STATE OF DELAWARE
EXECUTIVE DEPARTMENT
OFFICE OF MANAGEMENT AND BUDGET

State of Delaware

Body Cameras

Request for Information

Request No. GSS 15761-BODYCAM

September 23, 2015

- Deadline to Respond -
October 6, 2015
1:00 PM (Local Time)

Date: September 23, 2015

REQUEST for INFORMATION NO. GSS15761-BODYCAM

This Request for Information (RFI) will **not** result in award of a competitively bid contract.

The State of Delaware, Government Support Services, is seeking market information on body cameras to be worn by law enforcement officials. The information gathered may or may not lead to the issuance of a Request for Proposals.

The State of Delaware has determined the most effective and efficient information gathering approach for this particular need is to solicit printed documentation from manufacturers and suppliers of body cameras **in conjunction with** a 30 – 45 day trial period of the total solution. Respondents will be asked to provide 12 units to be deployed at the direction of the Department of Safety and Homeland Security as a part of the trial period for evaluation. Responses to this Request for Information will remain confidential until such time as a determination is made on whether the State will move forward with a Request for Proposal. If a decision is made to move forward with a Request for Proposal, the responses to this Request for Information will remain confidential until the completion of the Request for Proposal process.

All responses to this Request for Information shall be submitted in a sealed envelope **clearly displaying the request for information number and vendor name** by October 6, 2015 at 1:00 (Local Time).

Responses must be mailed to:

State of Delaware
Government Support Services
RFI #GSS15761-BODYCAM
100 Enterprise Place, Suite 4
Dover, DE 19904-8202

Please review and follow the information and instructions contained in this Request For Information (RFI). Should you need additional information, please call Bruce Krug at 302-857-4534 or email bruce.krug@state.de.us.

I. Background

To ensure transparency in law enforcement activities, the State of Delaware has identified a need to assess the market options for body cameras to be worn by law enforcement officials throughout the State. Recognizing there is a substantial breadth of offerings in this market sector, the State has determined the most effective way of analyzing the variables is to solicit written materials in conjunction with a 30-45 trial program. Respondents will be asked to provide 12 units to be deployed at the direction of the Department of Safety and Homeland Security as a part of the trial period for evaluation. This approach will allow the State to determine how best to craft requirements related to the procurement of body cameras and associated support equipment and services.

II. Responses to this Request for Information:

A respondent shall provide one (1) paper copy and one (1) electronic copy of its response

III. Definitions

A. Body Camera: A camera capable of capturing real time activities of a law enforcement official that is worn on the enforcement official

B. Data Record**:** A system capable of retaining the images of real time activities captured by the body camera.

C. Cloud**:** An information technology platform allowing for storage of a data record in a manner that does not require the State of Delaware to dedicate brick and mortar square footage to the retention of a data record.

D. System: The body cameras, data record, and technology platform as a whole

IV. Core Body Camera and Data Record Requirements:

A. The State is interested in respondents recommendations related to system functionality for the wearer. The respondent's recommendations will be used to develop specifications for the tactical application of law enforcement officials body cameras.

V. Scope of coverage

A. The respondent must have a system capable of providing coverage for the entire State of Delaware. This includes law enforcement officials at the State, County, and City / Town levels.

VI. Data Record Retention

A. The State is interested in systems that are cloud based.
B. The State must have full access to the data record for information gathering
C. The State is interested in systems that can accommodate evolving policies and procedures relative to the system's use

VII. Trial Period Program Requirements

A. All technology functionality must be capable of complying with RFI Section VI. Core Information Technology and Cloud Requirements
B. All data records will be the property of the State of Delaware
C. The trail period will run for 30-45 days as mutually agreed between the State and the Respondent
D. Respondents should limit the trial period and devices to a fixed number and recommend geographical demonstration of functionality in consultation with the Department of Safety and Homeland Security (DSHS).

VIII. Core Information Technology and Cloud Compliance Requirements

A. The critical requirements are identified in Appendix A of this RFI

IX. Service / Support

A. Any response to this RFI must identify an organizational structure that includes the ability for 24/7 service and support for all components of the system.

Appendix A

NON-PUBLIC DATA OWNED BY THE STATE OF DELAWARE

State of Delaware Cloud and/or Offsite Hosting Specific Terms and Conditions

	Terms and Conditions Clauses 1-10 are mandatory for every engagement. Exceptions will be considered non-compliant and non-responsive.
1	**Data Ownership:** The State of Delaware shall own all right, title and interest in its data that is related to the services provided by this contract. The Service Provider shall not access State of Delaware User accounts, or State of Delaware Data, except (i) in the course of data center operations, (ii) response to service or technical issues, (iii) as required by the express terms of this contract, or (iv) at State of Delaware's written request.
2	**Data Protection:** Protection of personal privacy and sensitive data shall be an integral part of the business activities of the Service Provider to ensure that there is no inappropriate or unauthorized use of State of Delaware information at any time. To this end, the Service Provider shall safeguard the confidentiality, integrity, and availability of State information and comply with the following conditions: a) All information obtained by the Service Provider under this contract shall become and remain property of the State of Delaware. b) At no time shall any data or processes which either belongs to or are intended for the use of State of Delaware or its officers, agents, or employees, be copied, disclosed, or retained by the Service Provider or any party related to the Service Provider for subsequent use in any transaction that does not include the State of Delaware.
3	**Data Location**: The Service Provider shall not store or transfer non-public State of Delaware data outside of the United States. This includes backup data and Disaster Recovery locations. The Service Provider will permit its personnel and contractors to access State of Delaware data remotely only as required to provide technical support.
4	**Encryption:** a) The Service Provider shall encrypt all non-public **data in transit** regardless of the transit mechanism. b) For engagements where the Service Provider stores sensitive personally identifiable or otherwise confidential information, this data shall be **encrypted at rest.** Examples are social security number, date of birth, driver's license number, financial data, federal/state tax information, and hashed passwords. The Service Provider's encryption shall be consistent with validated cryptography standards as specified in National Institute of Standards and Technology FIPS140-2, Security Requirements. The key location and other key management details will be discussed and negotiated by both parties. When the Service Provider cannot offer encryption at rest, they must maintain, for the duration of the contract, cyber security liability insurance coverage for any loss resulting from a data breach in accordance with the Cloud and Offsite Hosting Policy. Additionally, where encryption of data at rest is not possible, vendor must describe existing security measures that provide a similar level of protection.
5	**Breach Notification and Recovery**: Delaware Code requires public breach notification when citizens' personally identifiable information is lost or stolen. Reference: 6 Del. C. § 12B-102. Additionally, unauthorized access or disclosure of non-public data is considered to be a breach. The Service Provider will provide notification without unreasonable delay and all communication shall be coordinated with the State of Delaware. When the Service Provider or their sub-contractors are liable for the loss, the Service Provider shall bear all costs associated with the investigation, response and recovery from the breach including but not limited to credit monitoring services with a term of at least 3 years, mailing costs, website, and toll free telephone call center services. The State of Delaware shall not agree to any limitation on liability that relieves a Contractor from its own negligence or to the extent that it creates an obligation on

	Terms and Conditions Clauses 1-10 are mandatory for every engagement. Exceptions will be considered non-compliant and non-responsive.
	the part of the State to hold a Contractor harmless.
6	**Notification of Legal Requests**: The Service Provider shall contact the State of Delaware upon receipt of any electronic discovery, litigation holds, discovery searches, and expert testimonies related to, or which in any way might reasonably require access to the data of the State. The Service Provider shall not respond to subpoenas, service of process, and other legal requests related to the State of Delaware without first notifying the State unless prohibited by law from providing such notice.
7	**Termination and Suspension of Service:** In the event of termination of the contract, the Service Provider shall implement an orderly return of State of Delaware data in CSV or XML or another mutually agreeable format. The Service Provider shall guarantee the subsequent secure disposal of State of Delaware data. a) Suspension of services: During any period of suspension or contract negotiation or disputes, the Service Provider shall not take any action to intentionally erase any State of Delaware data. b) Termination of any services or agreement in entirety: In the event of termination of any services or agreement in entirety, the Service Provider shall not take any action to intentionally erase any State of Delaware data for a period of 90 days after the effective date of the termination. After such 90 day period, the Service Provider shall have no obligation to maintain or provide any State of Delaware data and shall thereafter, unless legally prohibited, dispose of all State of Delaware data in its systems or otherwise in its possession or under its control as specified in section 7d) below. Within this 90 day timeframe, vendor will continue to secure and back up State of Delaware data covered under the contract. c) Post-Termination Assistance: The State of Delaware shall be entitled to any post-termination assistance generally made available with respect to the Services unless a unique data retrieval arrangement has been established as part of the Service Level Agreement. d) Secure Data Disposal: When requested by the State of Delaware, the provider shall destroy all requested data in all of its forms, for example: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST) approved methods and certificates of destruction shall be provided to the State of Delaware.
8	**Background Checks:** The Service Provider shall conduct criminal background checks and not utilize any staff, including sub-contractors, to fulfill the obligations of the contract who has been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration for a minimum of 1 year is an authorized penalty. The Service Provider shall promote and maintain an awareness of the importance of securing the State's information among the Service Provider's employees and agents.
9	**Data Dictionary:** Prior to go-live, the Service Provider shall provide a data dictionary in accordance with the State of Delaware Data Modeling Standard.
10	**Security Logs and Reports:** The Service Provider shall allow the State of Delaware access to system security logs that affect this engagement, its data and or processes. This includes the ability for the State of Delaware to request a report of the records that a specific user accessed over a specified period of time.