Discussion of Warranties, Agreements, Terms and Conditions

Full details regarding warranties for Utility's platform solution can be accessed in the documents described below and through the links provided.

Utility EOS Hardware Warranty

The Utility EOS body camera Hardware Warranty describes the warranty provided on Utility's EOS devices. Under this agreement, Utility guarantees that its devices are free from defects, and agrees to replace any parts or devices that have not been broken under malicious intent or subjected to extreme conditions. *Please refer to the Service Agreement below*.

Utility Rocket Hardware Warranty

The Utility Rocket IoT Hardware Warranty describes the warranty provided on Utility's Rocket IoT manufactured devices. Under this agreement, Utility guarantees that its devices are free from defects, and agrees to replace any parts or devices that have not been broken under malicious intent or subjected to extreme conditions. *Please refer to the Service Agreement below*.

Service Level Agreement

The Service Level Agreement describes the levels of service, software agreement, and terms andconditions that the client will receive from Utility (the supplier).

The client depends on Utility IT equipment, software and services, some of which are of critical importance to the client. As such, the SLA sets out what levels of availability and support the client is guaranteed to receive, forms an important part of the contract, and enables the two parties to work together effectively.

The Utility "System as a Service" Agreement (SaaS Agreement) describes Utility's service commitment of system provided to client. The document details the services that will be provided, the environment under which the software will operate, how the software may be upgraded, the uptime of the service, and the hours where support can be reached. Further, the document details permitted usage of the software, restrictions on software usage, the fees that will be assessed, and the terms under which they are due.

The Utility Terms and Conditions detail the conditions under which Utility conducts sales of its proprietary products. This includes liability limitations, logistics of product transfer, protection of intellectual property, payment information, and the jurisdiction under which legal action may be taken. *Due to page restrictions, we have not included the Service Agreement. We are happy to provide it upon request.*

Data Security

Utility Data Security Documentation

Utility's Data Security Documentation is a summary overview of the security, performance, reliability, and scalability for Utility hardware, software as a service, and hosting environment. Utility uses a combined hardware and software defense-in-depth architecture to protect theconfidentiality, integrity, and availability of customer information. The security and performance architecture adapts automatically to changes in technology, internal and external threats tonetworks and applications, and to client operations. Third party security risk evaluations are performed to ensure the effectiveness of our procedures, methodology, equipment, facilities, and personnel. *The client may request Utility's Data Security Documentation after contract award.*

Amazon Web Services (AWS)

Utility purchases services from Amazon Web Services to provide backend processing and storage for its software packages. The following documentation explains Amazon's security standards, obligations, and assurances provided for the safety, security, and accessibility of all client data.

AWS Service Organization Controls 3 Report

The AWS Service Organization Controls 3 Report provides an overview of how Amazon maintains operation of technology, people, data, and infrastructure supporting its AWS services.

AWS Overview of Security Processes

The AWS Overview of Security Processes describes the systems put in place to assure that Amazon is able to meet the high service and security standards that its clients demand. This includes an in-depth review of how Amazon maintains both physical and electronic security over its cloud services.

CJIS Compliance on AWS

The CJIS Compliance on AWS document provides Amazon's perspective on and approach to being fully compliant with Criminal Justice Information Standards (CJIS). These standards are set nationally by the Federal Bureau of Investigation (FBI) for information storage, usage, and sharing within law enforcement.

Procurement Information on CJIS Compliance

Utility's digital evidence platform is a Cloud-based solution that meets and exceeds standards for CJIS Compliance and offers a scalable digital management and storage platform with high availability and dependability. Cloud-based solutions outperform the alternate — on-premise storage — and protect the confidentiality, integrity, and availability of criminal justice information and data. Cloud-based solutions are fundamental to credibility, by projecting transparency, and preserving your Community's trust.

Security *Cloud-based storage is unparalleled security and redundancy.*

Rest assured that your video data in the Cloud is much more secure than what lives on a tower or in your server room. Those with the most to protect – from leading defense agencies to global companies - have chosen Cloud-based storage. There is a long and successful track record of law enforcement customers using the Cloud for a wide range of sensitive federal and state government workloads, including CJIS data.

Reliability *Cloud-based storage provides unparalleled reliability.*

A Cloud-based provider platform virtually eliminates the risk of downtime. Amazon S3, for example, isdesigned to provide 99.999999999% durability and 99.99% availability over a given year, redundantly stored on multiple devices across multiple facilities in geographically separate locations. It is an illusion to think criminal justice information is more reliable in a Department's on-premises local storagefacility. One incident with rebuilding 'on-prem' crashed servers - and its unbudgeted cost - is all it takes to prove it. You don't want to be that case study.

Budget *Without the Cloud, agencies spend a lot of their IT budget to manage storage.*

That takes funding off the streets and requires hiring that is difficult to defend and pay for. With cloud storage, that's no longer an issue. Now, you can focus on how the police camera video solution will help you further yourlaw enforcement mission. The video IT piece belongs to someone else.

Flexibility *Scale up and down to meet your current needs.*

In business, this flexibility is key. In government, new expenditures are tough to defend and pay for. With Cloud-based solutions, you no longer have to build for the future, or be constrained by decisions made or contracts signed in the past. You can adjust your video storage expenditures to meet your agency's immediate needs.

Resiliency *No law enforcement agency can ignore resiliency threats.*

Yet few have the resources alone to deliver security when your Community itself is in harm's way. Cloud providers' resiliency programs identify, respond to, and recover from a major incident, with contingency management, business continuity, and disaster recovery plans. Cloud-based providers identify critical system components required to maintain the availability of the system and recover services in the event of an outagefrom physically separate locations, maintain authoritative backups, employ continuous infrastructure capacity planning, and monitor to ensure successful replication. Cloud-based resiliency means you can keep your promises "To Serve" when most needed in your Community.

Procurement Information on CJIS Compliance

Continued

Cost -*Using Cloud technology reduces your storage and maintenance fees.*

No more servers, software, and update fees. Many of the hidden costs typically associated with video storage, (and with software implementation, customization, hardware, maintenance, and training) are rolled into a transparent subscription fee. No more need to explain any unanticipated cost – you are covered.

It's Mobile *Internet standards and web services allow you to interconnect services.*

Today's cloud-based solutions for law enforcement are managed under secure controls, and in continuous alignment with federal, state and local law enforcement Criminal Justice Information Security (CJIS) policy. This means that you can centralize your law enforcement video and access it from anywhere in the world, onany computer or mobile device, at any time. Your mission-critical video information is fully mobile.

A UNIVERSE OF SOLUTIONS
ADVANCED BODY CAMERAS
DIGITAL EVIDENCE MANAGEMENT
IN-CAR VIDEO/ALPR SYSTEM
WIRELESS COMMUNICATION SOLUTION
UTILITY