Ensuring CJIS Security Policy Compliance with Wasabi

Table of Contents

Executive Overview

Wasabi is an affordable and fast cloud storage service. Law enforcement agencies can use Wasabi for a variety of purposes including primary storage, secondary storage for backup or disaster recovery, and cold storage for data archival. Wasabi is ideal for maintaining and storing a wide variety of law enforcement application data and digital content including criminal justice information (CJI).

The U.S. Criminal Justice Information Services (CJIS) Security Policy has established minimum security requirements and controls to protect criminal justice information such as biometric data, digital evidence and electronic criminal records. The Federal Government does not provide a formal CJIS Security Policy assessment or certification process. Instead, individual law enforcement agencies are responsible for ensuring their IT systems and practices comply with the Security Policy.

Law enforcement agencies can use Wasabi to store and maintain CJI in accordance with the CJIS Security Policy statute. Wasabi uses security best practices and technologies to ensure the physical security of its facilities and to maintain the privacy, security and integrity of electronic data and digital records. In addition, following a thorough audit, the Wasabi service was awarded the official CJIS ACE Compliance Seal by Diverse Computing, a trusted third-party law enforcement agency solution provider with deep CJIS audit and compliance expertise.

This white paper provides an overview of the Criminal Justice Information Services Security Policy and explains how Wasabi helps law enforcement agencies comply with CJIS guidelines for safeguarding the privacy of criminal justice information.

Introduction – CJIS Security Policy Overview

The Criminal Justice Information Services Division of the FBI gives federal, state and local law enforcement and criminal justice agencies controlled access to a wide range of criminal justice information such as digital fingerprint records, arrest and stolen property reports, criminal records, and digital evidence such as dashboard and body-worn camera video.

A wide variety of agencies, external organizations and individuals may need to access CJI. To that end, the CJIS has established a Security Policy defining the minimum set of security controls required for interacting with CJI. The CJIS Security Policy applies to every individual—contractor, private entity, non-criminal justice agency representative, or member of a criminal justice entity—with access to, or who administers criminal justice services and information including private contractors such as cloud service providers. All private contractors who process CJI must sign the CJIS Security Addendum, a uniform agreement that ensures the contractor's IT systems and practices are consistent with the CJIS Security Policy.

While the CJIS provides uniform information security requirements, guidelines, and agreements, the Security Policy is left to the individual states and local jurisdictions to interpret. Specific administrative, technical and contractual requirements vary from state to state, and from locality to locality.

CJIS Security Policy Data Privach and Security Implications

The latest version of the CJIS Security Policy (version 5.6, issued June 2017) specifies 13 Policy Areas for safeguarding CJI, including provisions for maintaining data security and privacy. Law enforcement agencies must ensure digital information, electronic records, and personally identifiable information (PII) are not deleted improperly, corrupted, tampered with, or disclosed to unauthorized individuals. Agencies must put strong security systems and practices in place to protect access to confidential data and to safeguard the integrity of electronic records throughout their lifecycle. The rules apply to data and records maintained on-premises, in a hosted facility (colocation center), or in the cloud.

The CJIS does not offer a formal Security Policy accreditation process. The onus is on the individual agency to ensure its IT systems and practices comply with state and local CJIS data privacy and security requirements.

Wasabi engaged Diverse Computing, a respected third-party law enforcement agency solution provider to evaluate Wasabi's security architecture, systems and practices for CJIS Security Policy compliance. Diverse Computing solutions are used by of 1,600 agencies across the U.S. and the company is a recognized authority in CJIS audit and compliance. After a thorough review, the company awarded Wasabi its official CJIS ACE Compliance Seal.

Wasabi Hot Storage Overview

Wasabi hot storage is affordable, fast and reliable cloud object storage—for any purpose. Unlike legacy cloud storage services with confusing storage tiers and complex pricing schemes, Wasabi hot storage is easy to understand and implement, and cost-effective to scale. One product, with predictable and straightforward pricing, supports virtually every cloud storage application.

Law enforcement agencies can use Wasabi for:

- Low-cost primary storage for on-premises or cloud-based applications
- Economical secondary storage for backup, disaster recovery in the cloud, or data migration initiatives
- Affordable and reliable archival storage for long-term data retention

Wasabi hot storage is ideal for a wide variety of law enforcement agency applications including:

- Electronic records storage and retention
- Digital evidence preservation
- Body, dashboard and surveillance camera video retention
- Electronic imaging and biometric data storage

Ensuring CJIS Security Policy Compliance with Wasabi Hot Storage

Law enforcement agencies can use Wasabi to store and maintain CJI in accordance with CJIS security regulations. The Wasabi cloud storage service is engineered to ensure the protection, privacy and integrity of customer data. The service is built and managed according to security best practices and standards, with CJIS security guidelines in mind, and has received the CJIS ACE Compliance Seal from Diverse Computing.

Wasabi takes a "defense-in-depth" approach, employing multiple layers of security to address relevant CJIS Security Policy Areas. Wasabi ensures the physical security of its data centers; institutes strong authentication and authorization controls for all its cloud compute, storage and networking infrastructure; and encrypts data at rest and in transit to safeguard CJI.

Physical Security

The Wasabi service is hosted in premier Tier IV data center facilities that are highly secure, fully redundant, and certified for SOC-2 and ISO 27001 compliance. Each site is staffed 24/7/365 with on-site security personnel to protect against unauthorized entry. Security cameras continuously monitor the entire facility—both indoors and outdoors. Biometric readers and two-factor or greater authentication mechanisms secure access to the building. Each facility is unmarked so as not to draw attention from the outside.

Secure Network Architecture

Wasabi employs advanced network security elements, including firewalls and other boundary protection devices to monitor and control communications at internal and external network borders. These border security devices segregate customers and regulate the flow of communications between networks to prevent unauthorized access to Wasabi infrastructure and services.

Data Privacy and Security

Wasabi supports a comprehensive set of data privacy and security capabilities to prevent unauthorized disclosure of CJI. Strong user authentication features tightly control access to stored data. Access control lists (ACLs) and administratively defined policies selectively grant read/write and administrative permissions to users, groups of users, and roles.

Wasabi encrypts data at rest and data in transit to prevent leakage and ensure privacy. All data stored on Wasabi is encrypted by default to protect data at rest. And all communications with Wasabi are transmitted using HTTPS to protect data in transit.

Data Durability and Protection

Wasabi hot storage is engineered for extreme data durability and integrity. Wasabi provides eleven 9s object durability, protecting data against hardware failures and media errors. In addition, Wasabi supports an optional data immutability capability that protects data against administrative mishaps or malicious attacks.

An immutable object cannot be deleted or modified by anyone—including Wasabi. Wasabi data immutability protects the integrity of CJI, mitigating the most common causes of data loss and tampering including accidental file deletions, viruses and ransomware.

Customer Responsibilities

Wasabi customers typically interface with the Wasabi service using third-party file management applications and backup tools. To ensure CJIS Security Policy compliance, IT personnel must ensure the storage management tools and applications they use are configured to take advantage of Wasabi security features. For example, HTTPS must be enabled to encrypt data in transit. In addition, customers must encrypt all content and data (with the exception of surveillance, bodycam and dashboard cam video) prior to uploading it to Wasabi.

Law enforcement IT organizations must also ensure they have strong security systems and practices in place to safeguard other elements of their on-premises and cloud-based infrastructure. The Wasabi storage service is typically employed as part of a larger public or hybrid cloud IT implementation that includes multiple compute, storage and networking components.

CJIS Security Addendums

All private contractors (including cloud service providers) who process CJI must sign the CJIS Security Addendum. Wasabi will sign CJIS Security Addendums as required by state or local law.

Conclusion

The CJIS Security Policy introduces stringent data privacy and security requirements for law enforcement agencies. The CJIS does not provide formal Security Policy certification mechanisms, so the onus is on every law enforcement agency to ensure its IT systems and practices comply with state and local statutes.

Wasabi's cloud storage service ensures the protection, privacy, and integrity of criminal justice information, helping agencies comply with the CJIS Security Policy. Wasabi ensures the physical security of its data centers, employs strong authentication and authorization controls to safeguard infrastructure and services, and encrypts data at rest and in transit to prevent unauthorized information disclosure.

Wasabi is typically used in conjunction with other compute, storage and networking platforms and services. Law enforcement agencies must implement strong security systems and practices across all on-premises and cloud-based infrastructure to fully protect CJI and comply with the CJIS Security Policy requirements.

Additional Information

For additional information about CJIS and Wasabi consult the following resources:

- FBI CJIS website
- CJIS Security Policy resource center
- CJIS Solution Page

About Wasabi

Wasabi is the hot cloud storage company delivering low-cost, fast, and reliable cloud storage. Wasabi is 80% cheaper and 6x faster than Amazon S3, with 100% data immutability protection and no data egress fees.

Created by Carbonite co-founders and cloud storage pioneers David Friend and Jeff Flowers, Wasabi is on a mission to commoditize the storage industry. Wasabi is a privately held company based in Boston, MA.

Tel 1-844-WASABI-1
Email info@wasabi.com

hot cloud storage

www.wasabi.com