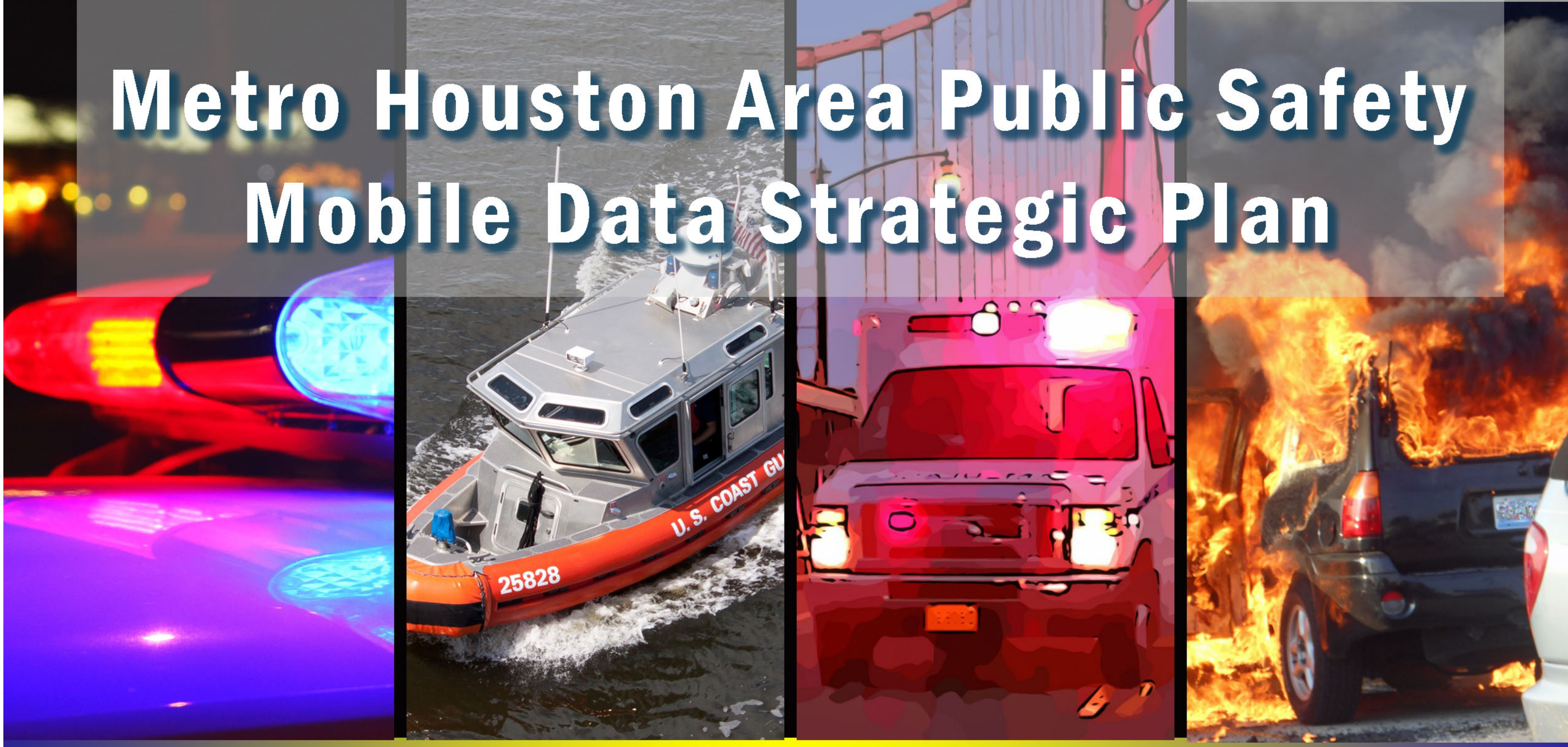
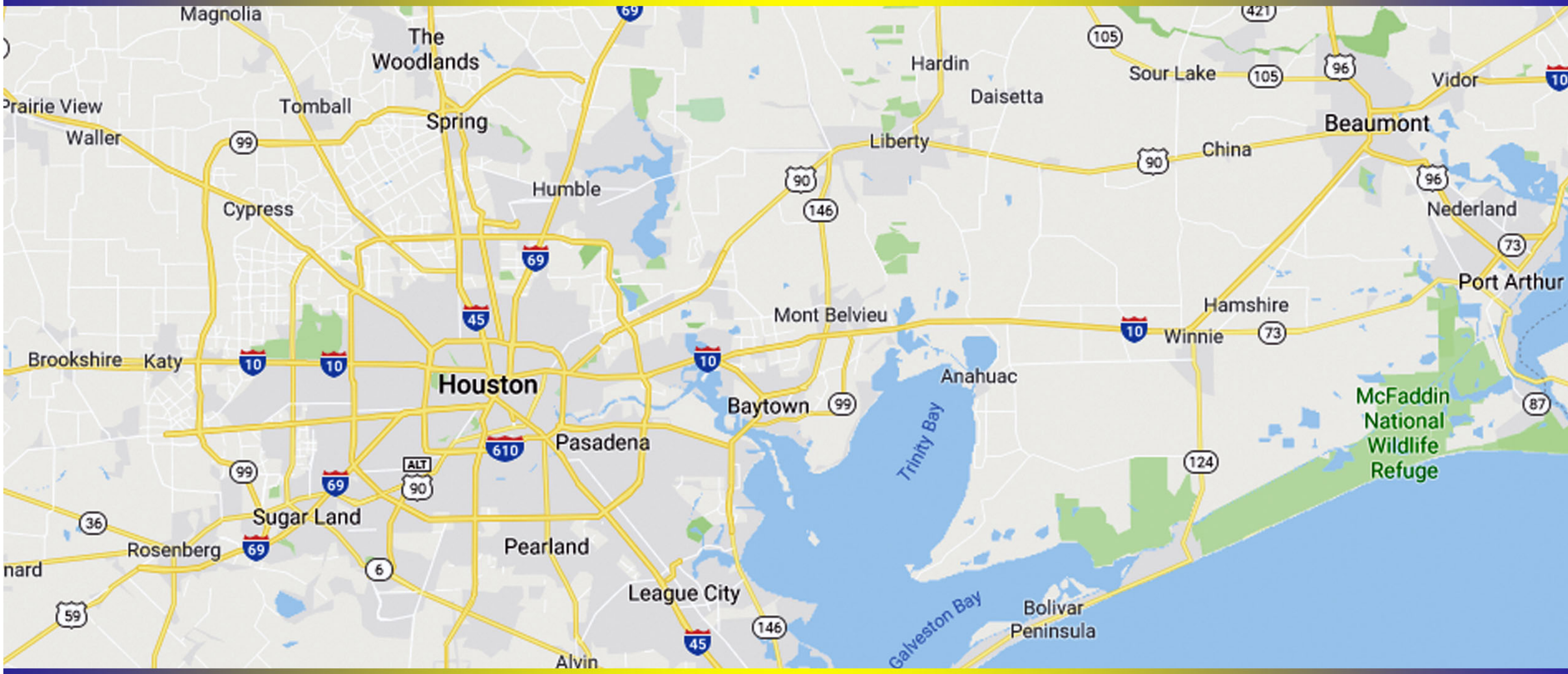
Metro Houston Area Public Safety Mobile Data Strategic Plan





M4bility
Public Safety

Houston/Harris County Regional Mobility Plan

Produced For: Department of Homeland Security (DHS)
Science & Technology Directorate (S&T)

Date Published: September 16, 2019

Prepared by: Mobility 4 Public Safety

Principle Author: Niki Papazoglakis

Contributing Authors: Michael Jumonville, Mobility 4 Public Safety

Please send comments to: Niki Papazoglakis, Principal
Mobility 4 Public Safety
1307 Waugh Dr #787
Houston, TX 77019
Phone: 346-291-5575
Email: niki@mobility4ps.com

Other Contributors and Acknowledgements

Name	Title / Role	Agency
Mike Bell	Chief Technology Officer	Houston Police Department
Brian Cantrell	Chief	Waller County
Chris Collier	Emergency Service & Response Manager	Southeast Texas Regional Advisory Council (SETRAC)
Jim McMillan	Director Public Safety Technology	Harris County Universal Services
Sam Miller	Field Services Manager	Texas Division of Emergency Management
Mike Mulligan	President	Harris County Firefighters Association
Tom Munoz	Emergency Management Coordinator	City of Texas City
Jeff Newbold	Chief Technology Officer	Texas Division of Emergency Management
Rolf Nelson	Major	Harris County Sheriff's Office
Rodney Reed	Assistant Chief	Harris County Fire Marshal's Office
Rick Retz	Homeland Security Liaison	Houston Mayor's Office of Homeland Security
Colin Rizzo	Emergency Manager	Port of Houston Authority
Jared VandenHeuvel	Program Coordinator - Public Safety Solutions	Texas Department of Public Safety

Table of Contents

Executive Summary

From 2013 - 2018, Harris County served as a network operator and mobility solution provider for all public safety stakeholders within the FirstNet Early Builder network footprint. Due to the operational effectiveness of mobility deployments during special events including Super Bowl LI (SBLI), Houston Livestock Show and Rodeo (HLSR), World Series, Astros Championship Parade, Houston Marathon, and others, public safety personnel realized the benefits that mobile broadband technologies could have for augmenting voice-only communications.

As an Early Builder, the Harris County LTE (HCLTE) program had the unique opportunity to support all public safety practitioners regardless of agency, jurisdiction, or discipline. This level of support played a key role in facilitating unprecedented information sharing across city, county, state, and federal agencies. As an experimental program, HCLTE was able to operate without many of the traditional barriers to innovation and interoperability. Recognizing the value of having a regional mobility solution provider and the non-traditional nature of the Early Builder program, regional stakeholders sought funding under the U.S. Department of Homeland Security (DHS) to form the Mobility Acceleration Coalition (MAC). The goal was to build upon the successes achieved under HCLTE and formalize a sustainable and scalable program to support the continued adoption of interoperable mobility solutions throughout the region.

A regional Mobility Working Group was formed in October 2018 representing a variety of stakeholders throughout the greater Houston/Harris County region. Working Group members acknowledged that without a coordinated plan for the adoption of mobility technologies, the region would face inevitable interoperability problems as experienced with other public safety communications technologies such as Land Mobile Radio (LMR) and Computer Aided Dispatch (CAD). Mobility Working Group Member Profiles can be found in Appendix A.

The Working Group broke into 4 subcommittees to address: 1) Governance, 2) Identity, Credential, and Access Management (ICAM), 3) Cloud Strategy, and 4) Device Management. The deliverables from each subcommittee are compiled in this report and serve as the preliminary *Greater Houston Area Regional Mobility Plan*. Key elements of the plan include:

1) Proposal to the Houston UASI Committee to form a Mobility Committee
2) Development of a high-level Regional ICAM Plan and formation of a Southeast Texas Regional ICAM Working Group
3) A Cloud Strategy Report including educational materials for securely migrating to cloud-hosted technologies
4) Device Management Report documenting best practices for managing caches of shared devices to accelerate mobility deployments

We hope that these strategic planning efforts will serve as the foundation for a sustainable program to accelerate the adoption of interoperable mobility technologies and provide a repeatable framework for other parts of the country.

Program Overview

The Houston/Harris County region has been leading the nation in adopting interoperable public safety broadband solutions since 2016. As a FirstNet Early Builder, public safety agencies had the opportunity to deploy these technologies several years before the rest of the nation with unprecedented results. One of the key factors in this success was the role that Harris County played as the network operator and custodian of the public safety spectrum. Unlike most other programs which must adhere to legal, financial, and jurisdictional realities, the HCLTE program was responsible for supporting all first responders within the network footprint. This allowed the county to operate largely agnostic of otherwise complex government circumstances to act as the mobility solution provider regardless of jurisdiction or discipline.

With the spectrum lease set to expire in 2018, local stakeholders anticipated a vacuum with no entity having the funding or authority to serve as the ongoing solution provider for the region. To avoid losing the momentum developed, stakeholders including Harris County Central Technology Services (CTS), Harris County Sheriff's Office (HCSO), Harris County Fire Marshal's Office (HCFMO), Houston Police Department (HPD), and Houston Fire Department (HFD) joined agencies from the Los Angeles region to pursue DHS funding to form the MAC to maintain the momentum of the Early Builders and accelerate the operationalizing of mobility solutions.

The goal of the MAC was to share lessons learned between the two remaining FirstNet Early Builder programs in the Houston/Harris County and Los Angeles regions. These two Early Builder programs took very different paths, in part driven by the Key Learning Conditions (KLC) associated with their respective FirstNet spectrum leases.

Harris County had significant end-user adoption fueled by the KLC for Special Events which required them to deploy mobile technologies over their LTE network for Super Bowl LI (SBLI) on February 5, 2017. The relationships developed throughout the planning process along with the unanticipated success accelerated interest throughout the region for adopting mobility solutions. Based on the size of SBLI and diversity of public safety organizations supporting the event, the HCLTE program was able to work closely with city, county, state, and federal agencies across public safety disciplines. Following SBLI, the program shifted focus from special events to mobility deployments supporting daily operations and incident response. These deployments continued to produce statistically significant operational results.

While the region was able to demonstrate the value of mobility solutions particularly for multi-agency operations, it was understood that the program was experimental and did not have the foundational elements for sustainability.

The Los Angeles Regional Interoperable Communications System (LA-RICS) is a quasi-governmental organization formed under the California Joint Powers Authority (JPA) Act. LA-RICS focused on formal governance, policies and procedures, and public safety grade network deployment.

The goal of the MAC was to leverage 1) use cases from the Houston region to drive end user adoption in Los Angeles and 2) lessons learned from LA-RICS to formalize a regional mobility program in the greater Houston/Harris County area. The MAC was designed to combine strategic planning with tactical deployments to develop Strategic Regional Mobility Plans in both areas which could serve as a basis for other regions around the country.

The first step for developing the Greater Houston Area Regional Mobility Plan was to form a Regional Working Group. Key public safety organizations were identified and invited to participate. The MAC aimed to be inclusive and representative of all stakeholders while having a manageable size working group to meet the aggressive deliverables schedule.

The Working Group identified key areas that any region would need to address to develop a sustainable mobility program including:

The Working Group broke into subcommittees to address these topics. It was soon decided that many of the topics could not be effectively addressed without a governance model to steer regional activities. Topics like mobility portfolio, resources, and support needed to be developed once a strategic plan was in place with formal oversight. Ultimately, the following subcommittees were formed:

1. Governance
2. Identity, Credential, and Access Management (ICAM)
3. Cloud Strategy
4. Device Management

Governance Subcommittee

The Governance subcommittee recognized that there is a very low appetite for Special Districts in Texas which would be the equivalent of a JPA in California. The group began by evaluating alternatives by assessing all regional bodies to determine if "ownership" of regional mobility fit within an existing entity. The conclusion was reached that no entity existed with the authority, charter, funding, and/or skills to take on responsibility for a regional mobility program. The group then utilized a Logic Model to define short, medium- and long-term goals. Based on the goals, they identified the resources, activities, and inputs necessary to achieve the desired outcomes.

After thorough evaluation and analysis, the Governance subcommittee concluded that the most viable means of standing up a regional mobility program to coordinate the adoption of interoperable mobility technologies was to request the formation of a Mobility Committee under the Houston Urban Area Security Initiative (UASI) Committee. The proposal requested that the Mobility Committee support two elements atypical of standing UASI committees:

1. Oversee mobility projects funded by non-UASI funding sources (in addition to any approved UASI-funded projects)
2. The regional mobility program be open to voluntary participation by organizations in the Houston-Galveston Area Council (H-GAC) and other parts of Southeast Texas outside the Houston UASI region

The Houston UASI Committee was determined to be the best possible fit because of its formal governance structure, ability to issue contracts, and auditability. By forming a committee to accommodate the exceptions listed above, Working Group members believed that this solution would yield numerous benefits including:

1. Minimize overhead of forming a new entity
2. Maintain continuity with other regional programs
3. Aid in the coordinated expansion of existing regional systems to support mobile access
4. Allow maximum participation throughout the region
5. Leverage multiple funding streams to achieve economies of scale procuring mobility technologies for the region

The full proposal can be found in Chapter 1.

Identity, Credential, and Access Management (ICAM) Subcommittee

The ICAM Subcommittee was chaired by the Southeast Texas Regional Advisory Council (SETRAC). MAC ICAM subcommittee activities were coordinated with work being conducted under a separate program through the State Homeland Security Program (SHSP) to develop a Regional ICAM Plan. While the MAC ICAM work was focused specifically on ICAM for mobility deployments, the SHSP grant was to develop a comprehensive regional ICAM plan.

The MAC ICAM focus was narrowly on mobility, while the SHSP was broadly addressing all aspects of ICAM with mobility being one piece of it. Based on the complimentary nature of these programs, the decision to coordinate the activities was intended to:

- Avoid stakeholder fatigue with numerous meetings for separate ICAM planning activities
- Mitigate the development of competing regional ICAM plans

The SHSP grant application focused on developing a regional plan to facilitate access control during incident response to authorized and credentialed first responders. The MAC ICAM efforts were focused on sharing identities across organizations and developing secure means of issuing credentials for access to mobile applications.

The influence of both programs on the other was deemed mutually beneficial for both grant projects. Working group members successfully gained buy-in from stakeholders throughout the region to support further development of a regional framework to share first responder identities throughout Southeast Texas.

The first version of the Regional ICAM Plan can be found in Chapter 2. This serves as a high-level strategic plan which outlines the vision and general next steps for developing a regional ICAM plan. An ICAM Working Group has been formed as a result of Phase 1 to evolve the plan to develop a technical framework and tactical department-level actions to move achieve regional federated identity sharing.

Cloud Subcommittee

Much of the success of the HCLTE program in achieving multi-agency interoperability was achieved through the use of cloud-hosted mobile apps, in particular a collaboration app which allowed thousands of users across organizations and disciplines to seamlessly communicate during special events, daily operations, and incident response. Many systems utilized by public safety organizations are deployed inside a secure enterprise environment intended to only be accessed by authorized, internal users. Sharing information with users from third party organizations is often difficult, particularly without a federated ICAM framework.

"The cloud" is creating its own paradigm shift in how information is stored, accessed, and managed. Cloud hosted systems generally offer more flexibility, reduced speed of deployment, greater accessibility, and lower costs than many legacy systems. Yet while cloud-hosted systems offer many advantages, they also introduce an entirely new set of risks and challenges.

For public safety agencies, communicating and sharing information across organizations through secure, cloud-hosted apps offers tremendous opportunity. The goal of the Cloud Subcommittee was to develop a regional strategy for adopting cloud-based mobile systems to augment internal agency systems for multi-organizational information sharing.

In conducting research to develop the plan, working group members found the majority of literature about public sector adoption of cloud was focused on moving enterprise systems from legacy, self-hosted applications to more efficient cloud-hosted systems. Cloud-based systems, whether privately or publicly hosted, are designed to better optimize network resources than most legacy on-premise systems. Legacy systems were typically designed to support users accessing them from the organization's internal network. These older systems were often built on complex databases which users would enter data or conduct queries from a workstation client. The user experience of these systems is dependent on the available network bandwidth to transmit information between the workstation and the server. The Cloud Strategy can be found in Chapter 3.

Device Management Subcommittee

The region recognizes the need for cache phones to deploy during special events and disaster response. Managing cache phones is different than managing cache phones or computers. This subcommittee evaluated lessons learned, best practices, challenges and limitations for provisioning and managing cache mobile devices. The subcommittee worked with the Texas Division of Emergency Management (TDEM) to compare processes and technologies. TDEM manages over 7,000 phones that get deployed throughout the State of Texas. They provided invaluable lessons learned which are documented in the Device Management Report in Chapter 4.

Chapter 1: Governance Subcommittee

Chairperson: **Richard Retz**, Homeland Security Liaison
Houston Mayor's Office of Homeland Security & Emergency Management

Committee Members:

Mike Bell, Chief Technology Officer
Houston Police Department

Brian Cantrell, Emergency Management Coordinator
Waller County

Darren Hess, Emergency Management Coordinator
Montgomery County

Mike Mulligan, Chief
Atascocita Fire Department
Harris County Firefighters' Association (President)

Tom Munoz, Emergency Management Coordinator
City of Texas City

Rolf Nelson, Major
Harris County Sheriff's Office

***Jeff Newbold**, State Coordinator*
Texas Division of Emergency Management

Rodney Reed, Assistant Chief
Harris County Fire Marshal's Office

Jared VandenHeuvel, Public Safety Broadband Coordinator
Texas Department of Public Safety

Proposed UASI Mobility Committee

Executive Summary: The U.S. Department of Homeland Security (DHS) provided funding to the Houston Region to examine lessons learned from the early deployment of a Public Safety LTE network and to identify issues that still need to be addressed. While there are many findings and recommendations being made back to DHS, local working group members have identified one critical issue that can be resolved locally and with minimal effort. The region needs a framework that can provide voluntary guidance for the acquisition and use of mobile technology applications to help further interoperability and collaboration among public safety members. The working group is requesting the creation of a new committee under the Houston UASI Program to oversee this effort. It is hoped that this new committee can help prevent the missteps that occurred during the early days of land mobile radio deployment and thereby enhance the use of mobile broadband among our public safety community.

Program Overview: Harris County Central Technology Services (CTS) was one of five FirstNet Early Builder Programs authorized to deploy a Public Safety LTE network in advance of the FirstNet nationwide network. In exchange for the spectrum lease, Harris County LTE (HCLTE) was required to provide lessons learned for the broader network deployment. One of those lessons learned was around the deployment of mobile broadband during special events, specifically Super Bowl LI on February 5, 2017. The success of that event demonstrated the operational impact that mobile broadband technologies can have as well as the importance of multi-agency technology planning and adoption. With the sunsetting of the HCLTE program in 2018, DHS funded the Mobility Acceleration Coalition (MAC) to support the continuation of the momentum in the region and develop a strategic plan for the coordinated, sustainable adoption of interoperable mobile data systems.

The Houston/Harris County area MAC working group is comprised of representatives from a variety of jurisdictions and public safety disciplines throughout the region. The working group convened in November 2018 to begin work on a regional strategic mobility plan. At the core of the planning efforts is the development of a recommendation for a governance model to facilitate and oversee a regional mobility program.

Justification: First Responders are unable to effectively collaborate across agency boundaries in steady state or during emergency response. There is a need for a mechanism to coordinate the adoption of mobile technology used by first responders within the region. The governance recommendations are based around 5 key assumptions:

1. FirstNet allows for priority connectivity but does not ensure application interoperability and/or information sharing between agencies.
2. Not all agencies may choose to convert to FirstNet.
3. The value of cooperating with others outweighs going it alone.
4. The region wants to keep the momentum established under the Early Builder program.
5. Better initial coordination of mobile technology acquisition will ensure a more effective outcome.

If there is a framework for our region that provides voluntary guidance for the acquisition and use of mobile technology application, the interoperability among various public safety end users is enhanced.

A thorough analysis was conducted of existing entities to serve as the governance body for a regional mobility program; however, it was determined that there was no existing body with a "natural" responsibility to oversee mobility. The public safety industry is rapidly moving to a more mobile world with the availability of reliable, broadband wireless networks. This move towards mobility brings with it numerous opportunities, as well as a variety of new challenges. Cloud-based mobile apps have already demonstrated their effectiveness in solving long-standing operational communications issues across agencies in the region. These cloud-based apps also require new policies and procedures for coordinated, compliant and secure information sharing.

Proposal: After evaluating a variety of existing organizations and exploring the feasibility of a new body, the group came to consensus that the most logical place for the governance of a regional mobility body is the Houston UASI Program. Houston UASI offers a formal body that can support regional policy development and influence technology adoption.

Given that mobility crosses so many lanes, the MAC working group asks that the UASI Executive Committee consider the establishment of a new UASI Mobility Committee with subject matter representatives from the First Responder Fire and Law Enforcement committees, Intelligence and Information Sharing, Interoperable Communications, and the Regional Collaboration committees to provide the governance structure to oversee a formalized regional mobility program.

Unlike many existing UASI regional projects, it is envisioned that future funding for this effort will not come exclusively or possibly even predominantly from the UASI grant. It is also requested that the regional mobility program not be restricted to only UASI jurisdictions but participation be open to any interested public safety entities within the region. (E.g., the State of Texas is conducting research in this area and could be a potential asset and valuable partner in the future.)

Goals:

1. Create a regional mobility program that provides sufficient value for voluntary participation by public safety agencies throughout the region
2. Improve regional collaboration and information sharing for first responders through coordinated adoption of mobile technologies (Mitigate interoperability challenges of fragmented mobility deployments and investments)
3. Improve operational efficiencies through the adoption of mobile technologies
4. Provide a framework for secure identification and credentialing of first responders mobile devices and applications throughout the region

Objectives:

1. Develop regionally accepted policies and procedures for coordinated mobility technology adoption
2. Identify funding sources outside of the traditional UASI funding stream
3. Oversee technology selection and facilitate product acquisition
4. Aggregate funding sources to maximize benefit and reduce costs through regional economies of scale
5. Incorporate emerging guidance and best practices from national level initiatives as the public safety mobility market evolves and matures

Chapter 2: Identity, Credential, & Access Management (ICAM) Subcommittee

Chairperson: **Chris Collier**, Emergency Service and Response Manager
Southeast Texas Regional Advisory Council (SETRAC)

Committee Members:

Mike Bell, Chief Technology Officer
Houston Police Department

Tom Munoz, Emergency Management Coordinator
City of Texas City

Richard Retz, Homeland Security Liaison
Houston Mayor's Office of Homeland Security & Emergency Management

Jared VandenHeuvel, Public Safety Broadband Coordinator
Texas Department of Public Safety

Executive Summary

Identity, Credentialing and Access Management (ICAM) is a broad term that encompasses a variety of challenges for verifying the identity of first responders and other personnel authorized to access physical locations and virtual systems in the performance of public safety operations.

Historically, the management of physical access control systems (PACS) and logical access to information systems have been separate and distinct functions typically managed by different organizational units. Technology is evolving to provide the ability to:

1. Utilize standard processes for verifying identity across departments and jurisdictions
2. Issue credentials which provide authorized access to both physical and logical systems
3. Build frameworks to trust the identities and credentials of practitioners across organizations

These advancements offer tremendous opportunities to improve security and information sharing across departments.

As more buildings are automating access control and implementing other “smart building” technologies, the management of physical and virtual access control systems is converging. Meanwhile, the availability of reliable mobile broadband is allowing public safety agencies to adopt mobile technologies at an accelerated pace. At the same time that public safety is becoming more electronic, automated and mobile, hackers and terrorists are also becoming more sophisticated and posing even greater threats.

It is critical that public safety leaders understand the importance of developing ICAM plans and implementing systems that meet industry standards and best practices to ensure the safety and security of first responders and the communities they serve.

Due to the rapid technology advancement in recent years and the complexity of ICAM, industry efforts to develop solutions to address these problems have been fragmented. There are arguably four primary efforts leading the innovation and thought leadership in public safety cybersecurity:

1. National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) - NCCoE efforts have focused predominantly on building an open framework for implementing standards-based technologies for authentication, federation and single sign on.
2. Department of Homeland Security (DHS) Emergency Communications Division (ECD) & SAFECOM - the DHS/SAFECOM work has centered around the development of the Trustmark Framework to build a federated model for public safety agencies to establish trust relationships to share identities across agencies and manage authorized access to information systems.
3. DHS Science & Technology Directorate (S&T) - DHS S&T has conducted extensive research in developing an ICAM framework that utilizes an exchange hub to manage identities and credentials for secure information sharing. This work has focused largely on developing repeatable, low-cost, standards-based solutions for smaller public safety agencies with limited internal IT resources.
4. Federal Emergency Management Agency (FEMA) - The FEMA ICAM Working Group has been leading the adoption of the Personal Identity Verification Interoperable (PIV-I) card to allow non-federal agencies to follow the federal processes, guidelines, and standards for identity proofing and credentialing to issue physical ID cards which can allow federal and non-federal government personnel to share secure access to facilities and information systems.

Problem Statement

First Responders in the H-GAC region currently have no mechanism for confirming the identity of authorized response personnel in multi-jurisdictional / multi-discipline incident response. Terrorists are increasingly impersonating first responders and using “cloned” emergency vehicles to carry out acts of terrorism around the world, so having the ability to verify identity and restrict or permit access to buildings, incident scenes and information is vital to our community safety.

Credentialing is essential to the emergency response community in that it ensures and validates the identity and attributes (e.g., affiliations, skills, or privileges) of individuals or members of response teams. Having established standards allows the community to plan for, request, and have confidence in resources deployed from other jurisdictions for emergency assistance. Credentialing ensures that personnel resources match requests, and it supports effective management of deployed responders. With no current responder credentialing system, approved ICAM plan, guidelines, or common approach implemented in the Houston area leaves the region’s jurisdictions vulnerable for terrorist attacks. The development of a regional ICAM plan will address the region’s risk by implementing - through the development of a systematic region-wide approach - a plan for addressing ICAM and credentialing of first responders; giving law enforcement and authorities the ability to authenticate credentials and control access when needed to critical sites, incidents sites, and critical information for disaster response.

There is not a regional identity management approach or strategy universally accepted or implemented that provides a pathway for members of public safety agencies to have trusted access to critical information at either their desktops or on mobile devices. Law enforcement, justice, and public safety entities need access to this information on a regular basis from mobile devices, and the methods to access information need to be low-cost, simple, and standardized. Today, Individual jurisdictions have identification systems in place however there is no regional credentialing system or plan in place that crosses all disciplines/jurisdictions meeting United States Federal Government FIPS-201 standards; with capabilities and oversite needed to implement/manage a regional FRAC program; additionally not meeting NIMS Credentialing Criteria.

In spite of the successes in improving information sharing, identity verification, and access management both physically and digitally, great difficulty still exists in making the connection to the last mile—primarily the officer, deputy sheriff, firefighter, and paramedic in a vehicle or in the field. The access to critical information and the ability to verify responders on the ground enhances the region’s capability to prevent, protect against, and respond to high profile incidents or suspected acts of terrorism. A regional ICAM plan will help reduce identified gaps by:

- Fostering effective region-wide identity and access management
- Aligning regional agencies around common identity and access management practices
- Reducing the identity and access management burden for individual agencies by fostering common interoperable approaches
- Ensuring alignment across all identity and access management activities that cross individual agency boundaries
- Collaborating with external identity management activities through inter-agency cooperation to enhance interoperability
- Identity proofing of network users—the process of verifying a user’s identity

Regional ICAM Plan: Program Summary

Step 1: Conduct Regional ICAM Educational Seminar

Hold an educational seminar involving regional stakeholders, for the purpose of generating involvement and consensus for a Regional ICAM Plan.

Invite Subject Matter Experts (SME) from STRAC, FEMA, DHS, NCCoE, FTI, and other state/local executives with successful ICAM programs to showcase best practices.

Step 2: Gain executive support for Regional ICAM Initiative

Conduct executive meetings with key stakeholder organizations
Ensure representation of jurisdictions and disciplines throughout the region

Step 3: Assemble Regional ICAM Working Group

Executive Steering Committee

- Develop priorities for the region (i.e. changing policies, adopting technologies, standardizing purchasing/procurement procedures, legislative updates, etc.);

Technical Working Group

- Support regional education/outreach
- Conduct data collection for existing systems

Step 4: Develop a Baseline Regional ICAM Plan

Tactical Actions for Individual Departments/Jurisdictions

- Adopt federally approved ICAM standards & protocols
  - Multi-Factor Authentication (MFA)
    - Personal Identity Verification Interoperable (PIV-I)
    - Fast Identity Online (FIDO)
  - Single Sign-On
    - OAuth
  - Federation
    - Security Assertion Markup Language (SAML)
    - OpenID Connect
- Provide standardized ICAM procurement language for new systems
- Identify and apply for eligible grant funding

Strategic Planning - Regional Coordination for Sharing First Responder Identities & Credentials

- Define **WHAT** information organizations want to share
- Identify **WHO** organizations want to share with
- Develop a regional framework for **HOW** organizations share identities an information

Technology Requirements: Standards-Based Approach

Homeland Security Presidential Directive 12 (HSPD-12) mandates a standard for a secure and reliable form of identification to be used by all Federal employees and contractors. Signed by President George W. Bush in August 2004, HSPD-12 initiated the development of a set of technical standards and issuance policies (Federal Information Processing Standard 201 [FIPS 201]) that create the Federal infrastructure required to deploy and support an identity credential that can be used and trusted across all Federal agencies for physical and logical access.

The federal government's standardization on PIV cards and infrastructure has produced numerous benefits for federal agencies and owners of critical infrastructure including:

1. Enhancing secure access to facilities and information systems
2. Streamlining access procedures to secure facilities for authorized personnel
3. Reducing the cost of PIV cards to be competitive with other MFA technologies

These same benefits are being leveraged by state and local organizations around the country. Cities like San Antonio, TX, and Victoria, TX have implemented multi-agency, multi-jurisdictional ICAM systems that have produced other benefits including a variety of operational efficiencies and cost savings.

For departments wanting to move to a standards-based MFA solution for Logical Access Control Systems (LACS) and enhance Physical Access Control Systems (PACS) to allow authorized First Responders access as operationally necessary, investment in PIV-I technology offers security, control, compliance, flexibility, and interoperability.

The federal government commits significant resources in vetting products and maintaining lists of compliant products and product combinations. The Approved Products List (APL)[1] provides federal agencies with products and services that have been approved for FICAM implementation based on rigorous security vulnerability and interoperability testing performed by the FIPS 201 Evaluation Program[2].

The Federal government's standardization around the policies, procedures, and technologies to build a trusted federal identity framework over the last 15 years has yielded irrefutable benefits. On May 21, 2019, the Executive Office of the President, Office of Management and Budget (OMB) issued OMB Memorandum M-19-17[3] updating the Federal Government's ICAM policy to expand guidance to support evolving technology requirements.

> HSPD-12 remains the Government-wide policy for the promulgation of standards-based, secure, and reliable forms of identification issued by the Federal Government to its employees, contractors, and other enterprise users. Additionally, Federal Information Processing Standard (FIPS) 201-2, Personal

[1] https://www.idmanagement.gov/approved-products-list/

[2] https://www.idmanagement.gov/fips201

[3] https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

> Identity Verification (PIV) of Federal Employees and Contractors (or successive version), remains the Government-wide standard for common identification, as called for by HSPD-12. In accordance with this standard, NIST guidelines, and Office of Personnel Management (OPM) requirements, a PIV credential is the aggregate output of the processes used for identity proofing, vetting, and authoritatively binding the identity of a human credential holder to an authenticator. However, as technology evolves, the Government must offer flexible solutions to meet changing technology needs and shift the focus from managing the lifecycle of credentials to the lifecycle of identities.

This memorandum emphasizes the importance of adhering to the established and proven PIV standard for common identification while also enhancing flexibility to adopt other compatible, standards-based solutions to support evolving technology requirements.

> **IV. Shifting the Operating Model beyond the Perimeter**
> The interwoven technical architecture of the Federal Government creates complexity in managing access to resources, safeguarding networks, and protecting information. While hardening the perimeter is important, agencies must shift from simply managing access inside and outside of the perimeter to using identity as the underpinning for managing the risk posed by attempts to access Federal resources made by users and information systems. To ignite adoption of this new mindset around ICAM capability deployment across the Federal Government, each agency must harmonize its enterprise-wide approach to governance, architecture, and acquisition.

As enterprises are becoming more mobile, IT and cybersecurity personnel must evaluate ICAM technologies that support physical, logical and mobile access. As these technologies converge, a regional plan should address the various requirements to include multiple platforms within an interoperable ICAM framework.

The architecture of mobile technologies differs from traditional Windows-based systems. And the smaller form factors of phones and tablets are not as conducive to utilizing an ID card to provide multi-factor authentication. Considering all of these factors along with recent federal guidance, below is a list of the best practices for moving towards a regional ICAM framework for public safety.

Identity

- Leverage the trusted identity vetting process of the FIPS 201-2 standard for common identification of all First Responders throughout the region

Credentialing

- Issue PIV-I cards to First Responders for physical and logical access
- Issue derived credentials for mobile access through systems which support the FIDO 2 standard on mobile devices

Access Management

- Install/upgrade federally-compliant PACS during new construction, building renovations and/or replacement of existing, end-of-life access control systems

- Integrate PIV-I to provide MFA for accessing logical systems
- Follow federal best practices guidance when implementing mobile systems which support standards and protocols to enable information sharing
    - Multi-Factor Authentication (MFA): Fast Identity Online (FIDO)
    - Single Sign-On: OAuth
    - Federation
        - Security Assertion Markup Language (SAML)
        - OpenID Connect

Financial Overview

Security vulnerabilities and regulatory changes are forcing public safety organizations to adopt MFA solutions. Many departments in the H-GAC region are actively procuring and/or testing MFA technologies. Investing in products that meet federal standards will enhance our region’s ability to move towards a truly interoperable ICAM framework.

Procurement: organizations can leverage federal and regional procurement vehicles currently in place for PIV-I solutions.

Funding: the region should explore grant opportunities to offset the costs of obtaining PIV-I credentials for First Responders and explore regional procurement opportunities for upgrading the necessary PACS and LACS to maximize the value of the PIV-I cards by expanding the physical and logical systems they can be used with.

Implementation Plan

Achieving a truly interoperable identity framework throughout the region will require a combination of individual department-level actions along with a variety of regionally coordinated planning, funding, and policy development activities.

Regional Coordination

Many public safety executives understand the operational necessity of sharing access to facilities and information with personnel from other organizations. Security vulnerabilities and regulatory changes are forcing departments to address some of these challenges. In order to securely share physical and logical access across organizations, they must be able to 1) trust identities of personnel from other organizations 2) issue credentials which can be shared across organizations, and 3) control what access is granted to who and when.

There is agreement by many public safety stakeholders in the H-GAC region on the value of a regional approach to ICAM, and numerous successful programs around the country provide evidence and lessons learned. Since there is no funding or mandate for this initiative, the choice to participate in a regional effort is up to each individual department/jurisdiction. As with any decision, the value to each organization of participating must outweigh the cost.

The establishment of a regional H-GAC ICAM Working Group can coordinate strategic planning efforts while suggesting tactical department and/or jurisdictional level activities. Below is a list of the types of strategic and tactical actions that should be addressed moving forward by organizations interested in participating in a regional ICAM initiative.

Strategic Planning Activities

1. Define regionally approved standards/protocols based on federal guidance and best practices
2. Develop common procurement language which can be utilized for all technology projects
3. Ensure all grant-funded projects adhere to the regional ICAM framework
4. Define the Vision and Goals for Regional Identity Sharing
    - Define **WHAT** information organizations want to share
    - Identify **WHO** organizations want to share with
    - Develop a regional framework for **HOW** organizations share identities and information

Chapter 3: Cloud Strategy

Chairperson: **Mike Bell**, Chief Technology Officer
Houston Police Department

Committee Members:

Jim McMillan, Director of Public Safety Technology
Harris County Universal Services

Colin Rizzo, Emergency Manager
Port of Houston Authority

Cloud Strategy Introduction

The job of the first responder is becoming increasingly dynamic, and they need quick and immediate access to resources and information to do their jobs. Public safety agencies migrating to the cloud can provide the necessary tools and mobile applications to their first responders in the field to do their jobs better, and more importantly, safer. Tangible, meaningful and reliable data and information is critical in the field.

This publication is a primer about key concepts public agencies need to know about cloud computing and creating a regional mobility strategy. Cloud computing makes it possible for first responders to use mobile devices (e.g. smartphones and tablets) to perform typical desktop functions.

At a simple and very basic level, the cloud is the ability to access software via the internet from a desktop or mobile device or from somewhere inside an agency's network. The software is "on" the cloud versus the local device. Since the software is available and being managed, whether it's third-party software or in-house custom developed web-services, it is essentially being managed by the provider and the end-user or first responder does not have to worry about it. Third-party cloud-based software and mobile apps are generally available by subscription or pay-as-you-go.

The capabilities of cloud computing are constantly evolving. The official definition for cloud computing, according to the U.S. Department of Commerce, National Institute of Standards and Technology (NIST) is as follows, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.[4]"

In addition, the NIST definition introduces the supporting concepts of three cloud service models, five essential characteristics, and four types of cloud deployments. In total, the NIST Cloud Computing Definition is composed of 14 interrelated terms and their associated definitions:

Core definition of the cloud computing model

Five essential characteristics

- **On-demand self-service**
- **Broad network access**
- **Resource pooling**
- **Rapid elasticity**
- **Measured service**

Three service models

- **Software as a Service (SaaS)**
- **Platform as a Service (PaaS)**
- **Infrastructure as a Service (IaaS)**

Four deployment models

- **Public**
- **Private**
- **Community**
- **Hybrid"**

[4] https://www.nist.gov/news-events/news/2011/10/final-version-nist-cloud-computing-definition-published

There are also unique types of public cloud data storage offerings including shared servers and storage, dedicated storage and dedicated servers and storage.

Benefits. Public safety agencies, whether law enforcement, the fire service, EMS, 911 telecommunications or emergency management and allied emergency responders can leverage cloud computing benefits to streamline agency administrative business processes (e.g. eScheduling) and tactical operations (e.g. mapping tools to maximize situational awareness and readiness).

Value. Many public safety agencies are migrating to the cloud because they see the value in easy and quick electronic access to pertinent information whether from a desktop computer or mobile device. Being able to access a report within a matter of seconds when a first responder is in the field saves agencies time and resources, which translates to a financial return on investment. In addition to long-term cost savings, cloud computing gives first responders nearly immediate access to critical information, which may help save a life (e.g. ability to access a CPR mobile app). Cloud solutions offer greater scalability and simpler integration with external data sources than legacy systems.

Success story. Law enforcement, fire, EMS, 911 telecommunications and emergency management professionals see the value in migrating to the cloud for a variety of new capabilities not otherwise possible with legacy Information Technology (IT) systems. For example, mobile apps for CPR administration are available to first responders and the general public. In April 2018, an off-duty paramedic alerted by a mobile app saved a nearby woman who collapsed. The mobile app issued an alert that someone needed CPR. Any user who is trained in CPR and wishes to receive these alerts will receive them through an alert notification.[5]

Not only do mobile apps help first responders, they also help the citizens they serve. In December 2018, a minor believed he was about to be kidnapped by an alleged child molester and used a panic alert app that users can simply push to gain immediate contact with emergency services agencies and provide location information.

This report should be used to ignite interagency discussions about how public safety agencies can work together to develop a regional mobility strategy for information sharing.

Traditional Enterprise IT Limitations

Public safety agencies realize that technology is evolving. The public's expectations, skewed partially by television, movies and video games, is that public safety agencies have immediate access to information about a suspect, a crime scene or event across regional, state and international boundaries. Agencies that are not leveraging the cloud and mobile apps face myriad challenges, including but not limited to:

1. Inability to access records and data from mobile devices in the field.

[5] https://www.ems1.com/ems-products/cpr-resuscitation/articles/379534048-Off-duty-paramedic-alerted-by-app-saves-nearby-woman-who-collapsed/

2. Inability to dictate and submit field incident reports.
3. Inability to determine available resources (e.g. special K9).
4. Inability to track emergency response personnel when outside of a vehicle.
5. Decreased on-scene situational awareness.
6. Coordination of resources across multiple agencies/jurisdictions

Each of the six points above can arguably be lifesaving. For example, the first point discusses the need for immediate access to records. When an officer makes a traffic stop, he or she must run the individual's driver's license data through its state's criminal justice information system and the FBI's National Crime Information Center to see if the person has any active wants or warrants and poses a threat to the officer's or general public's safety. Several scenarios can be provided for each of the six points above for each public safety discipline. The takeaway is that public safety agencies need to provide first responders access to mobile apps while in the field to improve operational efficiency.

Traditional network architectures are often significantly more expensive than cloud-based systems which offer higher throughput through commercial broadband networks. Many public safety agencies rely on private Wide Area Networks (WAN) to connect data centers, facilities, and their Internet Service Provider (ISP) using infrastructure such as dedicated T1 lines and Multiprotocol Label Switching (MPLS). Private WANs can cost 20-100 times more than commercial internet service. While these dedicated connections offer a high level of security, they are expensive and typically provide lower speeds than commercial internet. They also run the risk of being cut during things like road construction projects, so departments typically pay for redundant paths to not lose service in the event the primary connection goes down. This adds significantly to the costs of building and maintaining these networks. Cloud systems which utilize the Internet are able to intelligently route network traffic with higher speeds and reliability at lower cost.

Cloud-based systems are built on different architectures than legacy systems which were designed generally for use on private networks. The client-server model splits the workload between the client machine and the server requiring a constant connection between the computer and the server. This workload split requires sufficient bandwidth to support processing activities happening on both ends. Cloud systems are designed to centralize the majority of the computing tasks in the cloud with small packets of information being pushed to the client device.

The rapid adoption of reliable, mobile broadband networks is furthering the value that cloud-based solutions can offer public safety. Traditional enterprise systems require Virtual Private Networks (VPNs) to remotely connect to agency-hosted systems. VPNs create a secure "tunnel" between the remote user and the server. These tunnels consume a portion of available bandwidth to separate the data passed through them from other data moving across the public network. Because VPN tunnels utilize a portion of available bandwidth, some legacy applications can be rendered unusable without enough bandwidth between the user and the system being accessed. Hard wired networks typically offer higher data throughput speeds and capacity than wireless networks, so the end user experience utilizing VPNs is less likely to be compromised on a wired network. Due to differences in architecture, cloud-based systems generally offer better performance on mobile platforms because of the more efficient use of bandwidth, even when VPNs are required for security. This is an important consideration for adopting cloud-based systems to support mobile deployments when availability of bandwidth can fluctuate significantly.

Improving Operations

As a result of the unique circumstances of the Harris County LTE program, many agencies in the Houston-Galveston area have experienced the benefit of leveraging cloud-based mobile apps to improve operational effectiveness. The first major operational deployment of regional mobile apps was during Super Bowl LI in 2017 in which ten city, county, state and federal agencies across multiple jurisdictions were able to seamlessly share information and significantly reduce response times. The success of this event not only demonstrated the value of cloud-hosted mobile apps to augment voice radio communications, but it also demonstrated the importance of regional collaboration in the planning, selection and deployment of these technologies.

Increased mobility. First responders that use mobile devices and secure, eligible mobile apps in the field have countless opportunities to improve their response strategy. Mobile apps give first responders the opportunity to communicate with one another using secure messaging apps, the ability to track personnel during an incident, the ability to access records and data to get critical information, and they can get improved on-scene situational awareness. This is a small fraction of the types of mobile apps available to first responders. The ability to be mobile, and not dependent on data accessible only on a computer in an office or a vehicle, is important for the first responder while on-scene during an incident or a detail assignment (e.g. a special event). The ability to access critical information or even submit field incident reports via a mobile device saves time, money and resources. Mobile first responders are able to continue their work in the field without being tied to a vehicle.

Interoperability defined. Interoperability is a technology and communications function and a philosophy. In a testimony by Derek Orr, a Program Manager for Public Safety Communications Research in the Office of Law Enforcement Standards (OLES) at the National Institute of Standards and Technology (NIST), he stated that, “Interoperability for public safety communications is defined as "the ability to share information via voice and data signals on demand, in real time, when needed, and as authorized."[6]

The *International Public Safety Association’s Interoperability and Unified Command InfoBrief* describes interoperability more theoretically “as a continuous and end-state process. It is a continuous process because the ability of agencies to rapidly and effectively integrate during a crisis depends upon the degree to which those agencies have previously worked together to develop joint response protocols, policy and procedures and training. If agency executives and command leadership fail to adopt interoperability as a continuous process philosophy, the desired end-state cannot occur.”[7]

Increased interoperability. Post 9/11, agencies from around the United States realized the importance of interoperability across agencies and jurisdictional boundaries. Several data centers were stood up and traditional enterprise IT strategies were adopted. And while interoperability improved, challenges remained. Agencies that employ a regional mobility strategy for sharing information are performing a great service to their community and their first responders. A regional mobility strategy will improve interoperability between agencies and first responders on-scene because they have quick access to

[6] https://www.nist.gov/speech-testimony/interoperability-public-safety-communications-equipment

[7] https://www.joinipsa.org/Publications International Public Safety Association Interoperability and Unified Command InfoBrief. April 2018.

information at their fingertips. They can get immediate access to mission critical information and share it among each other.

Mobile Apps

Public safety mobile apps allow first responders to harness their operational productivity through the ability to access tools and resources while in the field and on scene. Officers, firefighters and EMS professionals are using mobile apps daily. However, their use of mobile apps is not necessarily promoting interoperability.

Integrating multiple systems across multiple agencies and developing a regional mobility strategy is how to establish interoperability. Disparate use of mobile apps among first responders in the field does not yield interoperability.

Below are just a few examples of the types of mobile apps that first responders are using to improve their duty functions while on scene.

- Law enforcement
    - Narcotic detection
    - eCitations
    - Spanish for police
    - Messengers/communications/chat
    - GIS Mapping
- Fire service
    - CPR apps
    - Fire flow/pump pressure calculator
    - Rescue knots
    - Hazmat guidebook (index of dangerous items)
    - Fire crew trackers
- EMS
    - Dopamine eCalculator
    - Medical Spanish
    - AED locator
    - Emergency radio
    - Hospital locator
- 911 telecommunicators
    - Caller locator
    - Spanish for police, fire, EMS
    - CPR apps
    - AED locator
    - Hospital locator

The above list is a small fraction of available mobile apps. Public safety agencies also have the opportunity to create customized apps for their region.

Public safety agencies need to establish policies for first responders about which mobile apps they can use securely for operational purposes. Reminding first responders that just because they can access an app and download it to their mobile device, does not mean that it is secure or compliant with agency policy. Accessing apps that are unsecure poses several unique threats that first responders may not be aware of.

In addition to identifying eligible mobile apps, public safety agencies need to determine what functionality they need in their apps to ensure continuity of operations. Below is a list of some mobile app functions that agencies should include in their requirements.

- Search features
- Ability to work off-line
- Location tracking
- Alerts
- Simple interface/design
- High performance
- Security
- Integration / Extensibility
- Interoperability

Public safety agencies need to discuss and document which mobile app functions are critical to their operations and which app functions are nice-to-have.

When developing a regional mobility strategy, public safety agencies need to prioritize which mobile apps they will initially test and, ultimately, adopt and which mobile apps they will pilot in the future. This phased deployment approach will yield lessons learned and the opportunity to apply those lessons for future mobile app rollouts. Further, a phased approach is a cost-effective way to manage a regional mobility initiative. Leveraging regional volume discounts offers an additional means of offsetting the burden of cost for adopting mobile technologies.

Benefits

There are several operational, administrative, technical and financial benefits of multi-agency information sharing from cloud-based systems that cross agency boundaries that would be extremely difficult, if not impossible, with proprietary systems behind enterprise firewalls.

A regional mobility strategy with multiple agencies using the same cloud-based information, is argued to be more cost-effective than if each participating agency purchased a separate system (hardware, software, infrastructure). In addition to the costs associated with the initial purchase of separate systems, using a single cloud service provider will minimize separate, on-going maintenance costs.

Adopting a regional cloud-based mobility strategy will improve data sharing, and first responders in the field will have access to information they would not have in a traditional enterprise IT framework. Access to this data in real-time means improved safety and the ability to be truly interoperable across multiple agencies.

Multiple agency data sharing also improves regional data analytics. Analyzing regional data will help agency command staff and leadership understand and learn trends and subsequently how to effectively allocate resources in the field.

Numerous agencies in the Houston-Galveston area have benefited from unprecedented multi-agency information sharing via cloud-hosted mobile apps. During Hurricane Harvey, Harris County Constable Precinct 5 was able to copy call for service information from the county's Computer Aided Dispatch system (CAD) into a mobile app to dispatch Houston Police Department (HPD) resources for high-water rescue operations. Another success story is the adoption of a collaboration app for security operations at the Houston Ship Channel which has revolutionized communications between the US Coast Guard (USCG), Harris County Sheriff's Office (HCSO) and HPD among other agencies. This mobile app has provided statistically significant operational results for things like apprehending security zone violators, responding to various hazards along the ship channel, and search and rescue (SAR) operations.

FedRAMP: A Government Cloud Model

The Federal Risk and Authorization Management Program (FedRAMP) is a program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services for the US federal government.

According to the FedRAMP Policy Memo dated December 18, 2011, "Cloud computing offers a unique opportunity for the Federal Government to take advantage of cutting-edge information technologies to dramatically reduce procurement and operating costs and greatly increase the efficiency and effectiveness of services provided to its citizens. Consistent with the President's International Strategy for Cyberspace and Cloud First policy, the adoption and use of information systems operated by cloud service providers (cloud services) by the Federal Government depends on security, interoperability, portability, reliability, and resiliency"[8].

"FedRAMP enables Agencies to rapidly adapt from old, insecure legacy IT to mission-enabling, secure, and cost-effective cloud-based IT.

FedRAMP created and manages a core set of processes to ensure effective, repeatable cloud security for the government. FedRAMP established a mature marketplace to increase utilization and familiarity with cloud services while facilitating collaboration across government through open exchanges of lessons learned, use cases, and tactical solutions"[9].

FedRAMPs Goals:

- Accelerate the adoption of secure cloud solutions through reuse of assessments and authorizations
- Improve confidence in the security of cloud solutions and security assessments
- Achieve consistent security authorizations using a baseline set of agreed-upon standards for cloud product approval in or outside of FedRAMP
- Ensure consistent application of existing security practices
- Increase automation and near real-time data for continuous monitoring

[8] https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf
[9] https://www.fedramp.gov/

FedRamp supports 100+ federal agencies with > 5 million assets with 1/3 of the world's internet traffic going through the program. Participating agencies re-use authorizations an average of 6x yielding $130 million in cost avoidance[10].

FedRAMP is a highly successful program which not only offers countless use cases for successful adoption of cloud technologies, but also a framework for developing consistent, repeatable standards and security practices for cloud-based IT adoption across multiple departments. The FedRAMP model of "do once, use/reuse many times" has proven to be highly effective in increasing scalability and reducing costs.

Next Steps: Regional Mobility Strategy

Unlike federal agencies who must comply with the directive of the single US Chief Information Officer (CIO) in the Executive Office of the President, state and local departments support autonomous jurisdictions with their own executives, CIOs and IT departments. Public safety regional-level initiatives require buy-in from multiple stakeholders from city management, county officials, local officials and even state and possibly federal agencies depending on the type of data that is going to be managed, shared, accessed and stored. Additionally, existing IT investments, IT staff and budgets vary widely across departments and jurisdictions. These factors must all be taken into account when developing a viable regional mobility plan.

Cloud-based technologies offer unique opportunities for public safety data interoperability and information sharing, so a cloud strategy should be a key component for a regional mobility plan. At a high-level, there are several general cloud considerations that public safety agencies need to think about including increased data access, increased security and disaster recovery. While the cloud allows for business process improvement and public safety operational efficiency, there are factors to consider for achieving safe, secure and scalable cloud adoption.

Governance. A governance structure will need to be established that includes leadership from each participating entity, IT personnel from the CIO to systems analysts and developers, as well as end-users (first responders). The governing body is charged with developing policies, procedures and is responsible for rolling out timely training about the documented policies and procedures. The governing body will determine the use cases where cloud is acceptable and who governs each respective policy. The governing body will also need to discuss the following:

- Freedom of Information Act (FOIA) and Public Records Requests (PRR)
- Benefits and Risks Assessment
    - Define use cases
    - Identify risks/benefits per use case
    - Decide which use cases are primary candidates for cloud
- Information sharing
    - Policies
    - Procedures
- Product Selection

[10] https://www.fedramp.gov/about/

  - Defined standards
  - Cybersecurity requirements
- Hosting models
  - Bigger agencies becoming hosts
- Connectivity methods
  - VPN Over Internet
  - Certificate based
  - Point to point connections
- Support models
- Compliance
  - FBI CJIS
  - HIPAA
- Cost-Sharing
- Minimum participation levels
- Onboarding/Offboarding requirements of participants/organizations

Regional cloud computing initiatives will require a review of legislation, possible legislative changes, and interagency agreements between all parties. After these policy issues are agreed upon then the benefits will be realized. The benefits include interoperability, cost savings, data quality improvement and the ability to communicate effectively across disciplines and jurisdictional boundaries when disaster strikes.

There will be challenges that regional cloud computing initiatives will encounter. These challenges include budgeting, data management, data ownership, data security, permissions/roles among hundreds of end-users and on-going training about policies and procedures as enhancements are made.

Budgeting. "When an agency makes a capital investment in infrastructure and fixed storage capacity, it can often involve guesswork about how the resources will be used and how much infrastructure capacity is needed. With cloud computing, you don't have to make an upfront investment in capacity you might not use; you pay only when you consume computing resources and based on how much you consume. If an agency needs more data storage and computing power, cloud computing allows you to scale up and down as required, with only a few minute's notice."[11]

The financial impacts to public safety agencies at the onset may seem excessive if the agency needs to purchase new equipment to fully maximize its return on using the cloud. Public safety agencies will need to adequately budget for the upfront costs associated with a cloud migration strategy. Agencies will also need to plan on the continued operating costs of subscription based mobile app services and compatible mobile devices.

Public safety agencies must factor in the financial impacts migrating to the cloud will have, and many are resistant to change because they perceive that everything is working fine. While this may be somewhat true, settling for fine is not necessarily the best operational decision when it comes to supporting first responders in the field and preserving their safety.

[11] https://www.policeone.com/police-products/software/Data-Information-Sharing-Software/articles/478121006-How-the-cloud-helps-police-agencies-manage-data-costs/

Data management. With multiple agencies, and third parties, contributing different data elements at different points throughout the lifecycle of an incident, data management is an important issue. Management includes sending the data to a repository (such as a cloud server) where it can be accessed by applications, appending relevant metadata such as timestamps and device source, and ensuring the data are properly formatted. Agencies may also need to consider situations where both agencies are contributing their own streams of the same type of data.

Many agencies have existing data sharing agreements in place for regional and/or departmental enterprise systems. Cloud-hosted systems, particularly those managed by third parties, create new opportunities for information sharing which may require existing agreements to be modified. Entirely new mobility agreements may be necessary for certain products and/or types of information sharing.

Data ownership. For each data element, the data sharing agreement specifies which entity (an agency which is a party to the agreement, another government agency, the building owner, individual residents, etc.) has ownership, and whether any circumstances (such as sharing the data with other parties) affects data ownership. The agencies define rules for retaining or sharing ownership of data generated before, during, and after the incident. For example, agencies may collaborate before the incident to populate the situational awareness dashboard with static information, such as the locations of building hazards, water mains, and other utilities. Some of these data may derive from other city agencies or private businesses, and are thus owned by third parties, whereas the agencies may claim sole or shared ownership of data they collectively generate specifically for fire response planning. They may choose to claim joint ownership of certain data elements, while other data elements are owned by whichever agency creates them.

Data security practices. According to the NIST Cybersecurity Framework, the agreement specifies physical and logical security procedures required by all agencies in order to participate in data sharing. The agencies have agreed to certain cybersecurity practices for both stationary and mobile communication devices, such as installing anti-virus software, requiring two-factor authentication for mobile devices at least once per 24-hour period, monthly security audits, and identity management requirements such as revocation of user access in a timely manner.[12] They also specify how physical access to IT infrastructure, including incident command posts, is controlled.

Data retention. Most agencies have data retention policies for legacy IT systems. They likely also have agreements in place for sharing certain types of information or querying systems like criminal history databases. Cloud-based systems offer much more diverse forms of information sharing, so policies for data retention become more complex when sharing information outside of individual departments. Agencies should evaluate whether each data element will only be shared during an incident or will be stored after the incident. Streaming data with no long-term storage has the benefit of avoiding storage costs, security risks and associated legal liabilities. However, some data may need to be retained (e.g. to create forensic records) or may be useful for research and training purposes. In some cases, there may also be a legal requirement to retain

[12] https://www.nist.gov/cyberframework.

data (e.g. video from body-worn cameras).[13] Agencies should consider that data may be stored temporarily, even if it is not explicitly stored in a long-term repository (e.g. browser caching, server transmission), which may still carry legal and security liabilities. Agencies may wish to establish procedures for verifying how long data are stored and that data have been deleted.

For example, the Consumer Reports Digital Standard[14] provides a comprehensive list of elements which consumers can evaluate for a given digital device, including data security, encryption, manufacturer security policies, product support lifecycle, user data control, data retention and deletion, data shared with third parties, data ownership, and many other aspects. For each element, the Digital Standard includes criteria for defining the requirement and indicators and evaluation procedures for recognizing whether the product meets the requirement. For example, regarding third party data use, the criterion states that the vendor discloses every way in which user data is used, indicators include explicit disclosures of the identities of any third parties with which the vendor shares user data, and evaluation procedures include analyzing public information released by the company or network traffic to identify third party domains contacted by the product. While it would be difficult or impossible for an individual consumer to interrogate every one of these elements for a product, public safety agencies could negotiate with potential vendors about these features and include specifications and disclosures in RFPs. Programs such as the Department of Homeland Security's (DHS) Software Assurance Marketplace (SWAMP) program offer no cost security vulnerability assessments for public safety products to evaluate many of the items described above.

Performance. By design, the cloud network is highly flexible, but there are some necessary items to measure and test when it comes to cloud computing performance. In general, performance problems typically revolve around speed, response time, load time and poor scalability. Public safety agencies will have to undergo different types of performance testing to ensure expectations are met. This might include load testing, stress testing, endurance testing, spike testing, volume testing and scalability testing.

FBI CJIS compliance. Law enforcement data is often regarded as sensitive information and agencies have unique data management requirements governed by the FBI's Criminal Justice Information Services Division (CJIS). Law enforcement agencies, rural and large, are required to protect sensitive and encrypted data for storage and transmission in a CJIS-secure environment. They also must continually monitor the environment to prevent security threats. Law enforcement agencies should only consider a cloud service provider with a CJIS-secure environment to alleviate burden on the agency's IT department. There are several well-known cloud hosting providers that are CJIS compliant. Each department should also ensure that users accessing Criminal Justice Information (CJI) on mobile devices adhere to the guidelines in the CJIS Mobile Appendix.[15]

[13] Brennan Center for Justice, Collection of policies on retention and release of police body-worn camera video, July 8, 2016. https://www.brennancenter.org/sites/default/files/Retention_and_Release.pdf.

[14] Consumer Reports, "The Digital Standard," 2018. Detailed indicators and procedures are provided in individual Github files. https://www.thedigitalstandard.org.

[15] https://www.fbi.gov/file-repository/cjis-mobile-mobile-appendix-20121214.pdf/view

HIPAA compliance. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is United States legislation that provides data privacy and security provisions for safeguarding medical information. A HIPAA covered entity can use a cloud service to store or process electronic protected health information (ePHI). The United States Department of Health and Human Services provides public safety agencies guidance on security, privacy and breach notifications.[16]

Security. Cloud security is a shared responsibility between the public safety agency and the cloud service provider. According to NIST, "Organizations should be aware of the security issues that exist in cloud computing and of applicable NIST publications such as NIST Special Publication (SP) 800-53 'Recommended Security Controls for Federal Information Systems and Organizations.' As complex networked systems, clouds are affected by traditional computer and network security issues such as the needs to provide data confidentiality, data integrity, and system availability. By imposing uniform management practices, clouds may be able to improve on some security update and response issues. Clouds, however, also have potential to aggregate an unprecedented quantity and variety of customer data in cloud data centers. This potential vulnerability requires a high degree of confidence and transparency that cloud providers can keep customer data isolated and protected. Also, cloud users and administrators rely heavily on Web browsers, so browser security failures can lead to cloud security breaches. The privacy and security of cloud computing depends primarily on whether the cloud service provider has implemented robust security controls and a sound privacy policy desired by their customers, the visibility that customers have into its performance, and how well it is managed."[17]

An article by McAfee outlined an easy-to-read bullet list of common types of security threats for SaaS, IaaS and private cloud[18]. Note that this is not a comprehensive list of security issues.

SaaS

1. "Lack of visibility into what data is within cloud applications.
2. Theft of data from a cloud application by malicious actor.
3. Incomplete control over who can access sensitive data.
4. Inability to monitor data in transit to and from cloud applications.
5. Cloud applications being provisioned outside of IT visibility (e.g., shadow IT).
6. Lack of staff with the skills to manage security for cloud applications.
7. Inability to prevent malicious insider theft or misuse of data.
8. Advanced threats and attacks against the cloud application provider.
9. Inability to assess the security of the cloud application provider's operations.
10. Inability to maintain regulatory compliance.

IaaS

1. Cloud workloads and accounts being created outside of IT visibility (e.g., shadow IT).
2. Incomplete control over who can access sensitive data.
3. Theft of data hosted in cloud infrastructure by malicious actor.

[16] https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html
[17] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf
[18] https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/security-issues-in-cloud-computing.html

4. Lack of staff with the skills to secure cloud infrastructure.
5. Lack of visibility into what data is in the cloud.
6. Inability to prevent malicious insider theft or misuse of data.
7. Lack of consistent security controls over multi-cloud and on-premises environments.
8. Advanced threats and attacks against cloud infrastructure.
9. Inability to monitor cloud workload systems and applications for vulnerabilities.
10. Lateral spread of an attack from one cloud workload to another.

Private cloud

1. Lack of consistent security controls spanning over traditional server and virtualized private cloud infrastructures.
2. Increasing complexity of infrastructure resulting in more time/effort for implementation and maintenance.
3. Lack of staff with skills to manage security for a software-defined data center (e.g., virtual compute, network, storage).
4. Incomplete visibility over security for a software-defined data center (e.g., virtual compute, network, storage).
5. Advanced threats and attacks."

Whether a public safety agency is using hard copy or electronic copy for data sharing, security is a key factor when it comes to deciding where to store that information, how it can be retrieved and who has permission to view it. There are unique challenges when it comes to cloud computing security and it is important for public safety agencies to discuss and document business requirements.

Vulnerabilities. Like every piece of technology, equipment and operation, there are vulnerabilities. Cloud computing has some unique weaknesses that don't exist in traditional IT data centers. Below are some examples that were highlighted in an article from Carnegie Mellon University's Software Engineering Institute.[19]

1. A reduction of the agency's visibility and control.
2. On-demand self-service simplifies unauthorized use (e.g. an officer using a mobile app on the department's network without IT consent).
3. Internet-accessible management application programming interfaces (APIs) can be compromised.
4. Data deletion is difficult to verify.

In addition to the above vulnerabilities that are unique to cloud computing, below are additional areas of weakness that occur in both the cloud and traditional IT centers that public safety agencies need to address.

1. "Credentials are stolen.

[19] https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html

2. Vendor lock-in complicates migrating to other cloud service providers.
3. Increased complexity strains IT staff.
4. Insiders abuse authorized access.
5. Stored data is lost.
6. CSP supply chain is compromised.
7. Insufficient Due Diligence Increases Cybersecurity Risk."[20]

Disaster recovery. Public safety agencies need to develop a cloud disaster recovery (cloud DR) plan. When systems go down, technology fails and first responders are unable to access information they're dependent on or unable to communicate with one another, the environment can quickly become unstable and put lives at risk. It is critical to have a cloud DR strategy in place for continuity of operations and to include it in the agency's operating budget. The cloud DR plan needs to include input from end-users, agency executives and IT. To get started, agencies need to perform at a minimum, a business impact analysis, a risk assessment, a risk management strategy and then configure and test the cloud DR configuration.

Cloud Deployment Models

There are different cloud deployment models available, and public safety agencies will need to select which type of model is best for its current and future regional mobility strategy.

According to NIST, "in SP 800-145, cloud deployment models describe how the cloud is operated and who has access to the cloud service resources. The four deployment models are defined in SP 800-145 as follows:

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organization comprising multiple cloud service consumers (CSCs) (e.g., business units, end-users). It may be owned, managed, and operated by the organization, a third party, or some combination of them, and it may exist on or off premises.

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of CSCs from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off premises.

Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound

[20] https://insights.sei.cmu.edu/sei_blog/2018/03/12-risks-threats-vulnerabilities-in-moving-to-the-cloud.html

together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)."[21]

The Evaluation of Cloud Computing Services Based on NIST SP 800-145 (NIST SP 500-322) report provides additional information about the details of the various cloud deployment models.

Public safety agencies will need to discuss the four above cloud deployment models with key stakeholders from the organizations participating in the regional mobility strategy. Using the model that meets the regional mobility strategy's functional and technical requirements will enhance interoperability between multi-agency first responders.

Cloud Service Providers

There are several cloud service providers (CSPs) available in today's market. Selecting the most commonly known CSP is not always the best choice for an agency's business and operational needs. Given this, public safety agencies must do their due diligence before signing a contract with a CSP. This typically starts with the agency documenting its internal business requirements. As the region is seeking to develop a cloud strategy as a part of the regional mobility plan, the business requirements need to include input from participating agencies that will leverage the cloud services. This leading practice, of documenting business requirements, will help ensure that the CSP the region selects is the CSP it needs.

In the above section, general cloud considerations were highlighted. While not an exhaustive list of CSP considerations, important factors such as FBI CJIS[22] and HIPAA compliance, need to be included in the decision-making of a CSP and documented in the business requirements. Further, public safety agencies should make sure that the CSP meets NIST guidelines for managing security and privacy (NIST guidelines[23]). In addition, public safety agencies will want to weigh the CSP's performance, compliance, accessibility and operational impact.

Public safety agencies should review the Evaluation of Cloud Computing Services Based on NIST SP 800-145 (NIST SP 500-322). Below is an important caption that debunks common marketing tactics and provides clarity about how to identify actual cloud services:[24]

> *"In the absence of clarification, organizations are at risk of adopting "services" that do not provide characteristics of cloud computing. For example, some vendors reportedly decide to label their computing offerings as "cloud services," even if the offerings do not support the essential characteristics of a cloud service in the NIST definition.*

[21] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-322.pdf (page 12)

[22] https://www.fbi.gov/file-repository/cjis-cloud-computing-report_20121214.pdf/view

[23] https://www.nist.gov/news-events/news/2012/01/nist-issues-cloud-computing-guidelines-managing-security-and-privac

[24] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-322.pdf

Furthermore, the frequent and common usage of the informal "aaS" (as a Service) suffix in marketing, as in "EaaS" (Enterprise as a Service), "DaaS"(Desktop as a Service or Data as a Service), "STaaS" (Storage as a Service, and even "XaaS" (Everything as a Service) is confusing, and (unintentionally) obfuscating the architecturally well-founded distinction of Software as a Service (SaaS), Platform as a Service, (PaaS), and Infrastructure as a Service (IaaS). These "cloud service types" are generally coined by appending the suffix "aaS" after a type of computing capability or marketing term. This makes it difficult to determine whether something is a cloud service and has unintended consequence for organizations trying to satisfy their cloud-first objectives.

To demystify the ambiguity surrounding cloud services, the NIST Cloud Computing Services Public Working Group analyzed the NIST cloud computing definition and developed guidance on how to use it to evaluate cloud services.

This document clarifies the cloud computing service models as published in NIST Special Publication (SP) 800-145, The NIST Definition of Cloud Computing. [2] The NIST Definition was intended for the stated purpose of "broad comparisons of cloud services and deployment strategies, and to provide a baseline for discussion from what is cloud computing to how to best use cloud computing."

The clarification supports the proper planning for cloud migration, deployment, and retirement of relevant legacy systems. The Government Accountability Office (GAO) recommended in [3] July 2012 that seven audited federal agencies should establish estimated costs, performance goals, and plans to retire associated legacy systems for each type of cloud-based service as well as the same for retiring legacy systems, as applicable, for planned additional cloud-based services."

Below are selected authoritative resources that public safety agencies need to review and become familiar with before selecting a cloud service provider. This is not a comprehensive list.

- The NIST Definition of Cloud Computing[25]
- Evaluation of Cloud Computing Services Based on NIST SP 800-145 (NIST SP 500-322)[26]
- NIST Cloud Computing Reference Architecture (SP 500-292)[27]
- FedRamp[28]
- FBI CJIS: Recommendations for Implementation of Cloud Computing Solutions[29]
- HHS: Guidance on HIPAA & Cloud Computing[30]

[25] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
[26] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.500-322.pdf
[27] https://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_SP_500-292_-_090611.pdf
[28] https://www.fedramp.gov/documents/
[29] https://www.fbi.gov/file-repository/cjis-cloud-computing-report_20121214.pdf
[30] https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

Chapter 4: Device Management

Chairperson: **Colin Rizzo**, Emergency Manager
Port of Houston Authority

Committee Members:

Brian Cantrell, Emergency Management Coordinator
Waller County

Chris Collier, Emergency Service and Response Manager
Southeast Texas Regional Advisory Council (SETRAC)

Sam Miller, Field Services Manager
Texas Division of Emergency Management

Executive Summary

As the public safety community adopts mobile broadband, departments are already beginning to purchase larger quantities of department issued cell phones. Some departments are issuing phones to individual users, while others are deploying caches of shared phones due to the cost constraints of providing all users individually assigned phones.

As in the early days of Personal Computers (PC), cell phones are currently designed predominantly around individual, consumer use. The tools and processes for provisioning and managing mobile phones are fundamentally different than those employed for other mobile assets such as laptop computers and radios. Information Technology (IT) and Communications personnel will need to employ new tools for deploying and managing large quantities of phones - whether individually issued or shared across personnel. The implications of these new technologies and methods should be considered by department executives when making decisions about the pace and scale of mobility adoption.

Smartphone Management Compared to Other Mobile Assets

Most enterprises today, particularly in government and public safety, deploy laptops and Mobile Data Terminals (MDTs) running the Operating System (OS) Microsoft Windows. Over the decades, Windows has evolved beyond supporting local hardware on a PC to supporting complex networked computers that allow the sharing of hardware with users across the enterprise. This evolution has been enabled by the deployment of a full ecosystem of tools that centralize user management, control access to hardware and information inside secure networks, and support the migration and/or replication of data from local storage on a PC to networked infrastructure accessible from most enterprise-connected devices.

IT departments build images with the necessary software packages, network settings, security tools and other customizations required by the organization. They use automation tools to quickly load the pre-configured image onto new PCs/laptops. Most updates are then pushed remotely over the network without manual configuration by a desktop support technician. User profiles and information are managed at the enterprise level, so an individual's credentials can be used on just about any networked PC in the organization to access their personal files.

Radios are programmed in a similar manner. Templates are built with designated channels and hardware settings which are then easily installed on large quantities of radios using automation tools. Unlike PCs and phones, radios do not require unique user credentials. Users have access to the channels programmed onto the radio. For deployments of shared/cached radios, channels are pre-configured into the radios. Often, instructions are provided to users for which channels to use for which type of communication or group to communicate with.

Mobile platforms such as smartphones and tablets are a relatively new technology and still in the early stages of maturity. While there are a number of hardware manufacturers, the mobile device market is dominated by two OS platforms: iOS and Android. Early use of mobile devices was predominantly personal. Private industry began operationalizing mobility technologies shortly after the launch of the Smartphone. And over the last decade, tools for automation and remote security have evolved. But the overall market is still rather immature for enterprise deployments, particularly for shared devices.

Project Overview

The public sector in general, and especially the public safety vertical, have only recently begun to operationalize these mobile technologies. This adoption is being fueled by the availability of reliable, mobile broadband networks. There are three models for enterprise mobile device deployments:

1. Individually issued devices funded and managed by the organization
2. Cache devices funded and managed by the organization and shared across users
3. Bring Your Own Device (BYOD) in which organizations allow personnel to use their personal device for work purposes which may or may not include some sort of stipend

Most organizations have systems and procedures in place for managing individually issued department devices. The BYOD model relies on department policies but leaves device acquisition, provisioning, and management to individual users with little or no burden on department resources. This assessment focuses on the management of shared devices. The shared device model offers reduced financial burden from individually issuing devices and improved security over BYOD; however, it brings with it the most challenges and complexities.

One objective of the Mobility Acceleration Coalition (MAC) is to explore methods for streamlining the management of device caches to enhance scalability for the public safety industry. The MAC sought to evaluate existing technologies and procedures, identify gaps and document current best practices in order to:

1. Provide feedback to industry partners to build and/or enhance tools available to automate shared device management and enhance the affordability and scalability for public safety
2. Document lessons learned from tools and processes tested to help public safety agencies accelerate mobility adoption

The lessons learned in this report were derived from a combination of:

1. Multiple shared device deployments for pre-planned events
2. Interviews with other departments managing large caches of phones
3. A tabletop exercise to compare tools and procedures

Device Provisioning

In order for phones to be useful, they must be provisioned with the necessary apps and settings. This is true whether the use is personal or business. For personal use, users must install their apps of choice for messaging, shopping, social media, banking, games, photo editing and a whole host of other uses. This process has evolved in recent years with cloud-based back-ups which allow for automating many of the previously manual tasks associated with configuring a new phone.

The technology is continuing to evolve for the management of mobile devices used for business purposes. Provisioning phones includes 1) configuring device settings 2) installing applications and 3) logging into apps. Individuals use personal preferences to configure device settings, install the apps they want, and use personal credentials for each app they acquire. Organizations typically have security policies such as requiring a PIN to unlock the phone, set sleep and lock times, and possibly even prevent the use of open Wi-Fi networks. Organizations also typically control app usage by whitelisting (allowing only “approved” apps to be installed) or blacklisting (blocking the installation of “unauthorized” apps). These policies are enforced through tools known as Mobile Device Managers (MDM) or Unified Endpoint Managers (UEM). This section will outline the tasks associated with each of the three models employed by the MAC.

The physical tasks of unboxing, labeling, and powering on/off phones are the same across all methods of provisioning. When managing large volumes of mobile devices - workspace, charging infrastructure, transportability, storage, and network bandwidth all significantly impact efficiency. Examples of ways to improve efficiencies include:

1. Multi-unit charging banks
2. Multi-unit transport cases
3. Augmented bandwidth at provisioning facility
4. Batch label making

Manual

A cache of Sonim XP8s was utilized for the 2019 Chevron Houston Marathon. Due to delays for procuring the MAC devices associated with the federal government shutdown, FirstNet built by AT&T loaned us the necessary phones to conduct this planned deployment. The phones were brand new and in their original state, other than having the FirstNet SIMs pre-installed.

The tasks and associated times were logged for a sample of 15 phones to determine the average time to manually provision devices. It is important to note that provisioning activities can vary significantly based on factors such as:

- Hardware
- SIM: pre-installed or requires installation
- OS and version
- Network connectivity - app installation times can vary significantly
- Number of apps being installed
- Accessibility of apps - available in public app stores or acquired through another manner
- User proficiency with device and applications
- Type of labels/label maker (if used)

For the 2019 Houston Marathon, device assignments and app account creation were completed prior to the start of device provisioning and not included in this assessment. Depending on the complexity of the deployment, these activities can be quite time-consuming.

As demonstrated in the table below, the provisioning of 15 devices with 2 mobile apps took 3 hours and 27 minutes with an average of 14 minutes per device.

Step	Task	Start Time	End Time	Total Time	Time / Phone
1	Power on phone and attach inventory label	9:15	9:40	0:25	0:01
2	Update AT&T software and reboot phones	9:40	9:59	0:19	0:01
3	Add device assignment labels	9:47	10:02	0:15	0:01
4	Login to Google Play	10:03	10:30	0:27	0:01
5	Install collaboration app	10:31	10:38	0:07	0:00
6	Install Situational Awareness (S/A) app	10:40	11:03	0:23	0:01
7	Login S/A app and set user icons	11:04	11:20	0:16	0:01
8	Move app icons to home screen	11:22	11:33	0:11	0:00
9	Login collaboration App	1:35	1:45	0:10	0:00
10	Clean-up Collaboration timelines	1:45	2:14	0:29	0:01
11	Create channels in Situational Awareness app	2:14	2:29	0:15	0:01
12	Set phone security settings (PIN, Lock screen & Sleep)	2:30	2:35	0:05	0:00
13	Remove Gmail account	2:35	2:40	0:05	0:00
	Total			**3:27**	**0:14**

FirstNet Built by AT&T provided 100 loaner Sonim XP8s for the Los Angeles Marathon. Every phone has a unique identifier called an International Mobile Equipment Identifier (IMEI). FirstNet Built by AT&T requires that the SIM card be tied to the IMEI of the specific device in order to activate public safety priority and preemption. Due to the delay in the purchasing approval process, the loaners were provided just days before the event. With such short notice, the phones were shipped with the SIMs not installed. The process of matching the SIM to each individual phone was incredibly time-consuming. Once the SIMs were matched to the correct phones, they then had to be installed. The overall process added approximately 14 hours, or roughly 8.4 minutes per phone, to the provisioning process.

Manufacturer’s Provisioning Tool

Some manufacturers offer provisioning tools to aid in inventory management and automate some device provisioning activities. MAC members tested the provisioning tool, Sonim SCOUT, for a jail communications pilot. The findings below are not an exact comparison against the manual provisioning process. Due to the secure nature of the jail environment, the key feature was the use of the Kiosk Mode which restricts what users are able to access on the device. The time to develop and test the Kiosk configuration inside of Sonim SCOUT was not measured.

The table below outlines the tasks required for provisioning devices utilizing Sonim SCOUT.

Step	Task
1	Power on phone and attach inventory label
2	Update software and reboot phones
3	Add device assignment labels
4	Scan Sonim SCOUT QR Code
5	Sonim SCOUT tool automatically installed apps & configured phone settings
6	Login App(s)

Utilizing a manufacturer's tool allows some settings to be provisioned automatically that most third-party tools cannot or often do not support such as setting the device PIN. It is estimated that the use of Sonim SCOUT reduced the time for provisioning by 75-80% over manual provisioning (excluding the time to create and test the Kiosk profile). The biggest limitation of the tool was the network bandwidth to provision numerous devices simultaneously.

As a provisioning tool, it is designed to assist in initial device configuration rather than full device management. Over-the-Air (OTA) update capabilities are limited, so updates typically require each device to be physically touched. Updates can be done very easily by creating a new QR code for individual changes such as adding a new application or the entire profile can be updated through a single QR scan.

The SCOUT kiosk mode provides more flexibility in managing what device settings can be accessed while in kiosk mode. Administrators can block Settings altogether or manage which settings can be adjusted from kiosk mode. One advantage of the SCOUT tool is the ability to securely set fingerprints within kiosk mode without having to completely exit kiosk mode.

Mobile Device Manager / Unified Endpoint Manager

The use of an MDM or UEM is important for automation, security and inventory management. The MAC used MobileIron as the UEM to provision and manage the majority of devices acquired for this project. We also conducted interviews with the Texas Division of Emergency (TDEM) followed by a tabletop exercise to compare tools and processes to document best practices for managing device caches.

The MAC acquired 200 Sonim devices. By utilizing MobileIron, the provisioning process was very similar to the process used with Sonim SCOUT. The major difference is that devices are populated in the Sonim SCOUT portal through importing a CSV file. Devices are automatically registered in the MobileIron portal once the username and password are entered and the device contacts the MobileIron server through the MobileIron Go app.

As with the jail deployment, kiosk mode was used for the LA Marathon and other MAC deployments. The kiosk profile was built prior to device provisioning. Below is the list of tasks for device provisioning with MobileIron.

Step	Task
1	Power on phone and attach inventory label
2	Tap screen 6 times to exit “Setup” mode and open the QR scanner
3	Scan the QR code to install MobileIron Go
4	Enter MobileIron username / password
5	Set device PIN
6	MobileIron auto-configured phone
6	Add device assignment labels
7	Login App(s)

One significant advantage of UEMs is the ability to support OTA updates. The apps deployed differed across events and user groups. For example, a survey app was utilized by fire/medical personnel during the LA Marathon to track patient contacts. Law enforcement did not use this app. Therefore, we utilized two kiosk profiles with the survey app being included in the fire/medical profile but not law enforcement.

As the devices were used for different deployments, the kiosk profiles were updated in the admin portal and changes were pushed automatically to specific devices.

Verizon Wireless provided 100 of the loaner Sonim devices for the LA Marathon. At the end of the event, the phones were required to be factory reset prior to returning them to Verizon. The process was incredibly simple using MobileIron. The Verizon phones were filtered in the MobileIron portal and a bulk “Wipe” command was sent. As each phone was powered on, it would begin the factory reset process immediately upon connecting to the network. Once the factory reset process was complete, phones were powered down and put back into their assigned bag for shipping.

TDEM manages a cache of approximately 7,500 iPhones for disaster response around the entire state of Texas. Over the past several years, TDEM personnel have acquired tools and developed sophisticated processes for device management. Unlike MAC deployments for pre-planned events and daily operations with dedicated support personnel, TDEM deployments are typically in support of no-notice events around the entire state. TDEM devices are generally deployed for single application use such as evacuation tracking, Push-To-Talk (PTT), personnel tracking, damage assessments, etc.

TDEM uses the MDM Airwatch to provision and manage their cache of phones. Due to the dynamic nature of TDEM deployments, their basic configuration provides an Airwatch App Catalog containing approved apps that end-users can install based on operational requirements.

Other General Provisioning Considerations

Network Connectivity

The single biggest limitation to provisioning phones is network bandwidth. TDEM has expedited this process by caching data locally on an Apple laptop and connecting the phones via a USB cable. This wired provisioning significantly improves download and update speeds. If network bandwidth cannot be optimized, staff must be increased as the device number increases to get them provisioned quickly enough.

The location of device provisioning is important. If a strong commercial LTE signal is available and devices have cellular service activated, provisioning can be done directly over the carrier network using any of the methods of device provisioning outlined above. If commercial signal is poor or the devices do not have active service, they must be put on a Wi-Fi network if wired provisioning is not supported. The number of devices that can be provisioned simultaneously depends on the available bandwidth. TDEM has built a robust Wi-Fi network at its headquarters facility dedicated to the provisioning of cached phones. This augmented infrastructure has reduced the overall time and manpower required for device management.

Automation

Provisioning mobile devices involves significantly more manual tasks than provisioning computers or radios. Having tools that allow the device to be plugged into a powered USB hub on a computer allows auto-population of things that must be entered multiple times such as MDM credentials, Wi-Fi network information, etc.

Another mechanism for automating manual device management tasks is through the use of QR or barcode scanning for items that must be done manually on each phone. Tasks such as connecting to Wi-Fi, setting a device PIN, and entering credentials can be significantly expedited through the use of QR/barcode scanning.

Charging

Ensuring devices stay charged is important for provisioning and deployment. Multi-port charging banks, cables, and power strips should be acquired to support the number of devices being managed. For longer-term deployments, charging cables should be sent with the device. Having a second set of power cables that can be permanently installed at a central provisioning facility can reduce the time for unpacking and plugging/unplugging cables. While this may seem trivial, it can become quite time consuming when managing large quantities of mobile devices. Some manufacturers such as Sonim provide multi-bay charging banks similar to radio charging banks. In lieu of this, multi-port USB charging banks and extra cables can be used. It is important to estimate the amount of power required to charge the types of devices being managed and to factor that into the type of charging banks purchased as well as the number and type of power strips/surge protectors used.

Device Management

Inventory management for shared mobile devices is in some ways similar to shared radios; however, there are distinct differences.

Service

Radios are privately owned and operate on dedicated networks. Most mobile devices require active cellular service unless exclusively used in dedicated facilities operating on a local wireless network. Commercial carriers offer different types of plans for public safety agencies that allow for service to be activated for periods of deployment and then deactivated or suspended between operations. Service is activated/deactivated through an administrative portal. Processes must be developed to support rapid service activation of designated devices, especially for no-notice events.

Asset Management

Mobile devices are identified through IMEIs and/or phone numbers. Most organizations utilize internal asset management systems to track equipment inventory. Tracking the issuance of laptops, radios and other mobile equipment is typically done by assigning a user in the organization’s directory to the asset in the asset management system. To date, the majority of public safety deployments of cached phones support temporarily assigned phones to users across different agencies for different operations. Traditional asset management systems and processes do not support this type of deployment model.

Below is an overview of multiple inventory tracking methods employed for mobile devices:

1) **Spreadsheet** - the least sophisticated method of tracking inventory is to have a spreadsheet with a list of each device. Columns can then be added to track the individual, agency and contact information of device assignments. This method is highly manual and prone to mistakes. When doing large deployments with multiple support personnel issuing phones, using a cloud-hosted spreadsheet that each team member can update simultaneously has proven to be easier to keep accurate and updated than individual, locally stored files that require version control and reconciliation.
2) **Manufacturer tool** - Our only experience is with Sonim CLOUD. This tool allows you to import a list of devices and assign them to groups and/or users. If adequately maintained and kept up to date, the tool provides a database that is searchable.
3) **MDM/UEM** -

Airwatch requires an Active Directory account, so TDEM created a generic Active Directory account which is tied to a single Airwatch account used for all shared phones. Since all devices use one generic account, Airwatch uses the phone # or IMEI to identify individual devices.

MobileIron can be deployed with or without an Active Directory account. If using an enterprise version of MobileIron which requires an AD account, one method employed was to create generic AD service accounts for each device. In this model, we created service accounts with the format LTExxxxx with the x's representing the last five numbers of the IMEI.

Alternatively, the cache of phones managed by the MAC were not tied to Active Directory. Each device was assigned a MAC inventory number which was assigned to the phones in MobileIron.

Labeling

When dealing with large quantities of devices, it is important to have an inventory label where it can be easily identified. Some departments put the inventory label with return contact information on the inside of the battery cover. This model can work for individually issued devices; however, when provisioning phones for shared deployments, it is important to have a label visible from the outside identifying the specific phone - either an assigned inventory number, phone number or reference to the IMEI (i.e. LTE-XXXXX with the last 5 digits). After multiple deployments, we have found that a straight-forward, consecutive numbering system is much easier for locating and provisioning large quantities of phones than utilizing IMEI or phone numbers which are longer strings of numbers and not consecutively numbered.

When transporting phones in pelican cases with foam cutouts, labels on printer sheets do not seem to adhere as well as the label tape. Printing sheets of labels is much quicker and easier than printing on commercial label maker machines.

Finally, the type, size, color, and placement of labels should be considered with a small group of test phones before labeling large quantities of devices.

Device Updates

When managing cached phones, there are often gaps between deployments. During that time, there are often updates to firmware, operating systems, and apps. TDEM has implemented a process where cache phones are turned on and updated once per quarter. Based on the size of Texas and the time to get phones distributed to no-notice events, TDEM changed the model of storage from all centrally stored in San Antonio to being distributed around the state. Phones are assigned to a local "Device Manager" from a particular organization. That person is responsible for following the TDEM device management guidelines. This process also ensures that batteries and overall device health are verified quarterly to ensure they are in good condition and can be rolled out quickly for no-notice events.

User Assignments

When sharing devices, it is important to know who will need to be assigned a device. This process varies significantly based on operational requirements. In general, there are 3 operational contexts for device sharing:

1) Pre-planned events
2) Daily operations
3) Incident response

Hardware, apps, automation tools, and department policies and procedures can differ widely throughout the industry, so this report will provide example use cases for assigning shared devices under each of the 3 operational models listed above. These examples are intended to provide general guidance for considerations in developing shared device programs, but each deployment must take into account the specifics associated with the hardware, apps, automation tools, staffing/support resource availability, and department policies and procedures to ensure a successful mobility deployment.

Special Event Device Assignments

Pre-planned events have the advantage of knowing resource requirements in advance of the operational period. By working with event planners, device users should be identified during the planning process based on the Concept of Operations (ConOp) for how mobility technologies will be utilized and assigned based on the Event Action Plan (EAP). The operational requirements of the event should drive the type of devices and apps utilized as well as which resources should be assigned devices. In many cases, the individual person may not be known until shortly before the event, but the number and types of resources should be known in advance.

The device assignment models for the MAC deployments during the 2019 Chevron Houston Marathon and Sketchers Los Angeles Marathon are the basis for this assessment. Tasks included:

1. Identify resources
2. Confirm quantity of devices required
3. Validate apps used by user group

For large special events, users are often identified by resource or post rather than the individual name or ID number. This is useful in being able to pre-assign devices and allow for staffing changes without impacting device provisioning activities. Device assignments can be managed electronically through an asset management tool or spreadsheet.

Labeling devices is critical to the successful deployment and management of pre-assigned devices. Unlike radios, app credentials are unique to the user and are typically logged in prior to device distribution. More details will be provided later in this report on the use of app credentials for resources (as opposed to individual users). In addition to the standard inventory label, shared device deployments typically require a user label identifying the resource it is assigned.

Daily Operations

Shared devices for daily operations can vary significantly based on operational requirements. The two examples provided include a jail communications pilot at the Harris County Sheriff's Office (HCSO) and "Connected Cop" deployment with the Inglewood Police Department.

Jail Pilot

The jail deployment represented a challenging operational environment to support shared devices due to the current state of technology. One requirement based on the secure nature of the facility was to use fingerprints to unlock the device and only allow supervisors to know the unlock PIN in the event a device reboot is required. It also posed a challenge for creating user accounts. Due to scheduling complexities and staff shortages for such a large facility, personnel often move around to different posts. The ConOp was designed around knowing the position that you needed to reach as opposed to the individual person (i.e. 3rd Floor Control Center or Pod 5A). Devices were assigned to each designated post.

Connected Cop

Another pilot under the MAC was to test the feasibility of replacing the Mobile Data Computer (MDC) in the police cruisers at Inglewood Police Department (IPD) with a smartphone which would wirelessly cast information from the phone worn on the officer's body onto a "dummy" tablet mounted to the dashboard with a swivel keyboard installed on the passenger side to allow the keyboard real estate of a computer when officers needed to write reports or do more typing than simple queries from the touchscreen.

IPD had a more straight-forward device assignment model due to the consistent nature of their staffing. Prior to the launch of the Connected Cop pilot, IPD had restructured its staffing to have 4 officers assigned to each patrol vehicle - one from each of their 4 shifts. Given the predictability of users, devices were assigned to the cruiser and the fingerprints of the 4 officers were pre-provisioned into the phones by the IPD Administrator.

No-Notice Events

To support the diverse requirements of different types of "No-Notice Events", TDEM utilizes an app catalog or pre-approved mobile apps that can be downloaded when the phones are assigned to the users. Each operation typically uses 1-2 apps, so users are provided instructions with the phone packet on how to download from the Airwatch app catalog.

The cache of phones is distributed around the state for rapid deployment. Incident commanders and communications personnel determine device assignments.

User App Credentials

One of the most challenging aspects of deploying mobile apps is the creation of secure app accounts and assignment of user credentials. Integrating app credentials to a department's directory and utilizing Single Sign-On (SSO) is the most straightforward method of managing user credentials. Public safety mobile app adoption is still in its infancy, so very few departments have the tools available to support SSO. Multi-organizational deployments pose a greater challenge when supporting users from different organizations who all have separate organizational directories.

The methods and technologies for managing and securing user credentials, particularly across organizations and apps, is a broad and complex topic that is rooted in Identity, Credential, and Access Management (ICAM). This report will address the current processes for issuing app credentials in shared device deployments. Additional information on this subject can be found in various mobile ICAM publications including the National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) Special Publication 1800-13 Mobile Application Single Sign-On: Improving Authentication for Public Safety-First Responders[31].

In most public safety operations, there are users who need to be identified by name such as Incident Commanders, Supervisors and other special detail personnel. Other users need to be identified by the position/post they fill or resource ID.

Individual

Individually assigned accounts typically utilize a person's email address or some other unique username with a private password. The user is identified in the application by name or callsign indicating their rank and/or position in the event/incident.

Shared

Other users need to be identified by 1) the post they are filling such as "Gate 6" or "Hazmat Team 1" or 2) the resource type such as Quick Response Vehicle (QRV) - QRV3. In large-scale operations, many members may not know the person staffing each particular post or resource type. In these situations, they need to be able to find the person in a particular location or with particular skills and/or equipment such as Advanced Life Support (ALS) versus Basic Life Support (BLS). In these cases, user accounts are created based on the post or resource. Shared devices are pre-configured with the apps necessary for the operation and apps are often pre-logged in. The management of who was actually issued the device at a particular time is managed through the device distribution process described below.

[31] https://www.nccoe.nist.gov/publication/1800-13/

Device Distribution & Collection

Distribution & Collection

Shared devices must be distributed/collected in different ways for different types of operations. Below are some examples of the different models which can be considered during implementation planning.

Pre-planned events - the size, footprint, and duration of events will impact the distribution strategy.

1. For smaller events with a single roll call location, administrators or other operational personnel assigned to distributing devices can stage equipment at the roll call/staging location in a manner similar to radio distribution. The only difference is that phones must be assigned based on the post or user it is configured for as opposed to just keeping a log of which person took possession of which device #.
2. Larger events, especially that span multiple days and/or have multiple staging locations, typically work better by having an individual assigned by the department to be responsible for distributing, charging, and collecting a pre-assigned cache of devices at the end of each shift and returning them at the conclusion of the operation.
3. Larger events with pre-defined staging and demobilization areas can incorporate distribution and collection activities at these specified locations.

Daily Operations - the operational environment again impacts the best management and accountability of shared devices.

1. For operations in fixed facilities such as a jail, having a secure, permanent location with ample charging banks and space for distribution/collection at shift change is necessary. Defining roles for administering the checking out and in of devices is important. This is typically a supervisor or their designee.
2. For mobile deployments like in patrol vehicles, assigning the phone to a particular unit and coupling it with a Mobile Data Computer (MDC) can improve accountability versus having officers pick them up from a central location during or after roll call. This can also assist when using Bluetooth devices such as mobile fingerprint scanners to ensure that paired equipment stays together.

Incident Response - deploying large numbers of phones during a no-notice event presents additional challenges and requires more sophisticated processes and tools for rapid deployment and distributed collection. TDEM has distributed its cache of phones in strategic locations throughout the State of Texas assigned to Device Managers in various state and local agencies. These phones are issued as needed in a kit that includes the original box with charging accessories, including an AC adapter, and a pre-paid FedEx return envelope. At the end of a operation, responders simply package the phone with all accessories into the FedEx envelope and drop-off at any nearby location.

User Check Out/In

Several asset management systems were evaluated to find a low-cost, stand-alone, out-of-the-box inventory management system to support the check-out/in process for shared phones across different organizations. No viable platform was identified in time for the exercises and deployments conducted under this program. The primary limitations were:

1. Lack of enterprise asset management system for multi-jurisdictional users across multiple directories
2. Cost
3. Ease of use

Prior to the 2019 LAM deployment, device distribution was managed through spreadsheets and/or paper logs. This method of check out/in is not scalable and prone to errors. While exploring automated solutions for managing device check out/in, M4PS contacted TDEM on their lessons learned from managing thousands of phones across the State. Due to limitations of funding to procure a solution and technical skills to build a system in-house, TDEM provided instructions on how to create a web form to capture user contact information and log when the user received the phone. This was a method employed early by TDEM before building a custom database which integrates to their WebEOC platform.

Web Form

A Google Form was created to populate contact information of the person receiving a loaner phone. A custom URL was created for each device with the device number being pre-populated to prevent user data entry errors.

The phones were deployed in MobileIron kiosk mode which placed a link to the custom URL on the home screen of each phone. As each phone was distributed, users clicked the link to enter name, phone number, email address, department, and position worked. Once submitted, the information was logged and time stamped.

Conclusion

It is clear that mobile devices and apps offer tremendous potential to improve public safety communications by augmenting voice radio with tools such as personnel location tracking, Push-To-Talk (PTT), evacuation tracking, collaboration, situational awareness, and many more. The adoption of these tools will continue to grow as the availability of reliable, mobile broadband networks becomes more ubiquitous.

The use of shared, cache devices can accelerate the availability of these technologies until public safety agencies have the budgets to provide all first responders with department-issued smartphones. Cache devices also support interoperability by allowing responders from outside agencies secure access to mobile apps during joint operations.

As outlined in this paper, the provisioning and management of smartphones is a complex task. Department executives should carefully consider the implications of device management when deciding how many devices to purchase and the rate of adoption.

As with the evolution of personal computers, many of these challenges can be lessened as the industry matures products to support multiple users. Industry advancements for supporting multiple user profiles and using temporary facial recognition to unlock phones offer significant potential for expanding the viability of shared device deployments.

M4PS would like to offer a special thanks to TDEM for sharing their lessons learned over recent years in managing thousands of phones across the very large State of Texas. Tips and tricks they shared have helped streamline the provisioning, distribution, and collection of hundreds of cache phones for the various MAC deployments to-date saving countless hours and ensuring all equipment was successfully returned after each operation.

Appendix A – Houston Mobility Working Group Member Profiles

Mike Bell
CTO
Houston Police Department

Brian Cantrell
Chief
Waller County

Joey Clements
Logistics Sup.
Harris County OHSEM

Darryl Coleman
Chief
Harris County Sheriff's Office

Chris Collier
Emergency Svc & Response Mgr
SETRAC

Patrick Hagan
Emergency Ops Tech Specialist
Houston Fire

Hamilton Howard
Sr. Microcomputer Analyst
Houston OEM

Richard Mann
Executive Assistant Chief
Houston Fire

Jim McMillan
Director Infrastructure & Comms
Harris County CTS

Lach Mullen
Reg Emergency Public Info Sys Admin
Fort Bend County

Mike Mulligan
President / Chief
Harris County Firefighters

Tom Munoz
EMC
City of Texas City

Rolf Nelson
Major
Harris County Sheriff's Office

Amy Ramon
Board Mbr / Chief
Harris County Firefighters

Rodney Reed
Assistant Chief
Harris County Fire Marshal's Office

Rick Retz
Homeland Security Liaison
Mayor's Office of PS & HLS

Colin Rizzo
Emergency Manager
Port of Houston Authority

Chris Turrentine
Operational Liaison
Harris County Fire Marshal's Office

Mike Bell

CTO

Houston Police Department
mike.bell@houstonpolice.org
713-308-1820 Office
832-745-3188 Cell

Mike Bell is a 25 year veteran of the technology sector and currently serves as the CTO for the Houston Police Department. In this capacity he is responsible for supporting the IT initiatives for the city's 5,200 uniformed officers and oversees a staff of 140 IT professionals across the enterprise. Mike previously served for 9 years as the CIO for the Texas Dept. of Criminal Justice and is a veteran of the US Navy. He is a member of the IJIS Law Enforcement Advisory Committee and FBI Infraguard. In 2013, Mike was honored as the Texas Public Sector "CIO of the Year" by the CIO Academy.

He currently holds several active IT certifications including PMP, CISSP, CISA, & CISM and earned his MS degree in Technology Management from Texas A&M University.

Brian Cantrell

Chief

Waller County

b.cantrell@wallercounty.us

979-826-7785

Brian Cantrell began his law enforcement career at Waller County Sheriff's Office in 1999 as a Deputy Sheriff and has held various positions within the department, including Narcotics Task Force Investigator and Criminal Investigative Sergeant/Lieutenant in the Crimes Against Women and Children Division.

He held assignments to the FBI's Joint Terrorism Task Force and the Houston Metro Internet Crimes against Children Task Force. Chief Cantrell served as the Captain over Patrol and Criminal Investigations from 2013 to September of 2015. In 2015, he was appointed Chief Deputy to oversee operations of the Waller County Sheriff’s Office. In 2017, Chief Cantrell was appointed by Commissioners’ Court to serve as the Director/Chief of the Waller County Fire Marshal’s Office. Additionally, he currently serves County Judge Trey Duhon as Emergency Manager for Waller County.

Chief Cantrell graduated from SHSU in 2001 with a Bachelor of Arts in Criminal Justice. In 2010, he graduated from the 246th FBI National Academy where he earned a Masters Certificate in Police Administration. In 2014, he returned to Sam Houston State University where he earned his Master Degree in Criminal Justice Leadership and Management.
Chief Cantrell grew up in Cypress, TX and attended Cypress Falls High-School, he currently lives there today in the same neighborhood he grew up in. He has one hobby-Golf. He is a proud husband and father of two daughters ages 5 and 10.

Joey Clements

Logistics Supervisor

Harris County Office of Homeland Security &
Emergency Management
Joey.Clements@oem.hctx.net
713-426-9564

Darryl Coleman
Chief

Harris County Sheriff's Office
Criminal Justice Bureau
Darryl.coleman@sheriff.hctx.net
713-755-6891

Chief Darryl A. Coleman is the Commander of the Criminal Justice Command. In this assignment he is responsible for the 1200 and 701 Housing Bureaus as well as the Processing and Courts Bureau consisting of approximately 2,600 personnel, both classified and civilian.

He began his career with the Harris County Sheriff's Office in September 1986 after serving in the United States Army. He holds a Bachelor's of Science Degree in Organizational Leadership and a Master Peace Officer's Certification.

Chief Coleman has held assignments in the Detention, Patrol, Patrol Support and Homeland Security Bureaus. In his career, he has also served as a supervisor and commander of the Traffic Enforcement Division (T.E.D.) (Currently named as Vehicular Crimes Division) where he attained his certification as an Accident Reconstructionist. He has also held commands in the Patrol Bureau as a District Commander and in the Homeland Security Bureau as the Tactical Commander for the High Risk Operations, Marine, Aviation and Emergency Management Unit. Chief Coleman is married to his wife Stephanie of twenty-six years. They have two children, Trevor who is an officer in the U.S. Navy and Sydney, who is a teacher in Cypress-Fairbanks Independent School District.

Chris Collier

Emergency Service & Response Manager

Southeast Texas Regional Advisory Council

Chris.Collier@setrac.org

832.849.7305

Chris Collier has nearly 20 years' experience in Fire / EMS Operations with the last 6 serving as the Emergency Service and Response Manager for the Southeast Texas Regional Advisory Council (SETRAC). In this role, Mr. Collier is responsible for developing regional response plans, maintaining operation-ready critical response assets for the region, and coordination of response resources to large scale incidents in Southeast Texas. In addition to his role with SETRAC, Mr. Collier is a member of Texas Task Force - 1 (TX-TF1) Urban Search & Rescue team which is one of 28 Federal Teams under the DHS / FEMA National Response System holding the positions of Logistic Specialist and FEMA water rescue specialist. Most recently, Mr. Collier deployed for a combined 30 days to Hurricanes Florence and Michael during the 2018 hurricane season. Mr. Collier is also a member of the Texas Emergency Medical Task Force having served as a Task Force Leader, Medical Incident Support Team Member, and Ambulance Staging Manager.

Patrick Hagan

Emergency Operations Technical Specialist

Houston Fire Department

Patrick.Hagan@houstontx.gov

281-409-9772

Emergency Operations Technical Specialist, 8-year member of the Houston Fire Department. Bachelor's Degree in Public Service Leadership, University of Houston – Clear Lake. Advanced training in Incident Command System structure and application. Deployed in multiple roles during Super Bowl LI, Hurricane Harvey, & 2017 World Series. FAA Remote Pilot and Program Manager for Houston Fire Department sUAS. Developing programs regarding: Rapid Response sUAS Deployment, Virtual Reality Training for the Fire Service, & Local Incident Management Teams. "All of the programs I develop have one goal: Ensure responders make it home to their family when the job is done."

Hamilton Howard

Senior Microcomputer Analyst

Office of Emergency Management

Hamilton.Howard@houstontx.gov

713-826-0104

Richard Mann

Executive Assistant Fire Chief

Houston Fire Department

Fire Prevention, Planning & Homeland Security

Richard.Mann@houstontx.gov

281-878-9406

Jim McMillan

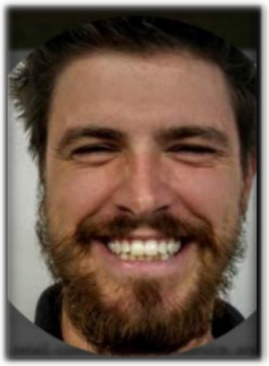
Director

Harris County Central Technology Services

Infrastructure and Communication Services

Jim.McMillan@cts.hctx.net

713-274-8837



Lach Mullen

Regional Emergency Public Info System Admin

Office of Emergency Management

Fort Bend County

Lach.Mullen@fortbendcountytx.gov

Lach Mullen is a self-taught "techie" who has embraced the internet in nearly all of it's forms. A member of the County's Public Information team, Lach plays a critical role in developing public information policies and practices for information dissemination before, during and in the aftermath of local disasters. During an activation of the Emergency Operations Center, Lach's duties shift to regional public information dissemination and may require him to work outside the County in an effort to assist other jurisdictions in our region with critical incident information. Lach is a frequent conference and workshop presenter. His knowledge of today's social media applications have garnered numerous invitations to present best practices.

Prior to joining the County, he worked for a start-up company in the Seattle area which helps companies worldwide engage with the public using the internet. Lach joined Fort Bend County in 2008 as the Regional Crisis Communications and Public Information Systems Administrator. In addition to his PIO responsibilities, Lach also manages the Jetty System for the Houston/Galveston area region. Originally from the northern states, Lach now resides in Houston with his wife and daughter.

Mike Mulligan

President / Chief

Harris County Firefighters Association

Attascocita Fire Department

mmulligan@avfd.com

281-731-6896

Mike Mulligan is the Chief of Department for the Atascocita Fire Department in Northeast Harris County. Mike has been in the fire service since 1985. He's served at four fire departments at a volunteer and career member. He's been with Atascocita since 2006 and has risen through the ranks from backstep volunteer to his current position. Finally, he currently serves as President of the Harris County Firefighters' Association.

Tom Munoz

Emergency Manager & Homeland Security Director

City of Texas City

tmunoz@texascitytx.gov

409-739-4799

Thomas Munoz is an Emergency Manager and Homeland Security Director with 26 years of first responder and emergency management experience. As the Emergency Manager and Homeland Security Director with Texas City, he is responsible for the safety of all its citizens along with managing the crisis communication plan with local industry and major stakeholders. Texas City is home base for 19 low-to-high risk chemical plants. The Port of Texas City is the 7th busiest port in the country. Tom also responded to the Santa Fe ISD shootings where he served as the Liaison and Logistics Officer during this event. He has testified in front of the Senate Select Committee and the House of Representatives on Violence in Schools and School Security.

Prior to his arrival to Texas City, Tom was a 24 year member of the Houston Fire Department in which he achieved the rank of Assistant Chief of Homeland Security and Planning. Part of his duties included planning for major city events, which included the NCAA Finals, Presidential and Dignitary visits, the Houston Marathon and the Olympics Marathon Trials. He was also the Human Relations Chairperson for the International Associations of Fire Chiefs

Tom served in the United States Coast Guard Reserves and retired as Commander. During his time in the United States Coast Guard, he served as the USCG Deputy Incident Commander for Hurricane Katrina-New Orleans Vessel Removal Project, the Texas City Y Spill as a Liaison Officer and most recently served as the Hurricane Maria Emergency Preparedness Liaison Officer in San Juan, PR. Tom also served on the Commandants Diversity Advisory Council.

Tom is currently an Adjunct Professor at the University of Houston-Downtown where he teaches Safety, Emergency Management and Crisis Communication.

Tom holds a Master's Degree in Emergency Management and is currently working on his second Masters in Homeland Security from American Military University. He has a BA in Political Science from the University of Houston. Tom completed the Executive Leadership and Management Certification Program from the University of Notre Dame Mendoza School of Business. He is also a graduate from the Naval Postgraduate Homeland Security Executive Leadership Program as well as the National Defense University in Washington, DC.

Rolf Nelson
Major
Harris County Sheriff's Office
Homeland Security Bureau
rolf.nelson@sheriff.hctx.net
713-877-5201

Homeland Security Bureau Maj. Rolf Nelson began his career with the Harris County Sheriff's Office as a deputy in 1990. Over the course of his career, he has served in Detentions, Patrol, Accident Investigations, Homicide, Special Operations, Homeland Security, and the Training Academy.

Maj. Nelson holds a Master Peace Officer Certificate, is an Instructor, and a Firearms Instructor with the Texas Commission on Law Enforcement (TCOLE). He received his Bachelor's Degree in Criminal Justice from Midwestern State University and is pursuing his Master's in Criminal Justice Leadership and Management at Sam Houston State University. In 2012, he graduated from the prestigious FBI National Academy, Session No. 249. Maj. Nelson is also a proud veteran of the United States Army.

In addition to his military and law enforcement service, he took a leave of absence from 2005 – 2006 and accepted an assignment with the United States Department of State to consult and train Iraqi police forces in the Baghdad and Ninawa Provinces during the early years of the Iraq War.

Major Nelson and his wife Stefani have three wonderful children, Samantha, Kathryn, and Aiden.

Amy Ramon

Board Member / Chief

Harris County Firefighters Association
Cy-Fair Volunteer Fire Dept
Amy.Ramon@cyfairvfd.org
281-550-6663

Amy Ramon is the Fire Chief of Cy-Fair Volunteer Fire Department, with over 28 years' of fire service experience. She earned her Doctor of Jurisprudence from South Texas College of Law and is a licensed attorney. She holds various certifications including Licensed Paramedic and SFFMA Master Firefighter.

Rodney Reed

Assistant Chief

Harris County Fire Marshal's Office
Rodney.Reed@fmo.hctx.net
713-274-1717

Rodney Reed is the Assistant Chief of Operational Support for the Harris County Fire Marshal's Office, with over 14 years' fire service experience. He earned a Bachelors' degree in Communications and Masters in Emergency Management Services. He holds various certifications including a State-Certified COM-L, TCFP Fire/Arson Investigator, Firefighter, HazMat Technician, and international instructor. He is also a member of the DHS First Responders Resource Group and member of the Environmental Crimes committee of the International Association of Chiefs of Police.

Rick Retz

Homeland Security Liaison

Mayor's Office of Public Safety & HLS

City of Houston

Richard.Retz@houstontx.gov

832-393-0924

Richard Retz is a Master Peace Officer and TCLEOSE Instructor with over 30- years of service with the City of Houston Police Department. He is currently assigned to the Mayor's Office of Public Safety & Homeland Security, which acts as the principal liaison with State and Federal partners responsible for the coordinated development and implementation of regional strategies to improve the area's homeland security posture.

Colin Rizzo
Emergency Management Coordinator
Office of Emergency Management
Port of Houston Authority
crizzo@poha.com
713.670.3636

Colin Rizzo is the Emergency Manager for the Port of Houston Authority, a position he has filled since its creation in January of 2012. Colin is responsible for the direction and day-to-day operations of the Emergency Management Department planning and directing emergency and disaster preparedness and response within the Port of Houston Authority. He works closely with local, state and federal partners.

Before coming to the Port of Houston Authority, Colin worked for the Galveston County Office of Emergency Management where he held many titles including Community Emergency Response Team (CERT) Coordinator, Homeland Security Coordinator, and Operations Coordinator.

Colin graduated from Stephen F. Austin State University in Nacogdoches, Texas with a degree in Public Administration and a minor in Geography. He is TCOLE certified police officer, TCFP certified fire inspector and arson investigator and certified by the International Association of Emergency Managers as a Certified Emergency Manager (CEM). Recently the Emergency Management Association of Texas named Colin the Texas Emergency Manager of the Year for 2017.

Chris Turrentine

Operational Liaison

Harris County Fire Marshal's Office

Christopher.Turrentine@fmo.hctx.net

832-588-6919

Chris Turrentine is the Operational Liaison for the Harris County Fire Marshal's Office. In this role, he works to facilitate communication and collaboration between law enforcement, fire, and EMS in the Greater Houston/Harris County region. He is no stranger to public safety, having spent over 23 years in fire and law enforcement where he has worked as a Patrol Officer, Detective, Firefighter, EMT, and 911 Dispatcher. Chris graduated in 2014 with a bachelor's degree from the University of North Texas and in 2015, earned a master's degree in Emergency & Disaster Management from the prestigious Georgetown University. He also holds various certifications including TCOLE Master Peace Officer, TCFP Fire/Arson Investigator, Firefighter, and Hazardous Materials Technician. Chris lives in Houston with his wife of 10 years, Elizabeth, and their two children Emerson and Alexandra.