Microsoft

Using Microsoft Azure Government for Police Body-Worn Cameras

Many law enforcement agencies are weighing their options around the implementation of body-worn cameras. Evidence suggests that using this type of surveillance dramatically reduces use-of-force complaints, improves safety for officers and private citizens, creates better community relationships, and strengthens evidence documentation.

Microsoft and its broad network of body-worn camera partners are working closely with agencies to deliver solutions that support the requirements for digital video storage, media management, and the Criminal Justice Information Services (CJIS) Security Policy.

Criminal Justice Information Services (CJIS) Security Policy

Microsoft Azure Government goes above and beyond industry standards to deliver a contractual commitment to the CJIS Security Policy for its customers. This level of service includes conducting personnel security background checks, providing security-awareness training, undergoing regular formal audits, and implementing thorough security-incident response procedures.

CJIS contractual steps:

1. CJIS Information Agreement	2. FBI CJIS Security Addendum	3. Customer enrollment agreements
• State level; signed by state CJIS officer and Microsoft • Aggregates the right to examine (audit) • Aggregates adjudication (background check)	• Signed by Microsoft • Immutable document/standard set by FBI • Public validation of Microsoft commitment	• Executed at customer level • References 'aggregated' responsibilities in CJIS Information Agreement • Commitment realized at time of customer deployment

Media asset protection

Achieving compliance support for any media service requires meeting industry standards for the transfer, storage, and delivery of content. Azure Government delivers a robust solution designed to exceed U.S. government standards, utilizing powerful resources such as AES encryption and Microsoft PlayReady Digital Rights Management (DRM) and to keep assets well-protected during upload, while at rest in storage, and during playback.

Transfer

Azure Government enables multiple video formats and supports a variety of playback devices and resolutions. In addition, agencies can upload content from building and city surveillance systems, interview rooms, and network videos recorders (NVR).

- Enables secure video writing to the cloud and directly from the source with encrypted Virtual Private Network (VPN) over the Internet
- Offers pay-as-you-go pricing for predictable operating expenses

Store

Azure Government provides the flexibility and resiliency to securely store, backup, and retrieve large amounts of unstructured data, such as media files with Azure Blobs. Agencies can also control access from the Internet, permit traffic only to customer-defined endpoints, and provide load balancing and Network Address Translation (NAT) at the cloud-access layer.

- Stores data in the cloud 3x to protect against hardware failure in a geographic region; uses geo-replication to further protect against regional impacts such as natural disasters
- Is operated by U.S. citizens and adheres to a broad set of security and privacy policies

Deliver

Azure Government helps law enforcement personnel view data stored in the cloud. With Azure Media Services, agencies can choose from a collection of Microsoft and third-party components and technologies for media discovery and analytics scenarios that are curated, ready-to-use, and integrated into a single platform to deliver content to any device, anywhere, anytime.

- Securely encodes and packages video or audio for delivery to a wide array of device endpoints
- Offers live video streaming or on-demand viewing at Olympic scale using Azure Media Services and encrypts and protects content with DRM