that can take many years. A data exchange or integration layer[9] is also a promising solution, but requires the mapping of common data elements and attributes, and may also take years to fully fund and implement.

---

[6] For a graphic of this messaging protocol fragmentation over time, see: https://cdn.sameroom.io/chat-timeline.pdf
[7] Steven Vaughan-Nichols, "The Great Instant-messaging Foul-up," ZDNet, 2017.
[8] SAFECOM, *Interoperability Continuum*, Department of Homeland Security, 2004.
[9] John Contestabile, "Concepts on Information Sharing and Interoperability," *Domestic Preparedness*, 2011.

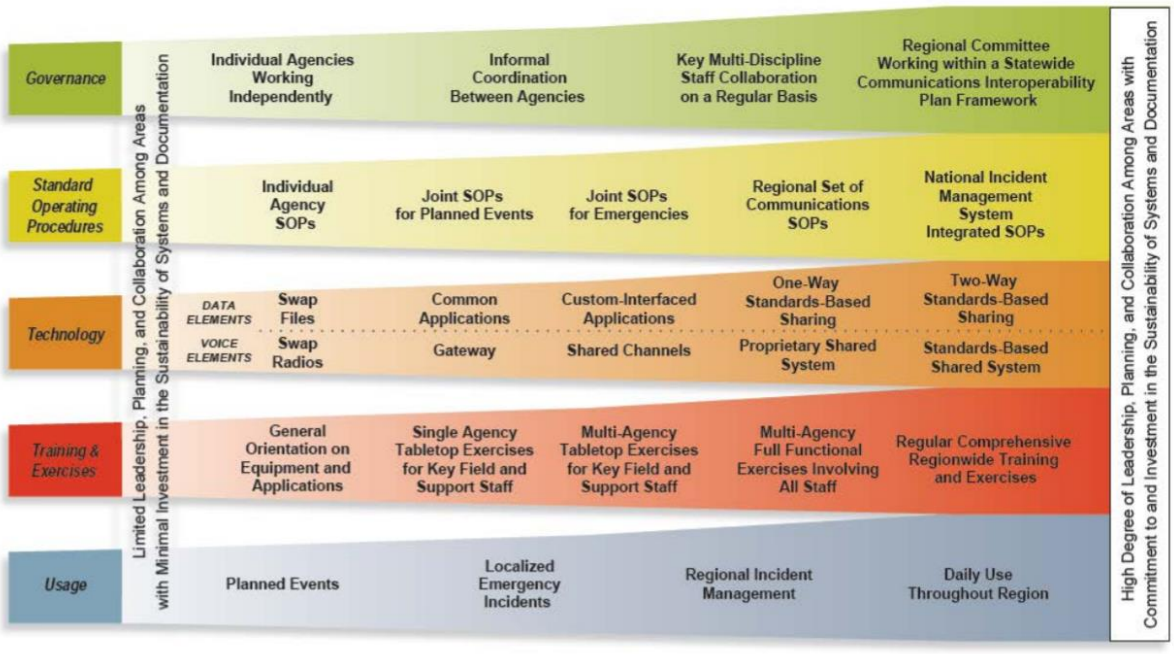

Fig. 2. DHS SAFECOM Interoperability Continuum

Despite the practical realities and limitations of standards and/or data exchange layers, the data interoperability challenges many stakeholders fear can be mitigated through interventions such as:

1. Proactive, voluntary coordination by regional, statewide, or nationwide stakeholders to develop data sharing policies[10]
2. Dedicated federal, state, or regional funding and/or request for proposal (RFP) guidance to drive the coordinated adoption of public safety messaging

12. Public Safety Messaging Requirements List

In lieu of an interoperable messaging solution, the Texas Broadband SAG has worked to generate a list of preliminary requirements for messaging and collaboration solutions in public safety. The SAG encourages feedback from interested stakeholders on the list below, as it seeks to refine it, and potentially use it as a template for future guidance on acquiring or implementing other broadband applications.

The list is organized into 1) Core Requirements, which should be considered the minimum baseline capabilities for an effective messaging solution and 2) Desirable Requirements, which add considerable value, but may still be developmental or may complicate potential future integration efforts.

[10] Britta Voss and Eric Anderson, "Interoperability of Real-Time Public Safety Data: Challenges and Possible Future States," NIST Interagency/Internal Report 8255, 2019. 47-48.

13. Core Requirements

1. Real-time Text

Description: The solution shall allow authorized users to pass real-time text to individuals (one-to-one) and to groups of individuals in a chat/message room (one-to-many).

Benefit: Allows for flexible, fast, and efficient communications. Users can move between private individual conversations to receiving text updates in a room with many users.

2. Dedicated Rooms

Description: Solution shall support dedicated rooms that can stay open indefinitely, allowing authorized users to discover, enter, and leave them when needed.

Benefit: Rooms can act as known rallying points, similar to radio talk groups/mutual aid channels. They can also be incorporated into regional and state communication plans before an event happens. This makes messaging very different from ad-hoc group texts or group emails, because a room administrator does not need to know and manually invite every individual who might need to join the room.

3. Room History

Description: Rooms shall have the option to show a full, sequential history of their messages and attached files, including for new members who have just joined the room or those who have been disconnected and rejoined. This setting shall be configurable by the room or agency administrator.

Benefit: Easy for commanders, oncoming shifts, and other new members to quickly review and catch up on or search room history, enhancing situational awareness while reducing the number of status update questions and calls. Also helps with generating after action reports and logs.

4. Encryption

Description: The solution shall support end-to-end encryption to facilitate compliance with information security and privacy standards.

Benefit: Beyond the implicit benefits of securing data, for enhanced interoperability and adoption, many groups require a minimal level of encryption for data types such as HIPAA or CJIS (e.g., a minimum of AES-128 bit encryption or FIPS 140-2 validation).

5. File Sharing

Description: The solution shall allow authorized users to upload and download files.

Benefit: Flexibility and speed in distributing information. May help with sharing some large files that cannot be sent due to email size restrictions.

6. Affordable

Description: The solution shall be affordable for a variety of public safety users and use cases. Public safety users range from donation-funded volunteer fire departments to statewide agencies with thousands of users. An ideal solution would have flexible revenue models to accommodate different-size agencies as well as large events with potential surges in temporary users.

Benefit: Allows for a more rapid and complete rollout. Affordable solutions will also be of interest to other large sectors that are potential users of the system (Healthcare, Education, Transportation, Energy, etc.)

7. Information Integrity

Description: The solution shall generate auditable records/exportable logs for defined events with enough information to establish what and when events occurred, the sources of the events, and the outcomes of the events. The solution shall also have the capability to ensure information integrity through the detection and protection against unauthorized changes to software, hardware, and information within the system.

Benefit: Privacy protection, chain of custody, evidentiary compliance, FOIA compliance. The organization can define what is classified as an "event", but the FBI CJIS Security Policy mandates a minimum level of events that are required to be logged, as well as the content of each event. These audit logs should be configurable to meet various department retention requirements.

8. User and Room Management

Description: The solution shall allow administrators fine-grained options to set room permissions, including access criteria and user privileges upon entry into a room. The solution should support a variety of access control methods, from discretionary to role or attribute-based. The solution may also include features such as artificial intelligence or chatbots to facilitate user and/or room management during large-scale events.

Benefit: Enhances security and need-to-know while also providing access control flexibility according to operational needs and event scale.

9. Multiple Login Instances

Description: The solution shall allow users the option to access the chat/message room(s) from multiple devices at once. This setting shall be configurable by the room or agency administrator.

Benefit: Allows users multiple access points and redundancy (e.g., switching from desktop to mobile) to maintain situational awareness.

10. Date/Time Stamp

Description: The solution shall support the ability to show date and time stamps associated with each message.

Benefit: Facilitates logging, reporting, auditing, and situational awareness.

11. Device/Operating System Agnostic

Description: The solution shall work on a variety of desktop and mobile devices and shall support various operating systems and browsers. The solution shall not rely on a phone number in order to create a user account.

Benefit: Flexibility in deployment. Public safety uses a range of devices (e.g., phones, radios, wearables, laptops, tablets) that could be used to transmit text. It is critically important that public safety tools support both desktop and mobile environments, thus benefitting operations centers and field users equally.

12. Hosted Information

Description: Information shall be stored at the server with the ability to centrally delete synced content stored locally on user devices. Information shall also be accessible across multiple devices logged in from a single user account. Cloud/server hosted content shall be able to be revoked from specific users as roles or operational requirements change.

Benefit: Compliance with privacy laws, CJIS, HIPAA, etc, and facilitates a bring-your-own-device deployment. Information can be recovered via the cloud, alleviating the need to subpoena an individual's personal device. The ability to centrally correct or revoke a message for all end users helps minimize the dissemination of misinformation.

13. Searchability

Description: The solution shall support search options. These can be in the form of keyword searches, filters, system metadata, user-generated data tags, etc.

Benefit: Facilitates faster decision-making and analysis, as well as compliance with discovery laws such as the Michael Morton Act (Texas Code of Criminal Procedure, Article 39.14), freedom of information act (FOIA) requests, and records retention policies.

14. Constrained Network Operation

Description: The solution shall be able to operate in low-bandwidth modes for congested/constrained network environments (e.g., not automatically downloading attachments, omitting read notifications, etc).

Benefit: First responders often work in environments with poor signal or congested networks. A low-bandwidth mode can help ensure that vital messages still get through.

15. Resilience and Availability

Description: The solution shall have a high level of reliability and resiliency. This could encompass uptime, stability, efficient use of bandwidth, and automatic rejoining after connection disruptions, as examples.

Benefit: Public safety users operate in austere conditions and potentially with lives at stake. Their communication tools need to work when they try to use them.

14. Desirable Requirements

16. Live Voice

Description: The solution should allow users to share live audio and audio conferencing.

Benefit: Provides another communication tool and a natural bridge from an operational messaging environment to a web conference.

17. Live Video

Description: The solution should allow users to watch or share live video streams. This could be used for video conferences, or sharing video from sources such as aircraft, security cameras, or the camera on a user's smartphone.

Benefit: Enhances situational awareness and facilitates web conferencing, as above.

18. Task Management

Description: The solution should have some form of task management features to help assign and track action items (e.g., a to-do checklist).

Benefit: When CAD-to-CAD interoperability is unavailable, task management features in a messaging room can be a fast, flexible, and low-tech solution to a common problem: managing the effective use of public safety resources between different organizations.

19. Location Services

Description: The solution should provide an option to pass the location information of users in a chat/message room. This could be in the form of coordinates for mobile users, and location estimates or user-specified locations for static/desktop users. For maximum training and reporting value, the solution could attach geographic metadata to each message.

Benefit: Easier to locate personnel, enhancing situational awareness and enabling faster decision-making and response time.

20. Read Receipts

Description: The solution should support the option of showing message delivery and/or read receipts when the recipient has viewed messages.

Benefit: This aids situational awareness, allowing the sender to know that the recipient is still connected to the network, and it obviates the need for follow-up prompts such as "did you receive my message?" as well as textual or verbal receipt confirmation, which adds clutter to the messaging room or radio channel, respectively.

21. Extensibility

Description: The solution should support integration with other platforms via open standards and published APIs. As the broadband environment matures, this could include a defined list of APIs that are deemed critical for public safety operations.

Benefit: Integrating a messaging tool into other public safety systems can aid situational awareness and communication. Open standards facilitate interoperability and cost savings for customers. The ability to access other systems through a messaging app can enhance the use of the tool during incident response due to the "muscle memory" developed by using it on a daily basis for various operational and administrative communications.

22. Access Methods

Description: The solution should be accessible in a secure manner over multiple disparate methods including broadband, cellular, narrowband data, satellite data, high frequency radio, and store-and-forward.

Benefit: Diversity in access methods increases resiliency and the likelihood of successfully transmitting messages.

23. Interoperable

Description: The solution should support the integration/bridging of rooms and/or users between different messaging tools.

Benefit: Public safety agencies may adopt different applications across various jurisdictions and disciplines. This should not be a barrier to interoperate during emergencies, when responders may not have the time or ability to download and learn a new messaging tool.

24. FedRamp Authorized

Description: The solution should be authorized under the Federal Risk and Authorization Management Program (FedRAMP).

Benefit: FedRAMP is mandatory for federal agency cloud deployments. Federal agencies work extensively with other jurisdictions during routine operations as well as emergencies and special events. A collaboration tool that precludes federal participation has limited value for sharing information.

25. Off-Network Operation

Description: The solution should have alternate means to preserve communication links when a user is outside of a cellular service area.

Benefit: Coverage extension, service for cell edge and off-network operations. LTE coverage may not always be available to the user. Other transport methods (e.g., Bluetooth, LTE direct mode/ProSe) would aid reliability and resiliency.

26. Global Directory

Description: The solution should allow users to search, discover, and communicate with other public safety users based on common attributes (e.g., name, organization, location, public safety discipline, jurisdiction, etc.).

Benefit: Discovery of users in the community, aiding the creation and discovery of groups, and of locating and communicating with users.

27. Identity, Credential, and Access Management

Description: Although the public safety community lacks a federated solution to identity, credential, and access management (ICAM), messaging applications should support

emerging ICAM guidance and best practices from organizations such as SAFECOM[11], the National Council for Statewide Interoperability Coordinators, and the National Cybersecurity Center of Excellence.

Benefit: ICAM is necessary to achieve single sign-on, which prevents users from having to maintain multiple passwords or to go through frequent password reset procedures. ICAM can also be a component of integration with organization directories, as above. Having a repository of users and their respective attributes reduces the administrative overhead of provisioning user accounts into a system, facilitates faster information sharing, and helps assure that the right people are able to access the right information at the right time.

15. Next Steps

The members of the Texas Broadband SAG hope that this paper helps highlight the value of messaging and contributes to the broader national discussion around data interoperability. The group welcomes community feedback, as it intends to evolve its recommendations to align with consensus best practices as they emerge.

Stakeholders are encouraged to use the requirements generated above to help find and evaluate potential messaging solutions. The TXICC may reference this document when developing future interoperability guidance and communications plans. Lastly, the group hopes that interested solutions providers will partner with the Texas public safety community to develop affordable, interoperable messaging solutions that can be deployed at scale.

Reliable mobile broadband service is becoming widely available across the country. It is time to focus on using that improved service to find solutions that improve information sharing for the public safety community. OTT messaging is one example of an ascendant technology that can greatly improve communications.

First responders are already commonly using free, unsecured, and non-interoperable versions of these applications because they fill a very real communications need. Without feedback from the public safety community however, the existing market of messaging applications will remain fragmented, creating yet another costly barrier to communication between public safety practitioners.

[11] SAFECOM/NCSWIC Identity Credential and Access Management Working Group, *SAFECOM and NCSWIC Encourage Public Safety to Adopt Trustmark Framework*, 2017.

16. Strategic Advisory Group Members

David Abernathy, Texas A&M Forest Service
Eric Baker, Texas Department of Public Safety
Edgardo Centeno, Harris County
Sean Crandall, Civil Air Patrol/Texas Department of Public Safety
Nick Curran, City of Houston
Thomas Gilbert, Brazos Valley Council of Governments
Thomas Gonzalez, Texas Department of Public Safety
Karla Jurrens, Texas Department of Public Safety
Brian Kassa, First Responder Network Authority
Derek Ladd, Harris County
Nelson Martinez, Roma Police Department
Jim McMillan, Harris County
Jeff Newbold, Texas Department of Public Safety
Daniel Nichols, Texas Military Department
Niki Papazoglakis, Mobility Acceleration Coalition
Juan Carlos Pruneda, City of Laredo
Thomas Randall, First Responder Network Authority
Jared Reinhardt, Texas Military Department
Mike Simpson, City of Austin
David Smith, San Marcos Hays County Emergency Medical Services
Clinton Thetford, Lubbock County
Robert Turner, City of Austin
Jared VandenHeuvel, Texas Department of Public Safety
Cynthia Wenzel Cole, Texas Department of Public Safety

17. References

Texas Interoperable Communications Coalition. *Texas Statewide Interoperable Communications Plan*. September, 2018. https://www.dps.texas.gov/LawEnforcementSupport/communications/interop/documents/texasSCIP.pdf

Chen, Brian. "Text Messaging Is in Decline in Some Countries." *The New York Times*. January 1, 2012. https://bits.blogs.nytimes.com/2012/01/01/text-messaging-is-in-decline-in-some-countries/

IDC Research. "The Business Value of Slack." 2017. https://a.slack-edge.com/202df/marketing/downloads/resources/rebrand/IDC_The_Business_Value_of_Slack.pdf

Eovito, Brian. "An Assessment of Joint Chat Requirements from Current Usage Patterns" (Master's thesis). Naval Postgraduate School. June, 2006. https://apps.dtic.mil/dtic/tr/fulltext/u2/a451327.pdf

Harris County Central Technology Services. *Super Bowl LI: FirstNet After Action Report*. June 27, 2017. https://hclte.harriscountytx.gov/Documents/SBLI%20FirstNet%20AAR%20Final.pdf

Sameroom.io. "A Brief History of Chat Services." Sameroom.io. 2017. https://cdn.sameroom.io/chat-timeline.pdf

Vaughan-Nichols, Steven. "The Great Instant-messaging Foul-up." ZDNet. March 14, 2017. https://www.zdnet.com/article/the-great-instant-messaging-foul-up/

SAFECOM. *Interoperability Continuum*. Department of Homeland Security. 2004. https://www.dhs.gov/sites/default/files/publications/interoperability_continuum_brochure_2.pdf

Contestabile, John. "Concepts on Information Sharing and Interoperability." *Domestic Preparedness*. January 21, 2011. https://www.domesticpreparedness.com/site/assets/files/6374/informationsharing_interoperability_concepts.pdf

Voss, Britta, and Eric Anderson. "Interoperability of Real-Time Public Safety Data: Challenges and Possible Future States." NIST Interagency/Internal Report 8255. June 19, 2019. https://doi.org/10.6028/NIST.IR.8255

SAFECOM/NCSWIC Identity Credential and Access Management Working Group. *SAFECOM and NCSWIC Encourage Public Safety to Adopt Trustmark Framework*. May 16, 2017. https://www.dhs.gov/safecom/blog/2017/05/16/safecom-and-ncswic-encourage-public-safety-adopt-trustmark-framework