Security, Privacy, and Compliance in the Cloud

Authors
IJIS Institute's CJIS Advisory Committee
CJIS Compliance and Transition to Cloud Solutions Working Group

Acknowledgements

This document is a product of the IJIS Institute; a private, nonprofit collaboration network working to maximize safety, efficiency, and productivity in the public sector by promoting and enabling technology to expand the use of information.

We would like to extend a special thanks to the CJIS Compliance and Transition to Cloud Solutions Working Group.

IJIS Mission

To drive public sector technology innovation and empower information sharing to promote safer and healthier communities.

CJIS Advisory Committee

Jim Pingel, Chair
Mission Critical Partners

Catherine Miller, Co-Chair
Montgomery County, MD Police

Todd Thompson, Secretary
Caliber Public Safety

Kyle Comer
Full Circle Training Solutions

Justin Cook
FBI/CJIS UCR Program

Heather Davis
Alabama LEA–CJIS Division (ASUCRP Rep.)

Akbar Farook
Global Justice Solutions

Tanya Fussinger
Hexagon

Gerard Gallant
Amazon

Michael Haas
DOJ Office of the CIO

Brian Isaac
Texas DPS, ASUCRP

Mike Lesko
NEC Corporation of America

Mike Lyons
Mission Critical Partners – Retired

Joe Mandala
Kansas Bureau of Investigation

Patrick Mellin
Hexagon

Wyatt Pettengill
Idemia

Dianna Poor
Houston Police Department

Charlie Schaeffer
Microsoft

Erica Smith
US DOJ, BJS

Karl Wilmes
Law Enforcement Practitioner (Ret.)

Richard Zak
Microsoft

CJIS Cloud Solutions Working Group

Richard Zak, Chair
Microsoft

Tony Abate
Nlets

Christopher Armstrong
Tyler Technologies

James Buckley
CPI

Brian Day
DXC Technology

Gerard Gallant
Amazon Web Services (AWS)

David Jackson
Thomson Reuters Case Center

Michael McDonald
Motorola Solutions

Comments and Questions

Your comments and questions are welcome!
Please contact the IJIS Institute at info@ijis.org or **1-703-726-3697**.

Table of Contents

1 Overview

The cloud can provide tremendous benefits for criminal justice agencies, but they often face opposing viewpoints that the cloud is either too risky to manage criminal justice information or that leveraging the cloud will require no work on their part. Neither statement is true and well-established operational and technical strategies have been developed for cloud-based solution implementations that fully comply with the stringent requirements for the security and privacy of criminal justice information.

This paper follows on from the CJIS Compliance and Transition to Cloud Solutions Working Group's first whitepaper, Cloud Fundamentals, published in December 2020 by the IJIS Institute (https://www.ijis.org/page/Reference_Papers). Cloud Fundamentals describes the basics of cloud computing and the role that the cloud can play in public safety. This second paper, Security, Privacy, and Compliance in the Cloud, provides the major considerations for agencies considering or planning for the transition to the cloud. The authors include representatives from several global cloud service providers with extensive experience supporting criminal justice agencies.

Every cloud implementation for a criminal justice agency is based on a shared responsibility model which describes how a criminal justice agency, its cloud service provider, and trusted application provider work together to ensure the privacy and security of data stored and processed in the cloud. Unlike an on-premises solution where management responsibility rests solely with an agency, a cloud deployment requires collaboration with a cloud provider, with the agency maintaining control and ownership of its data. This shared responsibility model is supported in the FBI's Criminal Justice Information Services (CJIS) Security Policy – the CSP – which provides both agencies and cloud providers with guidance to ensure that they can support the compliance of criminal justice agencies in the cloud.

This paper starts with a review of the shared responsibility model and then covers three specific areas important in any plan to leverage a cloud-hosted environment – security, privacy, and compliance.

- Security is the most common area of focus for agencies and one of the largest considerations when contemplating a move to the cloud. Network security, data security including access controls to the data, device security, and user access security are all critical components that cannot be passively overseen by an agency. Security oversight requires an active and ongoing level of participation on the part of the criminal justice agency or data owner in any shared management model.

- Data privacy and protection, especially encryption and encryption key management, are also important to criminal justice agencies that are responsible by statute and Regulation 28 CFR Part 20.33 for protecting Criminal Justice Information (CJI) and CHRI (Criminal History Record Information).

- Compliance with the CJIS Security Policy controls and processes is essential to criminal justice agencies that are held accountable not just for their data, stored either on-premises or in a cloud solution, but also for information derived from national systems that are stored in their repositories.

2 Shared Responsibility Model

In the past, organizations managed their own IT infrastructures with complete responsibility for security, reliability, performance, and operations of the data center and the data within. When leveraging public cloud service providers, agencies transfer some of the management responsibilities to these companies, but not the accountability to ensure that the Criminal Justice Information is being managed in compliance with the CJIS Security Policy. Public cloud providers have a strong incentive to provide secure services and support an agency's compliance with the CJIS Security Policy with deep expertise in providing secure clouds for both governments and the private sector. Cloud providers have well-trained staff, economies of scale, significant hardware redundancy, and resources to invest as needed. Cloud providers also have the required capabilities in Security Information and Event Management (SIEM), threat intelligence, and detecting cyber intrusions as they occur.

To support this approach, the CJIS Security Policy operates under the Shared Responsibility Model for the "information security requirements, guidelines, and agreements reflecting the will of law enforcement and criminal justice agencies for protecting the sources, transmission, storage, and generation of Criminal Justice Information (CJI)."[1] The Shared Responsibility Model defines the division of responsibilities for the safety and security of data stored in the cloud between the cloud service provider and the agency to ensure accountability for the data. One important benefit of the shared responsibility model is that it reduces an agency's operational burden because the cloud provider operates, manages, and controls the layers of IT components from the host operating system and virtualization layer down to the physical security of the facilities in which the services operate.

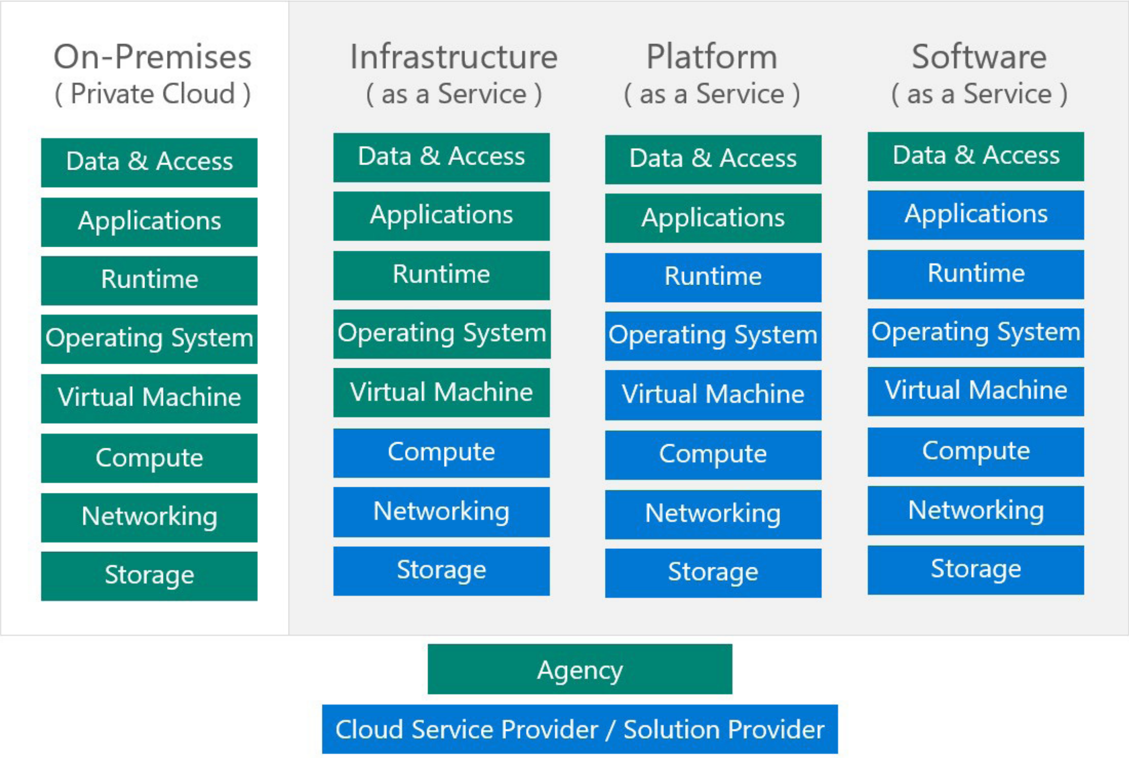
There are different ways that an agency could use cloud services:

Type	Description	Example
Infrastructure as a Service (IaaS)	Cloud service provider delivers the computer processing/storage/ network infrastructure on which the agency runs software of its choosing	Virtual Machine
Platform as a Service (PaaS)	Agency builds applications or uses independent software vendor (ISV) applications that leverage services and databases from the cloud platform	Web Application Firewall
Software as a Service (SaaS)	The agency uses applications from a cloud service provider or independent software vendor (ISV) running on cloud infrastructure that the vendor manages	Hosted CAD or RMS solutions

[1] https://www.fbi.gov/services/cjis/cjis-security-policy-resource-center

Shared Responsibility Model

The table below illustrates how the responsibilities change depending on the type of cloud services used. For example, if an agency uses Infrastructure as a Service, the agency is responsible for patching the guest operating systems running on the virtual machines in the cloud - although cloud providers can also provide automatic patching of the operating system. As an agency moves to Software as Service that responsibility is typically moved to the application solution provider who provides the software. While there are variations on these "as a Service" categories, generally the agency will rely more on their solution and cloud providers as their degree of direct control over the cloud compute resources declines. This is very similar to many cloud services such as photo storage, email, and online movies that we enjoy today in our personal lives – people rely on the providers of these services to operate the cloud infrastructure and protect peoples' data according to the published standards.



On-Premises (Private Cloud)	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
🟩 Data & Access	🟩 Data & Access	🟩 Data & Access	🟩 Data & Access
🟩 Applications	🟩 Applications	🟩 Applications	🟦 Applications
🟩 Runtime	🟩 Runtime	🟦 Runtime	🟦 Runtime
🟩 Operating System	🟩 Operating System	🟦 Operating System	🟦 Operating System
🟩 Virtual Machine	🟩 Virtual Machine	🟦 Virtual Machine	🟦 Virtual Machine
🟩 Compute	🟦 Compute	🟦 Compute	🟦 Compute
🟩 Networking	🟦 Networking	🟦 Networking	🟦 Networking
🟩 Storage	🟦 Storage	🟦 Storage	🟦 Storage

🟩 Agency

🟦 Cloud Service Provider / Solution Provider

It is important that while the criminal justice agency and the cloud service provider share responsibility, they should not share "trust." Agencies and other organizations have run on the "trust but verify" approach but in the shared responsibility model for the cloud, the appropriate approach is "never trust – always verify." Instead of assuming that everything behind the agency's cloud firewall is safe, this "Zero Trust" approach verifies everything explicitly, provides the least required access to users and operates as if there has already been a breach. As a result, every access request is treated as a potential threat and fully authenticated, authorized, and encrypted before being granted.

Where the agency retains full responsibility is in the area of data classification, which is true whether its data is stored in the cloud or an agency's own data center – the agency must ensure that its solutions and data are securely identified, labeled, and correctly classified to meet any compliance obligations. This includes distinguishing between sensitive agency data and content designed to be public. Data classification can be a complex process but is a critical element in security, privacy, and compliance. Connected to data classification is the requirement that a law enforcement agency is following the appropriate dissemination rule – including redaction of data elements – based on the purpose and audience of the dissemination.

3 Security

To successfully protect criminal justice data and related services that are hosted in the cloud, the essential set of security controls should be properly implemented by the cloud service provider and by the agency or their trusted application solution provider. These shared security controls fit well with the shared responsibility model where the cloud service provider provides for the "security of the cloud" and the agency is responsible for the "security in the cloud." While the cloud provider will do much of the "undifferentiated heavy lifting" for physical and infrastructure layer security, agencies must understand that the same types of information security controls that would be used in an on-premises application environment are still required in a cloud environment. For example, just as an agency would configure firewall security rules in an on-premises environment, similar firewall rules must be configured to protect an agency's virtual cloud boundaries.

The cloud and cloud service provider should be enablers for an agency as it implements an information security program for applications and data in the cloud. They should allow an agency to implement the most restrictive set of privileges that are required to protect sensitive data, limiting any system damage resulting from an accident, error, or unauthorized use. This principle of least privilege is one of the most fundamental underpinnings of the CJIS Security Policy and is based on a "need-to-know, right-to-know" standard. To implement this least privilege approach in the cloud, agencies and their trusted application solution providers must be in full control of where their data is stored, who can access it, and be able to see fine-grained identity and access audit information to ensure that only authorized resources have access to sensitive data. All requests for data access must be verified by the cloud service provider's identity and access management services – regardless of where the request originates or what resource it accesses – and every access request must be fully authenticated and authorized before being granted.

While implementing least privilege will help ensure that only people authorized and authenticated by an agency can access its criminal justice information, encryption must be employed for all data in-transit between an agency's site and the cloud service provider. It's recommended that data be encrypted at-rest as well, with access to unencrypted data only by cloud service provider employees who have been screened according to the CJIS Security Policy, Section 5.12. The CJIS Security Policy requires symmetric encryption (asymmetric encryption is not permitted) for in-transit data, protecting it from being readable by unauthorized users. Symmetric encryption for at-rest data outside the boundary of a CJIS-defined physically secure location is also required. Your cloud service provider should enable agencies to easily use symmetric encryption technologies with limited to no impact on the speed and performance of your systems. Simply put, encryption at scale in the cloud is critical to an agency's security posture, just as it should be in on-premises systems. The belief in some agencies that encryption is not necessary for on-premises systems has been countered by the numerous reports of cyberattacks that gained access to city/county/agency networks and exposed unencrypted data.

Without secure management of encryption keys, agencies cannot have full confidence in their encryption properly protecting their sensitive CJI, similar to locking your front door and leaving the key under the mat – sooner or later someone will find the key. If an agency elects to satisfy the CJIS Security Policy through encryption rather than the Policy's technical and personnel controls, its cloud encryption keys (so-called customer-managed master encryption keys) should be stored in a FIPS 140-2 validated hardware security module (HSM) directly or through a key management service that removes the complexity of interacting with the HSM, but still stores the master keys securely in the HSM. These master keys should never leave the FIPS validated hardware security modules unencrypted and should not be accessible or visible to any cloud vendor personnel, similar to putting your house key in a lockbox with a combination key dial – you cannot access the key without the lockbox combination. Such symmetric encryption key services are available today in the cloud. Agencies and

Security

their trusted software application partners can then be confident that their CJI stored, transmitted, and processed is consistently protected while at rest, in transit, or in-process when encryption keys are properly managed. Details on strategies to meet the CJIS Security Policy requirements are found in the Compliance section of this paper below.

Implementing strong access controls, encrypting your data, and securely managing your encryption keys will provide a solid foundation for agencies wanting to move to the cloud. Comprehensive and continuous monitoring and logging of all cloud activities will provide agencies the visibility needed to spot issues before they impact data and mission and will allow agencies to improve their security posture and reduce the risk profile of their environment. Monitoring and logging should include all account activity across all functions in your cloud environment, system-wide performance and health measurement, and threat detection that continuously monitors for malicious activity and unauthorized behavior with an automated response action to stop such activity before it becomes harmful.

[2] Symmetric encryption is a data encryption method whereby the same key is used to encode and decode information.

4 Privacy

The privacy requirements governing criminal justice data impose some special considerations for criminal justice agencies deploying a cloud-based implementation. Under the Shared Responsibility Model, what is referred to as "privacy" typically falls under the customer's responsibility to keep the data private. In the criminal justice space, privacy issues are made more complex by the fact that many participants (not only the accused, but victims and even witnesses) lose many of the privacy rights they might expect in other situations. Clearly, the justice system cannot function unless this is the case, however, it does raise complex considerations for both agencies and the vendors that support them.

Privacy starts and ends with an agency retaining ownership of its data – including the ability to access, modify, or delete data – and also taking action with a cloud provider if the controls stop working. Maintaining control over data is not only important but is also in line with emerging global privacy standards including the European Union's General Data Protection Regulation (GDPR)[3] and ISO/IEC 27018[4], the first international code of practice for cloud privacy. It's an agency's responsibility to ensure that the cloud provider shares independent audit reports on compliance that align with all the applicable critical standards.

The situation may be made more complex if the agency is entrusting data to applications provided in the cloud by SaaS application vendors. In this situation the agency needs to work with the vendor to ensure:

- Users are given clear, concise, and accurate privacy policies which respect the rights of users within their legal jurisdiction. The agency may need to work with the vendor to achieve a compromise, especially since most vendors will already have such policies and may be reluctant to change if they support many different customers.

- The Application vendor offers sufficient technical controls to allow the user to select the choices they are entitled to, concerning how their data is processed.

- The vendor's application code is sufficiently robust to always respect those choices.

- Appropriate security settings are selected such that the user's privacy choices cannot be breached, such as via a data breach.

The agency needs to further ensure that the SaaS application vendor is meeting its obligations under the Shared Responsibility Model and can demonstrate that the cloud platform it leverages is providing its required security controls.

It is an agency's responsibility to ensure that cloud platforms and solutions are correctly configured to ensure the appropriate level of data privacy. There is a data management model known as the "CIA Triad" – Confidentiality, Integrity, and Availability – and privacy can be viewed as a function that spans all three. Confidentiality mandates that data be protected in a manner to be kept private, Integrity focuses on the trustworthiness of the data, and Availability means that the data is readily accessible by authorized users. The confidentiality of data stored in the cloud can be achieved through either technical controls and personnel screening or the encryption described above. Integrity for data in the cloud is supported through user and access monitoring, and availability must be maintained at the appropriate level to support an agency's operations.

[3] General Data Protection Regulation (GDPR) Compliance Guidelines

[4] ISO - ISO/IEC 27018:2019 - Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

5 Compliance

Remaining compliant with the CJIS Security Policy ensures that your Criminal Justice Information is protected through electronic and physical controls as well as the required processes and procedures outlined in the policy. In an on-premises data center, this means the agency is solely responsible for adherence to the policy, which can be a resource burden both financially and in staffing. Cloud providers offer an opportunity to offload some of that effort, which can allow the agency to focus on its mission instead of on its technology infrastructure. When examining cloud providers, it is important to consider their understanding of the CJIS Security Policy and their ability to fully support an agency's compliance with it.

Given all the complexity around maintaining compliance, it can be a great benefit to understand the cloud provider's approach to how agencies can maintain CJIS Security Policy compliance when CJI is hosted in the cloud. This understanding can allow for easier management of policy controls, possibly be more automated, and allow an agency of any size to leverage the experienced staff of the cloud provider in addition to its security and technical staff. Major and specialized cloud providers typically have experience and expertise with several policy frameworks, including the CJIS Security Policy, so an agency can be assured they are working with compliant environments that are actively monitored and where incidents are quickly mitigated. In contrast, managing its own computing infrastructure can result in higher staffing costs, greater resource time spent on monitoring and mitigation, and less confidence in the implementation and management of policy controls which can lead to breaches or other unwanted behavior that puts the agency's data at risk.

The cloud provider must demonstrate their expertise to an agency's satisfaction through continuous monitoring of the cloud provider's performance. Continuous monitoring ensures that the provider is meeting the security, privacy, and compliance controls relevant to the environment of the agency on an ongoing basis. While outsourcing many of the management tasks that agencies previously managed themselves was one of the primary advantages of drawing them to the cloud in the first place, agencies should be actively involved and ever vigilant to the continued performance of the cloud provider almost as if they were managing these activities themselves.

Compliance is a key component in the trust relationship between an agency and a cloud provider. The agency benefits from reduced overhead in implementing and maintaining policy controls and the cloud provider establishes a foundation as a secure cloud provider. This mindset is the balance that in time will draw even more agencies to the cloud and simultaneously raise their confidence level to trust cloud environments for even their most mission-critical and sensitive data. For their part, cloud providers must constantly strive to over-deliver and exceed their customer's expectations for not doing so will threaten their cloud business.

6 Summary

Modern solutions and data management can play a critical role in the public safety mission, and the cloud can be a powerful tool for enabling them. With these capabilities comes the requirement that law enforcement agencies and their solution partners leverage the cloud in a way that supports their compliance with critical standards including the CJIS Security Policy. Through an understanding and execution of the Shared Responsibility Model, agencies can ensure that the cloud can help to support their mission while ensuring that the security, privacy, and compliance requirements for cloud solutions are met.