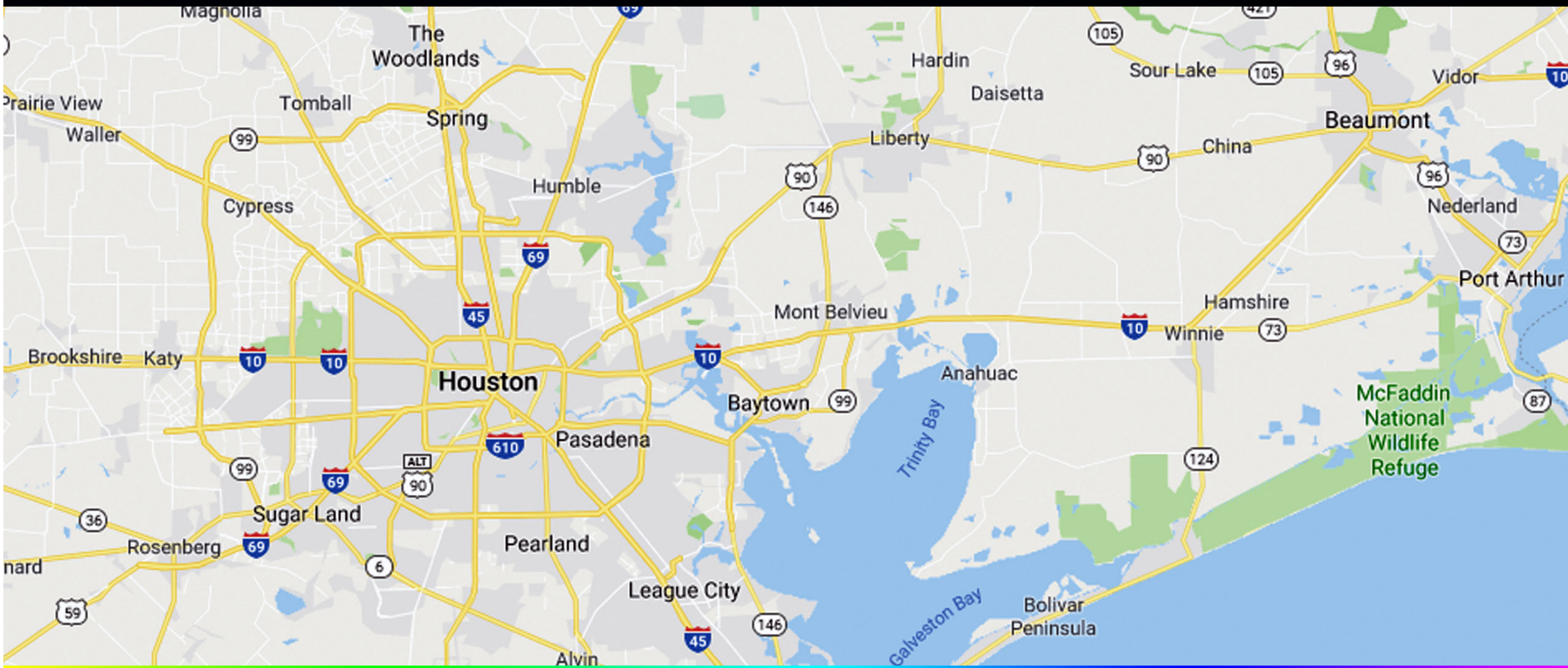
Houston Regional Public Safety Mobile Cloud Strategy



M4bility
Public Safety

Houston Regional Mobile Cloud Strategy

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
Jim McMillan	Director Public Safety Technology	Harris County Universal Services
Colin Rizzo	Emergency Manager	Port of Houston Authority
Jared VandenHeuvel	Program Coordinator - Public Safety Solutions	Texas Department of Emergency Management

Table of Contents

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.[1]"

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"**

[1] 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.[2]

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.
2. Inability to dictate and submit field incident reports.

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

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."[3]

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.”[4]

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

[3] https://www.nist.gov/speech-testimony/interoperability-public-safety-communications-equipment
[4] 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"[5].

"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"[6].

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

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

[6] 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[7].

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
    - Defined standards

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

  - 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."[8]

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.

[8] 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.[9] 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 data (e.g. video from body-worn cameras).[10] Agencies should consider that data may be stored temporarily, even if it is not explicitly stored in a long-term repository

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

[10] 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.

(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[11] 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.[12]

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.[13]

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

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

[13] https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

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."[14]

An article by McAfee outlined an easy-to-read bullet list of common types of security threats for SaaS, IaaS and private cloud[15]. 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.
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.

[14] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf
[15] https://www.mcafee.com/enterprise/en-us/security-awareness/cloud/security-issues-in-cloud-computing.html

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.[16]

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.
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."[17]

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

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 together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds)."[18]
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

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

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[19] 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[20]). 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:[21]

> *"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.*
>
> *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.*

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

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

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

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[22]
- Evaluation of Cloud Computing Services Based on NIST SP 800-145 (NIST SP 500-322)[23]
- NIST Cloud Computing Reference Architecture (SP 500-292)[24]
- FedRamp[25]
- FBI CJIS: Recommendations for Implementation of Cloud Computing Solutions[26]
- HHS: Guidance on HIPAA & Cloud Computing[27]

[22] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

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

[24] https://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/ReferenceArchitectureTaxonomy/NIST_SP_500-292_-_090611.pdf

[25] https://www.fedramp.gov/documents/

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

[27] https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html