SAFECOM

Considerations for Public Safety Cloud Computing Adoption

Cloud-based technology solutions and their adoption by public safety organizations must meet unique mission needs. Public safety requirements may demand additional capabilities beyond the standard one-size-fits-all cloud solution. Implementing cloud-based solutions for public safety communications and data sharing requires diligent planning to ensure uninterrupted service, technology interoperability, user-tailored experience, and compliance with security, evidentiary, and resiliency requirements. For example, public safety communication needs include:

	Operability: Public safety must communicate at all times and under all circumstances; organizations cannot afford any downtime
	Interoperability: Public safety requires decision-making immediacy and flexibility, often paired with on-demand coordination with diverse partners; the foundation of successful partnerships is often dependent on the linking of different systems that are all governed and operated by separate entities, as authorized
	Security: Public safety is increasingly seen as a prime target by malicious cyber actors seeking to compromise and disrupt communications and coordination; human errors, legacy equipment, and vulnerabilities from interconnected systems could also impact overall organizational security
	Resiliency: As mentioned above, public safety cannot afford any downtime; thus, they must maintain a separate testing environment for updates; they cannot sustain software errors or interruptions, including during patching and updates

Cloud-based solutions may alleviate or exacerbate these concerns depending on the configuration. When implemented to meet mission needs, solutions may provide benefits or improvements in:[1]

Broader support: Organizations may choose from a wide range of cloud vendors

Flexibility in design: Cloud services provide managed services such as document storage, database storage with replication, and application interfaces for automation

Scalable performance: Cloud services support a broad range of horizontal scalability[2]

Availability: Cloud services can manage failures of the underlying infrastructure for the organization and move running code with minimal interruption

Cost: Cloud services can increase efficiency while allowing organizations to direct financial resources toward mission-critical tasks

Disaster recovery and business continuity: Organizations with off-premises cloud data and infrastructure may be better positioned to handle and recover from adverse events at local offices (e.g., natural disasters)

Cybersecurity: Cloud services often provide options for different aspects of security, so individual organizations do not have to build support for them; however, it is crucial that organizations learn about the options and implement and configure the ones that are right for them

Cloud Adoption Considerations for Public Safety

To capture the potential benefits of cloud-based solutions, public safety organizations may choose from various cloud adoption strategies to suit their needs. Example strategies popularized by the cloud industry include rehost, refactor/rearchitect, revise/re-platform, rebuild, and replace.[3] However, regardless of model, strategy, or vendor, organizations are encouraged to explore the following considerations to ensure that cloud adoption is the right solution. In addition, it is recommended that organizations review guidance and materials on cloud security to avoid potential pitfalls of cloud-based implementation.[4]

[1] Cybersecurity and Infrastructure Security Agency (CISA), "Cloud Security Technical Reference Architecture Version 2.0," June 2022. https://www.cisa.gov/sites/default/files/publications/Cloud%20Security%20Technical%20Reference%20Architecture.pdf.
[2] The ability to add more machines to an organization's pool of resources.
[3] CISA, ibid, 17.
[4] For example, CISA recommends reviewing the Cloud Security Technical Reference Architecture, monitor the MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK ®) knowledge base for taxonomy of cyber adversary behavior, and review essential concepts such as Identity, Credential, and Access Management (ICAM) and endpoint security services.

Consideration #1: Needs and Scope

First, determine the organizational and operational needs to be addressed, as not all needs unique to public safety could be easily satisfied by cloud-based solutions. In addition, federal, state, local, tribal, and territorial (FSLTT) regulations may pose requirements to retain particular data and infrastructure on-premises for the purposes of security, redundancy, and continuity of operations.

EXAMPLE QUESTIONS TO CONSIDER INCLUDE:

- Is cloud computing[5] adoption appropriate for the organization, system, and/or application?
- Which cloud computing model best meets organizational needs (e.g., private cloud vs. hybrid cloud models)?
- Can existing networks and systems support mitigation to the cloud?
- Does the organization already own or operate its own servers, hardware, and data centers? How could cloud adoption impact these operations?
- Is qualified staff available to implement, manage, and support cloud adoption?
- Which cloud service provider (CSP) could fulfill the organization's needs?
- Which FSLTT requirements must organizations meet contractually should they migrate to the cloud? For example, are there laws that restrict the storage of sensitive data, and can the CSP meet this need?
- Who are the partners and stakeholders that should be a part of the decision-making, both at the onset and as the cloud services are maintained?
- How would one organization's adoption impact operation and interoperability with jurisdictional partners?

In addition to general considerations, operating and storage costs are major factors in migrating to the cloud. As physical servers and data centers are located off-premises and managed by the CSP, organizations may be able to redirect resources toward other missions or benefit from a reduction in operating costs. Cloud implementation may minimize the need for physical space, capital expenditures, or operating expenses. Furthermore, CSPs could offer different levels of support to alleviate organizations' staffing concerns.

EXAMPLE QUESTIONS REGARDING COST OPTIMIZATION AND STAFFING INCLUDE, BUT ARE NOT LIMITED TO:

- What is the cost-benefit ratio?
- Does the current budget allow for initial research and information gathering?

[5] NIST defines cloud computing in *NIST SP 800-145, The NIST Definition of Cloud Computing* as "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."

- Once adopted, how will the organization sustain and maintain the services?
- How should the organization document and evaluate spending on cloud procurements or acquisitions?
- Would CSPs require annual or other regular training and certification to maintain adequate proficiency levels?
- Are there positions in the organization that could be delegated or outsourced to CSPs? Will staff require training to manage the new portfolio, or will position descriptions require modification? Will additional staff need to be hired?
- If it's not feasible to begin cloud adoption in the near term, how should organizations work with their leadership to determine the necessity and allocate resources in the future?

Consideration #2: Requirements

After reaching a consensus to adopt cloud services, organizations should research and document the requirements in their request for proposal (RFP) and service level agreement (SLA). It is imperative to describe plainly and comprehensively organizational needs to ensure a successful adoption process. Furthermore, organizations should consult their legal, IT, and financial teams to ensure contractual agreements are clear and legal requirements are met. For example, it is common for organizations to consider a multi-cloud[6] solution. Still, this solution requires a different cybersecurity approach to optimize the environments while managing situational awareness with each respective CSP.

Additional topics for organizations to consider include, but are not limited to:

- What are the technical, security, and pricing requirements? What are the proposed qualification criteria for CSPs?[7]
- What are the security risks involved in cloud-based services? How would organizations address them? How would CSPs address them?
- What responsibilities will the CSP handle? What aspects of the cloud will the organization be responsible for?[8]
- How could cloud solutions meet public safety-specific security standards?[9]
- How could organizations maintain authority over their data? What are the distinctions between different cloud data ownership models (e.g., data created prior to cloud migration versus data produced in the cloud)?

[6] "The cloud infrastructure is a composition of two or more distinct cloud infrastructures that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability." *NIST SP 800-154, The NIST Definition of Cloud Computing*

[7] Example criteria include infrastructure, certifications, service characteristics, data and systems security, and cost control.

[8] Organizations should reference CSP customer responsibility matrices that define provider and customer security and update responsibilities.

[9] Example standards or requirements include the Federal Bureau of Investigation's (FBI) *Criminal Justice Information Services (CJIS) Security Policy*, Federal Risk and Authorization Management Program (FedRAMP), *Health Insurance Portability and Accountability Act (HIPPA)*, and additional FSLTT regulations.

	What are the requirements to ensure organizations maintain a chain of custody[10] of their data while using cloud services? What are the cloud data evidentiary requirements organizations must meet?
	How will cybersecurity incidents be managed, and what are the responsibilities of organizations and CSPs?
	Will a device management tool need to be installed on all devices linked to the cloud?
	How will cloud services improve secured access?
	How will CSPs support audit services?
	What jurisdictional or local requirements may influence data ownership, retention, storage, and privacy?

Consideration #3: Questionnaire to Solicit Key Information

Organizations could consider developing a questionnaire to better engage with potential providers to see if CSPs could meet organization-specific requirements.

EXAMPLE REQUESTS MAY INCLUDE, BUT ARE NOT LIMITED TO:

	• A company overview, including references and testimonies specific to public safety ○ What insurance policies does the company have in place? Do they meet mission requirements? How will the policy impact the customers? Are there additional public safety customers that could be contacted as references?

	• Indication of the CSP's ability to meet requirements
	  ○ How can the standardized offering be customized for mission needs? What is covered by the standard SLA(s)?
	  ○ Does a responsibility matrix exist to outline chains of command and required tasks for the organization and the CSP?
	  ○ When and how are updates and enhancements delivered to the organization?

	The company's retention rate and the length of the average customer relationship
	Differentiators from other CSPs focused on public safety
	Alternative solutions better suited for the organization's needs
	Pricing model and estimate based on the described scope and requirements

[10] "Chain of custody is a process used to track the movement and control of an asset through its lifecycle by documenting each person and organization who handles the asset, the date/time it was collected or transferred, and the purpose of the transfer." *CISA Chain of Custody and Critical Infrastructure Systems*

Conclusion

Due to cloud computing's ability to rapidly scale to meet fluctuations in computing power, mission-critical systems can avoid downtime and technical difficulties presented during times of high demand. Public safety organizations could leverage the multitude of benefits cloud computing offers. As highlighted in this document, several key consideration areas exist to determine if a cloud solution or architecture is suitable and how to work with CSPs to manage and maintain the service. While not all suggested considerations may apply to individual circumstances, they stimulate thought and initiate conversation with leaders and decision-makers. The transition to the cloud could appear intimidating to organizations of all sizes and backgrounds. By reviewing this document's considerations and referencing additional, pertinent guidance, public safety organizations could determine if cloud-based solution adoption is appropriate and what cloud adoption pathways may suit their structures and meet mission-critical needs.