REQUEST FOR PROPOSAL

RFP 3273

Body Worn Cameras

COPY – TECHNICAL PROPOSAL

Closing Date and Time: September 28th, 2016, 2pm

State of Nevada, Purchasing Division
515 E. Musser Street, Suite 300
Carson City, NV 89701

ATTN: Ronda Miller
Purchasing Officer II
rlmiller@admin.nv.gov
775.684.0182

Presented by:

Utility Associates, Inc

250 E. Ponce de Leon Avenue
Decatur, GA 30030
www.utility.com
404.816.0300

UTILITY

September 28, 2016

Ronda Miller
State of Nevada, Purchasing Division
515 E. Musser Street, Suite 300
Carson City, NV 89701

Subject: Request for Proposal 3273 for Body Worn Cameras

Thank you for the opportunity to present information on the BodyWorn™ camera and digital evidence solution by Utility. Utility is honored that the State of Nevada Department of Public Safety and Nevada Highway Patrol are considering our Company to provide their officers with our BodyWorn™ Camera System.

We are proud that our BodyWorn™ has been recognized as the industry's leading Generation 2 body worn camera solution for law enforcement agencies across the US. In fact, Utility is the sole vendor in this category winning the 2016 AWS City on a Cloud Innovation Challenge. We are totally committed to the success of body worn cameras for the State of Nevada Department of Public Safety and Nevada Highway Patrol (NHP).

BodyWorn™ has capabilities that provide unique benefits to State of Nevada and NHP:

- **Automatic, Policy-Based Smart Recording:** In addition to a manual Bluetooth remote, recording can be triggered automatically by custom policies your department creates: sensors in the vehicle, remote activation from dispatch or a supervisor, running and acceleration, entry into a designated mapped Action Zone or Geofence. As a result, more video is captured, freeing officers to focus on their jobs. This system can be integrated with your CAD system to institute dispatch policy and provide you with additional situational awareness tools.
- **Secure, Immediate Wireless Upload to the Cloud:** Video evidence uploads immediately upon being taken, in an encrypted file format to a secure cloud, resulting in reliable evidence capture and enhanced situational awareness between the officer and dispatch. This eliminates the added risk of losing video evidence by waiting until end of a shift to connect to a docking station.
- **Smart Waypoints:** A body worn camera's embedded storage is typically the least secure location within the video data ecosystem. Utility moves video data as fast as it is collected (in real-time, on-the-fly) from the BodyWorn camera to available secure storage Smart Waypoints within Utility's provided Eco-System. This eliminates the need for docking stations, their cost and risk of data loss, and protects chain-of-custody.
- **Real-Time Communications:** Utility's BodyWorn™ camera can communicate time sensitive information including BOLO, Amber, Silver and Officer Down alerts to the officer and to dispatch. Using the real-time, map-based situational awareness tools can improve officer safety and save lives.

- **Functional Fusion to the Uniform:** Traditional clip-on cameras bounce, are bulky and fall off. Utility's camera is built into the officer's uniform, is seamless, and reliably captures video evidence.
- **Smart, Automatic Redaction Capability**: Utility's redaction for Body and In-Vehicle Cameras address important privacy and FOIA concerns, but also allows the City to control and manage data storage costs. This cost savings can make all the difference, affording the most value for dollars spent.
- **Synchronized BodyWorn and In-Car video:** The BodyWorn™ and Rocket-IoT™ in-car video recording system seamlessly integrates into the same incident for Chain-of-Custody and playback review.

Utility's BodyWorn™ is scaleable, user-friendly, requires no ancillary devices, and no additional hardware or software. It is a complete system run on a familiar Android computing device porting proven video software in development and use for more than a decade. Moreover, BodyWorn™ is able to integrate with our Rocket™ mobile hotspot vehicle router, and our Rocket-IoT™ in-car video solution, for maximum interoperability.

We are privileged to work with the State and the Department on this project. We understand the goals and objectives of the Department in this important effort. We pledge to provide the optimum technology solution the State of Nevada Department of Public Safety needs, with the highest level of responsiveness in its implementation.

We are excited to work together and look forward to making your Body Worn Cameras program a resounding success!

Sincerely,

Christopher R. Lindenau, Chief Revenue Officer
Utility Associates, Inc.
crl@utility.com
770-500-2494

Amazon Web Services Names BodyWorn™ as 2016 Innovation Challenge Award Winner

Utility, Inc. has been recognized by Amazon as a winner of the 2016 Amazon Web Services (AWS) City on a Cloud Innovation Challenge. Utility's innovative use of Amazon cloud storage for its police body camera, in-vehicle recording and video redaction solutions were judged on uniqueness, number of users and the availability to governments in various regions that differ in size and scope. The award was presented at the 2016 Amazon AWS Public Sector Summit in Washington, D.C.

Robert McKeeman, CEO of Utility said "Being named as a winner by Amazon Web Services for our innovative solutions to solve a government challenge solidifies our work to meet our mission to make police officers' jobs safer, while protecting Privacy for Police Officers and Citizens, and enabling Police Accountability and Transparency. Through our partnership with Amazon Web Services, we provide our customers with a very reliable and cost-effective video management and redaction solution."

"I was honored to accept the award on behalf of Utility. However, the award was earned by our entire team who design, develop, sell, support, install, manage, and provide administration for our BodyWorn™, Rocket IoT™, in-vehicle recording and Smart Redaction™ solutions."

Utility was granted the award in the Partners in Innovation category, which goes to a technology partner that has deployed an innovative solution to solve a government challenge.

Utility's BodyWorn™ is a smart, policy-based, body-worn camera solution that allows police departments to set video recording policies with confidence the policies will be followed reliably and consistently. Officer Down Emergency reporting and BOLO alerts protect officer safety. Video is immediately and securely uploaded to the Amazon AWS Cloud automatically as it is being recorded. The Amazon-hosted AVaiL Web™ Evidence Management System allows users to categorize, search, and view video evidence, report officer and vehicle locations, and automatically redact video evidence, all through a web browser.

The AWS Cloud Storage is widely recognized as one of the largest and most sophisticated in the world, with ten times the video storage capacity of the next ten largest cloud storage providers combined. Video captured on Utility's BodyWorn™ camera is encrypted on the camera, in transit to, and in the AWS Cloud with AES-256 encryption, thus protecting the security and Chain of Custody of legal evidence at all levels in the Evidence Ecosystem.

Utility's customers can choose to access to Amazon AWS-based e-discovery, e-citation, secure image management, mobile forensics, crime forecasting, major risk event management, public records management, backup, archival and disaster recovery tools on the Amazon AWS Cloud.

TITLE PAGE

State of Nevada, Purchasing Division
RFP 3273 for Body Worn Cameras for Nevada Highway Patrol

Part IA – Technical Proposal	
RFP Title:	Body Worn Cameras
RFP:	3273
Vendor Name:	Utility Associates, Inc.
Address:	250 E. Ponce de Leon Ave, Suite 700, Decatur GA 30030
Opening Date:	9/28/16
Opening Time:	2:00 PM

State of Nevada
Request for Proposal: 3273 for Body Worn Cameras

Hardcopy Documents submitted:

- *Cost Proposal – One (1) Original marked 'MASTER' and four (4) identical copies...in a sealed package*
- *Confidential Financial Information - One (1) Original marked 'MASTER' and one (1) identical copy...in a sealed package*
- *Technical Proposal - One (1) Original marked 'MASTER' and four (4) identical copies...in a sealed package*

One Required MASTER Flash Drive submitted…in a sealed package:

- *One (1) 'MASTER' Flash Drive, containing: Part 1A- Technical Proposal; and Part II – Cost Proposal (NOTE: Utility does not require a Part 1B – Confidential Technical Proposal - Not Applicable)*

TECHNICAL PROPOSAL

Before Tab I Letter of Transmittal
Utility BodyWorn™ Named 2016 Innovation Challenge Award Winner by AWS

Tab I Title Page

Tab II Table of Contents

Tab III Vendor Information Sheet

Tab IV State of Nevada Documents

- Signature Page – Acknowledgment of Amendments
- Attachment A: Confidentiality and Certification of Indemnification
- Attachment C: Vendor Certifications
- Copies of Vendor Licenses and/or Hardware/Software Maintenance Agreements
  - Hardware Warranty – BodyWorn™
  - Hardware Warranty – Rocket-IoT™
  - Software as a Service (SaaS)
  - Utility Terms and Conditions

Tab V Attachment B

- Technical Proposal Certification of Compliance with Terms and Conditions of the RFP
  - Exceptions to Contract Form D, or Insurance Schedule E (- Not Applicable -)

Tab VI Scope of Work

- Attachment K: In-Car Video Comply Checklist
- Attachment L: Body Worn Specifications
- Utility Responses (***in bold/italics***) to Questions in the Scope of Work Narrative (Attachment K and Attachment L), including 3.12.15 Installation

Tab VII Company Background and References

- Utility Responses (***in bold/italics***) to Company Background Questions
- Utility Responses (***in bold/italics***) to Question in RFP Sections for:
  - 3.0 General Requirements and Provisions, and 3.2 General Requirements
  - 3.3 Project Management and Customer Service Questions
  - 3.6 Training, and 3.12.14 Training/Documentation

Tab VIII Attachment G: Proposed Staff Resumes

- Staff Resumes in the State of Nevada format

Tab IX Other Information Material

- Product Data Sheet for the BodyWorn™ and Rocket-IoT™ Solutions
- Research of Interest to State of Nevada Department of Public Safety/Nevada Highway Patrol

State of Nevada
Request for Proposal: 3273 for Body Worn Cameras

Table of Contents: (continued)

COST PROPOSAL (separate sealed package)
Tab I Title Page
Tab II Cost Proposal: Attachment H: Cost Schedule Body Worn Cameras; Cost Schedule In-Car Video
Tab III Attachment I: Cost Proposal Certification of Compliance with Terms and Conditions of RFP

CONFIDENTIAL FINANCIAL INFORMATION (separate sealed package)
Tab I Title Page
Tab II Financial Information and Documentation

Table of Contents: (continued)

Tab IX Other Information Material

- Product Data Sheet for BodyWorn™
- Mounting Options Data Sheet for BodyWorn™
- BodyWorn™ User Guide
- Product Data Sheet for SMART REDACTION™
- Product Data Sheet for AVaiL Web™
- Product Data Sheet for Rocket-IoT™
- Product Data Sheet for Multi-Band Attenna
- Product Data Sheet for Yard Smart Waypoint™
- Product Data Sheet for Rocket™ Locker

- Research of Interest to State of Nevada Department of Public Safety/ Nevada Highway Patrol
    i. Generation 2 Body-Worn Cameras and the Evidence EcoSystem
    ii. 5 Year Total Cost of Ownership
    iii. Police Transparency Versus Video Redaction Cost and Lead-Time
    iv. Police Officer Legal Risk from a Wide Field of View
    v. Eliminating Racial Bias in Recording Body-Worn Videos

- Public Opinion Polling Results for Body Cameras of Interest to State of Nevada Department of Public Safety/ Nevada Highway Patrol
    vi. Poll Results American Voters' Views on Body Cameras
    vii. Poll Results American Voters' Views Toplines
    viii. Body Cameras Poll A Detail
    ix. Body Cameras Poll B Detail

VENDOR INFORMATION SHEET FOR RFP 3273

Vendor Must:

A) Provide all requested information in the space provided next to each numbered question. The information provided in Sections V1 through V6 will be used for development of the contract;

B) Type or print responses; and

C) Include this Vendor Information Sheet in Tab III of the Technical Proposal.

V1	Company Name	Utility Associates, Inc.

V2	Street Address	250 E. Ponce de Leon Avenue, Suite 700

V3	City, State, ZIP	Decatur, GA 30030

V4	Telephone Number		
	Area Code: 404	Number: 816-0300	Extension:

V5	Facsimile Number		
	Area Code: 404	Number: 795-0525	Extension:

V6	Toll Free Number		
	Area Code:	Number:	Extension:

V7	***Contact Person for Questions / Contract Negotiations, including address if different than above***
	Name: Chris R. Lindenau
	Title: Chief Revenue Officer
	Address: 250 E. Ponce de Leon Avenue, Suite 700
	Email Address: crl@utility.com

V8	Telephone Number for Contact Person		
	Area Code: 770	Number: 500-2494	Extension:

V9	Facsimile Number for Contact Person		
	Area Code: 404	Number: 795-0525	Extension:

V10	***Name of Individual Authorized to Bind the Organization***	
	Name: Chris R. Lindenau	Title: Chief Revenue Officer

V11	Signature ***(Individual must be legally authorized to bind the vendor per NRS 333.337)***	
	Signature:	Date: 9/26/16

State of Nevada
Department of Administration
Purchasing Division
515 E. Musser Street, Suite 300
Carson City, NV 89701

Brian Sandoval
Governor

Jeffrey Haag
Administrator

SUBJECT:	Amendment 1 to Request for Proposal 3273
RFP TITLE:	Body Worn Cameras
DATE OF AMENDMENT:	September 14, 2016
DATE OF RFP RELEASE:	August 24, 2016
OPENING DATE:	September 28, 2016
OPENING TIME:	2:00 PM
CONTACT:	Ronda Miller, Procurement Staff Member

The following shall be a part of RFP ***3273.*** If a vendor has already returned a proposal and any of the information provided below changes that proposal, please submit the changes along with this amendment. You need not re-submit an entire proposal prior to the opening date and time.

---

1. What is the initial contract term for the project? Are there renewal options available?

   Per section 1.1.6 the initial term of contract will be 2 years, with an option of a 2 year extension.

2. How much budget was allotted for the project?

   $1,260,106 per Senate Bill 111.

3. Has the Department determined a funding source for this effort? If so, please indicate which source will be used.

   Yes, State Highway Fund.

4. Please provide the names of the vendors who provided information for RFI #NHP15-01.

   - **Digital Ally**
   - **L3 Mobile-Vision**
   - **Millenium**
   - **Panasonic**
   - **Point Blank**
   - **Presidio**
   - **Pro-Vision**
   - **Taser**
   - **Utility**
   - **VieVu**
   - **WatchGuard**

5. Section 1.1.6 states "This contract is anticipated to begin December 13, 2016 for a term of two (2) years, with the option of extension for an additional two (2) years." However, within the warranty section 3.5.1.5 it is requested as an option for an additional 4 years beyond first 12 months for maintenance and warranty. Can you please clarify the preferred contract and warranty options?

   The project is anticipated to be completed by 6/30/2017. Ongoing costs, including extended hardware warranties and software maintenance necessary to cover the equipment through a two (2) year period from the date the contract is approved, should be itemized and included in RFP cost responses. If the hardware useful life is three (3) years, costs to cover the equipment for three (3) years (1st 12 months + 2 additional years) should be included but separately identified.

6. Attachment K video system specification 3.12.2 states, "Color LED monitor with audio." Can the MDT (computer in the vehicle) function as the display for the in-car video system?

   DPS/HPD's long term goal is to utilize the MDC to fully control the In-Car Video system in efforts to reduce the amount of equipment in the patrol car. Currently out of the 465 potential users, we have 185 MDC's deployed and an additional 160 scheduled for early 2017. Until we are fully deployed with MDC's, a "Color monitor with audio" must be an available option.

7. Attachment K, 3.12.2 - Can the GPS coordinates be provided by an external router or other device? If NHP has GPS in their vehicles currently, would it be acceptable to get a GPS signal from an existing device rather than adding a separate GPS device and antenna?

   Yes. Currently, DPS/HDP utilizes two modems both made by Feeney Wireless. The first is a Cira X2 GX440 which is in the process of being phased out and the second is a Skyus-X modem. It would be acceptable and preferable to get a GPS signal from our existing devices to minimize the amount of antenna's, as long as all equipment can be shown to be compatible. Partnerships may have to be developed between parties before the sharing of equipment and testing can be accomplished. Vendors would have to work this all out.

8. Attachment K, 3.12.4 states "The DVR shall be capable of recording two video inputs from a powerful zoom, forward-facing camera, and a wide-angle rear-facing camera." Would NHP be willing to accept an HD forward-facing non-zoom camera that provides high enough resolution for video to be enlarged and enhanced after the fact? Traditional in-car video systems that utilize SD cameras require zoom capability to clearly identify objects at distances greater than that of a typical traffic stop, but HD video greatly improves this capability.

   Yes, DPS/HPD would be willing to accept this term.

9. Attachment K, 3.12.4 states "The DVR shall require a security feature (key, admin software rights) to prevent unauthorized users from accessing the on-screen menus to adjust video settings and perform file management functions." Would NHP be willing to accept a system that provided an administratively controlled central configuration management utility as part of the Digital Evidence Management System, which pushes configuration changes wirelessly over cellular or Wi-Fi to the in-car camera system rather than a system that required changes to be made at each DVR?

   Yes, DPS/HPD would be willing to accept this term.

10. Attachment K, 3.12.6 refers to an LCD Monitor. Can the MDT (computer in the vehicle) function as the display for the in-car video system?

DPS/HPD's long term goal is to utilize the MDC to fully control the In-Car Video system in efforts to reduce the amount of equipment in the patrol car. Currently out of the 465 potential users, we have 185 MDC's deployed and an additional 160 scheduled for early 2017. Until we are fully deployed with MDC's, a "Color monitor with audio" must be an available option.

11. Attachment K, 3.12.10 refers to a Video Management System in an on-premise server environment. Would NHP consider a central agency-wide cloud based Digital Evidence Management System that provides additional functionality and security such as the ability to digitally share evidence with an audit trail, the ability to manage any type of digital evidence, perform redaction of video and audio, geographic redundance for all data, as well as other features?

Yes. As per section 3.8.10, DPS/HPD is open to a server based, cloud based or a hybrid solution. 3.12.10 refers to the requirements to be met if a server based solution is proposed.

12. RFP Reference page 10, paragraph 3.2.1.4 - What is meant by a schematic rendering? Can the State provide clarification on what they are expecting to receive in response to this requirement?

Vendors to provide a system diagram, a visual model of the proposed system.

13. RFP Reference page 12, paragraph 3.5.1.5 - Most body worn cameras have a useful life of three years or less. Should vendors include the cost of a camera refresh in the price of the four year extended warranty?

The costs for the body camera hardware refresh / replacement should be itemized separately and supported by a replacement cost schedule under ongoing costs. Since these costs would fall outside of initial project expected to be completed by 6/30/2017, as well as the initial two (2) year contract, vendors should provide a hardware replacement schedule for camera and other hardware replacement required under ongoing costs consistent with their useful life. The State prefers that these costs be separately itemized from the four (4) year extended warranty.

14. RFP Reference page 13, paragraph 3.5.2.9 - Does this statement include hardware warranties and software maintenance, or is it only referring to software maintenance?

It is the intent of the State of pay for warranty and software maintenance in the period the service is incurred, however providing BWC hardware warranties consistent with the lifecycle of the proposed equipment is acceptable. Ongoing costs, for extended hardware warranties through the first two years or the contract should be included in RFP cost responses. If the hardware life is three (3) years, include the hardware warranty costs to cover the equipment for three (3) years (1st 12 months included + 2 additional years) in your response. As part of your response, provide expected the lifecycle for all video system components.

15. RFP Reference page 19, paragraph 3.11.3.6 - Can the State provide examples of automatic triggers, or desired functionality that would be acceptable to meet this specification?

DPS/HDP is interested in any standalone triggers that would activate the BWC without the assistance of the In-Car Video system. Examples include triggers based off a device in the vehicle or BWC that would activate the BWC with the light bar being turned on, the shotgun lock being released, a pre-designated speed being reached or an accelerometer to indicate a crash or foot pursuit just to name a few. Integration is a long term goal which won't be achieved right away, so we are open to any concept that helps reduce the human error aspect to activating the BWC, especially in high stress situations where the officer may forget or not have time to activate their BWC.

16. Can the State please identify how many shifts are operated per Precinct/Location on a 24-hour schedule? For example: 3x10hour shifts, 2x12hour shifts, etc.

Las Vegas and Reno are the only regional offices that operate 24 hours. The Elko regional office and 25 sub-stations operate on days and swing with a majority of the state being on 4x10 hour shifts. Refer to table 3.8.A and 3.8.B on pages 16, 17 and 18 of the RFP for further details of manpower.

17. During an "average" day, how many officers with cameras would be out on each individual shift?

Statewide, we estimate on average dayshift will have 105 offers per day, swing shift 105 officers per day and grave yard 27 officers per day. Refer to table 3.8.A and 3.8.B on pages 16, 17 and 18 of the RFP for additional details.

18. Can the State provide a list of Precincts/Locations?

Northern Command West:

Reno Regional Office
357 Hammill Lane
Reno, Nevada 89511

Carson City Sub-station
911 East Musser St.
Carson City, NV 89701

Fallon Sub-station
975 W. Williams Street
Fallon, NV 89406

Fernley Sub-station
770 W. Main Street
Fernley, NV 89408

Hawthorne Sub-station
1085 Highway 95, Suite C
Hawthorne, NV 89415

Incline Village/Tahoe Sub-station
625 Mount Rose Hwy
Incline Village, NV 89451-9111

Tonopah Sub-station
1137 S. Main St. Suite A4
Tonopah, NV 89049

Yerington Sub-station
215 West Bridge Street, #9
Yerington, NV 89447

Northern Command East

Elko Regional Office
3920 East Idaho Street
Elko, NV 89801

Austin Sub-station
184 Main St.
Austin, NV 89310

Battle Mountain Sub-station
101 Carson Road, Suite #6
Battle Mountain, NV 89820

Ely Sub-station
1200 Avenue "E"
Ely, NV 89315

Eureka Sub-station
790 South Monroe Street
Eureka, NV 89316

Jackpot Sub-station
1120 Snyder Way
Jackpot, NV 89825

Lovelock Sub-station
1155 Lovelock Ave
Lovelock, NV 89419

Wells Sub-station
1510 Lake Ave.
Wells, NV 89835

Wendover Sub-station
1111 Gene L Jones Way
West Wendover, NV 89803

Winnemucca Sub-station
3505 Construction Way
Winnemucca, NV 89445

Southern Command

Las Vegas Regional office
4615 West Sunset Road
Las Vegas, Nevada 89118

Alamo Sub-station
100 S. 1st W. Street
Alamo, NV 89801

Beatty Sub-station
211 Montgomery Street
Beatty, NV 89003

Moapa Sub-station
1501 State Highway 168
Moapa, NV 89025

Indian Springs Sub-station
851 McFarland
Indian Springs, NV 89018

Jean Sub-station
22680 Las Vegas South
Jean, NV 89019

Laughlin Sub-station
3650 South Pointe Circle, Suite 104B
Laughlin, NV 89029

Pahrump Sub-station
2250 East Postal Drive #6
Pahrump, Nevada 89048

Pioche Sub-station
1 Main Street
Pioche, NV 89043

19. Is it the intent of the State to have one central docking/download location or will the State be using multiple locations? Can the State provide the list of the location(s)?

Due to our geographical nature, we would require multiple locations as we have 3 regional offices and twenty-five substations throughout the state. Refer to question 18 for locations.

20. Can the State provide what the distance is from the server room to the download location(s)?

This information is challenging to provide as we have multiple locations, 3 regional offices and twenty-five substations throughout the state. With our current In-Car video system, we have 5 servers set up across the state. Reno, Carson City, Elko, Las Vegas and Winnemucca. Refer to question 18 for locations. All other substations have "Dummy" computers set up where video is uploaded to an external hard drive, which is later relayed to one of the main servers.

21. Can the State describe what the bandwidth and speed availability is between the download locations and main location they would like to store data?

This is dependent on the location where the video is uploaded. As described in section 3.8.1, a majority of our sub-stations are in rural communities and many locations have only 1.5 mbps of maximum available bandwidth. Other Urban locations have up to 600-800 Mbps of available bandwidth.

22. How many hours of video does the State expect to be collected during an average shift?

DPS/HPD anticipates each officer will collect approximately 2 hours of video per shift, per device with approximately 237 officers working each day, statewide.

23. How long does the State intend to retain the video collected?

Videos classified as "Non-Events" are retained for 30 days and all others are retained for 5 years, per our State retention schedule.

24. How does the State intend to store the video?

If DPS/HPD goes with a cloud based solution, it will be stored in the cloud for short and long term storage. If server based, all videos other than "Non-Events" will be archived to DVD or Blue Ray after 90 days.

25. Does the State require a backup solution?

Yes.

26. How long does the State intend to retain the video?

Videos classified as "Non-Events" are retained for 30 days and all others are retained for 5 years, per our State retention schedule.

ALL ELSE REMAINS THE SAME FOR RFP 3273.

Vendor must sign and return this amendment with proposal submitted.

Vendor Name: Utility Associates, Inc.

Authorized Signature:

Title: Chief Revenue Officer Date: 9/26/16

This document must be submitted in the "State Documents" section/tab of vendors' technical proposal.

ATTACHMENT A – CONFIDENTIALITY AND CERTIFICATION OF INDEMNIFICATION

Submitted proposals, which are marked "confidential" in their entirety, or those in which a significant portion of the submitted proposal is marked "confidential" **will not** be accepted by the State of Nevada. Pursuant to NRS 333.333, only specific parts of the proposal may be labeled a "trade secret" as defined in NRS 600A.030(5). All proposals are confidential until the contract is awarded; at which time, both successful and unsuccessful vendors' technical and cost proposals become public information.

In accordance with the Submittal Instructions of this RFP, vendors are requested to submit confidential information in separate binders marked "**Part I B Confidential Technical**" and "**Part III Confidential Financial**".

The State will not be responsible for any information contained within the proposal. Should vendors not comply with the labeling and packing requirements, proposals will be released as submitted. In the event a governing board acts as the final authority, there may be public discussion regarding the submitted proposals that will be in an open meeting format, the proposals will remain confidential.

By signing below, I understand it is my responsibility as the vendor to act in protection of the labeled information and agree to defend and indemnify the State of Nevada for honoring such designation. I duly realize failure to so act will constitute a complete waiver and all submitted information will become public information; additionally, failure to label any information that is released by the State shall constitute a complete waiver of any and all claims for damages caused by the release of the information.

This proposal contains Confidential Information, Trade Secrets and/or Proprietary information as defined in ***Section 2 "ACRONYMS/DEFINITIONS."***

Please initial the appropriate response in the boxes below and provide the justification for confidential status.

Part IB – Confidential Technical Information			
YES		NO	X
Justification for Confidential Status			
-NA-			

A Public Records CD or Flash Drive has been included for the Technical and Cost Proposal			
YES		NO (See note below)	X
Note: By marking "NO" for Public Record CD or Flash Drive included, you are authorizing the State to use the "Master CD or Flash Drive" for Public Records requests.			

Part III – Confidential Financial Information			
YES	X	NO	
Justification for Confidential Status			
Utility Associates, Inc. is a privately-owned corporation, not a publicly traded corporation. As such, Financial Information is proprietary and not widely distributed.			

Utility Associates, Inc.

Company Name

Signature

Chris R. Lindenau

Print Name

9/26/16

Date

This document must be submitted in Tab IV of vendor's technical proposal

ATTACHMENT C – VENDOR CERTIFICATIONS

Vendor agrees and will comply with the following:

(1) Any and all prices that may be charged under the terms of the contract do not and will not violate any existing federal, State or municipal laws or regulations concerning discrimination and/or price fixing. The vendor agrees to indemnify, exonerate and hold the State harmless from liability for any such violation now and throughout the term of the contract.

(2) All proposed capabilities can be demonstrated by the vendor.

(3) The price(s) and amount of this proposal have been arrived at independently and without consultation, communication, agreement or disclosure with or to any other contractor, vendor or potential vendor.

(4) All proposal terms, including prices, will remain in effect for a minimum of 180 days after the proposal due date. In the case of the awarded vendor, all proposal terms, including prices, will remain in effect throughout the contract negotiation process.

(5) No attempt has been made at any time to induce any firm or person to refrain from proposing or to submit a proposal higher than this proposal, or to submit any intentionally high or noncompetitive proposal. All proposals must be made in good faith and without collusion.

(6) All conditions and provisions of this RFP are deemed to be accepted by the vendor and incorporated by reference in the proposal, except such conditions and provisions that the vendor expressly excludes in the proposal. Any exclusion must be in writing and included in the proposal at the time of submission.

(7) Each vendor must disclose any existing or potential conflict of interest relative to the performance of the contractual services resulting from this RFP. Any such relationship that might be perceived or represented as a conflict should be disclosed. By submitting a proposal in response to this RFP, vendors affirm that they have not given, nor intend to give at any time hereafter, any economic opportunity, future employment, gift, loan, gratuity, special discount, trip, favor, or service to a public servant or any employee or representative of same, in connection with this procurement. Any attempt to intentionally or unintentionally conceal or obfuscate a conflict of interest will automatically result in the disqualification of a vendor's proposal. An award will not be made where a conflict of interest exists. The State will determine whether a conflict of interest exists and whether it may reflict negatively on the State's selection of a vendor. The State reserves the right to disqualify any vendor on the grounds of actual or apparent conflict of interest.

(8) All employees assigned to the project are authorized to work in this country.

(9) The company has a written equal opportunity policy that does not discriminate in employment practices with regard to race, color, national origin, physical condition, creed, religion, age, sex, marital status, sexual orientation, developmental disability or handicap.

(10) The company has a written policy regarding compliance for maintaining a drug-free workplace.

(11) Vendor understands and acknowledges that the representations within their proposal are material and important, and will be relied on by the State in evaluation of the proposal. Any vendor misrepresentations shall be treated as fraudulent concealment from the State of the true facts relating to the proposal.

(12) Vendor must certify that any and all subcontractors comply with Sections 7, 8, 9, and 10, above.

(13) The proposal must be signed by the individual(s) legally authorized to bind the vendor per NRS 333.337.

Utility Associates, Inc.

Vendor Company Name

Vendor Signature

Chris R. Lindenau

Print Name

9/26/16

Date

This document must be submitted in Tab IV of vendor's technical proposal

UTILITY ASSOCIATES
Limited Hardware Warranty
BodyWorn™ Body Worn Camera

Who is Covered?

This Limited Hardware Warranty extends only to the first consumer purchaser of the Product, and is not transferable.

What Does This Limited Warranty Cover?

Utility Associates (UA) warrants that UA "Products" (Products refers to BodyWorn Cameras, carriers, and BodyWorn Camera accessories) are free from defects in material and workmanship according to the following definitions, terms, and conditions:

The limited warranty for Products is for ONE (1) year beginning on the date of sale of the Product to the original purchaser ("Customer") of the product. The limited warranty is extended annually based upon payment of the AVaiL Web Video Management System ("AVaiL Web") annual fee for each subsequent year. The limited warranty is not assignable or transferable to any subsequent purchaser or user.

What Will Utility Associates Do?

During the limited warranty period, UA will repair or replace, at UA's sole option, any defective parts or parts that will not operate for their intended use, with new or refurbished parts as needed. UA may also choose to replace entire units.

Utility configures all BodyWorn devices in Decatur, GA and therefore inventories all parts on a constant basis. Under warranty, after a Support Ticket is opened there is 2-day advanced replacement for Hardware issues. For software issues immediate response time remotely once Support Ticket opened. Utility Associates will replace parts or replace total unit out of our home office located at 250 E Ponce De Leon Ave in Decatur, GA. Utility pays for shipping of parts or whole unit replacement under a RMA.

For original deployments covered under AVaiL Web and exceeding 100 units, a pool of "hot spares" equal to 2% of the original number of units purchased will be provided to facilitate maintenance exchange. This hot spare pool shall be housed at the customer's location for the length of the purchaser's AVaiL Web subscription. Hot spares provide ready replacements for units under going maintenance. Utility will replenish the hot spare pool as necessary during the AVaiL Web subscription.

Under no circumstances shall UA's liability under this limited warranty exceed the actual cash value of the Product at the time the Customer returns the product for repair, as determined by the price paid by the Customer for the Product less a reasonable amount for depreciation.

This Warranty Does Not Apply to:

(a) **Consumable Parts**, such as batteries or protective coatings designed to diminish over time unless failure has occurred due to a defect in workmanship.

(b) **Cosmetic Damage**, including but not limited to defects in appearance, cosmetic, decorative, or structural items including casing and non-operative parts.

(c) **Damage caused by use with non-UA products.** Defects or damage that result from the use of non-UA branded or certified Products, accessories or other peripheral equipment without limitation to housings, parts, or software are excluded from coverage.

(d) **Damage caused by accident, abuse, misuse, or other external causes;** including but not limited to: (i) improper usage (e.g. use cases outside those explained in UA provided training), or neglect; (ii) damage caused by physical abuse; (iii) exposure to improper operating environment including contact with liquids, water, rain, extreme humidity, heavy perspiration or other moisture; sand, food, dirt or similar substances

(except for Products sold as resistant to such substances, but only to the extent the damage was not caused by incorrectly securing the product's protective elements or subjecting the Product to condition beyond its stated specifications or limits); (iv) intentional damage (e.g. product dropped from excessive height); (v) external causes or acts which are not the fault of UA including but not limited to flood, fire, earthquake, tornado or other acts of God, are excluded from coverage.

(e) **Damage or intermittent operation caused by improper connection of any electrical power supply; improper grounding; or interference from other electrical devices or radios in proximity to the device.**

(f) **Faulty installation by a third party installer.**

(g) **Unauthorized service or modification.** Defects or damage resulting from service testing, adjustment, installation, maintenance, alteration or modification in any way, including but not limited to tampering with or altering the software, by someone other than UA, or its authorized service centers are excluded from coverage. Notwithstanding the foregoing, any Product which has had its operating system altered, including any failed attempts to unlock the operating system, is not covered by this warranty, regardless of whether such modifications are authorized approved, or otherwise sanctioned by UA.

(h) **A product has been modified in any manner without the written permission of UA.** Products that have been altered in any manner so as to prevent UA from determining whether such Products are covered under the terms of this Limited Warranty are excluded from coverage. The foregoing shall include but not be limited to (i) serial numbers, date tags or other manufacturer coding that has been removed, altered or obliterated; (ii) mismatched or duplicated serial numbers; or (iii) broken seals or other evidence of tampering.

Do not open the Product or attempt to repair the Product yourself; such conduct may cause damage that is not covered by this warranty.

(i) **Normal wear and tear or otherwise due to the normal aging of the Product.**

(j) **All software, including operating system software, third-party software, applications, and all other software of any kind.** Software distributed by UA is provided "AS-IS" and "AS AVAILABLE," "WITH ALL FAULTS" and without a warranty of any kind. The Limited Warranty does not apply to any non-UA product or any software, even if packaged or sold with UA hardware unless otherwise required by applicable local law.

If damage is outside the scope of warranty coverage, repair services may be available, but all costs associated with such out of warranty repair will be your responsibility.

What Other Limitations Are There?

- TO THE EXTENT PERMITTED BY APPLICABLE LAW, THIS LIMITED WARRANTY AND THE REMEDIES SET FORTH HEREIN ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES AND REMEDIES, WHETHER ORAL OR WRITTEN, STATUTORY, EXPRESS OR IMPLIED. NO ORAL OR WRITTEN REPRESENTATIONS MADE BY UA OR ANY SELLER, RESELLER OR DISTRIBUTOR OF THE PRODUCTS, INCLUDING EMPLOYEES AND AGENTS THEREOF, SHALL CREATE ANY ADDITIONAL WARRANTY OBLIGATIONS, INCREASE THE SCOPE, OR OTHERWISE MODIFY IN ANY MANNER THE TERMS OF THIS LIMITED WARRANTY.

- TO THE EXTENT PERMITTED BY APPLICABLE LAW, UA SPECIFICALLY DISCLAIMS ANY AND ALL STATUTORY OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT AND ALL WARRANTIES AGAINST HIDDEN OR LATENT DEFECTS. WHERE SUCH STATUTORY OR IMPLIED WARRANTIES CANNOT LAWFULLY BE DISCLAIMED, THEN TO THE EXTENT PERMITTED BY LAW, ALL SUCH WARRANTIES SHALL BE LIMITED IN DURATION TO THE DURATION OF THE EXPRESS LIMITED WARRANTY CONTAINED HEREIN AND THE REMEDIES OF REPAIR, REPLACEMENT, OR REFUND AS DETERMINED BY UA IN ITS SOLE DISCRETION SHALL BE THE EXCLUSIVE REMEDY OF THE CONSUMER.

- TO THE EXTENT PERMITTED BY APPLICABLE LAW, UA DOES NOT WARRANT THAT THE OPERATION OF ANY PRODUCTS OR SOFTWARE COVERED UNDER THIS LIMITED WARRANTY WILL MEET YOUR REQUIREMENTS, WORK IN COMBINATION WITH ANY HARDWARE OR SOFTWARE APPLICATIONS OR THIRD PARTY SERVICES, BE UNINTERRUPTED, ERROR-FREE, OR WITHOUT RISK TO, OR LOSS OF, ANY INFORMATION, DATA, SOFTWARE OR APPLICATIONS CONTAINED THEREIN, OR THAT DEFECTS IN THE PRODUCTS OR SOFTWARE WILL BE CORRECTED.

- TO THE EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL UA BE LIABLE, WHETHER IN CONTRACT, TORT OR UNDER OTHER LEGAL THEORY (INCLUDING NEGLIGENCE), FOR DAMAGES IN EXCESS OF THE PURCHASE PRICE OF THE PRODUCTS, OR FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR LOSS OF REVENUE OR PROFITS; LOSS OF BUSINESS; BUSINESS INTERRUPTION; LOSS OF OPPORTUNITY; LOSS OF GOODWILL; LOSS OF REPUTATION; LOSS OF, DAMAGE TO, OR CORRUPTION OF INFORMATION, DATA, SOFTWARE OR APPLICATIONS (INCLUDING ANY COSTS ASSOCIATED WITH RECOVERING, PROGRAMMING, OR REPRODUCING ANY INFORMATION, DATA, SOFTWARE OR APPLICATIONS STORED ON OR USED WITH UA PRODUCTS, OR ANY FAILURE TO MAINTAIN THE CONFIDENTIALITY OF ANY INFORMATION OR DATA STORED ON THE PRODUCTS); OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE ABILITY OR INABILITY TO USE THE PRODUCTS.

- SOME STATES OR JURISDICTIONS DO NOT ALLOW THE LIMITATION OR EXCLUSION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR THE EXCLUSION OR LIMITATION ON THE LENGTH OF AN IMPLIED WARRANTY, OR THE LIMITATION OR EXCLUSION OF DAMAGES FOR PERSONAL INJURIES CAUSED BY NEGLIGENCE, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY FROM STATE OR JURISDICTION.

UTILITY ASSOCIATES
Limited Hardware Warranty
Rocket IoT In-Car Router and Video Recording System

Who is Covered?

This Limited Hardware Warranty extends only to the first consumer purchaser of the Product, and is not transferable.

What Does This Limited Warranty Cover?

Utility Associates (UA) warrants that UA "Products" (Products refers to Rocket IoT Model S, Rocket IoT Model X, Rocket Lockers, Power Timers, and Antennas) are free from defects in material and workmanship according to the following definitions, terms, and conditions:

The limited warranty for Products is for ONE (1) year beginning on the date of sale of the Product to the original purchaser ("Customer") of the product. The limited warranty is extended annually based upon payment of the AVaiL Web Video Management System ("AVaiL Web") annual fee for each subsequent year. The limited warranty is not assignable or transferable to any subsequent purchaser or user.

What Will Utility Associates Do?

During the limited warranty period, UA will repair or replace, at UA's sole option, any defective parts or parts that will not operate for their intended use, with new or refurbished parts as needed. UA may also choose to replace entire units.

Utility manufactures all Products in Covington, GA and therefore inventories all parts on a constant basis. Under warranty, after a Support Ticket is opened there is 2-day advanced replacement for Hardware issues. For software issues immediate response time remotely once Support Ticket opened. Utility Associates will replace parts or replace total unit out of our home office located at 250 E Ponce De Leon Ave in Decatur, GA. Utility pays for shipping of parts or whole unit replacement under a RMA.

For original deployments covered under AVaiL Web and exceeding 100 units, a pool of "hot spares" equal to 2% of the original number of units purchased will be provided to facilitate maintenance exchange. This hot spare pool shall be housed at the customer's location for the length of the purchaser's AVaiL Web subscription. Hot spares provide ready replacements for units under going maintenance. Utility will replenish the hot spare pool as necessary during the AVaiL Web subscription.

Under no circumstances shall UA's liability under this limited warranty exceed the actual cash value of the Product at the time the Customer returns the product for repair, as determined by the price paid by the Customer for the Product less a reasonable amount for depreciation.

This Warranty Does Not Apply to:

(a) **Consumable Parts**, such as batteries or protective coatings designed to diminish over time unless failure has occurred due to a defect in workmanship.

(b) **Cosmetic Damage**, including but not limited to defects in appearance, cosmetic, decorative, or structural items including casing and non-operative parts.

(c) **Damage caused by use with non-UA products.** Defects or damage that result from the use of non-UA branded or certified Products, accessories or other peripheral equipment, including but not limited to: (i) an external cellular antenna was not connected to the Product when an external antenna "pigtail" connector was connected to a USB or PC Express Card cellular data card in the Product; (ii) an un-powered cellular booster was connected to the Product when an external antenna "pigtail" connector was connected to the USB or PC Express Card cellular data card in the Product; (iii) housings, parts, or software are excluded from coverage.

(d) **Damage caused by accident, abuse, misuse, or other external causes;** including but not limited to: (i) improper usage (e.g. use cases outside those explained in UA provided training), or neglect; (ii) failure to attach antennas to all 2.4GHz WiFi, 4.9GHz, and 5GHz antenna connectors on the Product; (iii) damage caused by physical abuse exceeding MIL STD 81 OF temperature and vibration standards; (iv) exposure to improper operating environment including contact with liquids, water, rain, extreme humidity, heavy perspiration or other moisture; sand, food, dirt or similar substances (except for Products sold as resistant to such substances, but only to the extent the damage was not caused by incorrectly securing the product's protective elements or subjecting the Product to condition beyond its stated specifications or limits); (v) intentional damage (e.g. pried from a dock or locker by force without unlocking the Product from the dock or locker); (vi) external causes or acts which are not the fault of UA including but not limited to flood, fire, earthquake, tornado or other acts of God, are excluded from coverage.

(e) **Damage or intermittent operation caused by vehicle electrical system voltage sags or surges** outside of the range of 10 to 18 volts DC; "momentary" sub—second vehicle voltage sags below 10 volts DC during vehicle cranking; installation without 5-amp fuse protection; blown fuses; improper connection of any electrical power supply; improper grounding; or interference from other electrical devices or radios in the vehicle.

(f) **Faulty installation by a third party installer.**

(g) **Unauthorized service or modification.** Defects or damage resulting from service testing, adjustment, installation, maintenance, alteration or modification in any way, including but not limited to tampering with or altering the software, by someone other than UA, or its authorized service centers are excluded from coverage. Notwithstanding the foregoing, any Product which has had its operating system altered, including any failed attempts to unlock the operating system, is not covered by this warranty, regardless of whether such modifications are authorized approved, or otherwise sanctioned by UA.

(h) **A product has been modified in any manner without the written permission of UA.** Products that have been altered in any manner so as to prevent UA from determining whether such Products are covered under the terms of this Limited Warranty are excluded from coverage. The foregoing shall include but not be limited to (i) serial numbers, date tags or other manufacturer coding that has been removed, altered or obliterated; (ii) mismatched or duplicated serial numbers; or (iii) broken seals or other evidence of tampering.

Do not open the Product or attempt to repair the Product yourself; such conduct may cause damage that is not covered by this warranty.

(i) **Normal wear and tear or otherwise due to the normal aging of the Product.**

(j) **All software, including operating system software, third-party software, applications, and all other software of any kind.** Software distributed by UA is provided "AS-IS" and "AS AVAILABLE," "WITH ALL FAULTS" and without a warranty of any kind. The Limited Warranty does not apply to any non-UA product or any software, even if packaged or sold with UA hardware unless otherwise required by applicable local law.

If damage is outside the scope of warranty coverage, repair services may be available, but all costs associated with such out of warranty repair will be your responsibility.

What Other Limitations Are There?

- TO THE EXTENT PERMITTED BY APPLICABLE LAW, THIS LIMITED WARRANTY AND THE REMEDIES SET FORTH HEREIN ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES AND REMEDIES, WHETHER ORAL OR WRITTEN, STATUTORY, EXPRESS OR IMPLIED. NO ORAL OR WRITTEN REPRESENTATIONS MADE BY UA OR ANY SELLER, RESELLER OR DISTRIBUTOR OF THE PRODUCTS, INCLUDING EMPLOYEES AND AGENTS THEREOF, SHALL CREATE ANY ADDITIONAL WARRANTY OBLIGATIONS, INCREASE THE SCOPE, OR OTHERWISE MODIFY IN ANY MANNER THE TERMS OF THIS LIMITED WARRANTY.

- TO THE EXTENT PERMITTED BY APPLICABLE LAW, UA SPECIFICALLY DISCLAIMS ANY AND ALL STATUTORY OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT AND ALL WARRANTIES AGAINST HIDDEN OR LATENT DEFECTS. WHERE SUCH STATUTORY OR IMPLIED WARRANTIES CANNOT LAWFULLY BE DISCLAIMED, THEN TO THE EXTENT PERMITTED BY LAW, ALL SUCH WARRANTIES SHALL BE LIMITED IN DURATION TO THE DURATION OF THE EXPRESS LIMITED WARRANTY CONTAINED HEREIN AND THE REMEDIES OF REPAIR, REPLACEMENT, OR REFUND AS DETERMINED BY UA IN ITS SOLE DISCRETION SHALL BE THE EXCLUSIVE REMEDY OF THE CONSUMER.

- TO THE EXTENT PERMITTED BY APPLICABLE LAW, UA DOES NOT WARRANT THAT THE OPERATION OF ANY PRODUCTS OR SOFTWARE COVERED UNDER THIS LIMITED WARRANTY WILL MEET YOUR REQUIREMENTS, WORK IN COMBINATION WITH ANY HARDWARE OR SOFTWARE APPLICATIONS OR THIRD PARTY SERVICES, BE UNINTERRUPTED, ERROR-FREE, OR WITHOUT RISK TO, OR LOSS OF, ANY INFORMATION, DATA, SOFTWARE OR APPLICATIONS CONTAINED THEREIN, OR THAT DEFECTS IN THE PRODUCTS OR SOFTWARE WILL BE CORRECTED.

- TO THE EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL UA BE LIABLE, WHETHER IN CONTRACT, TORT OR UNDER OTHER LEGAL THEORY (INCLUDING NEGLIGENCE), FOR DAMAGES IN EXCESS OF THE PURCHASE PRICE OF THE PRODUCTS, OR FOR ANY INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGES OF ANY KIND, OR LOSS OF REVENUE OR PROFITS; LOSS OF BUSINESS; BUSINESS INTERRUPTION; LOSS OF OPPORTUNITY; LOSS OF GOODWILL; LOSS OF REPUTATION; LOSS OF, DAMAGE TO, OR CORRUPTION OF INFORMATION, DATA, SOFTWARE OR APPLICATIONS (INCLUDING ANY COSTS ASSOCIATED WITH RECOVERING, PROGRAMMING, OR REPRODUCING ANY INFORMATION, DATA, SOFTWARE OR APPLICATIONS STORED ON OR USED WITH UA PRODUCTS, OR ANY FAILURE TO MAINTAIN THE CONFIDENTIALITY OF ANY INFORMATION OR DATA STORED ON THE PRODUCTS); OR OTHER FINANCIAL LOSS ARISING OUT OF OR IN CONNECTION WITH THE ABILITY OR INABILITY TO USE THE PRODUCTS.

- SOME STATES OR JURISDICTIONS DO NOT ALLOW THE LIMITATION OR EXCLUSION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, OR THE EXCLUSION OR LIMITATION ON THE LENGTH OF AN IMPLIED WARRANTY, OR THE LIMITATION OR EXCLUSION OF DAMAGES FOR PERSONAL INJURIES CAUSED BY NEGLIGENCE, SO THE ABOVE LIMITATIONS OR EXCLUSIONS MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS THAT VARY FROM STATE OR JURISDICTION.

Utility Associates, Inc.

COMMERCIAL TERMS AND CONDITIONS FOR SALES OF PROPRIETARY PRODUCTS

T-1. CONTRACT

Utility Associates (hereinafter SELLER) Terms and Conditions and order information set forth in this document or incorporated by reference and any modification made pursuant to it shall constitute the complete and exclusive written expression of the terms and conditions of the agreement between the parties, regardless of any conflicting, inconsistent or additional provisions proposed by BUYER, and supersedes all prior or contemporaneous proposals (oral or written), understandings, representations, conditions, warranties, covenants, and all other communications between the parties relating to the subject matter of this contract. The terms and conditions of this contract as set out herein may not in any way be explained or supplemented by a prior or existing course of dealings between the parties by any usage of trade or custom, or by any prior performance between the parties pursuant to this contract or otherwise and may not be modified in any way by any subsequent orders, proposals, acknowledgments, or other communications which relate to said order, unless specifically agreed in writing by BUYER and SELLER. SELLER is not responsible for typographical errors made in any of its publications, or for stenographic or clerical errors made in preparation of quotations, acknowledgments, or specifications. All such errors are subject to correction. All prices are based on the quantity and delivery shown on the quotation or acknowledgment.

T-2. LIMITED WARRANTY

Products manufactured by SELLER are warranted at time of shipment to be free from defects in material and workmanship under normal use and service. This warranty is only applicable to any of SELLER's products which BUYER returns to SELLER within one (1) year from the date of initial delivery, and which SELLER determines to be defective within the terms of this warranty. Products delivered by SELLER are warranted at time of shipment to be free from defects in material and workmanship under normal use and service. SELLE R's obligations, with respect to such applicable warranty returns, are limited to repair, replacement, or refund of the purchase price actually paid for the product, at SELLER's sole option. SELLER shall bear round-trip shipment costs of defective Items found to be covered by this warranty. Defective Products or parts thereof may be replaced with either new, factory refurbished, or remanufactured parts. Defective parts, which have been replaced, shall become the SELLER's property. This warranty does not extend to any product sold by SELLER which has been subjected to misuse, neglect, accident, improper installation, or a use for purposes not included or not in accordance with operational maintenance procedures and instructions furnished by SELLER, or which has been repaired or altered by BUYER or persons other than SELLER or which has been damaged by secondary causes, including but not limited to, improper voltages, adverse environment conditions, improper signals, or products which have had their serial number or any part thereof altered, defaced, or removed. SELLER liability does not cover normal wear and tear or deterioration. THE FOREGOING, WARRANTY IS IN LIEU OF ALL OTHER WARRANTIES, INCLUDING, BUT NOT LIMITED TO, WRITTEN, EXPRESS, IMPLIED OR STATUTORY WARRANTIES. IMPLIED WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE AND MERCHANTABILITY AND DESIGN WARRANTIES ARE SPECIFICALLY EXCLUDED AND SHALL NOT APPLY. SELLER'S OBLIGATIONS AND BUYER'S REMEDIES WITH RESPECT TO DEFECTIVE OR NONCONFORMING PRODUCTS ARE SOLELY AND EXCLUSIVELY AS STATED HEREIN.

T-3. LIMITATION OF LIABILITY

IN NO EVENT WILL SELLER BE LIABLE FOR ANY SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES INCLUDING, BUT NOT LIMITED TO, DAMAGES RESULTING FROM LOSS OF PROFIT OR REVENUE, INSTALLATION OR REMOVAL COSTS OR COSTS OF SUBSTITUTE PRODUCTS. BUYER AGREES THAT ANY BASIS FOR IMPOSING ANY LIABILITY ON SELLER FOR PROPERTY DAMAGE, PERSONAL INJURY, OR DEATH, OR LEGAL EXPENSES RELATING TO THE SALE OR USE OF SELLER'S PRODUCTS SHALL BE VOID AND UNENFORCEABLE TO THE EXTENT NOT PROHIBITED BY LAW. THE TOTAL LIABILITY OF SELLER ON ANY CLAIM, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE) OR OTHERWISE, ARISING OUT OF, CONNECTED WITH OR RESULTING FROM THE MANUFACTURE, SALE, DELIVERY, RESALE, REPAIR, REPLACEMENT OR USE OF ANY PRODUCT WILL NOT EXCEED THE PRICE PAID FOR THE PRODUCT OR PART THEREOF WHICH GIVES RISE TO THE CLAIM. BUYER AGREES TO HOLD SELLER HARMLESS FROM ALL LIABILITIES AND CLAIMS ARISING FROM USE OF SELLER'S PRODUCT.

T-4. DELIVERY

The shipment date set out herein is SELLER's best estimate of the time material will be shipped from its factory, and SELLER assumes no liability for loss, damage, or consequential damages due to delays for any reason. In no way shall SELLER be bound to a firm shipment or delivery date, regardless of the wording in the BUYER's order, except if expressly agreed to in writing by SELLER.

T-5. SHIPMENTS

All shipments are F.O.B. SELLER's factory. SELLER assumes no liability for loss, delay, breakage, or damage after delivering packaged products in good order to the carrier. All risks of loss transfer to the BUYER upon delivery of the goods to the carrier at the F.O.B. point. All transportation and shipment costs are the sole liability of the BUYER.

T-6. ACCEPTANCE

Final acceptance or rejection of the goods to the contractual requirements shall be at SELLER's factory in accordance with SELLER's standard factory acceptance procedure within thirty (30) days after written notice to BUYER of acceptance test schedule. Title shall pass to the BUYER upon acceptance of each line item at SELLER's factory. Upon acceptance of each unit of goods, BUYER waives any right to revoke such acceptance for any reason, whether known or unknown to BUYER at the time of acceptance. BUYER's sole and exclusive remedy regarding any defect or nonconformance becoming apparent in the goods after such acceptance shall be as set out in Clause T-2 hereof entitled WARRANTY.

T-7. FORCE MAJEURE

In no event shall SELLER be liable for any losses or damages (including incidental or consequential damages), delays or defaults occasioned by: (1) acts of God or of a public enemy, (2) acts of the United States or any state or political subdivision thereof, (3) fires, floods, explosions or other catastrophes, (4) epidemics and quarantine restrictions, (5) strikes, slowdowns or labor stoppages of any kind, (6) freight embargoes, (7) unusually severe weather (8) delays of a supplier, or (9) causes beyond the control of the SELLER.

T-8. TERMINATION

In the event of termination of all or any part of the order by BUYER or SELLER prior to completion of performance hereunder, SELLER shall be entitled to termination charges, if any, as reasonably determined by SELLER. Such charges shall include all expenses, liabilities, and obligations incurred with respect to manufacturing the goods or contracting for their manufacture, plus allowance for a reasonable profit.

T-9. PATENTS, TRADEMARKS, AND COPYRIGHTS
None of the SELLER's patent, trademark, copyright, or trade secret rights is transferred to BUYER other than the right to use SELLER-supplied products in the normal course of its business.

T-10. BUYER'S DATA
BUYER agrees that all data furnished in conjunction with its order together with any information furnished orally shall be free from proprietary or confidentiality restriction except as otherwise agreed in writing by SELLER.

T-11. PRICE, QUANTITY AND TAXES
The prices and quantities set out herein represent the quantity information contained in BUYER's order to SELLER, and SELLER's agreed-to-price therefore, and shall be controlling. In case of dispute, both parties shall in good faith seek to reach agreement in accord with the original agreed-to-order. BUYER agrees to pay all applicable federal, state and local revenue, excise, sales, use or similar taxes. BUYER, at SELLER's discretion, shall provide SELLER with a suitable tax-exempt certificate acceptable to the taxing authorities.

T-12. CHANGES
Any changes by BUYER relating to the work to be performed, method of shipment or packing, schedule, or place of delivery must be made by written order to SELLER. If such changes cause an increase or decrease in the cost of performance or in the time required for performance, SELLER shall be entitled to an equitable adjustment and the contract shall be modified accordingly prior to implementation of the change.

T-13. TERMS OF PAYMENT
Payment is due thirty (30) days from the date of shipment, contingent upon credit approval, unless otherwise specified on the invoice. Each shipment shall be considered a separate and independent transaction and therefore payment shall be made accordingly without any setoff. If shipments are delayed by or at the request of BUYER, Amounts outstanding and unpaid beyond the time specified in these terms may, at the sole discretion of the SELLER, accrue interest at 1.5% per month for the duration of the unpaid balance. Orders for custom or special products and/or services are irrevocable and may require advance payment. Failure of BUYER to make payments shall be grounds for SELLER to delay shipment, place the BUYER on Credit Hold or terminate the contract in whole or in part.

T-14. LETTER OF CREDIT
SELLER shall not be obligated to provide a letter of credit or other form of contract guarantee for payments received prior to final delivery.

T-15. ASSIGNMENT
Neither this contract nor any interest herein may be assigned by BUYER, either voluntarily or by operation of law without the prior written consent of SELLER. No consent shall be deemed to relieve BUYER of its obligations to fully comply with the requirements hereof. SELLER may, without BUYER's consent, assign any monies due or to become due hereunder.

T-16. JURISDICTION
This contract shall be governed by and construed according to the Laws of the State of Georgia, and exclusive jurisdiction and venue shall lie in the courts of the State of Georgia.

T-17. MERCHANDISE AND CLAIM TERMS
Orders cancelled by BUYER will be subject to a cancellation charge not to exceed 20% of the value of the cancelled order, at SELLER's discretion.

T-18. RETURNED GOODS
No merchandise will be accepted for return without written authorization. All returns must be unused, undamaged, in the original factory carton, and accompanied by a "Return Material Authorization (RMA) number and a copy of the SELLER invoice. Restocking charges apply to returned goods depending upon the circumstances of return and condition of product. All returned goods must be shipped prepaid, insured, and properly packed and the RMA number must be referenced on all correspondence and must be visible on the exterior of the carton.

T-19. GENERAL
SELLER reserves the right to make changes in design, at any time, without incurring any obligations to provide same on units previously purchased or to continue to supply obsolete units or parts. The invalidity in whole or in part of any provision of this contract shall not affect the validity of other provisions. The failure of either party to insist, in any one or more instances, upon the performance of any term or terms of this order shall not be construed as a waiver or relinquishment of that party's right to such performance or to future performance of such a term or terms, and the other party's obligation in respect hereto shall continue in full force and effect. SELLER specifically rejects and objects to BUYER issuance of any unilateral order not in full compliance and agreement with these SELLER Terms and Conditions of Sale, except if expressly agreed to in writing by SELLER.

SOFTWARE AS A SERVICE AGREEMENT

This Utility Associates, Inc. Software as a Service Agreement (the "Agreement") is entered into between Utility Associates, Inc. ("UA"), a Delaware corporation having its principal place of business at 250 East Ponce de Leon Ave., Suite 600, Decatur, Georgia 30030, and

_____

(the "Customer"). This Agreement shall be effective as of the date UA signs this Agreement (the "Effective Date"). The Parties agree as follows:

ARTICLE 1-SCOPE OF SERVICES

1.1.1 Access to Software. UA is the developer and owner of, or has rights to, certain enterprise mobile device tracking and messaging software known as "RCM – Remote Configuration Management", "DataSync", "AVaiL™", "AVaiL Web", "Vehicle Diagnostics", and "RFID Tracking" and related content to be provided to Customer; such software, its related content and any related documentation provided by UA, and the means used to provide the software to Customer and the services described herein are collectively referred to as the "Service". Subject to Customer's payment of the applicable fees and Customer's compliance with the terms of this Agreement, Customer, its affiliates and its and their employees ("Licensed Users") shall have the right to access and use the Service solely for Customer's and its affiliates' internal business purposes. UA will issue to one Licensed User ("Customer Administrator") an individual logon identifier and password ("Administrator Logon") for purposes of administering the Service. Using the Administrator's Logon, the Customer Administrator shall assign each Licensed User a unique logon identifier and password ("User Login") and provide such information to the Licensed Users and UA via the Service. Customer shall not provide a User Login to any individual or entity that is not a Licensed User to use the Service. Customer shall be responsible to ensure, by agreement or otherwise, that each Licensed User will: (a) be responsible for the security and/or use of his or her User Login; (b) not disclose such logon identifier or password to any person or entity; (c) not permit any other person or entity to use his or her User Login; (d) use the Service only in accordance with the terms and conditions of this Agreement and on the workstation software from which the Service is accessed. UA shall have the right to deactivate, change and/or delete User Logins of Licensed Users who have violated this Agreement and to deny or revoke access to the Service, in whole or in part, if UA reasonably believes Customer and/or its Licensed Users are in material breach of this Agreement. Customer shall be solely responsible for ensuring that the access to the Service by a Licensed User who ceases to be an employee of Customer or one of its affiliates is terminated. UA shall have no responsibility for managing, monitoring, and/or overseeing Customer's and its Licensed Users' use of the Service. Customer acknowledges that the Service may contain devices to monitor Customer's compliance with the terms and restrictions contained herein and Customer's obligations hereunder.

1.1.2 Operating Environment. Customer is solely responsible for acquiring, installing, operating and maintaining the hardware and software environment necessary to access and use the Service remotely via the Internet.

1.1.3 Changes to Service. UA may upgrade, modify, change or enhance ("Change") the Service and convert Customer to a new version thereof at any time in its sole discretion so long as such Change does not materially diminish the scope of the Service, in which event Customer shall have the right to terminate this Agreement upon thirty (30) days written notice to UA. During the term of this agreement, if UA upgrades the version of the Service Customer is using under this Agreement, Customer will not be charged an upgrade fee. Should UA offer additional optional software modules in the future that complement the Software, Customer may elect to purchase the optional software modules for an additional fee; however, Customer has no obligation to do so.

1.1.4 Help Desk. Between the hours of 9:00 a.m. and 5:00 p.m., Eastern Standard Time, Monday through Friday excluding UA holidays ("UA Business Hours"), UA shall provide Customer support in the form of a Help Desk. Customers reporting issues through email will receive confirmation of the issue within a reasonable time and will receive a callback the same business day if practical. The Help Desk is always subject to availability of our technical staff and clause 1.1.5 below. Outside of UA Business Hours, support calls are fielded by a 24 x 7 answering service and relayed to the on-call UA Support Staff.

1.1.5 **Uptime Commitment.**

a. **Availability.** The Service will be made available to Customer and its Licensed Users twenty-four hours a day, seven days a week less the period during which the Service are not available due to one or more of the following events (collectively, the "Excusable Downtime"):

(i) Scheduled network, hardware or service maintenance;
(ii) The acts or omissions of Customer or Customer's employees, agents, contractors, vendors, or anyone gaining access to the Service by means of a User Login;
(iii) A failure of the Internet and/or the public switched telephone network;
(iv) The occurrence of any event that is beyond UA's reasonable control, or
(v) At Customer's direction, UA restricting Customer's and its Licensed Users access to the Service.

b. **Commitment.** Customer is responsible for promptly notifying UA in the event of a suspected Service failure. For the purposes of establishing uptime herein, downtime begins upon such notification and ends upon restoration of Service. Subject to Customer satisfying its obligations herein, UA guarantees that the Service will be available to Customer and its Licensed Users at least 98% of the time during each calendar month, excluding Excusable Downtime ("Uptime Commitment"). If UA fails to satisfy the Uptime Commitment during a month, then UA will credit to Customer a pro-rated portion of the Fees in the first month of the next succeeding calendar quarter following the failure. For purposes of this Section, "pro-rated portion of the Fees" means the product obtained by multiplying the applicable Fees during the month of the failure by a fraction, the numerator of which will be the number of hours that the Service did not satisfy the Uptime Commitment, and the denominator of which will be the total number of hours during the month that such failure occurred less Excusable Downtime.

ARTICLE 2-USE OF THE SERVICE

2.1 Scope of Use. Subject to the terms and conditions of this Agreement, including, without limitation, Section 2.2 and 2.3 hereof and Customer's payment of all applicable Fees, UA hereby grants to Customer a limited, a non-exclusive, non-assignable, non-transferable license (the "License"), without the right to sublicense, to access and use the Service, during the Term, over the Internet for Customer's and its affiliates' internal business purposes, on a computer or a computer network operated by Customer, only by Licensed Users and only using the User Logins provided to UA for such Licensed Users for such use.

2.2 End User License Agreements. The Licensed software may incorporate software under license from a third party. If the third party requires Customer's notification of such use through an End User License Agreement (EULA), UA will provide such notification to the Customer. In order to use the Service, Customer agrees to be bound by all EULA(s) provided at the time of delivery whether by hardcopy or displayed upon Installation or use of the Service. Customer's use of the Service subsequent to such notice(s) shall constitute Customer's acceptance of the EULA(s).

2.3 Restrictions. Customer and its Licensed Users shall not: (a) copy the Service or any portion thereof other than as required to use the Service remotely as intended by this Agreement; (b) translate, decompile or create or attempt to create, by reverse engineering or otherwise, the source code from the object code of the Service; (c) modify, adapt, translate or create a derivative work from the Service; (d) use the Service to track more than the number of tracked asset units for which Fees have been paid pursuant Article 3 below; (e) sell, lease, loan, license, assign, sublicense, rent, transfer, publish, disclose, divulge, display, make available to third parties on a time-sharing or service bureau basis or otherwise make available for the benefit of third parties all or any part of the Service, including, without limitation, by transmitting or providing the Service, or any portion thereof, over the Internet, or otherwise, to any third party; (f) interfere or attempt to interfere with the operation of the Service in any way; (g) remove, obscure or alter any label, logo, mark, copyright notice, trademark or other proprietary rights notices affixed to or contained within the Service; (h) create any frames or other references at any other web sites pertaining to or using any of the information provided through the Service or links to the Service; or (i) engage in any action that constitutes a material breach of the terms and conditions of this Agreement. All rights not expressly granted hereunder are reserved to UA.

ARTICLE 3-FEES AND PAYMENT TERMS

3.1 Fees. As a condition to the License granted pursuant to Section 2.1 above, Customer shall pay Software as a Service annual usage fees ("Fees"). Customer shall, in addition to the Fees required hereunder, pay all applicable sales, use, transfer or other taxes and all duties, whether international, national, state or local, however designated, which are levied or imposed by reason of the transaction(s) contemplated hereby, excluding, however, income taxes on income which may be levied against UA ("Taxes"). Customer shall reimburse UA for the amount of any such Taxes. If Customer fails to pay any undisputed Fees within thirty (30) business days of the date they are due, the Service shall be suspended until all outstanding Fees have been paid. All Fees shall be non-refundable except as otherwise set forth herein.

3.2 Time-and-Materials Service. If Customer requests and UA agrees to provide services that are outside the scope of the Service, such services shall be provided at UA's then-current hourly service rates or as established within a separate agreement addressing these specific requests.

ARTICLE 4-REPRESENTATIONS AND WARRANTIES

4.1 Warranties. Each party (the "Representing Party") represents and warrants to the other that: (a) it has the authority to enter this Agreement and to perform its obligations under this Agreement; (b) the execution and performance of this Agreement does not and will not violate any agreement to which the Representing Party is a party or by which it is otherwise bound; and (c) when executed and delivered, this Agreement will constitute a legal, valid and binding obligation of the Representing Party, enforceable in accordance with its terms. In addition to the foregoing: UA warrants that the software provided as part of the Service will materially conform to the applicable then-current documentation relating to the Service when used in an operating environment that complies with the then-current documentation relating to the Service. If UA alters the documentation in a way that materially diminishes the scope of the Services, Customer shall have the right to terminate this Agreement upon thirty (30) days prior written notice to UA. In the event that the software which is part of the Service fails to perform in accordance with this warranty, Customer shall promptly inform UA of such fact, and, as Customer's sole and exclusive remedy, UA shall either: (i) repair or replace the Service to correct any defects in the software without any additional charge to Customer, or (ii) terminate this Agreement and provide Customer, as Customer's sole and exclusive remedy, with a pro rata refund (for the unexpired portion of the applicable Term) of the Fees paid to UA hereunder. Customer represents and warrants to UA that Customer and its Licensed Users (i) will use the Service only for lawful purposes; (ii) will not interfere with or disrupt the operation of the Service or the servers or networks involved with the operation of the Service; (iii) attempt to gain unauthorized access to the Service, other accounts, computer systems or networks connected to the Service, through any other means; or (iv) interfere with another user's use and enjoyment of the Service.

4.2 Export Restrictions. Customer represents and warrants that it and all Licensed Users will comply with all applicable laws, rules and regulations in the jurisdiction from which they access the Service, including those laws, rules and regulations which apply to the access, import, use and export of controlled technology or other goods. Customer also agrees that it and all Licensed Users will comply with the applicable laws, rules and regulations of the jurisdictions from which UA operates the Service (currently, the United States of America and the State of Georgia). In particular, Customer represents, warrants and covenants that it shall not, without obtaining prior written authorization from UA and, if required, of the Bureau of Export Administration of the United States Department of Commerce or other relevant agency of the United States Government, access, use, export or re-export, directly or indirectly, the Service, or any portion thereof or any Confidential Information of UA (including without limitation information regarding the use, access, deployment, or functionality of the Service) from the United States to (a) any country destination to which access, use, export or re-export is restricted by the Export Administration Regulations of the United States Department of Commerce; (b) any country subject to sanctions administered by the Office of Foreign Assets Control, United States Department of the Treasury; or (c) such other countries to which access, use, export or re-export is restricted by any other United States government agency. Customer further agrees that it is solely responsible for compliance with any import laws and regulations of the country of destination of permitted access, use, export or re-export, and any other import requirement related to a permitted access, use, export or re-export.

4.3 Warranty Disclaimer. CUSTOMER ACKNOWLEDGES THAT, EXCEPT AS PROVIDED HEREIN, THE SERVICE IS PROVIDED HEREUNDER WITH NO WARRANTY WHATSOEVER. CUSTOMER ACKNOWLEDGES THAT ITS USE OF THE SERVICE IS AT ITS OWN RISK. EXCEPT AS EXPRESSLY PROVIDED HEREIN, (a) THE SERVICE IS PROVIDED SOLELY ON AN "AS-IS" BASIS, AND (b) UA MAKES, AND CUSTOMER RECEIVES, NO WARRANTIES, EXPRESS, IMPLIED, OR OTHERWISE. UA EXPRESSLY DISCLAIMS ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, MERCHANTABLE QUALITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND/OR NONINFRINGEMENT AND ALL DUTIES AND OBLIGATIONS IMPLIED IN LAW. UA DOES NOT WARRANT THAT THE SERVICE SHALL BE OPERABLE, SHALL PROPERLY STORE DATA, SHALL OPERATE UNINTERRUPTED OR ERROR FREE, SHALL BE SECURE, SHALL KEEP DATA CONFIDENTIAL, SHALL FUNCTION OR OPERATE IN CONJUNCTION WITH ANY OTHER PRODUCT OR SHALL MEET CUSTOMER'S NEEDS.

ARTICLE 5-LIMITATION OF LIABILITY

5.1 General. EXCEPT FOR INDEMNIFICATION OBLIGATIONS SET FORTH HEREIN, IN NO EVENT SHALL EITHER PARTY, THEIR PARTNERS, PRINCIPALS, EMPLOYEES OR AGENTS BE LIABLE FOR ANY CONSEQUENTIAL, EXEMPLARY, SPECIAL, INDIRECT, INCIDENTAL OR PUNITIVE DAMAGES OR LOST REVENUE, LOST PROFITS OR ANTICIPATED BUSINESS ARISING FROM OR RELATING TO THIS AGREEMENT, THE SUBJECT MATTER HEREOF OR THE SERVICE, INCLUDING WITHOUT LIMITATION, DAMAGES ARISING FROM LOSS OF INFORMATION OR DATA, HOWEVER CAUSED (EVEN IF THEY HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES). EXCEPT FOR INDEMNIFICATION OBLIGATIONS SET FORTH HEREIN, THE AGGREGATE LIABILITY OF THE PARTIES WITH RESPECT TO ANY DAMAGES INCURRED IN ANY ONE YEAR PERIOD IN THE TERM FOR ANY OTHER DAMAGES ARISING FROM OR RELATING TO THIS AGREEMENT, THE SUBJECT MATTER HEREOF, OR THE SERVICE, HOWEVER CAUSED, UNDER ANY THEORY OF LIABILITY, SHALL NOT EXCEED THE AMOUNTS RECEIVED BY OR OWED TO UA FROM CUSTOMER RELATING TO ITS USE OF THE SERVICE DURING SUCH ONE

YEAR PERIOD. EXCEPT FOR INDEMNIFICATION OBLIGATIONS SET FORTH HEREIN, THIS LIMITATION APPLIES TO ALL CAUSES OF ACTIONS OR CLAIMS IN THE AGGREGATE INCLUDING WITHOUT LIMITATION, BREACH OF CONTRACT, BREACH OF WARRANTY, NEGLIGENCE, STRICT LIABILITY, MISREPRESENTATION, CLAIMS FOR FAILURE TO EXERCISE DUE CARE IN THE PERFORMANCE OF UA'S SERVICES HEREUNDER, AND OTHER TORTS. FURTHER, NO CAUSE OF ACTION WHICH ACCRUED MORE THAN TWO (2) YEARS PRIOR TO THE FILING OF A SUIT ALLEGING SUCH CAUSE OF ACTION MAY BE ASSERTED HEREUNDER. CUSTOMER AND UA EXPRESSLY ACKNOWLEDGE AND AGREE THAT THE LIMITATIONS AND EXCLUSIONS CONTAINED HEREIN REPRESENT THE PARTIES' AGREEMENT AS TO THE ALLOCATION OF RISK BETWEEN THE PARTIES IN CONNECTION WITH THIS AGREEMENT. THE PAYMENTS PAYABLE TO UA IN CONNECTION HEREWITH REFLECT THIS ALLOCATION OF RISK AND THE EXCLUSION OF CONSEQUENTIAL AND OTHER DAMAGES AND THE OTHER LIMITATIONS HEREIN.

5.2 Indemnification. Customer agrees to defend, indemnify, reimburse and hold harmless UA and its partners, principals, employees and agents with respect to any claim, demand, action, debt, loss, liability, cost and expense (including reasonable attorneys' fees, costs and expenses) arising "*in a reasonably foreseeable manner"* from breach of this Agreement or any of the representations, warranties, obligations, covenants or agreements herein by Customer or its affiliates, or by any of the agents, employees or Licensed Users thereof, or in connection with use of the Service by or through Customer or it affiliates or any Licensed User. *As used in the immediately preceding sentence, the term "reasonably foreseeable manner" means that a reasonable person familiar with this Agreement and the nature of the Service (including without limitation the use of such Service by other customers of UA), after careful consideration of the nature of the applicable breach of this Agreement or use of the Service, could have anticipated that the applicable claim, demand, action, debt, loss, liability, cost or expense might result from such breach or use.* UA shall indemnify, defend, reimburse and hold harmless Customer and its affiliates and the directors, officers, employees and agents of the foregoing with respect to any claim, demand, action, debt, loss, liability, cost and expense (including reasonable attorneys' fees, costs and expenses) to the extent based upon any third party claim (an "Infringement Claim") that the aspects of the Service that are proprietary to UA in the form originally licensed to Customer infringes any U.S. copyright or patent rights of any third party; *provided, however,* that UA shall have no obligation pursuant to the foregoing to the extent based on or related to (i) any use of the Service in violation of this Agreement or the then-current documentation relating to the Service, (ii) any use of the Service in conjunction with any product, data, hardware or software not contemplated in the then-current documentation relating to the Service, (iii) any data or information of Customer or its affiliates, or (iv) any modifications to the Service made by anyone other than UA (unless otherwise authorized in writing by UA). *Moreover, notwithstanding any provision hereof to the contrary, Customer's exclusive remedy for loss of use of the Service due to any Infringement Claim shall be to suspend its payment of Fees to UA hereunder for the period during which its use of the Service is actually prohibited by reason of such Infringement Claim, and UA shall have no liability for any other actual, special, incidental or consequential damages based on such loss of use.* The foregoing states the entire liability of UA with respect to any Infringement Claim, and Customer hereby expressly waives any other obligations or liabilities.

5.3 Indemnification Procedures. A Party seeking indemnification hereunder (an "Indemnified Party") shall give the Party from whom indemnification is sought (the "Indemnifying Party"): (i) reasonably prompt notice of the relevant claim; *provided, however,* that failure to provide such notice shall not relieve the Indemnifying Party from its liability or obligation hereunder except to the extent of any material prejudice directly resulting from such failure; (ii) reasonable cooperation, at the Indemnifying Party's expense, in the defense of such claim; and (iii) the right to control the defense and settlement of any such claim; *provided, however,* that the Indemnifying Party shall not, without the prior written approval of the Indemnified Party, settle or dispose of any claims in a manner that affects the Indemnified Party's rights or interest. The Indemnified Party shall have the right to participate in the defense at its own expense.

ARTICLE 6-CONFIDENTIAL INFORMATION

6.1 Confidential Information. As used herein, the term "Confidential Information means all technical, business and other information relating to the Service, which (i) is possessed or hereafter acquired by UA and disclosed to Customer or Licensed Users, (ii) derives economic value from not being generally known to persons other than UA and its customers, and (iii) is the subject of efforts by UA that are reasonable under the circumstances to maintain its secrecy or confidentiality. Confidential Information shall include, but shall not be limited to, oral or written (including, without limitation, storage in electronic or machine readable media) information with respect to UA's trade secrets, know-how, proprietary processes, operations, employees, contractors, prospects, business plans, product or service concepts, business methods, hardware, software, codes, designs, drawings, products, business models and marketing strategies, in each case relating to the Service. Confidential Information shall not include any information which Customer can demonstrate (a) has become generally available to and known by the public (other than as a result of a disclosure directly or indirectly by Customer, any of its affiliates or any of its or their respective employees, contractors or agents), (b) has been made available to Customer on a non-confidential basis from a source other than UA, provided that such source is not and was not bound by a confidentiality agreement with UA or any other legal obligation of non-disclosure, or (c) has been independently acquired or developed by Customer without violating any of its obligations under this Agreement.

6.2 Non-Disclosure of Confidential Information. Customer shall hold confidential all Confidential Information (as defined in Section 6.1) of UA and shall not disclose or use (except as expressly provided in this Agreement) such Confidential Information without the express written consent of UA. Confidential Information of UA shall be protected by the Customer with the same degree of care as Customer uses for protection of its own confidential information, but no less than reasonable care. Customer may disclose Confidential Information only to those of its employees who have a need to know the Confidential Information for purposes of performing or exercising rights granted under this Agreement and only to the extent necessary to do so. At any time upon the request of UA, the Customer shall promptly, at the option of UA, either return or destroy all (or, if UA so requests, any part) of the Confidential Information previously disclosed and all copies thereof, and the Customer shall certify in writing as to its compliance with the foregoing. Customer agrees to secure and protect the Confidential Information in a manner consistent with the maintenance of UA's rights therein and to take appropriate action by instruction or agreement with its Licensed Users to satisfy its obligations hereunder. Customer shall use its reasonable commercial efforts to assist UA in identifying and preventing any unauthorized access, use, copying or disclosure of the Confidential Information, or any component thereof. Without limitation of the foregoing, Customer shall advise UA immediately in the event Customer learns or has reason to believe that any person has violated or intends to violate these confidentiality obligations or the proprietary rights of UA, and Customer will, at Customer's expense, cooperate with UA in seeking injunctive or other equitable relief in the name of Customer or UA against any such person. In the event Customer is required to disclose any Confidential Information by law or court order, it may do so, provided that UA is provided a reasonable opportunity to prevent such disclosure, and, in the event of a disclosure, that the Customer apply reasonable commercial efforts to ensure that available confidentiality protections are applied to such information. In such event, Customer shall not be liable for such disclosure unless such disclosure was caused by, or resulted from, in whole or in part, a previous disclosure by Customer, any of its affiliates or any of its or their respective employees, contractors or agents, not permitted by this Agreement. UA Confidential Information shall not include information which can be demonstrated by Customer: (i) to have become part of the public domain except by an act or omission or breach of this Agreement on the part of Customer, its employees, or agents; (ii) to have been supplied to Customer after the time of disclosure without restriction by a third party who is under no obligation to UA to maintain such information in confidence; or (iii) required to be disclosed by law or court order, provided that UA is provided a reasonable opportunity to prevent such disclosure, and, in the event of a disclosure, that Customer apply reasonable commercial efforts to ensure that available confidentiality protections are applied to such information.

6.3 Non-Disclosure of Customer Confidential Information. Notwithstanding any provision of this Agreement to the contrary, UA shall hold confidential all information disclosed to UA (a) concerning the business affairs or proprietary and trade secret information of Customer, (b) any information that derives economic value from not being generally known to persons other than Customer and its employees, and (c) any information that is the subject of efforts by Customer that are reasonable under the circumstances to maintain its secrecy or confidentiality, whether disclosed to UA by Customer in oral, graphic, written, electronic or machine readable form ("Customer Confidential Information") and shall not disclose or use such Customer Confidential Information without the express written consent of Customer. Customer Confidential Information shall be protected by UA with the same degree of care as UA uses for its own confidential information, but no less than reasonable care. UA may disclose Customer Confidential Information only to those of its employees who have a need to know the Customer Confidential Information for purposes of performing or exercising rights granted under this Agreement and only to the extent necessary to do so. At any time upon the request of Customer, UA shall promptly, at the option of Customer, either return or destroy all (or, if Customer so requests, any part) of the Customer Confidential Information previously disclosed and all copies thereof, and UA shall certify in writing as to its compliance with the foregoing. UA agrees to secure and protect the Customer Confidential Information in a manner consistent with the maintenance of Customer's rights therein and to take appropriate action by instruction or agreement with its employees to satisfy its obligations hereunder. UA shall use reasonable commercial efforts to assist Customer in identifying and preventing any unauthorized access, use, copying or disclosure of the Customer Confidential Information, or any component thereof. Without limitation of the foregoing, UA shall advise Customer immediately in the event UA learns or has reason to believe that any person has violated or intends to violate these confidentiality obligations or the proprietary rights of Customer, and UA will, at UA's expense, cooperate with Customer in seeking injunctive or other equitable relief in the name of UA or Customer against any such person. Customer Confidential Information shall not include information which can be demonstrated by UA: (i) to have become part of the public domain except by an act or omission or breach of this Agreement on the part of UA, its employees, or agents; (ii) to have been supplied to UA after the time of disclosure without restriction by a third party who is under no obligation to Customer to maintain such information in confidence; or (iii) required to be disclosed by law or court order, provided that Customer is provided a reasonable opportunity to prevent such disclosure, and, in the event of a disclosure, that UA apply reasonable commercial efforts to ensure that available confidentiality protections are applied to such information.

6.4 Passwords. Any and all logon identifiers and passwords provided hereunder are deemed Confidential Information of UA. Customer and Licensed Users are responsible for maintaining the confidentiality of such logon identifiers and passwords. Customer agrees to (a) immediately notify UA of any unauthorized use of such logon identifiers or passwords or

any other breach of security pertaining to the Service, and (b) ensure that Licensed Users exit from their accounts at the end of each session. UA can not and will not be liable for any loss or damage arising from Customer's or any Licensed User's failure to comply with this Section 6.4.

6.5 Term. With regard to Confidential Information that constitutes trade secrets, the obligations in this Section shall continue for so long as such information constitutes a trade secret under applicable law. With regard to all other Confidential Information, the obligations in this Section shall continue for the term of this Agreement and for a period of five years thereafter.

ARTICLE 7-PROPRIETARY RIGHTS

7.1 Proprietary Rights. No right (except for the License right granted in Article 2), title or interest in any intellectual property or other proprietary rights are granted or transferred to Customer hereunder. UA and its third-party licensors and service providers retain all right, title and interest, including, without limitation, all patent, copyright, trade secret and all other intellectual property and proprietary rights, inherent in and appurtenant to the Service and all derivative works connected therewith.

ARTICLE 8-TERM AND TERMINATION

8.1 Term; Termination. The term of this Agreement (the "Term") shall commence on the Effective Date and shall continue for an initial term of one (1) year thereafter, unless terminated earlier or renewed as set forth herein, and shall automatically renew for additional one (1) year terms unless either party cancels such renewal by written notice to the other party at least sixty (60) days in advance of the expiration of the then-current term. Either party may immediately terminate this Agreement in the event that: (a) the other party breaches any material obligation, warranty, representation or covenant under this Agreement, (b) the other party becomes insolvent or is unable to pay its debts as due, enters into or files (or has filed or commenced against it) a petition, arrangement, action or other proceeding seeking relief or protection under the bankruptcy laws of the United States or similar laws of any other jurisdiction or transfers all of its assets to another person or entity, or (c) Customer has not used the Service for a consecutive six (6) month period. If timely payment of undisputed Fees is not received by its due date, UA reserves the right to either suspend or terminate Customer's or Licensed User's access to the Service. Upon termination or expiration of this Agreement for any reason, the License and the Service shall terminate, Customer will be obligated to pay any and all Fees due hereunder up through the date of such termination or expiration and UA shall have no further obligations to Customer. Sections 2.2, 2.3, and 4.3 and Articles 5, 6, 7, 8, and 9 hereof shall survive the expiration or termination of this Agreement for any reason.

ARTICLE 9-MISCELLANEOUS

9.1 Notices. Any written notice required or permitted to be delivered pursuant to this Agreement will be in writing and will be deemed delivered: (a) upon delivery if delivered in person; (b) three (3) business days after deposit in the United States mail, registered or certified mail, return receipt requested, postage prepaid; (c) upon transmission if sent via telecopier/facsimile, with a confirmation copy sent via overnight mail; (d) one (1) business day after deposit with a national overnight courier;

If to UA:	**If to Customer:**
Utility Associates, Inc. 1484 Brockett Road Tucker, Georgia 30084 Attn: Ted M. Davis, President Fax: 404 795-0525 E-Mail: tmd@utility.com	_____ _____ _____ _____ _____

9.2 Governing Law and Venue. This Agreement, and all the rights and duties of the parties arising from or relating in any way to the subject matter of this Agreement shall be governed by, construed and enforced in accordance with the laws of the State of Georgia (excluding any conflict of laws provisions of the State of Georgia). Any suit or proceeding relating to this Agreement shall be brought in the courts, state and federal, located in Fulton County, State of Georgia.

9.3 UCITA Disclaimer. THE PARTIES AGREE THAT THE UNIFORM COMPUTER TRANSACTIONS ACT OR ANY VERSION THEREOF, ADOPTED BY ANY STATE, IN ANY FORM ("*UCITA*"), SHALL NOT APPLY TO THIS AGREEMENT. TO THE EXTENT THAT UCITA IS APPLICABLE, THE PARTIES AGREE TO OPT OUT OF THE APPLICABILITY OF UCITA PURSUANT TO THE OPT-OUT PROVISION(S) CONTAINED THEREIN.

9.4 Assignment. Customer will not assign, sublicense or otherwise transfer this Agreement, in whole or in part, nor delegate or subcontract any of its rights or obligations hereunder, without UA's prior written consent, except in the event of an assignment to an affiliate

9.5 Force Majeure. Neither party shall have any liability to the other or to third parties for any failure or delay in performing any obligation under this Agreement due to circumstances beyond its reasonable control including, without limitation, acts of God or nature, actions of the government, fires, floods, strikes, civil disturbances or terrorism, or power, communications, satellite or network failures; provided, however, this Section 9.5 shall not apply to Customer's obligation to pay any of the Fees in accordance with Article 3 hereof. .

9.6 Modifications. All amendments or modifications of this Agreement shall be in writing signed by an authorized representative of each party hereto. The parties expressly disclaim the right to claim the enforceability or effectiveness of: (a) any amendments to this Agreement that are not executed by an authorized representative of UA and Customer; (b) any oral modifications to this Agreement; and (c) any other amendments based on course of dealing, waiver, reliance, estoppel or similar legal theory. The parties expressly disclaim the right to enforce any rule of law that is contrary to the terms of this Section.

9.7 Waiver. The failure of either party to enforce, or the delay by either party in enforcing, any of its rights under this Agreement will not be deemed to be a waiver or modification by such party of any of its rights under this Agreement.

9.8 Severability. If any provision of this Agreement is held by a court of competent jurisdiction to be invalid or unenforceable, in whole or in part, such holding shall not affect the validity or enforceability of the other provisions of this Agreement.

9.9 Headings. The headings used herein are for reference and convenience only and shall not enter into the interpretation hereof.

9.10 Entire Agreement. This Agreement (including the Schedules and any addenda hereto) contains the entire agreement of the parties with respect to the subject matter of this Agreement and supersedes all previous communications, representations, understandings and agreements, either oral or written, between the parties with respect to said subject matter.

Signatures on the Following Page

IN WITNESS WHEREOF, UA and Customer have executed this Agreement as of the date set forth below. All signed copies of this Agreement shall be deemed originals.

_____	Utility Associates, Inc, _____
("Customer")	("UA")
_____	_____
By (Signature)	By (Signature)
_____	Ted M. Davis_____
Name (Print)	Name (Print)
_____	President_____
Title	Title
_____	_____
Date (the "Effective Date")	Date

ATTACHMENT B – TECHNICAL PROPOSAL CERTIFICATION OF COMPLIANCE WITH TERMS AND CONDITIONS OF RFP

I have read, understand and agree to comply with ***all*** the terms and conditions specified in this Request for Proposal.

YES X I agree to comply with the terms and conditions specified in this RFP.

NO _____ I do not agree to comply with the terms and conditions specified in this RFP.

If the exception and/or assumption require a change in the terms in any section of the RFP, the contract, or any incorporated documents, vendors ***must*** provide the specific language that is being proposed in the tables below. If vendors do not specify in detail any exceptions and/or assumptions at time of proposal submission, the State will not consider any additional exceptions and/or assumptions during negotiations.

Utility Associates, Inc.

Company Name

Signature

Chris R. Lindenau

Print Name

9/26/16

Date

Vendors MUST use the following format. Attach additional sheets if necessary.

EXCEPTION SUMMARY FORM

EXCEPTION #	RFP SECTION NUMBER	RFP PAGE NUMBER	EXCEPTION (Complete detail regarding exceptions must be identified)

ASSUMPTION SUMMARY FORM

ASSUMPTION #	RFP SECTION NUMBER	RFP PAGE NUMBER	ASSUMPTION (Complete detail regarding assumptions must be identified)

This document must be submitted in Tab V of vendor's technical proposal

IN-CAR VIDEO COMPLY CHECK LIST

The In-Car Video portion of this RFP is contingent upon funding anticipated to be approximately one (1) year from contract award. Vendors proposing In-Car Video must be compatible with proposed Body Worn Cameras.

Vendors must respond check either yes or no to each section below: Where section asks to provide details or response, vendors must respond to the corresponding RFP section not in this document.

	Comply	
3.12 STANDARD SPECIFICATIONS	**Yes**	**No**
All mobile video systems and related audio equipment must conform to the applicable minimum standards as set by the following: Electronic Industries Association (EIA); Federal Communications Commission (FCC) rules/ regulations; Institute of Electrical and Electronic Engineers (IEEE); International Electro-technical Commission (IEC); International Organization for Standardization (ISO); National Fire Protection International (NFPA); National Highway Transportation Safety Administration (NHTSA); Society of Automotive Engineers (SAE); Underwriters Laboratories Inc. (UL); and	✓	
Vendors must provide documentation that validates that their systems adhere to the minimum specifications in the International Association of Chief of Police (IACP) Specifications for In-Car Video (dated 11/21/2008), and that the technology used is generally accepted in the relevant field.	✓	

	Comply	
3.12.2 VIDEO SYSTEM SPECIFICATIONS	**Yes**	**No**
The minimum acceptable components consist of the following parts: o Front camera o Back seat camera o Color LED monitor with audio o Body worn camera must act as a wireless transmitter for audio with in-car & home charger. o Covert secondary hard-wired microphone o Digital Video Recorder- DVR o Integrated GPS receiver and antenna; o Collision sensor o Controller center o Means to transfer media data from In-car to storage solution o Video viewer capability o Hardware/software necessary to submit videos as evidence o All mounts and cables for power, interfaces, cameras, and antennas o Documentation, o Warranty and maintenance, o Training o Shipping and handling	✓	
3.12.3 DIGITAL VIDEO RECORDER (DVR)		
The digital video recorder (DVR) offered shall be in full commercial production. Prototypes will not be considered.	✓	
Programming of the in-car recording system shall be restricted to authorized personnel only.	✓	
All controls and indicators shall have adjustable backlighting.	✓	
The officer shall have the option of recording primary, rear-facing, or both cameras simultaneously.	✓	
A collision sensor covering 360 degrees, to trigger recordings, without requiring connection to the vehicles airbag system, shall be included. If a collision is detected, the video recorder (including pre-event memory) shall be automatically activated so the collision and video leading up to the collision is recorded.	✓	
The in-car digital video system shall be provided with all necessary cables and hardware (e.g. fuse holders, mounting brackets) required for installation.	✓	
Each digital video recording system shall be supplied with a comprehensive installation/ programming/ operations manual. The manual shall specify all brackets, hardware and mounting locations for installing camera systems.	✓	

	Comply	
3.12.4 DIGITAL VIDEO RECORDER (DVR)	**Yes**	**No**

The DVR shall mount in standard equipment consoles between the seats, or overhead.	✓	
No permanent modifications shall be required to install the DVR system.	✓	
The DVR system shall be capable of being installed as to not hinder the operation of the police unit.	✓	
The DVR shall be capable of recording two video inputs from a powerful zoom, forward-facing camera, and a wide-angle rear-facing camera.	✓	
The DVR shall provide a choice of at least one of the following upload options. o **Wireless Ethernet**- provided 802.11n base station includes encryption, supports multiple simultaneous uploads and is upwardly scalable. The system should be capable of comfortably uploading from multiple vehicles in the regional command centers (depicted in the scope of work section of this RFP) simultaneously. In addition, a backup upload system must be provided, should the wireless transfer system fail. o **Removable Hard Disc Drive (HDD)** with provided hard drive docking stations that support plug and play hard drive insertion. o **Removable Compact Flash Device**-Device with provided docking stations that support plug-and-play flash card insertion. o **Cellular** - Upload media via LTE connectivity that is compatible with the Feeney Wireless Skyus-X modem.	✓	
The DVR shall have the ability to record up to 8 hours of video before reaching the capacity of the storage media at maximum resolution. For the recording media available, specify the recording and playback times, resolution, and MB per second.	✓	
Video resolution, frame rates, and quality on the DVR shall be preset but can be changed by an administrator. These settings shall be independently configurable for recording modes of both video cameras. Please specify levels for: video resolution video frame rate video quality	✓	
The DVR shall require a security feature (key, admin software rights) to prevent unauthorized users from accessing the on-screen menus to adjust video settings and perform file management functions.	✓	
The DVR shall include a GPS receiver to provide vehicle position, course and speed information. The GPS receiver shall also be used to set the internal DVR clock to the proper time and date so that all vehicles display and record proper time.	✓	

The DVR shall include indicators visible outside of the vehicle to confirm that the system is recording and that the wireless audio transmitter is activated. This indicator does not need to be visible to occupants inside the vehicle.	✓	
The DVR shall be capable of initiating a recording by both automatic and manual means. The DVR shall begin recording automatically when any of the following are activated:. ▪ Vehicle's emergency/pursuit lights; ▪ Siren, and ▪ The systems integrated crash sensor. (This activation shall include capturing the "look back" buffer memory to video-record the collision, should it be in view of the active camera	✓	
The audio input associated with the forward-facing camera shall record audio using the internal microphone inside the vehicle. When the wireless audio transmitter/BWC is activated, the audio input shall be automatically switched to the wireless audio transmitter's microphone. The system shall automatically revert to the internal microphone when the wireless audio transmitter/BWC is deactivated.	✓	
The DVR shall include a programmable pre-event recording mode allowing it to capture images a minimum of 30 seconds prior to the activation of the RECORD mode. Please specify pre-event recording capability of proposed DVR.	✓	
The DVR shall be capable of capturing date/time, user identification information, emergency light indication, siren indication, speed indication (w/ radar interface), braking indication, and whether the microphone is activated. The information shall not be overlaid on the recorded video, and should be stored as secured metadata.	✓	
The DVR shall allow video to be played back in the vehicle. When the DVR PLAY button is pressed a list of all prior recordings shall appear on the display screen provided.	✓	
The DVR shall record video in a format that allows playback on multiple devices.	✓	
The DVR shall provide a means to ensure the integrity of the recorded video has not been compromised. The video must be able to be authenticated at any time, including when it is played back outside of the police vehicle	✓	
The DVR shall provide a means to ensure the integrity of the recorded video has not been compromised. The video must be able to be authenticated at any time, including when it is played back outside of the police vehicle.	✓	
The Control Center/DVR firmware shall allow in-system programming for future updates. Please describe how updates are made.	✓	
The DVR or related display (Mobile Data Computer, tablet etc.) shall have backlit controls for record; stop; play/pause; forward/reverse, fast forward/ reverse; trace, and lighted indicators for power on; record; and play.	✓	
The power control switch shall allow the DVR to automatically power on after the vehicle's ignition is switched on	✓	
The DVR shall automatically power down after the vehicle's ignition is turned off provided the DVR is not in "Record" and is not in the process of downloading files or other type of file save.	✓	

The DVR should provide a means to tag an incident at the time it is recorded with a priority designation. Once a recording is stopped, the DVR should automatically prompt the officer to select from the pre-defined drop-down list(s).	✓	
The DVR shall be capable of operating within the range of interior temperatures found within a law enforcement vehicle in Nevada without the need for supplemental heating or cooling. Specify your DVR's operating range and acceptability for the extreme temperature range in Nevada	✓	

	Comply	
3.12.4 **COMPACT CCD COLOR CAMERA**	**Yes**	**No**
The low-light CCD color camera shall use a Sony EXview® HAD CCD or equivalent image sensor to provide high quality nighttime images while minimizing blooming and glaring from bright sources of light. Proof of "equal" shall be the responsibility of the bidder and shall be submitted with the bid if not using the Sony EX VIEW chipset.	✓	
The forward-facing camera shall be a solid state imaging system that is not subject to burn in, or interference by magnetic fields.	✓	
The forward-facing camera shall operate within the range of temperatures from 0 to 120 degrees Fahrenheit or between -17.8 and 48.9 degrees Celsius	✓	
The camera shall be compact so as not to obstruct the driver's forward or peripheral view thru the windshield, or provide any obstruction of factory installed airbags or mirrors.	✓	
The camera shall be a single unit, including power lens, mounted on the windshield or roof of the vehicle and operate on 12 VDC power source.	✓	
The camera shall provide a minimum field of view of 24 feet width at distance of 35 feet (40 degrees).	✓	
The camera shall have manual and automatic focus capabilities, which are user selectable.	✓	
The front camera should have a minimum 120X zoom (10x optical zoom with 12x digital zoom). Please specify _____ mode.		✓
The minimum LUX rating of the forward facing camera shall be rated at less than 1 LUX at full shutter speeds and 0.05 LUX in night view mode.	✓	
The camera shall automatically adjust for varying light levels from day to night. The camera and lens will be equipped with auto focus, automatic exposure, and automatic white balance.	✓	
The camera shall have a minimum color resolution of 450 horizontal lines	✓	
All cameras shall default to auto focus. An override system should be configurable to prevent operation while the vehicle is in motion.	✓	
The camera shall offer a signal-to-noise ratio of at least 46db.	✓	
The camera shall have backlight compensation setting.	✓	
The camera shall be compact. List the size and weight of the proposed CCD camera.	✓	
The camera shall mount with a heavy-duty controlled pivot mount that does not obstruct the driver's field of view. Camera shall be able to be rotated 360 degrees and can pan and tilt to +/- 90 degrees. Adjustment shall require no tools.	✓	
An optional rear view camera shall be available.	✓	

	Comply	
3.12.5 **BACK SEAT CAMERA SPECIFICATIONS**	**Yes**	**No**
The back-seat camera shall utilize a micro compact with wide angle 1/3" Super HAD image device (or equivalent) with approximately 420 lines of resolution. Proof of "equal" shall be the	✓	

responsibility of the bidder and shall be submitted with the bid. This must be included in the system at no charge.		
The rear-facing camera shall be capable of being mounted covertly in the cab.	✓	
The rear facing camera shall be capable of recording the entire rear seat area of the police vehicle.	✓	
The rear-facing camera shall have a minimum lux rating of .03. Please specify the rating	✓	
The rear-facing camera shall utilize infrared illumination to capture video in no-light conditions.	✓	

	Comply	
3.12.6 **COMPACT COLOR LCD MONITOR**	**Yes**	**No**
The monitor shall be a full color high quality LCD, active matrix (TFT) screen that measures at least 3.0" measured diagonally.	✓	
The monitor shall be capable of displaying a live picture from the camera when powered, even if recording is not in progress.	✓	
The monitor shall operate between 32 and 120 degrees Fahrenheit.	✓	
The monitor shall include a system speaker, with volume control, to provide monitoring of live audio or playback from all system microphones.	✓	
The monitor shall have controls/indicators that mimic the DVR and include record; stop; play/pause; forward/reverse; brightness; volume; and power. The monitor should also include a button for disabling the monitor when the system in standby, and accessing a menu for programming.	✓	
The monitor should have the capability to display: date/time, user identification information, emergency light indication, siren indication, latitude and longitude, speed (w/ radar interface), braking indicator and microphone activation indicator. The information shall not be overlaid on the recorded video; rather, it should be stored as external secure meta-data (or equivalent) in the video file.	✓	
The monitor should support a full-screen video mode (without the auxiliary data) using a single key press on the control center	✓	
The monitor shall operate independently from the recording device. For covert operation it should possible to operate the DVR in RECORD mode with the monitor turned off.	✓	
The monitor shall be provided with an adjustable mounting bracket that will allow it to be mounted in a variety of locations within the law enforcement vehicle.	✓	
The monitor shall have the capability to display the approximate amount of storage remaining on the media in an HH:MM format. An audible beep or other form of tone shall warn operator prior to or when there is 10%, or less, time remaining on the media.	✓	

	Comply	
3.12.7 **MICROPHONES**	**Yes**	**No**
The system shall come equipped with a digital wireless microphone that is incorporated into the BWC and an in-car microphone. The in-car microphone shall be mountable anywhere within the vehicle.	✓	
Audio from the interior microphone and the wireless microphone/BWC shall record on separate audio channels.	✓	
The wireless microphone/BWC shall be self-contained and include a re-chargeable battery; mountable charger/docking station; internal microphone; internal antenna. Transmitters that rely on the microphone cable for an antenna, or which utilize an external antenna shall not be permitted.	✓	
The wireless microphone/BWC system shall be FCC type accepted.	✓	

The wireless microphone/BWC shall have a minimum effective operating range 1,000 feet under line-of-sight conditions.	✓	
The wireless microphone/BWC must have a minimum stand-by battery life of ten (10) hours without recharging or additional batteries, with pre-record on.	✓	
The wireless microphone/BWC should be capable of automatically activating the DVR system; additionally, the wireless audio transmitter/BWC shall be capable of being activated by the DVR system when a recording is started.	✓	

	Comply	
3.12.8 **CONTROL CENTER SPECIFICATIONS**	**Yes**	**No**
The control center shall be compact in design and mounted overhead, or in the equipment console between the seats.	✓	
The control center shall not obstruct the driver's forward or peripheral view or provide any obstruction of factory installed airbags or mirrors.	✓	
The control center shall not require any permanent modifications to the police vehicle.	✓	
The control center shall accommodate the mounting of the front and rear-facing cameras, the monitor and keypad.	✓	

	Comply	
3.12.9 **VIDEO VIEWING SOFTWARE/HARDWARE**	**Yes**	**No**
A video viewer/software shall be provided to allow recorded video files to be played on any computer and display date/time, user identification, emergency light indication, siren indication, latitude and longitude, speed (w/ radar interface), braking indication and the microphone activation indicator. This information shall not be overlaid on the recorded video; it shall be displayed outside the video frame.	✓	
Support for this software shall include version updates provided free of charge for the lifetime of the system.	✓	
Vendors shall provide all hardware (media readers/drives) and software necessary duplicate, share and present digital video in a court acceptable format. Please describe transfer steps needed to convert captured video to court acceptable evidence without the need for a server based infrastructure.	✓	
The video management software should be capable of converting a video from the proprietary format to the standard DVD Video format, and authoring a DVD capable of being played in a standard DVD player.	✓	

	Comply	
3.12.10 **SERVER BASED VIDEO MANAGEMENT SYSTEM (VMS) Backend (Optional)** Vendors may propose systems with a server based digital evidence management, but are not obligated to do so. If a server based Video Management Software System (VMS) component is proposed the following specifications apply.	**Yes**	**No**
The server based VMS should include server infrastructure in our Northern, Southern, and Central regional command offices and assume manual downloading of all rural substations into the regional command centers to which they report (see Table 1.2.A).	N/A	N/A
The server based VMS shall be a turn-key component and fully installed, serviced, warranted, and maintained by the vendor.	N/A	N/A
The server based VMS should include RAID-5 video storage servers or equivalent for all regional offices to capture video information, workstation(s) for managing and viewing stored video, equipment racks to mount equipment, and uninterruptible power supplies (UPS).	N/A	N/A

The server based VMS should provide a configurable DVD archive unit that can automatically archive video copies based on set parameters, and copy video files to a DVD-Video or equivalent court acceptable format.	N/A	N/A
Pricing for the server based VMS shall be provided on the Pricing Schedule in the vendor's response. Pricing must be included for all proposed hardware (workstations, servers, archiving hardware, video back up systems, access points), wiring, software, installation, configuration, and training.	N/A	N/A
If a server based video management back office component is proposed, a schematic of the back end infrastructure shall be included with responses to the RFP.	N/A	N/A
The server based VMS file storage shall be equipped with sufficient storage to comfortably manage video that would be generated from cars depicted in the scope of work in this RFP. Please list and itemize the size of proposed storage for each regional command center identified.	N/A	N/A
If wireless downloading capability is proposed for vehicles assigned to each regional office, provide download times for video captured based on the video compression and resolution capabilities of proposed cameras, the proposed number of access points, and the proposed servers/wiring infrastructure.	N/A	N/A
The server based VMS shall include a database that contains a record for each recorded video file. The database shall store sufficient information to support the search capabilities and provide chain-of-evidence documentation.	N/A	N/A
The server based VMS shall be capable of searching stored video files by: department ID, time, date, officer ID, vehicle ID, camera, recording mode, and status (online or archived).	N/A	N/A
The server based VMS shall be capable of providing custom fields that may be used to store department-defined information (e.g. suspect's name, license plate number, etc.)	N/A	N/A
The server based VMS should allow videos to be categorized using department-defined drop-down lists. This classification shall be used for searching and to define how long each category of video is to be kept before it is automatically deleted.	N/A	N/A
The server based VMS shall provide a means to ensure the integrity of the recorded video. Video integrity must be checked when the video is uploaded, anytime it is played back or archived, and shall be verifiable on demand.	N/A	N/A
The server based VMS shall provide the capability to duplicate, share and present digital video in a court acceptable format. Describe the transfer steps, if any, needed provide video to the courts as acceptable evidence. Describe the way and format the proposed system archives recorded video files, and how these files will be stored and backed up for safeguarding.	N/A	N/A
When a video file is copied or archived to digital media, the Video Management Software shall store a unique archive ID and maintain a virtual directory to recall the archived video file(s).	N/A	N/A
The Video Management Software shall be capable of converting a video from the proprietary format to the standard DVD Video format, and authoring a DVD capable of being played in a standard DVD player.	N/A	N/A
The support for this software shall include version updates and be provided free of charge to the agency for the lifetime of the system.	N/A	N/A

	Comply	
3.12.11 **CONTROL CENTER SPECIFICATIONS**	**Yes**	**No**
An optional radar interface shall integrate directly with the Agency Bee III radar equipment. Collected information shall include speed of the target, the "locked" target speed, and the patrol vehicle.	✓	
The State is interested in a system that can be configured for motorcycle use. All of the specifications described for the DVR and wireless microphone shall be applicable. Is a motorcycle option available for your solution? If so, does the configuration utilize a weatherproofed monitor and camera? Please explain.	✓	

	Comply	
3.12.12 **OFFICER SAFETY**	**Yes**	**No**

All equipment shall be capable of installation in the following vehicles while still meeting the other requirements stated herein: Chevrolet Tahoe, Dodge Charger, Ford Interceptor Utility/Sedan and Ford F150 Pick-up.	✓	
Describe dimensions and vehicle mounting options for your camera, recorder, wireless microphone, transmitter/ receiver and any other required equipment.	✓	
Equipment must not be installed in such as manner as to interfere with a passenger in the front passenger seat.	✓	
No part of the system shall interfere in any way with the driver's field of view. The camera shall be a single unit, including power lens, mounted on the windshield or roof of the vehicle and operate on 12 VDC power source All connections to the camera, for power and video, shall be made by a single cable that attaches using a quick release connector.	✓	
The in-car system shall be protected from damage due to input of voltage, reverse polarity, and electrical transients that may be encountered.	✓	
No item installed in the interior of the passenger compartment shall increase the risk of injury to occupants during events related to a vehicle crash.	✓	
Any items installed in the interior of the vehicle shall meet the requirements stated in Federal Motor Vehicle Safety Standard 201 [October 1, 2002] Occupant Protection in Interior Impact as referenced in the In-Car Video Camera Systems Performance Specifications - Digital Video Systems provided by the International Association of Chiefs of Police. (11/21/2008).	✓	
All controls and components should be located and designed to minimize driver distraction. The control pad should be designed and organized to minimize officer workload. The record button should be readily identifiable by size, color, location and/or other design features. The record button should be easily accessible by officers wearing gloves.	✓	
System components shall be capable of being illuminated for ready identification during periods of darkness. The illumination level shall be capable of being controlled over a range from bright to dark.	✓	
All wiring shall meet industry standards applicable to the wire application including Underwriters Laboratory (UL) as well as the Society of Automotive Engineers (SAE).	✓	
Manufacturers shall provide information in their installer's guide or owner's manual that specifies the proper wiring, fuses, connectors, connection points with the vehicle electrical system and grounding points.	✓	
No parts that can come into contact with human skin shall be allowed to reach a temperature capable of causing a burn injury, Reference UL 60950 "Safety of Information Technology Equipment" as amended December 1, 2000	✓	
Any system component carried on the officer's person shall meet all Underwriters Laboratory Standards for shock/electrocution and burn prevention. All batteries used in such devices shall meet Underwriters Laboratory Standards for safety.	✓	
The In Car Video System shall operate on a power source that is filtered, regulated, and short-circuit protected. The voltage supplied to the In Car Video System components shall meet the manufacturer's specifications and shall not vary with fluctuations of the vehicle's electrical system of between 9 and 18 volts.	✓	

	Comply	
3.12.13 **RELIABILITY**	**Yes**	**No**
The video systems shall maintain consistent audio/visual recording quality. The in-car recording system shall not be affected by transmissions from the police communication or interference from the following sources: high-powered television stations; other radio frequency interference (e.g. UHF, VHF & HF); automobile alternator, ignition, electrical systems; automobile heaters / air conditioner fan motors; or other patrol vehicle electrical systems.	✓	
All equipment shall have a lifecycle of at least 3 years under law enforcement agency usage, or have replacement coverage under warranty and maintenance. Please provide expected lifecycle for all video system components.	✓	

When in operation, the mobile video system must not generate electromagnetic or radiation that interferes with communications or other electronic equipment found within a police vehicle	✓	
Loss of power to the system shall not cause loss of any recorded data or result in the unit requiring reprogramming, reloading of software or operating system software.	✓	
The video system shall be able to return to a “ready to record” mode after sudden loss of power without requiring user intervention.	✓	
The system’s timekeeping device and the vehicle’s identifier shall be protected by a system battery backup to prevent loss of information in the event the vehicle battery is disconnected for up to a minimum of fourteen (14) days.	✓	
Date and time within video system shall be self-adjusting for daylight savings time and leap years.	✓	
The video system shall have self-charging backup battery that continues recording upon loss of power, and should gracefully shutdown prior to available power being exhausted. The battery backup that shall power the system for at least 2 minutes following loss of the vehicle’s battery power.	✓	

	Comply	
3.12.14 **TRAINING/DOCUMENTATION**	**Yes**	**No**
The vendor shall offer and provide, at no additional cost, training to all end users on the use of the video system and video viewing software	✓	
The vendor shall offer and provide, at no additional cost, training to electronic technicians at their Reno, Elko, and Las Vegas shop locations. This training will ensure proper operation, repair, and maintenance of the manufacturer's video system.	✓	
A system administrator class covering all aspects of the system shall be given at all the DPS/HPD Regional Command sites (Reno, Elko, and Las Vegas) upon award.	✓	
Trainers must be experienced instructors who are thoroughly familiar with all technical aspects of the system.	✓	
Provide a course syllabus for training classes to be provided with your RFP response.	✓	
Vendor shall include documentation for procedures on regular maintenance of video system components.	✓	
Vendor shall provide complete service manuals and service bulletins on all electronic components.	✓	
Vendor shall provide documentation of system that includes identification of all vehicle equipment and the physical configuration; all configurable system parameters; written installation instructions, user manuals; and system administrator manuals instructions covering the change of all configuration settings.	✓	

ATTACHMENT L BODY WORN SPECIFICATIONS

Vendors must respond check either yes or no to each section below: Where section asks to provide details or response, vendors must respond to the corresponding RFP section not in this document.

	Comply	
3.11.2 BWC Hardware Requirements	Yes	No
Cameras worn by officers shall be lightweight, preferably six ounces or less in total combined weight.	✓	
Cameras shall have minimal wiring, not exceed two wires or cables and shall be designed to disengage to prevent the wearer from becoming entangled.	✓	
Cameras shall have recording capability of at least ten continuous (10) hours (the State would prefer twelve (12) hours of continuous recording capability).	✓	
Cameras must have a minimum stand-by battery life of ten (10) hours without recharging or additional batteries, with pre-record on.	✓	
BWC Shall be user friendly that can be activated easily during times of stressful events.	✓	
BWC should have automatic triggers, as a standalone system.	✓	
Rechargeable battery must be able to reach full charge, from no power, in no more than six (6) hours.	✓	
Cameras must have a minimum of thirty-two (32) GB internal/integrated memory and storage media not be removable.	✓	
Rechargeable battery must be able to withstand at least three hundred (300) charging cycles, maintaining the 10 hour record time.	✓	
BWC lens must have a field of view from 95 to 145 degrees.	✓	
The recording speed shall be no less than 30 frames per second (fps).	✓	
Camera shall record video images in full color with a minimum resolution of 640 pixels x 480 pixels. Adjustable resolution is preferable.	✓	
Video compression shall be H.263 or higher.	✓	
Cameras shall have multiple mounting options to accommodate varying uniformed officers, plain-clothed officers, and tactical field situations. Examples include, but are not limited to, lapel, shoulder, eyeglasses, cap, helmet, holster, button shirt, zipper shirt, utility belt, snow suit etc. Mounts shall not require modification to current in-service uniforms.	✓	
Camera should allow for on scene (in the field) viewing? If so, describe the ability to playback or view video.	✓	
Camera shall provide feedback to user when activated, either via a visual indicator or audible tone.	✓	
Camera shall have the ability to be set to stealth mode while in the field.	✓	

Camera must have an indicator that shows current operating mode.	✓	
If the camera offers night vision enhancement, the State shall have the ability to enable or disable it.	✓	
The System should provide automatic indexing functionality of video files and be capable of interfacing with existing computer-aided dispatch (CAD) vendor, Spillman technologies.	✓	
Cameras shall automatically embed a time/date stamp in the recorded video.	✓	
Cameras shall prevent users from deleting recorded files without authorization.	✓	
Camera should have a method for adding desired metadata to video in the field prior to upload.	✓	
Officers should have the ability to playback or view video in the field on mobile cameras and/or MDC's (Panasonic FZ-G1 Tablet) wirelessly (i.e. Bluetooth).	✓	
Camera shall have a pre-event record feature (BWC should capture at least thirty (30) seconds of video prior to officer initiating the recording). Adjustable times are preferable.	✓	
Camera will export in a standard, open format, such that it can be replayed in freely available software without processing or conversion. Proprietary data formats shall not be accepted.	✓	
The Vendor must offer a multi-dock station capable of uploading digital evidence from multiple cameras simultaneously and have the capability to upload video via Wi-Fi and/or cellular LTE connectivity. If via cellular, product should be compatible with Fenny Wireless Skyus X modem.	✓	
The multi-dock station must charge the camera batteries, securely transfer files without loss of quality or metadata, and delete the files from the camera once transferred to the evidence management system.	✓	
The multi-dock station should not require a department computer to operate, connect or interface with the Internet (e.g. the multi-dock station should be a standalone device that connects to the cloud storage solution or server via an Ethernet connection).	✓	
The camera should not cause electromagnetic interference with nearby airwave radios (and other electronic equipment and radio communication systems).	✓	
Loss of power to the camera must not cause data to be lost/corrupted.	✓	
Cameras will be ruggedized. Cameras shall be able to survive a six-foot drop test. Cameras shall be able to operate at minimum temperature of -12 degrees Fahrenheit and a maximum temperature of 130 degrees Fahrenheit.	✓	
Vendor will state camera's Ingress Protection (IP) rating. The State prefers an IP rating of IP67.	✓	
Describe what features devices have in place to prevent accidental activations of camera by the user (without the need for accessories or alteration of equipment by user).	✓	
Vendor shall define the required time for automated indexing (specific time frame after upload of video evidence) and any expected error rate percentage upon indexing, if applicable.	✓	

The Vendor must state the transfer rate of video from the multi-dock station to the cloud in sixty or thirty-minute increments. Vendors shall break down transfer rates by video quality (i.e. Hi Def).	✓	
Describe device wireless activation features (e.g. device is automatically activated with the activation of patrol vehicle's light bar), if applicable.	✓	

	Comply	
3.11.4 VIDEO MANAGEMENT SYSTEM (VMS)	Yes	No
VMS shall either be an externally hosted cloud-based data storage solution with the capability of organizing/managing video/digital evidence, server based or consist of a hybrid solution and be accessible via the internet to multiple users simultaneously. The State prefers the Cloud or Hybrid solution.	✓	
VMS shall allow for remote access with complete functionality (review, enter metadata and send video) with NHP mobile devices and/or computers.	✓	
VMS shall provide an automatic audit trail for when files and videos are accessed.	✓	
VMS shall allow officers to enter additional metadata to recorded files, such as notes or comments.	✓	
Solution must support all major digital file types (avi, jpeg, mpeg, etc.).	✓	
VMS shall provide remote viewing of the stored video based on the permissions granted by the System Administrator.	✓	
VMS shall allow users to search video files by name, date of recording, date of upload, case number (CAD-generated), device number, as well as categorize and add notes to each file within the solution.	✓	
VMS must allow System Administrators the ability to grant access of specific files to specified persons for a specific period of time.	✓	
VMS shall have the ability to share files internally and externally via secure links over the Internet.	✓	
When videos are exported to a portable media device , all metadata shall transfer over without compromising its authenticity.	✓	
VMS shall grant System Administrators the ability to set variable retention rules per DPS/HPD preferences.	✓	
VMS shall have the ability to set time tables for automatic deletions of files.	✓	
VMS should have the ability to recover deleted evidence within a minimum of seven (7) days of deletion. The State would prefer a recovery period of 30 days.	✓	
The VMS will maintain a log/audit trail illustrating users who have viewed and copied video to an external source (e.g. DVD/ long term storage).	✓	
VMS must have the ability to preserve the raw file without editing.	✓	
VMS must securely store all videos and recordings in a way that only State-authorized users and users authorized by DPS/HPD can view.	✓	
VMS must provide redundant, security back-up of all data.	✓	
VMS should offer redaction capabilities.	✓	

VMS must be compatible with at least Windows 7 Professional Operating System or more recent versions) and Internet Explorer Version 11 web browser or more recent version(s).	✓	
Provide the minimum required memory (RAM), if applicable.	✓	
Provide the minimum required processor speed, if applicable.	✓	
Provide the minimum network speed to upload videos, if cloud based.	✓	
Upload times to the VMS will be defined in per hour or thirty-minute increments of video files.	✓	
Any required or expected 'buffering' times before video files are accessible in cloud storage (for view or adding metadata) will be clearly defined.	✓	
Describe System compatibility with mobile devices (iPhones and Android).	✓	
Vendor shall indicate the number of searchable fields in storage system and any 'wild card' searches that can be done to locate stored data.	✓	
Preferences:		
Users should have the ability to send email messages from hosted solution interface to end users.	✓	
VMS should send System Administrators administrative notifications when evidence files are about to be deleted.	✓	
VMS should send System Administrators administrative notifications when users need their credentials reset due to failed log on attempts.	✓	
VMS should offer auto-redaction capabilities, to include high-movement and low light video; preferred to minimize the amount of time to redact 30 fps for the entire length of video.	✓	
VMS should have the ability to capture data, report on video statistics and provide custom reports.	✓	

	Comply	
3.11.5 VIDEO STORAGE	Yes	No
If cloud based, the storage facility must be located within the continental United States.	✓	
Does your storage solution have the ability to upload video from multiple camera units simultaneously?	✓	
Storage solution should have the ability to view multiple linked videos simultaneously.	✓	
Solution should have two tier storage capacity for active video and long term storage needs as defined by the State.	✓	
Does proposed solution offer storage options for 'unlimited storage' of body camera video evidence?	✓	
Does your system provide a method to upload videos, via an access point? Please describe your process.	✓	
Is your system compatible with an EnGenius ENS500EXT access point?	✓	

Does solution have the ability to maintain and export audit trail along with video?	✓	
Define maximum storage capacity, if any.	✓	
Describe the capability of proposed solution to provide the State with the ability to export/download and migrate original recordings with all metadata to other storage media or, local storage inclusive of all metadata and chain of custody information.	✓	
Describe archival, hot and cold cloud storage solutions.	✓	
Describe archival solutions for server storage, if applicable.	✓	
Discuss different cost savings as defined by various storage solutions (active vs. long-term storage of files).	✓	
Describe capability to respond to requests to pull video from 'cold cloud storage', including time required to download video from storage.	✓	
Describe your solution to upload video in the rural areas that only have a maximum broadband speed of 1.5 Mbps	✓	

	Comply	
3.11.6 SYSTEM SECURITY	Yes	No
The VMS shall meet the minimal security requirements for the Criminal Justice Information Services (CJIS) Policy. In particular, the VMS shall comply with Policy Areas 2 through 13 in Section 5 of the CJIS Policy. The CJIS Policy can be viewed by accessing the following link: https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center	✓	
Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access? (5.5.6 Remote Access)	✓	
Will advanced authentication (AA) be required for access to CJI within a cloud environment (5.6.2.2 Advanced Authentication, 5.5.2.2.1 Advanced Authentication Policy and Rationale)	✓	
Does your cloud service provider's datacenter(s) used in the transmission or storage of CJI meet all the requirements of a physically secure location? (5.9.1 Physical Secure Location)	✓	
Are the encryption requirements being met? (5.10.1.2 Encryption)	✓	
Who will be providing the encryption as required in the CJIS Security Policy? (Client or cloud service provider)	✓	
Is the data encrypted while at rest and in transit?	✓	
What are the cloud service provider's incident response procedures? (5.3 Policy Area 3: Incident Response)	✓	
Will the cloud subscriber be notified of any incident?		
If CJI is compromised, what are the notification and response procedures?	✓	
Is the cloud service provider a private Vendor/vendor?		✓
If so, they are subject to the same screening and agreement requirements as any		

other private Vendors hired to handle CJI. (5.1.1.5 Private Vendor User Agreements and CJIS Security Addendum; 5.12.1.2 Personnel Screening for Vendors and Vendors)		
Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits? (5.11.1 Audits by the FBI CJIS Division; 5.11.2 Audits by the CSA)	✓	
The State may verify that Vendor is in compliance with CJIS by requesting a compliance audit of Vendor's technology deployment through the CJIS Systems Agency to the Federal Bureau of Investigation (FBI). The FBI CJIS Division shall perform the requested audit to verify compliance. 140-2.	✓	
System shall provide full conformance to Federal Information Processing Standards (FIPS) Publication	✓	
VMS shall provide user authentication with a unique username and password.	✓	
VMS will allow for authorized users to be established based on various roles and permissions by the System Administrator.	✓	
VMS will offer optional IP access restriction and security challenge questions upon access from an unknown or previously used location.	✓	
Any access to stored video shall be maintained in an automatic log or audit trail showing users that have viewed, shared or copied video to an external source (e.g. CD/DVD, local storage, etc.), and the audit trail should be capable of being exported	✓	
Log activities performed by specific user ID, IP address and time/date stamp all activities.	✓	
System Administrators shall have the ability to administratively manage accounts and assign rights and permissions to system users.	✓	
VMS shall provide ability to set an unsuccessful access attempt limit and suspend IDs after reaching the unsuccessful access threshold.	✓	
VMS shall provide ability to send alerts to System Administrators for unauthorized access attempts.	✓	
VMS shall enable automatic logoff of ID after a defined period of session inactivity, and perform subsequent re-log-on password authentication.	✓	
VMS shall provide ability to configure password parameters such as password lengths, user access to expiration settings and other behaviors, enabling alphanumeric characters, etc.	✓	
VMS shall provide ability to lock out user or group ID.	✓	
Vendor will provide a detailed explanation of data security standards, to include but not limited to: defining the physical environment, location of all host servers; protections against natural and man-made disasters; encryption; transfer; storage; redundancy and recovery of files.	✓	
Describe security standards for hardware (cameras) in place to prevent data from being accessed in the event a camera is lost or stolen.	✓	
Vendor will describe any previous loss of data occurring from criminal actions, as well as other issues that impact data integrity, such as unauthorized data access by contract personnel.	✓	

Provide a non-technical means for field personnel to remotely view stored video without altering original file (other than applying metadata to file).	✓	
Describe ability of system to enforce password expiration.	✓	
Describe ability of system to limit concurrent sessions.	✓	
Describe ability of system to log changes to administrative functions.	✓	

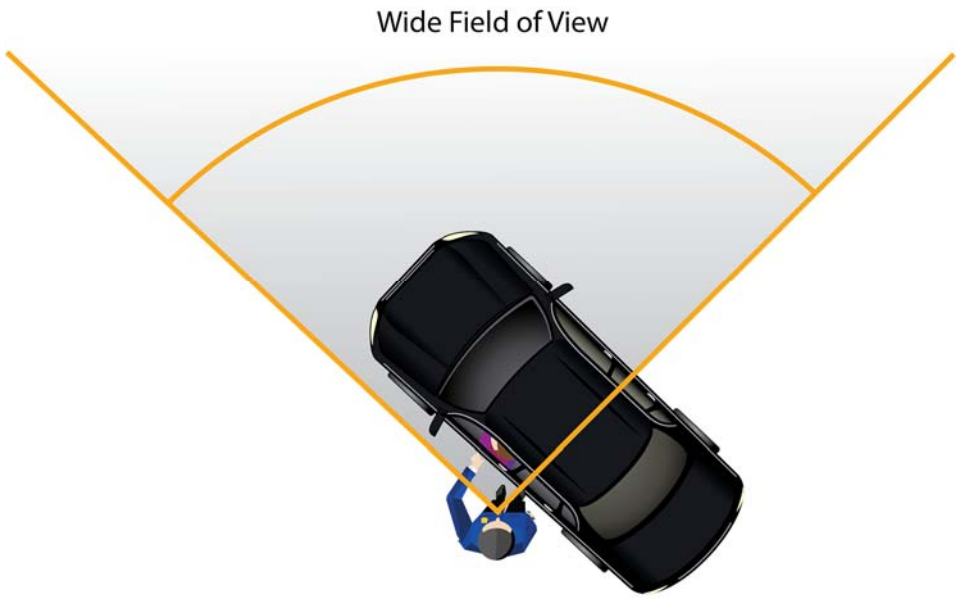
	Comply	
3.11.7 INFORMATION SECURITY	Yes	No
Vendor shall encrypt transmission of confidential data when transferred through publicly accessible networks such as the Internet.	✓	
Vendor shall ensure all transmission of information data files are transferred through a Secure Socket Layer (SSL), which creates a 128 bit encrypted connection which is password protected. All data files that are on Vendor's servers are encrypted once they have completed the upload and pre-process procedures.	✓	
All input data transmitted across public networks (all networks other than the State's) shall be encrypted during transit and decrypted electronically during processing to produce non-confidential output data. The decrypted data shall not be accessible by Vendor's employees unless otherwise limited on a "need to know" basis as determined by the Nevada Highway Patrol's designee.	✓	
The System shall have a host-based firewall technology preventing inappropriate/ unauthorized access. Vendor shall provide the following:	✓	
All intrusion detection system monitoring for unauthorized access attempts.	✓	
Must run anti-virus software.	✓	
Monitor daily logs for potential intrusions, file integrity.	✓	
Only allow access by uniquely assigned and auditable IDs.	✓	
All data transfers and administrative access must be in an encrypted format.	✓	

	Comply	
3.11.8 IN-CAR VIDEO INTEGRATION	Yes	No
BWC must have the ability to record audio for the In-car video system.	✓	
BWC must have the ability to activate recording off the In-Car video systems automatic triggers.	✓	

3.11.2 BWC Hardware Requirements

3.11.2.10 BWC lens must have a field of view from 95 to 145 degrees.

RESPONSE: Utility has incorporated the feedback from NHP for our BodyWorn by increasing the field of view of our system. Below is a diagram of the expected field of view from the new BodyWorn camera that will be implemented by NHP should Utility be selected for this project.



3.11.2.33 Vendor will state camera's Ingress Protection (IP) rating. The State prefers an IP rating of IP67.

RESPONSE: BodyWorn is IP67 rated.

3.11.2.34 Describe what features devices have in place to prevent accidental activations of camera by the user (without the need for accessories or alteration of equipment by user).

RESPONSE: BodyWorn is securely mounted inside of a vest and is activated via automated policy-based recording triggers or a bluetooth controller worn by the user. This prevents most accidental activations of the camera by the user, but a minimum recording duration can be configured, based on agency so that accidental activations are discarded if BodyWorn hasn't recorded for the minimum defined recording duration. For example, if BodyWorn is activated and the minimum recording duration is set to 5 seconds, it would have to record more than 5 seconds otherwise the recording is discarded and considered an accidental activation.

3.11.2.35 Vendor shall define the required time for automated indexing (specific time frame after upload of video evidence) and any expected error rate percentage upon indexing, if applicable.

RESPONSE: Not applicable - video is made available for review immediately after upload.

3.11.2.36 The Vendor must state the transfer rate of video from the multi-dock station to the cloud in sixty or thirty-minute increments. Vendors shall break down transfer rates by video quality (i.e. Hi Def).

RESPONSE: BodyWorn transfers video wirelessly to the cloud and as such, the transfer rate will vary depending on the amount of bandwidth available on the upload link. From our testing, we have observed transfer rates of 1GB of data in 90 seconds. Transfer rates will not vary depending on quality.

3.11.2.37 Describe device wireless activation features (e.g. device is automatically activated with the activation of patrol vehicle's light bar), if applicable.

RESPONSE: BodyWorn can be automatically triggered when used in conjunction with the Rocket IoT with no detectable latency. In addition, BodyWorn can be automatically triggered from policy-based events such as the light bar turning on, the door opening, shotgun being removed, etc. Action zones can be created by dispatch in the event of an emergency to cause specified devices to begin recording when they physically enter the action zone. In order to aid in communication during such an emergency, BodyWorn can provide a live stream to authorized users.

3.11.4 VIDEO MANAGEMENT SYSTEM (VMS)

3.11.4.20 Provide the minimum required memory (RAM), if applicable.

RESPONSE: Because AVaiL, our VMS, is cloud-based and accessed via a web browser, there are no specific minimum memory requirements.

3.11.4.21 Provide the minimum required processor speed, if applicable.

RESPONSE: Since AVaiL is cloud-based and accessed via a web browser, there are no specific minimum processor speed requirements.

3.11.4.22 Provide the minimum network speed to upload videos, if cloud based.

RESPONSE: Due to the way BodyWorn uploads evidence, there is no specific minimum network speed. We have observed successful upload of video to the cloud with upload throughputs as low as 0.5Mbps.

3.11.4.25 Describe System compatibility with mobile devices (iPhones and Android).

RESPONSE: AVaiL can be accessed from any operating system including iOS on iPhone and Android.

3.11.4.26 Vendor shall indicate the number of searchable fields in storage system and any 'wild card' searches that can be done to locate stored data.

RESPONSE: The search feature within AVaiL operates similar to how modern search engines function which means that keywords that are within the metadata can be used to search for incidents providing very powerful searching capabilities within the system. Some common search parameters include officer name, device name, classification type, title, GPS location, related incidents, etc.

3.11.5 VIDEO STORAGE

3.11.5.6 Does your system provide a method to upload videos, via an access point? Please describe your process.

RESPONSE: The BodyWorn video automatically uploads to the CJIS compliant Evidence Vault provided by the RocketIoT installed within the patrol vehicle. This automatic secure transfer of video evidence mitigates the risk of video being lost or damaged while on the body camera. Once the video has been transferred to the Evidence Vault within the patrol vehicle, it will be uploaded based on department policies via cellular or Wi-Fi depending on the priority of the incident. High priority items can be transferred immediately to the cloud while lower priority items offload over Wi-Fi through Smart Waypoints, provided by Utility, once the vehicle returns to the department. Physically docking body cameras is time consuming and a hindrance on operational efficiencies. Real-time wireless offload allows for true situational awareness and ensures Chain-of-Custody.

3.11.5.9 Define maximum storage capacity, if any.

RESPONSE: BodyWorn has a maximum storage capacity of 16GB (with options of expanding to 32GB or higher.) BodyWorn doesn't normally reach the maximum storage capacity since it automatically uploads video as it is recording to the RocketIoT Evidence vault installed within the vehicle.

3.11.5.10 Describe the capability of proposed solution to provide the State with the ability to export/download and migrate original recordings with all metadata to other storage media or, local storage inclusive of all metadata and chain of custody information.

RESPONSE: AVaiL supports the ability to export original recordings as H.264/AAC MP4 and metadata and chain of custody information as CSV.

3.11.5.11 Describe archival, hot and cold cloud storage solutions.

RESPONSE: AVaiL initially stores video evidence in immediately-available hot storage, enabling users to review and categorize fresh evidence without delay. After a set period, AVaiL will automatically move video evidence into cold storage for permanent archival. After evidence has been moved to cold storage, users can request evidence, and AVaiL will notify the user via email that the evidence is again available in hot storage.

3.11.5.12 Describe archival solutions for server storage, if applicable.

RESPONSE: This is not applicable as we offer a cloud storage solution.

3.11.5.13 Discuss different cost savings as defined by various storage solutions (active vs. long-term storage of files).

RESPONSE: The BodyWorn solution is offered with unlimited data storage as long as the department follows state mandated retention policies. This savings is included within the Utility proposal.

3.11.5.14 Describe capability to respond to requests to pull video from 'cold cloud storage', including time required to download video from storage.

RESPONSE: Users will use the normal AVaiL search functions to locate the evidence that they wish to review. If the evidence has already been moved to cold storage, then the user will use AVaiL to request access to the evidence. Within 4 to 5 hours, AVaiL will have the evidence available in hot storage and notify the user that it is available for review.

3.11.5.15 Describe your solution to upload video in the rural areas that only have a maximum broadband speed of 1.5 Mbps

RESPONSE: Utility uploads video and audio in one-minute increments, no matter what the local backhaul speed is.

The BodyWorn video automatically uploads to the CJIS compliant Evidence Vault provided by the RocketIoT installed within the patrol vehicle. This automatic secure transfer of video evidence mitigates the risk of video being lost or damaged while on the body camera. Once the video has been transferred to the Evidence Vault within the patrol vehicle, it will be uploaded based on department policies via cellular or Wi-Fi depending on the priority of the incident. High priority items can be transferred immediately to the cloud while lower priority items offload over Wi-Fi through Smart Waypoints, provided by Utility, once the vehicle returns to the department. Physically docking body cameras is time consuming and a hindrance on operational efficiencies. Real-time wireless offload allows for true situational awareness and ensures Chain-of-Custody.

3.11.6 SYSTEM SECURITY

3.11.6.6 Who will be providing the encryption as required in the CJIS Security Policy? (Client or cloud service provider)

RESPONSE: For BodyWorn Utility and Amazon will provide the encryption as required in the CJIS Security Policy. Data is secured with AES 256 bit encryption while on the device, in transit, and at rest in the cloud.

3.11.6.8 What are the cloud service provider's incident response procedures? (5.3 Policy Area 3: Incident Response)

RESPONSE: Full CJIS compliance and third party audit available for review.

3.11.6.10 If CJI is compromised, what are the notification and response procedures?

RESPONSE: In the very unlikely event of this occurring, Utility will notify the NHP Point of Contact of the compromise within 2 hours of discovery.

3.11.6.27 Vendor will provide a detailed explanation of data security standards, to include but not limited to: defining the physical environment, location of all host servers; protections against natural and man-made disasters; encryption; transfer; storage; redundancy and recovery of files.

RESPONSE: By using Amazon GovCloud Web Services, we are able to maintain 99.99999999999% resilience in the government cloud. Due to the way this type of infrastructure is designed, data is constantly replicated across various data centers within CONUS.

3.11.6.28 Describe security standards for hardware (cameras) in place to prevent data from being accessed in the event a camera is lost or stolen.

RESPONSE: All data on the device is encrypted at rest and only authorized users are able to view video and associated metadata. No user has access to the raw data stored on the device.

3.11.6.29 Vendor will describe any previous loss of data occurring from criminal actions, as well as other issues that impact data integrity, such as unauthorized data access by contract personnel.

RESPONSE: Utility BodyWorn has not lost any data due to criminal actions or unauthorized access by contract personnel.

3.11.6.31 Describe ability of system to enforce password expiration.

RESPONSE: AVaiL allows for customizable password expiration according to department policy.

3.11.6.32 Describe ability of system to limit concurrent sessions.

RESPONSE: A unique user can only have one unique session at any given time. In this way, a user cannot remain logged in at one workstation and log in to another workstation at the same time.

3.11.6.33 Describe ability of system to log changes to administrative functions.

RESPONSE: All changes to administrative functions are logged along with the user who made the changes and other various information.

3.12.3 DIGITAL VIDEO RECORDER (DVR)

3.12.3.6. The DVR shall have the ability to record up to 8 hours of video before reaching the capacity of the storage media at maximum resolution. For the recording media available, specify the recording and playback times, resolution, and MB per second.

RESPONSE: RocketIoT can record over 20 hours of video before reaching the capacity of the storage media at maximum resolution. RocketIoT video evidence is immediately captured and immediately available for playback at its native resolution. RocketIoT records front-facing and backseat video at a configurable resolution of 720p up to 1080p at 30 FPS at anywhere between 1.9MB and 6.9 MB per second.

3.12.3.7. Video resolution, frame rates, and quality on the DVR shall be preset but can be changed by an administrator. These settings shall be independently configurable for recording modes of both video cameras. Please specify levels for: video resolution, video frame rate, video quality

RESPONSE: By default, the cameras connected to RocketIoT are preset to 720p at 30FPS, but this can be configured for either camera up to 1080p.

3.12.3.13. The DVR shall include a programmable pre-event recording mode allowing it to capture images a minimum of 30 seconds prior to the activation of the RECORD mode. Please specify pre-event recording capability of proposed DVR.

RESPONSE: RocketIoT includes a programmable pre-event recording mode allowing it to capture images at configurable intervals such as 5 seconds, 30 seconds, or 60 seconds. This can be configured to different values for the front and rear cameras if desired.

3.12.3.19. The Control Center/DVR firmware shall allow in-system programming for future updates. Please describe how updates are made.

RESPONSE: Updates are pulled automatically by RocketIoT from the cloud. There is also a manual method for pulling updates which can be initiated from the local interface. The system supports flexible Over-The-Air (OTA) updates for the entire fleet, groups, and individual devices.

3.12.3.24. The DVR shall be capable of operating within the range of interior temperatures found within a law enforcement vehicle in Nevada without the need for supplemental heating or cooling. Specify your DVR's operating range and acceptability for the extreme temperature range in Nevada

RESPONSE: RocketIoT is capable of operating within the range of interior temperatures found within a law enforcement vehicle in Nevada without the need for supplemental heating or cooling. The operating range of RocketIoT is -4°F to 158°F.

3.12.4 COMPACT CCD COLOR CAMERA

3.12.4.1. The low-light CCD color camera shall use a Sony EXview® HAD CCD or equivalent image sensor to provide high quality nighttime images while minimizing blooming and glaring from bright sources of light. Proof of "equal" shall be the responsibility of the bidder and shall be submitted with the bid if not using the Sony EX VIEW chipset.

RESPONSE: As a standard RocketIoTX utilizes a robust IP66 weather resistant camera with a Sony Exmor CMOS image sensor. This camera offers excellent low light capability with a 0.1 Lux rating. CMOS has lower power consumption and less vertical smearing than the CCD sensors. The RocketIoTX has the ability to support various IP cameras with H.264 stream.

3.12.4.8. The front camera should have a minimum 120X zoom (10x optical zoom with 12x digital zoom). Please specify _____ mode.

RESPONSE: As a standard, RocketIoTX camera does not support optical or digital zoom on the camera itself due to the 1080P resolution. Image zooming can be accomplished within the AVaiL Video Management software once video is uploaded to the system. The compact form factor of the front facing camera offers a high degree of visibility to the vehicle driver by minimizing the intrusion of the AS1 line on the windshield of the vehicle. RocketIoTX has the ability to support various IP cameras with H.264 stream.

3.12.4.15. The camera shall be compact. List the size and weight of the proposed CCD camera.

RESPONSE: The dimensions for the camera are 0.9" x 3.8" and it weighs 0.3 lbs.

3.12.5 BACK SEAT CAMERA SPECIFICATIONS

3.12.5.1. The back-seat camera shall utilize a micro compact with wide angle 1/3" Super HAD image device (or equivalent) with approximately 420 lines of resolution. Proof of "equal" shall be the responsibility of the bidder and shall be submitted with the bid. This must be included in the system at no charge.

RESPONSE: The back-seat camera utilizes a micro compact with wide angle ⅓" Sony Super HAD image device with 420 lines of resolution.

3.12.5.4. The rear-facing camera shall have a minimum lux rating of .03. Please specify the rating

RESPONSE: RocketIoT's rear facing camera automatically switches to infrared mode in very low light, effectively requiring a minimum LUX rating of 0.

3.12.9 VIDEO VIEWING SOFTWARE/HARDWARE

3.12.9.3. Vendors shall provide all hardware (media readers/drives) and software necessary duplicate, share and present digital video in a court acceptable format. Please describe transfer steps needed to convert captured video to court acceptable evidence without the need for a server based infrastructure.

RESPONSE: Video evidence can be exported into MP4 or ISO format which can then be burnt to a DVD and will play on a DVD player in court.

3.12.11 CONTROL CENTER SPECIFICATIONS

3.12.11.2. The State is interested in a system that can be configured for motorcycle use. All of the specifications described for the DVR and wireless microphone shall be applicable. Is a motorcycle option available for your solution? If so, does the configuration utilize a weatherproofed monitor and camera? Please explain.

RESPONSE: A motorcycle option is available for Utility's solution that utilizes a weatherproofed monitor and camera.

3.12.11.4. Describe dimensions and vehicle mounting options for your camera, recorder, wireless microphone, transmitter/ receiver and any other required equipment.

RESPONSE: The RocketIoTX is a very compact solution by offering a combined wireless router and DVR within a single device. Dimensions are 197 x 150 x 44 (LxWxH) mm. The device is typically installed within the trunk of the vehicle or storage compartment within an SUV. The compact form factor of the front facing camera offers a high degree of visibility to the vehicle driver by minimizing the intrusion of the AS1 line on the windshield of the vehicle.

3.12.15 Installation

3.12.15.1 Describe your approach for installing camera systems if this service is requested by the State. The State reserves the right to do such installations either through its fleet shops, or through an accessory installation contract.

Utility has reviewed and understands the requirement. Utility's approach to installing camera systems in provided in the Project Management narrative above.

3.12.15.2 Provide an installation price per camera unit for each regional office.

Utility installation price per camera unit for each regional office is included in the Pricing for the Cost Proposal submitted in a separate sealed package as requested by the RFP.

3.12.15.2 Specify the companies that will provide installation of camera systems in our Reno, Elko and Las Vegas regional offices if requested by the State.

If Utility is contracted to perform installation, it is Utility's intention to use its own staff and resources to provide installation of cameras systems at these regional offices for the State of Nevada.

4. COMPANY BACKGROUND AND REFERENCES

4.1 VENDOR INFORMATION

4.1.1.1 Vendors must provide a company profile in the table format below.

Question	Response
Company name:	Utility Associates, Inc.
Ownership (sole proprietor, partnership, etc.):	Corporation
State of incorporation:	Delaware
Date of incorporation:	2001
# of years in business:	15
List of top officers:	Robert McKeeman, Chief Executive Officer Ted Davis, President/ Chief Technology Officer Chris Lindenau, Chief Revenue Officer Anthony Baldoni, VP of Operations Simon Araya, VP of Engineering Jason Blair, Chief Financial Officer
Location of company headquarters:	Decatur, GA
Location(s) of the company offices:	Decatur, GA and Covington, GA
Location(s) of the office that will provide the services described in this RFP:	Decatur, GA (headquarters) and Covington, GA (warehouse)
Number of employees locally with the expertise to support the requirements identifie this RFP:	60
Number of employees nationally with the expertise to support the requirements in this RFP:	65
Location(s) from which employees will be assigned for this project:	Decatur, GA and Covington, GA

4.1.2 **Please be advised**, pursuant to NRS 80.010, a corporation organized pursuant to the laws of another state must register with the State of Nevada, Secretary of State's Office as a foreign corporation before a contract can be executed between the State of Nevada and the awarded vendor, unless specifically exempted by NRS 80.015.

4.1.3 The selected vendor, prior to doing business in the State of Nevada, must be appropriately licensed by the State of Nevada, Secretary of State's Office pursuant to NRS76. Information regarding the Nevada Business License can be located at http://nvsos.gov.

Question	Response
Nevada Business License	Utility will obtain prior to contract
Number:	Utility will obtain prior to contract
Legal Entity Name:	Utility Associates, Inc.

Is "Legal Entity Name" the same name as vendor is doing business as?

Yes	X	No	

If "No", provide explanation.

4.1.4 Vendors are cautioned that some services may contain licensing requirement(s). Vendors shall be proactive in verification of these requirements prior to proposal submittal. Proposals that do not contain the requisite licensure may be deemed non-responsive.

4.1.5 Has the vendor ever been engaged under contract by any State of Nevada agency?

Yes		No	X

If "Yes", complete the following table for each State agency for whom the work was performed. Table can be duplicated for each contract being identified.

Question	Response
Name of State agency:	-NA-
State agency contact name:	-NA-
Dates when services were performed:	-NA-
Type of duties performed:	-NA-
Total dollar value of the contract:	-NA-

4.1.6 Are you now or have you been within the last two (2) years an employee of the State of Nevada, or any of its agencies, departments, or divisions?

Yes		No	X

If "Yes", please explain when the employee is planning to render services, while on annual leave, compensatory time, or on their own time?

If you employ (a) any person who is a current employee of an agency of the State of Nevada, or (b) any person who has been an employee of an agency of the State of Nevada within the past two (2) years, and if such person will be performing or producing the services which you will be contracted to provide under this contract, you must disclose the identity of each such person in your response to this RFP, and specify the services that each person will be expected to perform.

4.1.7 Disclosure of any significant prior or ongoing contract failures, contract breaches, civil or criminal litigation in which the vendor has been alleged to be liable or held liable in a matter involving a contract with the State of Nevada or any other governmental entity. Any pending claim or litigation occurring within the past six (6) years which may adversely affect the vendor's ability to perform or fulfill its obligations if a contract is awarded as a result of this RFP must also be disclosed.

Does any of the above apply to your company?

Yes		No	X

If "Yes", please provide the following information. Table can be duplicated for each issue being identified.

Question	**Response**	
Date of alleged contract failure or breach:	None	
Parties involved:	-NA-	
Description of the contract failure, contract breach, or litigation, including the products or services involved:		
Amount in controversy:	-NA-	
Resolution or current status of the dispute:	-NA-	
If the matter has resulted in a court case:	Court	Case Number
	-NA-	-NA-
Status of the litigation:	-NA-	

4.1.8 Vendors must review the insurance requirements specified in ***Attachment E, Insurance Schedule for RFP 3273.*** Does your organization currently have or will your organization be able to provide the insurance requirements as specified in ***Attachment E.***

Yes	X	No	

Any exceptions and/or assumptions to the insurance requirements ***must*** be identified on ***Attachment B, Technical Proposal Certification of Compliance with Terms and Conditions of RFP.*** Exceptions and/or assumptions will be taken into consideration as part of the evaluation process; however, vendors must be specific. If vendors do not specify any exceptions and/or assumptions at time of proposal submission, the State will not consider any additional exceptions and/or assumptions during negotiations.

Upon contract award, the successful vendor ***must*** provide the Certificate of Insurance identifying the coverages as specified in ***Attachment E, Insurance Schedule for RFP 3273.***

4.1.9 Company background/history and why vendor is qualified to provide the services described in this RFP. Limit response to no more than five (5) pages.

Utility (Utility Associates, Inc.) is a Delaware Corporation with Headquarters in Decatur, Georgia. The company was incorporated in 2001 and specializes in Software as a Service for Public Safety, Transit, and Utility companies within the US. With over 50,000 devices deployed, Utility has worked with many progressive first responders, transit agencies and utilities to incorporate industry best practices to help solve critical legal evidence capture and field situational awareness management challenges.

Utility is a vertically integrated US manufacturer and supplier of body worn cameras, in-car cameras, mobile routers, mobile Digital Multi-Media Evidence management systems, and situational awareness software solutions for the law enforcement community, transportation agencies, and utilities. Our systems preserve the reputations of law enforcement departments and their officers, discourage frivolous litigation, support prosecution, and promote officer safety.

Utility hardware and software is designed, developed, manufactured, packaged, and shipped at our state-of the-art locations in Decatur, Georgia and in Covington, Georgia. Many vendors outsource

engineering, software development and support, and/or manufacturing offshore. Rather, Utility's control of the design, development, manufacturing and customer support experience through our in-house team of professionals allows us to provide a secure, reliable solution, and eliminate an 8,000 mile supply chain, while rapidly innovating and responding to our customer's needs.

The Utility BodyWorn video recording software is the proven result of 10+ years of development and deployment in thousands of In-Car Video Recording systems around the US. The video recording software was originally developed between 2004 and 2008, developed and sold as video recording hardware and software for Police and Public Transit In-Car Video Recording systems. Approximately $70M of venture capital went into the legacy firm, with another $20M of venture debt. A significant portion of this capital funded the development of the mobile Chain of Custody Linux-based video recording software that was ported by Utility to run on Android mobile computing devices. Utility acquired the successor company in January 2013. Utility added further audit trail and functional capabilities to the Firm's video recording software.

The Utility BodyWorn software running on an Android mobile computing device, represents over 10+ years of proven police video recording software that has been ported to the Android platform.

Utility's most notable customers include:

- ***Colorado Springs CO Police Department***
- ***City of Long Beach CA Police Department***
- ***Bexar County TX Sheriff's Office***
- ***Marietta GA Police Department***
- ***City of Atlanta GA Police Department***
- ***DeKalb County Police Department***
- ***Department Florida Highway Patrol***
- ***Boca Raton FL Police Department***

Utility's Strengths Include:

- ***In-house Design Engineering with vast years of experience in developing and delivering industry standard products of highest quality and interoperability.***
- ***Deep experience in designing and assisting in network design for video flow and storage at public safety departments.***
- ***Knowledgeable in recent implemented CJIS requirements for agencies.***
- ***Ability to roll-out large-scale, complicated implementations in a tight time frame with success.***
- ***Advanced state of the art technology for in-car and body worn video.***
- ***Utility owns US Patent 6,831,556 for a "Composite Mobile Digital Information System" for public safety vehicles. This patent was issued on December 14, 2004, and describes a vehicle video recording system for capturing video, audio, and metadata information. Utility manufactures and sells a vehicle video recording system that is covered by US Patent 6,831,556. "Pre-Event Recording" is a key part of our patented system, and is a capability that the City should evaluate closely. Additional Patents pending. Utility holds the following Relevant Credentials to this RFP:***
  - ***6,831,556 – Composite Mobile Digital Information System***
  - ***7,768,548 – Mobile Digital Video Recording System***
  - ***8,781,475 – System for Switching between Cellular Networks***
  - ***9,246,898 – Method for Securely Distributing Legal Evidence***
  - ***9,282,495 – Method and Device for Switching between Cellular Networks***
- ***Experienced professional staff with many years of Digital Multi-Media Evidence experience.***
- ***All Utility solutions are Country of Origin USA, are manufactured in the USA.***
- ***Utility is fully committed to supporting the country through the Buy American Act and the American Recovery and Reinvestment Act. All Utility solutions are BAA and ARRA Compliant.***

4.1.10 Length of time vendor has been providing services described in this RFP to the public and/or private sector. Please provide a brief description.

Utility Associates, Inc. is leading the body worn camera industry with its state-of-the-art BodyWorn™ body camera, the only body camera available that automates the recording process. Our success in becoming the industry leader is attributed to not only developing cutting edge technology but our continual commitment to building successful partnerships with our customers.

For over a decade Utility has dedicated its efforts to serving the law enforcement, first responder, mass transportation, and utility communities. Specifically with BodyWorn™, the focus has been to preserve the reputations of law enforcement departments and their officers, discourage frivolous litigation, support prosecution, and promote officer safety while maintaining an easy to use, intuitive user application.

Currently, Utility supports varying sized agencies ranging from small units with 25 cameras to large, multi-precincts with over 600 hundred cameras. Utility has extensive experience serving state, county, and city law enforcement agencies with both body worn digital camera systems and in-vehicle video cameras and video management systems. Our large-scale, large department BodyWorn™ camera deployments include agencies from across the nation such as the DeKalb County, Georgia (600 BodyWorn™ cameras) and the City of Colorado Springs, Colorado (500 BodyWorn™ cameras and 250 in-vehicle units). Utility also has history of considerable experience in large-scale and accelerated in-vehicle deployments, including Florida Highway Patrol's deployment of more than 2,000 vehicles for in-car video; as well as 1,820 units for Chicago Transit Authority in 2012, and an additional 1,000 units in 2015.

4.1.11 Financial information and documentation to be included in Part III, Confidential Financial Information of vendor's response in accordance with Section 9.5, Part III – Confidential Financial Information.

4.1.11.1 Dun and Bradstreet Number

Utility has provided this information as requested, within the Confidential Financial Information package.

4.1.11.2 Federal Tax Identification Number

Utility has provided this information as requested, within the Confidential Financial Information package.

4.1.11.3 The last two (2) years and current year interim:

4.1.11.3.1 Profit and Loss Statement
4.1.11.3.2 Balance Statement

Utility has provided this information as requested, within the Confidential Financial Information package.

4.2 SUBCONTRACTOR INFORMATION

4.2.1 Does this proposal include the use of subcontractors?

Yes		No	X

4.3.2 BUSINESS REFERENCES

4.3.1 Vendor must provide at least three (3) law enforcement agencies within the last two (2) years as references, for which it is verifiable that the vendor has deployed at least 100 active BWS's that have been in service for at least six (6) months for each of those references.

Utility has provided this information as requested, see below.

4.3.2 Vendors must provide the following information for ***every*** business reference provided by the vendor and/or subcontractor:

The "Company Name" must be the name of the proposing vendor or the vendor's proposed subcontractor.

Utility has also submitted ***Attachment F, Reference Questionnaire*** to the business reference that is identified below, from ***Section 4.3.2***.

Reference #:	1		
Company Name:	City of Colorado Springs (CO)		
Identify role company will have for this RFP project (Check appropriate role below):			
X	***VENDOR***		***SUBCONTRACTOR***
Project Name:	City of Colorado Springs PD BodyWorn Cameras		
Primary Contact Information			
Name:	Commander James (Pat) Rigdon		
Street Address:	705 S. Nevada Avenue		
City, State, Zip:	Colorado Springs, CO 80903		
Phone, including area code:	719-444-7759		
Facsimile, including area code:	-NA-		
Email address:	rigdonja@ci.colospgs.co.us		
Alternate Contact Information			
Name:	-NA-		
Street Address:	-NA-		
City, State, Zip:	-NA-		
Phone, including area code:	-NA-		
Facsimile, including area code:	-NA-		
Email address:	-NA-		
Project Information			
Brief description of the project/contract and description of services performed, including technical environment (i.e., software applications, data communications, etc.) if applicable:	Deployment of 500 units BodyWorn camera system, with 250 integrated ruggedized vehicle-mount Rocket-IoT in-car video with WiFi Hot Spot, GPS to CAD, High Speed Offload of Video Data. Phase 1 completed 65 unit BodyWorn and 40 Rocket-IoT. Phase 2 in progress.		
Original Project/Contract Start Date:	6/1/16		
Original Project/Contract End Date:	6/30/18		
Original Project/Contract Value:	Confidential		
Final Project/Contract Date:	-TBD-		
Was project/contract completed in time originally allotted, and if not, why not?	Yes		
Was project/contract completed within or under the original budget/ cost proposal, and if not, why not?	Yes		

Utility has also submitted ***Attachment F, Reference Questionnaire*** to the business reference that is identified below, from ***Section 4.3.2***.

Reference #:	2		
Company Name:	City of Marietta (GA)		
Identify role company will have for this RFP project (Check appropriate role below):			
X	***VENDOR***		***SUBCONTRACTOR***
Project Name:	City of Marietta PD BodyWorn Cameras		
Primary Contact Information			
Name:	Ronald Barrett, Director of MIS		
Street Address:	205 Lawrence Street		
City, State, Zip:	Marietta, GA 30060		
Phone, including area code:	770-794-5287		
Facsimile, including area code:	-NA-		
Email address:	rbarrett@mariettaga.gov		
Alternate Contact Information			
Name:	-NA-		
Street Address:	-NA-		
City, State, Zip:	-NA-		
Phone, including area code:	-NA-		
Facsimile, including area code:	-NA-		
Email address:	-NA-		
Project Information			
Brief description of the project/contract and description of services performed, including technical environment (i.e., software applications, data communications, etc.) if applicable:	Deployment of 142 units BodyWorn camera system, 70 units in-car camera system in Police Department, additional 25 in Fire Department, and 200 units integrated ruggedized vehicle mount mobile router Rockets with WiFi Hot Spot, GPS to CAD, High Speed Offload of Video Data.		
Original Project/Contract Start Date:	6/1/16		
Original Project/Contract End Date:	6/1/17		
Original Project/Contract Value:	Confidential		
Final Project/Contract Date:	-TBD-		
Was project/contract completed in time originally allotted, and if not, why not?	Yes		
Was project/contract completed within or under the original budget/ cost proposal, and if not, why not?	Yes		

Utility has also submitted ***Attachment F, Reference Questionnaire*** to the business reference that is identified below, from ***Section 4.3.2***.

Reference #:	3		
Company Name:	City of Long Beach (CA)		
Identify role company will have for this RFP project (Check appropriate role below):			
X	***VENDOR***		***SUBCONTRACTOR***
Project Name:	City of Long Beach PD BodyWorn Cameras		
Primary Contact Information			
Name:	Sergeant Joe Gludt		
Street Address:	P.O. Box 90342		
City, State, Zip:	Long Beach, CA 90809		
Phone, including area code:	562-244-9746		
Facsimile, including area code:	-NA-		
Email address:	Joe.gludt@longbeach.gov		
Alternate Contact Information			
Name:	-NA-		
Street Address:	-NA-		
City, State, Zip:	-NA-		
Phone, including area code:	-NA-		
Facsimile, including area code:	-NA-		
Email address:	-NA-		
Project Information			
Brief description of the project/contract and description of services performed, including technical environment (i.e., software applications, data communications, etc.) if applicable:	Deployment of 500 units BodyWorn camera system, with 45 integrated ruggedized vehicle-mount Rocket with WiFi Hot Spot, GPS to CAD, High Speed Offload of Video Data. Phase 1 completed 60 units BodyWorn, 45 Rocket. Phase 2 in progress. Full deployment 900 units BodyWorn anticipated.		
Original Project/Contract Start Date:	3/1/16		
Original Project/Contract End Date:	3/1/17		
Original Project/Contract Value:	Confidential		
Final Project/Contract Date:	-TBD-		
Was project/contract completed in time originally allotted, and if not, why not?	Yes		
Was project/contract completed within or under the original budget/	Yes		

cost proposal, and if not, why not?	

4.3.3 Vendors must also submit ***Attachment F, Reference Questionnaire*** to the business references that are identified in ***Section 4.3.2***.

Utility has also submitted Attachment F, Reference Questionnaire to the business references that are identified above in Section 4.3.2.

4.3.4 The company identified as the business references must submit the Reference Questionnaire directly to the Purchasing Division.

Utility has asked Business References to submit Attachment F, Reference Questionnaire directly to the Purchasing Division.

4.3.5 It is the vendor's responsibility to ensure that completed forms are received by the Purchasing Division on or before the deadline as specified in ***Section 8, RFP Timeline*** for inclusion in the evaluation process. Reference Questionnaires not received, or not complete, may adversely affect the vendor's score in the evaluation process.

Utility acknowledges and understands the requirement.

4.3.6 The State reserves the right to contact and verify any and all references listed regarding the quality and degree of satisfaction for such performance.

Utility acknowledges and understands the requirement.

3. GENERAL REQUIREMENTS AND PROVISIONS

The general requirements and provisions the State is seeking are defined below. The purpose is to establish a minimum standard of quality and to ensure that the State of Nevada is provided with a system that allows for effective recordings that will be readily accepted by court system.

3.1.1 PROCESS

The process by which the Responses will be considered for award under this RFP consists of two (2) distinct stages.

3.1.1 First Stage

The first stage is a determination of whether or not the vendor qualifies. If a vendor is determined to not meet any one of the General Minimum Qualifications (below), the RFP response in its entirety will not be considered for award.

3.1.1.1 Vendor must have the following:

- Body Worn Cameras and a proprietary In-Car Video system;
- Two (2) years' experience providing Body Worn Cameras to law enforcement agencies;
- Deployed a minimum of 100 Body Worn Cameras to three (3) separate law enforcement agencies; and
- Evidence storage hardware/software.

Utility acknowledges and understands the above requirements. Utility meets these requirements. Utility is the manufacturer of the equipment and software for both a body-worn camera system (BodyWorn™) and an In-Car Video system (Rocket-IoT™), which are compatible with inter-operability.

Utility has more than two years' experience providing Body Cameras to law enforcement agencies.

Utility has deployed a minimum of 100 Body Worn Cameras to three (3) separate law enforcement agencies. Multiple such deployments are available as including three Business References as requested.

Utility's BodyWorn and Rocket-IoT solutions are complete solution, including evidence management storage hardware and software.

3.1.2 Second Stage

If the vendor meets all of the General Minimum Qualifications (above), the vendor's submitted proposal will be individually evaluated.

Utility asserts affirmatively that it meets all of the General Minimum Requirements above. We respectfully ask for the individual evaluation of our submitted proposal.

3.2 GENERAL REQUIREMENTS

3.2.1 System

3.2.1.1 System shall be of the manufacturer's current design and in full commercial production. Prototype, discontinued models, or used equipment will not be considered.

Utility has reviewed and complies with the requirements.

3.2.1.2 Vendor must be the original manufacturer, or distributor, and/or dealer authorized by manufacturer.

Utility has reviewed and complies with the requirements.
Utility is the manufacturer.

3.2.1.3 If the vendor and or the system have not performed as contracted, the vendor will be provided an opportunity to address non-performing issues. If the vendor is unable or unwilling to address the issues in accordance with the State's satisfaction, then the State will return the vendor's equipment for full reimbursement at the vendor's expense.

Utility has reviewed and will comply with the requirements.

3.2.1.4 Vendors shall submit a schematic rendering of the proposed BWC System.

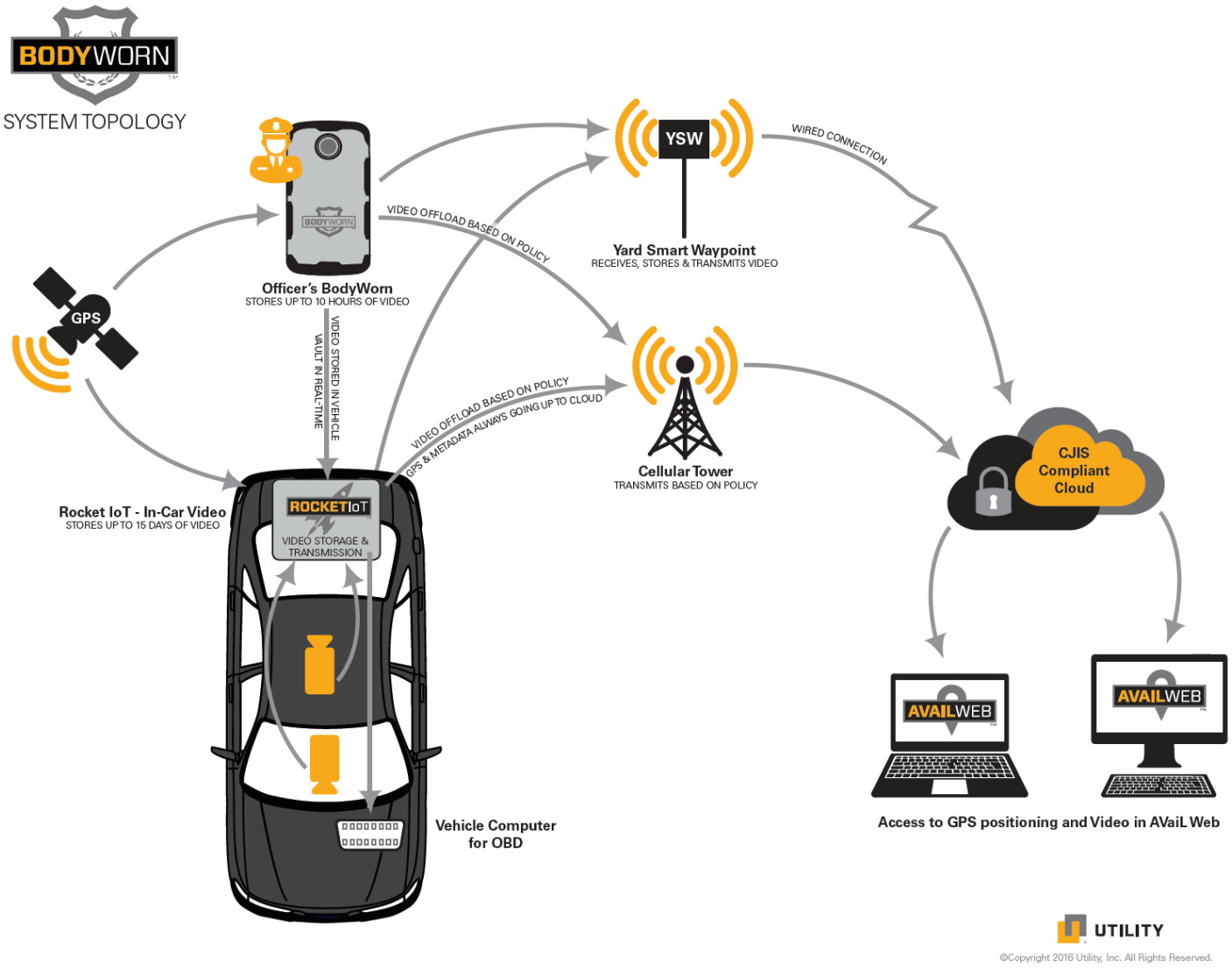
Utility has provided a schematic rendering of the BodyWorn ™ and Rocket-IoT™ System Topology on the following page.

3.2.1.4 Schematic rendering of the BodyWorn™ and Rocket-IoT™ System Topology

The Ultimate Ecosystem

Mission Critical Mobile Intelligence.

Protect What's Important:
Officers, Evidence and Community Transparency



©Copyright 2016 Utility, Inc. All Rights Reserved.

3.2.1.4 Schematic rendering of the BodyWorn™ and Rocket-IoT™ System Topology

The Ultimate Ecosystem

Mission Critical Mobile Intelligence.

Protect What's Important:
Officers, Evidence and Community Transparency

ROCKETIoT™

Always have a Wi-Fi connection with a vehicle-based mobile router. Upload BodyWorn and In-Car video instantly to the cloud.

AVAILWEB™

Utility's comprehensive user-friendly online platform allows the user to store, manage and retrieve important videos at the click of a button.

All data collected by Utility is encrypted and securely stored in the cloud. No need for cumbersome docking stations or server rooms. Eliminates risk of data loss.

BODYWORN™

Capture high-quality video with our one-of-a-kind integrated body camera. Use policy-based triggers to start and stop camera recording.

SMARTREDACTION

Share videos using our state-of-the-art automated redaction software to blur anything from large crowds to an identifiable mark.

3.3 PROJECT MANAGEMENT AND CUSTOMER SERVICE

3.3.1 Project management services shall be provided by the awarded vendor and/or designated sub-contractor throughout the duration of the contract. As part of the RFP response, vendors shall clearly describe their project management methodology and approach, and provide a project management plan including the following:

Utility has provided this project management information on the following pages.

3.3.1.1 On-site, face-to-face meetings will be required no less frequently than monthly with DPS/HPD for the project. In the event project delays or problems are caused by the vendor, the State reserves the right to modify the frequency of these meetings as deemed necessary and at no additional charge to the State.

Utility acknowledges and understands the requirement.

3.3.1.2 Provision of written status reports and updated/project schedules at each project management meeting to be held on-site at Department of Public Safety Highway Patrol Division, 555 Wright Way, Carson City, NV. All status reports shall be provided in a hard copy and/or electronic format. The meeting place may vary.

Utility acknowledges and understands the requirement.

3.3.1.3 Vendors shall clearly identify the project team assigned to the account including their background and experience, roles and responsibilities, and relevant experience with projects similar in scope to those requested. This information shall be listed in ***Section 4 ~ Company Background and Reference***s.

Utility has provided this information on the following pages.

3.3.1.4 Vendors shall provide an overview of their anticipated approach for training installers, administrators, and end users of the BWC systems. This shall include training methodology, scheduling, delivery, and support materials provided.

Utility has provided this information on the following pages.

3.3.1 and 3.3.1.1 and 3.3.1.2 Project Management Services

Proposed Timeline

Utility is positioned to begin implementation of the project immediately upon award of the contract with a proposed schedule to begin and complete deployment within 2017. For the purposes of illustration, our timeline assumes announcement of contract award and start date in the First Quarter 2017, with subsequent configuration and training throughout 2017, with deployment of up to 489 BodyWorn™ camera systems by the end of Fourth Quarter 2017.

The BodyWorn implementation will typically consist of five (5) phases

1. ***Finalize project charter based upon project purchase order***
2. ***Approved departmental procedural policy is implemented and in-place***
3. ***Deployment and training location set up and trainer scheduling***
4. ***Mobile device and uniform carrier distribution in conjunction with training***
5. ***Software training for admin staff and procedural acceptance of officers***

The Rocket-IoT In-Car installation projects will typically include six (6) phases.

1. ***Finalize Project Charter based upon Project Purchase Order***
2. ***Installation Location Setup and Install Crew Scheduling and Training***
3. ***Test Installation***
4. ***Test Installation Validation and Acceptance Testing***
5. ***Fleet installation***
6. ***Installation Location close-out***

Utility will provide internal staff for the duration of the implementation. The implementation team will ensure the successful testing and installation of the BodyWorn devices, any Rocket-IoT devices, and associated software. Utility staff will also work with the Department to establish a protocol that provides a successful handoff of the devices. Utility will work with an approved Departmental uniform vendor to ensure the necessary modifications required are in compliance with Client Agency policy and procurement. It is important to note that Utility has established relationships with most major uniform manufacturers, like Blauer, Elbeco, and Flying Cross, that support the BodyWorn solution.

An example schedule in Gantt chart format is provided below:

ID	Task Name	Duration	Start	Finish
1	[illegible]	[illegible] days	Tue 1/3/17	Mon 11/13/17
2	[illegible]	2 days	Tue 1/3/17	Wed 1/4/17
3	[illegible]	1 day	Tue 1/3/17	Tue 1/3/17
4	[illegible]	1 day	Tue 1/3/17	Tue 1/3/17
5	Network configuration	5 days	Wed 1/4/17	Tue 1/10/17
6	[illegible]	2 days	Wed 1/4/17	Fri 1/6/17
7	[illegible]	1 day	Wed 1/4/17	Wed 1/4/17
8	[illegible]	1 day	Wed 1/4/17	Wed 1/4/17
9	[illegible]	1 day	Wed 1/4/17	Wed 1/4/17
10	Policy Development	3 days	Wed 1/4/17	Fri 1/6/17
11	Training of Command staff and policy development, and Groups development	3 days	Wed 1/4/17	Fri 1/6/17
12	WIP Plan provide email address for officers, mics, and reporting scenario	3 days	Wed 1/4/17	Fri 1/6/17
13	Full Scale Deployment (1 - 1)	25 days	Mon 1/16/17	Fri 2/17/17
14	Train Location Staff	1 day	Mon 1/16/17	Mon 1/16/17
15	Train the Trainer	1 day	Mon 1/16/17	Mon 1/16/17
16	Training of Officers	4 days	Mon 1/16/17	Thu 1/19/17
17	Delivery of cameras, BodyWorn Cameras, and configuration of vehicles	25 days	Mon 1/16/17	Fri 2/17/17
18	Full Scale Deployment (1 - 2)	27 days	Mon 4/3/17	Tue 5/9/17
19	Train Location Staff	1 day	Mon 4/3/17	Mon 4/3/17
20	Train the Trainer	1 day	Mon 4/3/17	Mon 4/3/17
21	Training of Officers	6 days	Mon 4/3/17	Thu 4/6/17
22	Delivery of cameras, BodyWorn Cameras, and configuration of vehicles	25 days	Wed 4/5/17	Tue 5/9/17
23	Full Scale Deployment (1 - 3)	27 days	Wed 7/5/17	Thu 8/10/17
24	Train Location Staff	1 day	Wed 7/5/17	Wed 7/5/17
25	Train the Trainer	1 day	Wed 7/5/17	Wed 7/5/17
26	Training of Officers	6 days	Wed 7/5/17	Mon 7/10/17
27	Delivery of cameras, BodyWorn Cameras, and configuration of vehicles	25 days	Mon 7/10/17	Wed 8/9/17
28	Full Scale Deployment (1 - 4)	25 days	Mon 10/2/17	Fri 11/3/17
29	Train Location Staff	1 day	Mon 10/2/17	Mon 10/2/17
30	Train the Trainer	1 day	Mon 10/2/17	Mon 10/2/17
31	Training of Officers	4 days	Mon 10/2/17	Thu 10/5/17
32	Delivery of cameras, BodyWorn Cameras, and configuration of vehicles	20 days	Wed 10/4/17	Fri 11/3/17

Project: NHP
Date: Mon 9/26/16

Task		Project Summary		Manual Task		Start-only		Deadline	
Split		Inactive Task		Duration-only		Finish-only		Progress	
Milestone		Inactive Milestone		Manual Summary Rollup		External Tasks		Manual Progress	
Summary		Inactive Summary		Manual Summary		External Milestone			

Project Plan to Perform the Required Work

The project plan outline below illustrates the major deliverables to be produced, the steps of the deployment from project kick-off to project hand-off, and notates the responsibilities for the State, including implementation and training of all categories of relevant staff.

1. ***Project Kick Off: Pre-Deployment Meeting***
    a. ***Introductions and establish State points of contact***
    b. ***Schedule site surveys of State locations***
    c. ***State to provide Utility with planned testing locations and commands***
    d. ***Determine scope of project size***
        i. ***Administrative personnel***
        ii. ***Supervisory personnel***
        iii. ***Officers***
        iv. ***Specialized units***
2. ***Network Configuration by Utility in conjunction with State IT staff***
    a. ***Visit substations to collect Access Point data***
    b. ***Configure VPN and Firewall***
    c. ***Configure AVaiL Web roles and permissions***
    d. ***Configure AVaiL Web retention roles***
3. ***Project Implementation: Uniform Fitting***
        i. ***Utility will measure at designated locations predetermined by State.***
        ii. ***Establish corrective action plan for delays***
    b. ***Supervisory personnel fitting***
    c. ***Officer fitting***
    d. ***Specialized unit fitting***
4. ***Policy Development by State***
    a. ***Command and Administrative staff***
        i. ***Policy development***
            1. ***Establish retention policy***
        ii. ***Groups development***
    b. ***State to provide customization information***

        i. *Provide email addresses of users*
        ii. *Roles and permissions requirements*
        iii. *Reporting locations*
        iv. *State operational review for any additional add-ons or changes*

5. *Training by Utility*
    a. *Support staff, legal staff, and trainers*
        i. *Administrative training of evidence handling procedures*
        ii. *Chain of evidence reporting*
        iii. *Operational functionality for the review and playback of video*
        iv. *Exporting video for adjudication needs*
        v. *Review for any additional add-ons or changes*
    b. *Officers*
        i. *Classroom style setting for complete review of system*
    c. *All users*
        i. *Insertion and removal from carrier*
        ii. *Logging in and out*
        iii. *Recording*
            1. *Locally by user*
            2. *Remotely by supervisor, dispatch, and command*
            3. *Automatically*
                a. *Discussion of triggers*
                b. *Bluetooth controller*
                c. *Action zones and Geo fencing*
                d. *Physical actions*
        iv. *Video and photographic classification and officer notes*
        v. *AVaiL Web™ (software)*
            1. *User rights and functionality*
            2. *Administrative features*
            3. *Officer features*
        vi. *Smart Redaction™*
            1. *Solution navigation and usage*

6. *Full Scale Deployment*

a. ***Delivery of products***
b. ***Vehicle configurations***
c. ***Utility project hand off to State***
    i. ***Project transition to customer***
        1. ***Review on-going support procedures, perpetual services tied to warranties and software subscriptions***

Utility maintains and manages a Quality Control Plan to ensure the efficiency and effectiveness of hardware and software management and storage. Key to tracking delivery, control costs and maintain performance over the term of the implementation is careful planning. Project execution, design of a detailed Project Plan in partnership with the Client, and our joint experience and knowledge are key to success. Quality Control planning enables the Team to establish and successfully achieve Milestones, manage Critical Success Factors, and constantly communicate any assumptions that could affect a successful result.

Milestones

- ***Contract Purchase Order received***
- ***Project Charter with Implementation Schedule published***
- ***Properly configured and activated Modem Aircards are received***
- ***Properly measured and fitted uniform carriers are received***
- ***Rocket Installation location determined***
- ***BodyWorn deployment location determined***
- ***Installation Team Training completed, if required***
- ***Test Installation Completed and signed off on***
- ***Test BodyWorn Deployment completed***
- ***BodyWorn Team Training completed***
- ***Implementation Kickoff***
- ***Weekly Installation Status Reports published***
- ***Final Vehicle Install completed***
- ***Final BodyWorn Deployment completed***
- ***Implementation Location Closeout completed***

Critical Success Factors

- ***Project Charter published***
- ***Modem Aircards are delivered on schedule, are activated, and have been properly provisioned by the cellular carrier***
- ***Installation Procedures and Checklist are provided***
- ***Installation Team has appropriate installation skills***
- ***Installation Team is trained in approved Installation Procedures***
- ***Installation locations are covered with adequate heat and power***
- ***BodyWorn Deployment Team is prepared with approved Devices and Carriers***
- ***BodyWorn Deployment locations are suitable rooms for group training***
- ***Vehicles are delivered to the Installation Location(s) on schedule***
- ***BodyWorn units are delivered to the Deployment Location(s) on schedule***
- ***Installation and Acceptance Test Procedures are followed***

Assumptions

- ***NPD provides adequate covered Installation location(s) so that installation work can be completed during inclement weather within the allotted installation time***
- ***Suitable rooms for group training and distribution of BodyWorn units are provided***
- ***Modem Aircards are delivered on schedule, are activated, and have been properly provisioned by the cellular carrier.***
- ***Vendors and any Subcontractor staff have the requisite skills and training to properly install modems and deploy BodyWorn devices within the budgeted installation time.***
- ***Vehicles are delivered to the designated installation location(s), and BodyWorn units to the deployment sites according to the delivery schedule.***
- ***Vehicles are reasonably clean and installation crews have access to vehicle areas necessary to install antennas and Rocket Lockers.***

3.3.1.3 Project Team Assigned to State of Nevada

The Implementation is led by the Project Management Team, which in turn, is led by a highly experienced, single-point Project Manager who will work directly with the State, in an integrated, streamlined process for a seamless and efficient delivery of services for the Project. The Project Manager manages the Project Management Team, which includes the Deployment Manager. Detailed full-page resumes in the required State Format appear as Attachment G in Tab VIII, as requested. These resumes state the related experience with projects similar in scope to those requested by the State of Nevada for this project.

Project Management Team summary bios are highlighted below.

PROJECT MANAGEMENT TEAM

LONNIE MORRISON
PROJECT MANAGER

PROFESSIONAL BACKGROUND

Morrison is an experienced, Project Management Professional (PMP) trained manager, with strong communication and interpersonal skills. As Project Manager, Lonnie leads the PM Team through planning and execution of Utility's hardware and software solutions. He collaborates with Customer Support and Implementation to ensure that every part of the deployment is a success. His strong organizational and communication skills combine with deep technical experience in mobile data computers, vehicle tracking solutions, in-vehicle video and secure in-vehicle router networks, mobile high speed data, dispatch systems, and cellular networks.

CURRENT AND PAST RELEVANT EMPLOYMENT

Morrison joined Utility in 2014, in capacity of both Field Engineer and Project Manager. In his previous work, Morrison successfully collaborated on design/deployment of Cisco VPN and NetMotion VPN networks as a cost reduction measure; provided technical support to field engineers for installation of Cisco routers and virtual circuits; deployed high speed secure data connection to facilitate remote access to secure managed communications networking elements; and supervised and managed installation of multi-channel radio links, tactical satellite radios and remote extension switches. Morrison is a U.S Army veteran, serving as MSE Transmission Chief at Fort Bragg, North Carolina.

EDUCATION

Project Management Institute
Motorola iDEN EBTS, DCS T1 HDSL Network

CERTIFICATIONS

PMI, BodyWorn, AVaiL Web, Rocket IoT, Rocket

PROJECT MANAGEMENT TEAM

PAUL BRYANT
DEPLOYMENT MANAGER

PROFESSIONAL BACKGROUND

Bryant is an experienced deployment manager with a successful track record of on-time and structured deployments from 10 to 30,000. Clients attribute their successful implementations to his strong communication skills, detailed documentation, and highly organized approach that is project milestone driven.

CURRENT AND PAST RELEVANT EMPLOYMENT

As Deployment/ Implementation Manager, Paul orchestrates installation, training and the deployment of staff and resources to our customer's organizations. Paul Bryant has been with Utility since 2014 in various customer-facing roles including sales, support, project deployment and service support. He has over 14 years of experience in customer service operations.

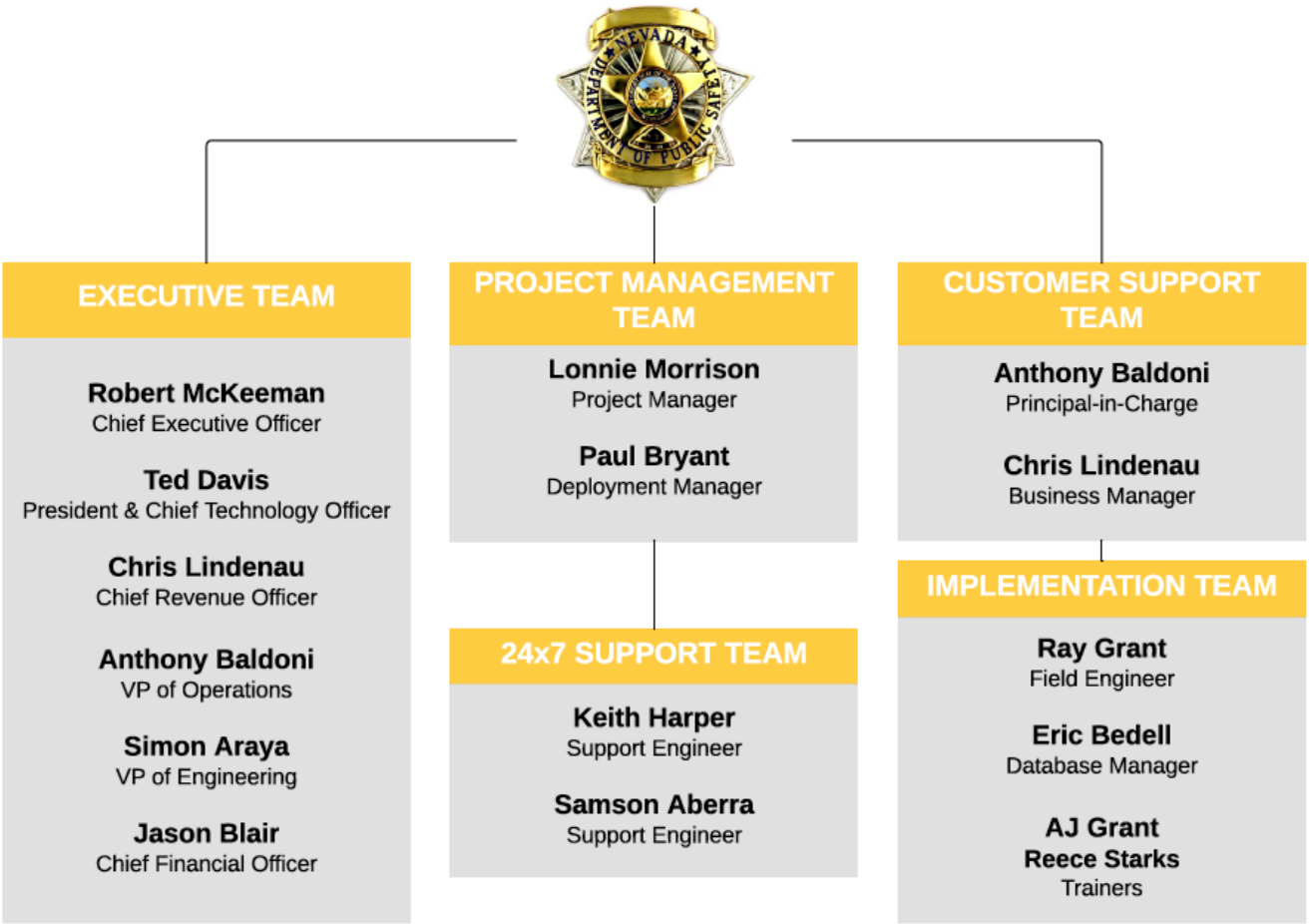
EDUCATION

Bachelor of Computer Science
DeVry University, Decatur, GA

CERTIFICATIONS

NetMotion Certification
Panasonic Certified Master Trainer and Installer

BodyWorn, AVaiL Web, Rocket IoT, and Rocket



3.3.1.4 Overview of Anticipated Approach for Training

Officer / End User Training

Training will be provided in a classroom environment. We propose a hands-on approach to training to ensure all respective individuals have complete understanding and are comfortable with using the system.

Estimated time: ***4 hours (2 hours training, 1.5 hours hands-on operation, 30 min for Q&A)***
Format: ***Classroom, PowerPoint, and hands on with demo system(s)***
The objectives of this training session are as follows:

- ***Operating the BodyWorn™ system***

- ***Using the BodyWorn™ application***
- ***Starting recording/stopping recording***
- ***Explaining triggers and how they work***
- ***Classifying video***
- ***Transfer the Digital Multimedia Evidence from BodyWorn™ to the storage system (this is a wireless automatic process but we will cover what happens so that the officers understand)***
- ***Enter evidence classification metadata and tags***

High Level/ Supervisor Training

Estimated time: 4 hours (2 hours training, 1.5 hours hands-on operation, 30 min for Q&A)
Format: Classroom, PowerPoint and hands on with demo system(s)
The objectives of this training session are as follows:

- ***Operating the BodyWorn system***
- ***Using the BodyWorn application***
- ***Start recording/stop recording***
- ***Explaining triggers and how they work***
- ***Classifying video***
- ***Equipment assignment in the Video Management Software***
- ***BodyWorn configuration assignment and settings***
- ***Hardware troubleshooting***
- ***RMA process***
- ***Advanced entering of evidence classification metadata and tags***
- ***Advance use of Video Management Software for video management, storage, and security***

Testing

The Utility team encourages and supports testing periods by providing two (2) BodyWorn™ cameras and carriers, at no cost to the State, including all necessary equipment for upload for up to a seven (7) day testing period, additional units and testing period is permissible if

necessary. The pilot test is performed using Utility's extensive functionality checklist and any additional parameters requested by the State.

The following is an example of the functionality checklist:

UTILITY

BODYWORN

BodyWorn Acceptance Testing WorkSheet

Utility FE:	
Customer:	
Training Date:	
Customer:	

Step#	Procedure/Execution of Function	Expected Result/Output	Pass/Fail
BWD 1	**BodyWorn Authentication**		
BWD 1.1	NFC Chip auto-login	BodyWorn device logs in with correct user name	
BWD 1.3	Manual Login	Users can log into BodyWorn Device via physical input	
BWD 1.1	Manual Logout	Users can log out BodyWorn Device via physical input	
	BodyWorn App Navigation		
BWD 2	**Duty Mode**		
BWD 2.1	Off Duty Mode	Users are able to designate themselves as "Off Duty"	
BWD 2.2	On Duty Mode	User are able to place themselves as "On Duty"	
	BodyWorn Media Capture		
BWD 3	**BodyWorn Recording Start and Stop**		
BWD 3.1	Bluetooth Controller Recording Start	Users understand the functionality of Bluetooth controller and can -Start Recording	
BWD 3.2	Bluetooth Controller Recording Stop	Users understand the functionality of Bluetooth controller and can -Stop Recording	
BWD 3.3	Running Recording Start	Users have tested the accelerometer functionality of the BodyWorn Device - Recording start Running	
BWD 3.3	Remote 911 Dispatch Recording Start	Remote Recording -Start Tested	
BWD 3.4	Remote 911 Dispatch Recording Stop	Remote Recording -Stop Tested	
BWD 3.5	GeoFence Recording Start	GeoFence Entry Recording - Start Tested	
BWD 3.6	GeoFence Recording Stop	GeoFence Entry Recording - Stop Tested	
BWD 3.7	Action Zone Recording Start	Action Zone Entry Recording - Start Tested	
BWD 3.8	Action Zone Recording Stop	Action Zone Entry Recording - Stop Tested	
BWD 3.10	BodyWorn Audio Capture Mute On	Users understand the functionality of 'Muting Audio" while recording - Start Tested	
BWD 3.11	BodyWorn Audio Capture Mute Off	Users understand the functionality of 'Un-Muting Audio" while recording - Start Tested	
	BodyWorn Media		
BWD 4	**Search and Classify Video/Image**		
BWD 4.1	Video	Users understand the functionality and way to Search for and Classify Video on the BodyWorn Device	
BWD 4.2	Image	Users understand the functionality and way to Search for and Classify Images on the BodyWorn Device	
BWD 5	**Capture Pictures**		
BWD 5.1	Capture Picture	Users understand the procedure of capturing a still image with the BodyWorn Device -Capture Tested	
BWD 5.2	Record Picture Voice Note	Users understand the procedure of capturing audio notes associated with photo or video -Functionality Tested	
BWD 6	**Receive BOLO Alert**		
BWD 6.1	Navigate to BOLO	Users understand the procedure of locating inbound Nonfictions - Tested	
BWD 6.2	View BOLO	Users understandsthe procedure of viewing inbound Nonfictions - Tested	
BWD 7	**Validate Media Files auto uploaded**		
BWD 7.1	Visual Confirmation of video upload	Users understand the procedure of confirming media upload -Functionality Tested	
Authorized Customer Signature :			

OFFICER TRAINING SYLLABUS

(Date)

Trainer: Reece Rios
Office: 404-816-0300
Mobile: 404-360-9000
Email: rrios@utility.com

Course Description:

This course is designed to prepare departments for the use of Utility's Ultimate Witness Ecosystem. This training course with Utility will be covering *BodyWorn™, Smart Waypoint Evidence Vault, Rocket IoT™ In Car Camera, and AVaiL Web Evidence Management Systems.* At the conclusion of this training session, trainees will be given a list of tasks to complete. Once successfully completed, a training contract will be signed identifying that the individual has proven sufficient proficiency on all topics discussed.

Material Requirements:

For training you will be required to have a computer with Internet access, your department issued email address, and current uniform with ballistic insert. All other course materials will be supplied by Utility.

Training Objectives:

This training is intended to improve the understanding, and comfort with Utility's Ultimate Witness Ecosystem. Our aim is to provide the trainee with the needed knowledge to display proficiency, and skill with our product outside of the training session.

UTILITY

Training Classes

Unit	Title	Objectives	Time
1.0	BodyWorn™ Gear	- Outer vest carrier - Holster & NFC - Bluetooth Controller - BodyWorn Device	30 min
2.0	BodyWorn™ User Interface	- Home Screen - Navigation Drawer - Media Library - Classifications and Notes - Custom Fields - Software & Firmware	30 min
3.0	BodyWorn™ Automatic & Manual Recording	- Bluetooth Controller - BodyWorn Device - I/O Triggers - Taps - Accelerometer - BodyWorn down - Geofence & Action Zone	30 min
4.0	Smart Waypoint Evidence Vault	- BodyWorn Video Offload - Smart Waypoint Offload - Priority Offload	30 min
5.0	AVaiL Web™	- Live - Reports - Media - Admin	1hr 30 min*
6.0	Rocket IoT™ In Car Camera Bundle	- Antenna Connectors - Antennae - Locker - Shutdown Timer Settings - Laptop Connectivity	10 min
7.0	Rocket IoT™ User Interface	- User Login - Rocket Status - Storage - Start/Stop - Recording - Live View - Incident Review - Docking	30 min

Advanced Class

Unit	Title	Objectives	Time
7.0	Exporting Media/Smart Redaction™	- Export Type - Redaction Types - Watermark - Drawing mode	1hr 30 min

ACTION ITEMS

Tasks to be completed after training

Officer

- ☐ Register NFC tag to user
- ☐ Authentication with NFC tag
- ☐ Initiate media recording in 3 unique ways *(Manual or Automatic)*
- ☐ Media Toolbar
  - ☐ Add a note to an incident *(on BodyWorn, AVaiL Web, or Rocket IoT)*
  - ☐ Add classification(s) to an incident *(on BodyWorn, AVaiL Web, or Rocket IoT)*
- ☐ Change password on AVaiL Web
- ☐ Connect to Rocket IoT with BodyWorn

Scenario Training

- ☐ Traffic Stop
  - ☐ Passenger approach
  - ☐ Driver side approach
- ☐ Citizen Contact
- ☐ Foot Chase

UTILITY

District Attorney

- View Media
- Export Media

Video Evidence Technician

- Search Media
  - Add classifications
  - Add notes
  - Add markers
- Flag Media
- Media Toolbar
  - Filter & Print Chain of Custody
  - Seal Incident
  - Share/Restrict Media
  - Export Media
    - Redact Video*
    - Modify Watermark Settings

UTILITY

Supervisor

- Search for a specific user
- View the user history
- Make a group of “favorite devices”
- Search Media
  - Add classifications
  - Add notes
  - Add markers
- Flag Media
- Media Toolbar
  - Filter & Print Chain of Custody
  - Seal Incident
  - Share/Restrict Media
  - Export Media
    - Redact Video*
    - Modify Watermark Settings
- Create Geofence
- Create Action Zone
- Send BOLO alert
- Reset a Password
- Create a User Account
- Run reports*
  - Geofence
  - GPS
  - User
  - Media

UTILITY

Dispatch

- ☐ Zoom and toggle through map
- ☐ Switch map interface layers
- ☐ Device interaction
  - ☐ Send a BOLO
  - ☐ Track a device
  - ☐ View/print device history
- ☐ Officer down alert
  - ☐ Handle
- ☐ Create a new location & home
- ☐ Create an Action Zone
- ☐ Create a Geofence

UTILITY

Admin *(AVaiL Web)*

- Search for a specific user
- Device interaction
  - Send a BOLO
  - Track a device
  - View/print device history
  - Make a group of "favorite devices"
- Search Media
  - Add classifications
  - Add notes
  - Add markers
- Flag Media
- Media Toolbar
  - Filter & Print Chain of Custody
  - Seal Incident
  - Share/Restrict Media
  - Export Media
    - Redact Video*
    - Modify Watermark Settings
- Create Geofence
- Create Action Zone
- Reset a Password
- Create a User Account
- Run reports*
  - Geofence
  - GPS
  - User
  - Media

3.3.2.3 Customer Service

3.3.1.1 Vendor will provide 24/7/365 technical support (phone, email etc.), and additional on-site or after-hours service cost should be noted separately.

Utility acknowledges and understands the requirement.

3.3.1.2 Cost for basic support services should be proposed as an annual cost.

Utility acknowledges and understands the requirement.

3.3.1.3 Vendor should provide a complete list of services and response times for help calls of varying priority.

Support Services
Guaranteed Response Times

When a client raises a support issue with the supplier, the supplier promises to respond in a timely fashion.

Response Times

Utility provides a 99% uptime/availability commitment. All systems have health monitoring that assures that issues are typically addressed 24/7/365 by Utility personnel before they become an impact to the performance of the service. For support provided to the customer directly, Utility has a tiered response to support that will escalate the level of support depending on the situation. Tier 1 would be on site support by the CSPD staff after they have been trained by Utility, which will alleviate most day-to-day issues that may pop up. Problems beyond Tier 1 scope will be escalated to Tier 2 and from there to Tier 3, which is onsite technical support from a Utility field engineer.

While most support calls are handled immediately, Tier 2 issues have guaranteed response times as shown below:

Item Priority	Fatal	Severe	Medium	Minor
1	1 Hour	1 Hour	2 Hours	3 Hours
2	2 Hours	2 Hours	4 Hours	6 Hours
3	4 Hours	4 Hours	8 Hours	16 Hours

Severity Levels

The severity levels shown in the tables above are defined as follows:

- ***Fatal: Complete degradation – all users and critical functions affected. Item or service completely unavailable.***
- ***Severe: Significant degradation – large number of users or critical functions affected.***
- ***Medium: Limited degradation – limited number of users or functions affected. Business processes can continue.***
- ***Minor: Small degradation – few users or one user affected. Business processes can continue.***

<u>Resolution Times</u>

Utility will always endeavor to resolve problems as swiftly as possible. It recognizes that the client's BWC systems are key to daily functions and must be functional in the field.

However, Utility is unable to provide guaranteed resolution times. This is because the nature and causes of problems can vary.

In all cases, the supplier will make its best efforts to resolve problems as quickly as possible. It will also provide frequent progress reports to the client.

<u>Warranty</u>

Utility Maintenance and Warranty provisions are detailed in the Terms and Conditions, Utility Software and as Subscription (SaaS) Agreement, and Limited Hardware Warranty in:

- ***Section Tab IV 'State of Nevada Documents' under 'Copies of Vendor Licenses and/or Hardware/Software Maintenance Agreements'***

4.3 VENDOR STAFF RESUMES

A resume must be completed for each proposed key personnel responsible for performance under any contract resulting from this RFP per ***Attachment G, Proposed Staff Resume.***

Utility has completed a Staff Resume per Attachment G for each Key Personnel as directed. Staff Resumes are provided in this Section on the pages that follow this cover sheet.

PROPOSED STAFF RESUME FOR RFP 3273

A resume must be completed for all proposed prime contractor staff and proposed subcontractor staff.

Company Name Submitting Proposal:	***Utility Associates Inc***

Check the appropriate box as to whether the proposed individual is prime contractor staff or subcontractor staff.

Contractor:	***Prime***	**Subcontractor:**	***NA***

The following information requested pertains to the individual being proposed for this project.

Name:	***Anthony Baldoni***	**Key Personnel: (Yes/No)**	***Y***
Individual's Title:	***Principal-in-Charge / VP of Operations***		
# of Years in Classification:	***12***	**# of Years with Firm:**	***12***

BRIEF SUMMARY OF PROFESSIONAL EXPERIENCE

Information should include a brief summary of the proposed individual's professional experience.

Over the past 12 years, Baldoni has focused on the mobile computing and communications needs of the first responder and utility industries. He has over 22 years of experience in customer service operations. As Vice President of Operations, Anthony Baldoni oversees the implementation of hardware and software platforms for both new and existing customers. Baldoni has been with Utility since 2003 in various customer-facing roles including sales, project deployment and service support. Baldoni served in the U.S. Army in the U.S. and South Korea.

RELEVANT EXPERIENCE

Information required should include: timeframe, company name, company location, position title held during the term of the contract/project and details of contract/project.

May 2016-Present, COLORADO SPRINGS (CO) POLICE DEPARTMENT, Principal in Charge, 500 BodyWorn, 250 Rocket-IoT In-Car
Oct 2015-Present, ATLANTA (GA) DEPARTMENT OF CORRECTIONS, Principal in Charge, 135 BodyWorn, Rockets in Transport Vans
Jun 2012-Present, CITY OF MARIETTA (GA), Marietta, GA, Principal in Charge, 142 BodyWorn, 70 Rocket-IoT In-Car

EDUCATION

Information required should include: institution name, city, state, degree and/or Achievement and date completed/received.

Bachelor of Science, Molecular Biology, University of California, Davis

CERTIFICATIONS

Information required should include: type of certification and date completed/received.

BodyWorn, AVaiL Web, Rocket IoT, Rocket

REFERENCES

A minimum of three (3) references are required, including name, title, organization, phone number, fax number and email address.

James (Pat) Rigdon, Commander, **COLORADO SPRINGS (CO) POLICE DEPARTMENT**, 719.444.7759,,rigdonja@ci.colospgs.co.us
Patrick Labat, Chief, **ATLANTA (GA) DEPARTMENT OF CORRECTIONS**, 404.865.8063, plabat@AtlantaGa.Gov
James Crosby, Sergeant, **FLORIDA HIGHWAY PATROL (FL)**, 386.736.5350, jamescrosby@flhsmv.gov

PROPOSED STAFF RESUME FOR RFP 3273

A resume must be completed for all proposed prime contractor staff and proposed subcontractor staff.

Company Name Submitting Proposal:	***Utility Associates Inc***

Check the appropriate box as to whether the proposed individual is prime contractor staff or subcontractor staff.

Contractor:	***Prime***	**Subcontractor:**	***NA***

The following information requested pertains to the individual being proposed for this project.

Name:	***Chris Lindenau***	**Key Personnel: (Yes/No)**	***Y***
Individual's Title:	***Business Manager / Director Sales and Revenue***		
# of Years in Classification:	***2***	**# of Years with Firm:**	***2***

BRIEF SUMMARY OF PROFESSIONAL EXPERIENCE

Information should include a brief summary of the proposed individual's professional experience.

As Director of Sales and Revenue, Lindenau leads business development and sales strategy for Utility Inc. with a customer-facing focus on our markets and solutions. He directs Utility's sales resources, and integrates strategy with operations to meet customer expectations and deliver successful results. Lindenau has worked in the IT Industry as both an Integrator and Manufacturer – and in his previous role as the Director of Global Sales and Marketing for Moog Sensor and Surveillance Systems, a division of the company's Space and Defense Group. During his six years on active duty as a Navy Diver, Search and Rescue Swimmer, and as a Supply Officer, he deployed to the Middle East to assist the U.S. effort during Operation Enduring Freedom and the Global War on Terrorism. After the military, Chris has fifteen years of experience working with domestic and foreign security issues.

RELEVANT EXPERIENCE

Information required should include: timeframe, company name, company location, position title held during the term of the contract/project and details of contract/project.

May 2016-Present, COLORADO SPRINGS (CO) POLICE DEPARTMENT, Business Manager, 500 BodyWorn, 250 In-Car Cameras
Jan 2016-Present, BEXAR COUNTY (TX) SHERIFF DEPARTMENT, San Antonio, TX, Business Manager, 300 BodyWorn, 230 In-Car
Jun 2016-Present**,** DEKALB COUNTY (GA) POLICE DEPARTMENT, Business Manager, 600 BodyWorn cameras, 230 In-Car

EDUCATION

Information required should include: institution name, city, state, degree and/or Achievement and date completed/received.

Bachelors Degree in Economics, United States Naval Academy
Masters Degree in Business Administration, Georgia Institute of Technology

CERTIFICATIONS

Information required should include: type of certification and date completed/received.

Board Member, Atlanta Chapter of ASIS International
BodyWorn, AVaiL Web, Rocket-IoT, Rocket

REFERENCES

A minimum of three (3) references are required, including name, title, organization, phone number, fax number and email address.

Robert Adelman, Public Safety Communications Manager, **BEXAR COUNTY (TX) SHERIFF,** 210.335.4601, radelman@bexar.org
Mike Booker, Chief, **DECATUR (GA) POLICE DEPARTMENT**, 404.373.6551, mike.booker@decatur.ga.com
James Conroy, Chief**, DEKALB COUNTY (GA) POLICE DEPARTMENT,** 770.724.7433, jwconroy@dekalbcountyga.gov

PROPOSED STAFF RESUME FOR RFP 3273

A resume must be completed for all proposed prime contractor staff and proposed subcontractor staff.

Company Name Submitting Proposal:	***Utility Associates Inc***

Check the appropriate box as to whether the proposed individual is prime contractor staff or subcontractor staff.

Contractor:	***Prime***	**Subcontractor:**	***NA***

The following information requested pertains to the individual being proposed for this project.

Name:	***Lonnie Morrison***	**Key Personnel: (Yes/No)**	***Y***
Individual's Title:	***Project Manager***		
# of Years in Classification:	***2***	**# of Years with Firm:**	***2***

BRIEF SUMMARY OF PROFESSIONAL EXPERIENCE

Information should include a brief summary of the proposed individual's professional experience.

Morrison is an experienced, Project Management Institute (PMI) professional, who leads the PM Team through planning and execution of Utility's hardware and software solutions. He collaborates with Customer Support and Implementation to ensure that every part of the deployment is a success. His strong interpersonal, organizational and communication skills combine with deep technical experience in mobile data computers, vehicle tracking solutions, in-vehicle video and secure in-vehicle router networks, mobile high speed data, dispatch systems, and cellular networks. Morrison joined Utility in 2014, in capacity of both Field Engineer and Project Manager. In his previous work, Morrison successfully collaborated on design/deployment of Cisco VPN and NetMotion VPN networks as a cost reduction measure; provided technical support to field engineers for installation of Cisco routers and virtual circuits; deployed high speed secure data connection to facilitate remote access to secure managed communications networking elements; and supervised and managed installation of multi-channel radio links, tactical satellite radios and remote extension switches. Morrison is a U.S Army veteran, serving as MSE Transmission Chief at Fort Bragg, North Carolina.

RELEVANT EXPERIENCE

Information required should include: timeframe, company name, company location, position title held during the term of the contract/project and details of contract/project.

May 2016-Present, COLORADO SPRINGS (CO) POLICE DEPARTMENT, Project Manager, 500 BodyWorn, 250 Rocket-IoT In-Car
Jan 2016-Present, BEXAR COUNTY (TX) SHERIFF DEPARTMENT, San Antonio, TX, Project Manager, 300 BodyWorn, 230 In-Car
Jun 2014-Present, CITY OF MARIETTA (GA), Project Manager, 142 BodyWorn, 70 Rocket-IoT In-Car Cameras

EDUCATION

Information required should include: institution name, city, state, degree and/or Achievement and date completed/received.

Project Management Institute; Motorola iDEN EBTS, DCS T1 HDSL Network

CERTIFICATIONS

Information required should include: type of certification and date completed/received.

BodyWorn, AVaiL Web, Rocket IoT, Rocket

REFERENCES

A minimum of three (3) references are required, including name, title, organization, phone number, fax number and email address.

James (Pat) Rigdon, Commander, **COLORADO SPRINGS (CO) POLICE DEPARTMENT**, 719.444.7759,,rigdonja@ci.colospgs.co.us
Patrick Labat, Chief, **ATLANTA (GA) DEPARTMENT OF CORRECTIONS**, 404.865.8063, plabat@AtlantaGa.Gov
Ronald Barrett, Director of MIS, **CITY OF MARIETTA (GA)**, 770.794.5287, rbarrett@mariettaga.gov

PROPOSED STAFF RESUME FOR RFP 3273

A resume must be completed for all proposed prime contractor staff and proposed subcontractor staff.

Company Name Submitting Proposal:	***Utility Associates Inc***

Check the appropriate box as to whether the proposed individual is prime contractor staff or subcontractor staff.

Contractor:	***Prime***	**Subcontractor:**	***NA***

The following information requested pertains to the individual being proposed for this project.

Name:	***Paul Bryant***	**Key Personnel: (Yes/No)**	***Y***
Individual's Title:	***Deployment Manager***		
# of Years in Classification:	***2***	**# of Years with Firm:**	***2***

BRIEF SUMMARY OF PROFESSIONAL EXPERIENCE

Information should include a brief summary of the proposed individual's professional experience.

Bryant is an experienced deployment manager with a successful track record of on-time and structured deployments from 10 to 30,000. Clients attribute their successful implementations to his strong communication skills, detailed documentation, and highly organized approach that is project milestone driven. As Deployment/ Implementation Manager, Paul orchestrates installation, training and the deployment of staff and resources to our customer's organizations. Paul Bryant has been with Utility since 2014 in various customer-facing roles including sales, support, project deployment and service support. He has over 14 years of experience in customer service operations

RELEVANT EXPERIENCE

Information required should include: timeframe, company name, company location, position title held during the term of the contract/project and details of contract/project.

May 2016-Present, COLORADO SPRINGS (CO) POLICE DEPARTMENT, Deployment Manager, 500 BodyWorn, 250 Rocket-IoT In-Car
Jan 2016-Present, BEXAR COUNTY (TX) SHERIFF DEPARTMENT, San Antonio, TX, Deployment Manager, 300 BodyWorn, 230 In-Car
Jun 2014-Present, CITY OF MARIETTA (GA), Deployment Manager, 142 BodyWorn, 70 Rocket-IoT In-Car Cameras

EDUCATION

Information required should include: institution name, city, state, degree and/or Achievement and date completed/received.

Bachelor of Computer Science, University – Decatur, GA

CERTIFICATIONS

Information required should include: type of certification and date completed/received.

NetMotion Certification, Panasonic Certified Master Trainer and Installer

REFERENCES

A minimum of three (3) references are required, including name, title, organization, phone number, fax number and email address.

James (Pat) Rigdon, Commander, **COLORADO SPRINGS (CO) POLICE DEPARTMENT**, 719.444.7759,,rigdonja@ci.colospgs.co.us
Patrick Labat, Chief, **ATLANTA (GA) DEPARTMENT OF CORRECTIONS**, 404.865.8063, plabat@AtlantaGa.Gov
Ronald Barrett, Director of MIS, **CITY OF MARIETTA (GA)**, 770.794.5287, rbarrett@mariettaga.gov

PROPOSED STAFF RESUME FOR RFP 3273

A resume must be completed for all proposed prime contractor staff and proposed subcontractor staff.

Company Name Submitting Proposal:	***Utility Associates Inc***

Check the appropriate box as to whether the proposed individual is prime contractor staff or subcontractor staff.

Contractor:	***Prime***	**Subcontractor:**	***NA***

The following information requested pertains to the individual being proposed for this project.

Name:	***Ray Grant***		**Key Personnel: (Yes/No)**	***Y***
Individual's Title:	***Sr. Field Engineer***			
# of Years in Classification:	***9***	**# of Years with Firm:**		***9***

BRIEF SUMMARY OF PROFESSIONAL EXPERIENCE

Information should include a brief summary of the proposed individual's professional experience.

Over the past 23 years, Grant has developed proven expertise in video management and its integration throughout Utility's digital communication solutions. He excels in various customer-facing roles, as well as the installation, configuration, integration and support of large-scale frame relay networks and server/workstations with an emphasis on network devices/routers and Internet connectivity. At Utility, Grant has played an instrumental role in developing product enhancements for the Public Safety market and implementing proven project. Grant has been actively working on the leading edge of video evidence collection since 2007. He is an analytical, proactive problem solver, quickly assessing complex situations, a respected coach/mentor, and a customer-focused Network and System Engineer with experience in the administration of global LAN/WAN infrastructure for leading corporations such as MCI/WorldCom and Reuters. Grant is accomplished at directing comprehensive voice/data installations, planning/ executing disaster recovery and providing day-to-day Level 2 and pre-sales support.

RELEVANT EXPERIENCE

Information required should include: timeframe, company name, company location, position title held during the term of the contract/project and details of contract/project.

May 2016-Present, COLORADO SPRINGS (CO) POLICE DEPARTMENT, *Field Engineer*, 500 BodyWorn, 250 Rocket-IoT In-Car
Jan 2016-Present, BEXAR COUNTY (TX) SHERIFF DEPARTMENT, San Antonio, TX, *Field Engineer*, 300 BodyWorn, 230 In-Car
Jun 2012-Present, CITY OF MARIETTA (GA), *Field Engineer*, 142 BodyWorn, 70 Rocket-IoT In-Car Cameras

EDUCATION

Information required should include: institution name, city, state, degree and/or Achievement and date completed/received.

Control Data Institute, New York, New York.

CERTIFICATIONS

Information required should include: type of certification and date completed/received.

Microsoft Certified Systems Engineer; Certified NetWare Engineer 5.x, 4.x, 3.x; BodyWorn, AVaiL Web, Rocket IoT, and Rocket

REFERENCES

A minimum of three (3) references are required, including name, title, organization, phone number, fax number and email address.

Ronald Barrett, Director of MIS, **CITY OF MARIETTA (GA)**, 770.794.5287, rbarrett@mariettaga.gov
Robert Adelman, Public Safety Communications Manager, **BEXAR COUNTY (TX) SHERIFF,** 210.335.4601 radelman@bexar.org
Mike Booker, Chief, **DECATUR (GA) POLICE DEPARTMENT**, 404.373.6551 mike.booker@decatur.ga.com

PROPOSED STAFF RESUME FOR RFP 3273

A resume must be completed for all proposed prime contractor staff and proposed subcontractor staff.

Company Name Submitting Proposal:	***Utility Associates Inc***

Check the appropriate box as to whether the proposed individual is prime contractor staff or subcontractor staff.

Contractor:	***Prime***	**Subcontractor:**	***NA***

The following information requested pertains to the individual being proposed for this project.

Name:	***Eric Bedell***	**Key Personnel: (Yes/No)**	***Y***
Individual's Title:	***Database Manager/ Director of Technology***		
# of Years in Classification:	***15***	**# of Years with Firm:**	***15***

BRIEF SUMMARY OF PROFESSIONAL EXPERIENCE

Information should include a brief summary of the proposed individual's professional experience.

As Director of Technology, Eric Bedell focuses on designing and implementing hardware and software solutions, concentrating on GUI and Windows-specific applications. After graduating from Georgia Tech in 1995, Eric joined PadSystems, a predecessor company to Utility, to work on mobile work management software. This background allowed for an easy transition to the Utility environment where Eric was part of the original team that designed AVaiL and RCM and has also been a major part of the design and roll out of DataSync, the Atlas camera backend software and most recently, AVaiLWeb. Eric has been with Utility since the inception of the company. He brings over 18 years of experience to Utility and has always worked with a focus on mobile technology. Having Eric here at Decatur headquarters is integral to our ability to manage our databases efficiently and make changes quickly when needed.

RELEVANT EXPERIENCE

Information required should include: timeframe, company name, company location, position title held during the term of the contract/project and details of contract/project.

May 2016-Present, COLORADO SPRINGS (CO) POLICE DEPARTMENT, Database Manager, 500 BodyWorn, 250 Rocket-IoT In-Car
Jan 2016-Present, BEXAR COUNTY (TX) SHERIFF DEPARTMENT, San Antonio, TX, Database Manager, 300 BodyWorn, 230 In-Car
Jun 2012-Present, CITY OF MARIETTA (GA), Database Manager, 142 BodyWorn, 70 Rocket-IoT In-Car Cameras

EDUCATION

Information required should include: institution name, city, state, degree and/or Achievement and date completed/received.

Bachelor of Science in Electrical Engineering, Georgia Institute of Technology

CERTIFICATIONS

Information required should include: type of certification and date completed/received.

BodyWorn, AVaiL Web, Rocket IoT, Rocket

REFERENCES

A minimum of three (3) references are required, including name, title, organization, phone number, fax number and email address.

Patrick Labat, Chief, **ATLANTA (GA) DEPARTMENT OF CORRECTIONS**, 404.865.8063, plabat@AtlantaGa.Gov
Ronald Barrett, Director of MIS, **CITY OF MARIETTA (GA)**, 770.794.5287, rbarrett@mariettaga.gov
Dan Lambright, VP Information Technology, **SOUTHERN CO/ATLANTA GAS LIGHT,** 404.584.356, dlambrig@aglresources.com

PROPOSED STAFF RESUME FOR RFP 3273

A resume must be completed for all proposed prime contractor staff and proposed subcontractor staff.

Company Name Submitting Proposal:	***Utility Associates Inc***

Check the appropriate box as to whether the proposed individual is prime contractor staff or subcontractor staff.

Contractor:	***Prime***	**Subcontractor:**	***NA***

The following information requested pertains to the individual being proposed for this project.

Name:	***A J Grant***	**Key Personnel: (Yes/No)**	***Y***
Individual's Title:	***Trainer***		
# of Years in Classification:	***2***	**# of Years with Firm:**	***2***

BRIEF SUMMARY OF PROFESSIONAL EXPERIENCE

Information should include a brief summary of the proposed individual's professional experience.

Grant is an experienced field technician with a record of success working with large customers on accelerated projects. Grant has led on-site installation of hardware, including communications and video recording equipment, in both body-worn camera and in-car video deployments. He also has managed large-scale accelerated rollouts of mobile hotspot Rocket router deployments in applications raging from small to commercial sized vehicles. Grant is a customer-focused professional who combines excellent communication skills with a technical aptitude and deep product knowledge to ensure successful deployment and implementation results for his customers. As Trainer, A.J. is responsible for the satisfaction of all management and technical issues relating to product implementation. He works with the sales and project management teams to ensure that every part of the deployment is a success. He also works with legacy customers as they renew software, upgrade hardware and expand their initial deployments. Grant has 8+ years of previous experience in customer service and service management positions. His curiosity, aptitude, technical skills propelled him to design and build the control system and scientific payload for a large scale, eight-foot model rocket capable of a mile-high trajectory, and to create a start-up company to tutor and field support amateur racecar drivers.

RELEVANT EXPERIENCE

Information required should include: timeframe, company name, company location, position title held during the term of the contract/project and details of contract/project.

May 2016-Present, COLORADO SPRINGS (CO) POLICE DEPARTMENT, Trainer, 500 BodyWorn, 250 Rocket-IoT In-Car
Jan 2016-Present, BEXAR COUNTY (TX) SHERIFF DEPARTMENT, San Antonio, TX, Trainer, 300 BodyWorn, 230 In-Car
Mar 2015-Aug 2015, FLORIDA HIGHWAY PATROL, Trainer, 1,937 Rocket mobile hotspot routers

EDUCATION

Information required should include: institution name, city, state, degree and/or Achievement and date completed/received.

Bachelor of Arts, Political Science, University of North Carolina – Charlotte

CERTIFICATIONS

Information required should include: type of certification and date completed/received.

BodyWorn, AVaiL Web, Rocket IoT, Rocket

REFERENCES

A minimum of three (3) references are required, including name, title, organization, phone number, fax number and email address.

James (Pat) Rigdon, Commander, **COLORADO SPRINGS (CO) POLICE DEPARTMENT**, 719.444.7759,,rigdonja@ci.colospgs.co.us
Patrick Labat, Chief, **ATLANTA (GA) DEPARTMENT OF CORRECTIONS**, 404.865.8063, plabat@AtlantaGa.Gov
James Crosby, Sergeant, **FLORIDA HIGHWAY PATROL (FL)**, 386.736.5350, jamescrosby@flhsmv.gov

PROPOSED STAFF RESUME FOR RFP 3273

A resume must be completed for all proposed prime contractor staff and proposed subcontractor staff.

Company Name Submitting Proposal:	***Utility Associates Inc***

Check the appropriate box as to whether the proposed individual is prime contractor staff or subcontractor staff.

Contractor:	***Prime***	**Subcontractor:**	***NA***

The following information requested pertains to the individual being proposed for this project.

Name:	***Reece Starks***		**Key Personnel: (Yes/No)**	***Y***
Individual's Title:	***Trainer***			
# of Years in Classification:	***2***	**# of Years with Firm:**		***2***

BRIEF SUMMARY OF PROFESSIONAL EXPERIENCE

Information should include a brief summary of the proposed individual's professional experience.

Starks is an experienced, client-focused professional with a solid understanding of both software and hardware implementations. He has installed and configured Utility's video management service for clients across the U.S. Reece's strong communication and interpersonal skills, and commitment to client satisfaction result in timely and precise execution of installations. Starks has experience in both Utility's sales team and field support organization. His background in sales strategy, production, deployment training, and customer support give him broad knowledge and experience to successfully manage Utility's service model to meet our customers' needs. As Trainer, Reece is responsible for the satisfaction of all management and technical issues relating to product implementation. He works with the sales and project management teams to ensure that every part of the deployment is a success. He also works with legacy customers as they renew software, upgrade hardware and expand their initial deployments. In his previous professional experience, Starks has experience in research, quantitative analysis, and served as a project manager for a global telecom company.

RELEVANT EXPERIENCE

Information required should include: timeframe, company name, company location, position title held during the term of the contract/project and details of contract/project.

May 2016-Present, COLORADO SPRINGS (CO) POLICE DEPARTMENT, Trainer, 500 BodyWorn, 250 Rocket-IoT In-Car cameras
Jan 2016-Present, BEXAR COUNTY (TX) SHERIFF DEPARTMENT, San Antonio, TX, Trainer, 300 BodyWorn, 230 In-Car cameras
Jun 2014-Present, CITY OF MARIETTA (GA), Trainer, 142 BodyWorn, 70 Rocket-IoT In-Car cameras

EDUCATION

Information required should include: institution name, city, state, degree and/or Achievement and date completed/received.

Bachelor of Science, Finance, Georgia State University

CERTIFICATIONS

Information required should include: type of certification and date completed/received.

BodyWorn, AVaiL Web, Rocket IoT, Rocket

REFERENCES

A minimum of three (3) references are required, including name, title, organization, phone number, fax number and email address.

Ronald Barrett, Director of MIS, **CITY OF MARIETTA (GA)**, 770.794.5287, rbarrett@mariettaga.gov
Robert Adelman, Public Safety Communications Manager, **BEXAR COUNTY (TX) SHERIFF,** 210.335.4601 radelman@bexar.org
Mike Booker, Chief, **DECATUR (GA) POLICE DEPARTMENT**, 404.373.6551 mike.booker@decatur.ga.com

THE **SMARTEST** BODY-WORN TECHNOLOGY

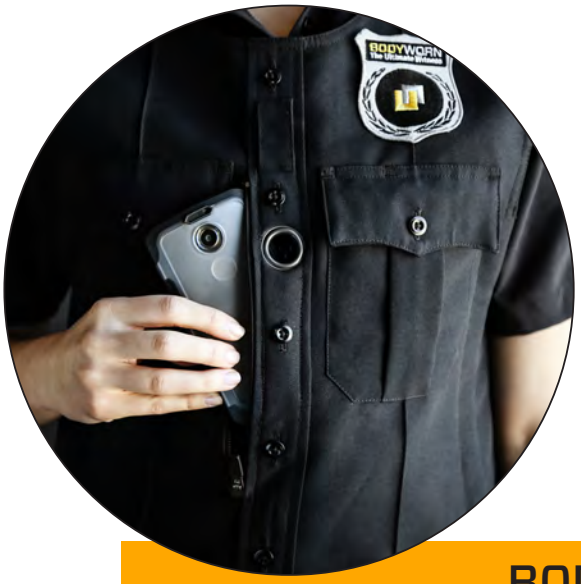
BodyWorn™ by Utility, Inc. is the smartest body-worn technology in the world. It is a future-proof solution that overcomes significant pitfalls that are found in competing police body-worn cameras. Utility developed this smart device to provide agencies with greater benefits than a manually operated camera. BodyWorn automatically records, based on policies when triggers are activated. Command centers and 911 dispatchers can send live messages to BodyWorn devices and view live streaming during critical moments. The video, audio and metadata automatically and securely uploads to cloud storage, eliminating the inconvenience of physically docking the device.

- **Automatic Policy-Based Recording**
- **Initiate Recording from Central Dispatch**
- **Hi-Definition Video**
- **Integration with the Rocket™ and Rocket IoT™**
- **4G LTE Internet Connectivity**
- **Internal GPS and Accelerometer**
- **Functional Fusion of Technology and Garment**
- **Emergency Two-Way Communicator**
- **Speech Recognition for Hands-Free Operation**
- **Secure Automatic Wireless Offload - CJIS Compliant**
- **Discrete Alerts for Backup Support**
- **Real-Time BOLO, Amber, and Silver Alerts**
- **Officer Down Alerts**
- **Live Video Streaming**

UTILITY

BODYWORN™

PRODUCT FEATURES & SPECIFICATIONS



FEATURES:

- Automatic Policy-Based Triggers
- Immediate and Secure Evidence Offload
- Real-Time Alerting
- Officer Down Alerting
- Live Video Streaming
- Securely Mounted in Uniform

BODY CAMERA

Video

- 720p HD Video Resolution
- 30 Frames per Second
- Automatic High Dynamic Range
- Video Stored in Secure Slice Files
- Automatic Wireless Media Offload Process
- Automatic Secure Wipe after Upload
- Bright LED for Night Recording

Interactive

- Integrated LCD Monitor
- Automatic Officer Assignment and Login with NFC chip
- Automatic Integration with In-Car Video Triggers and Metadata
- Voice/Touch Point Manual Operation Capable
- Covert Mode with Vibrating Notifications
- Bluetooth Communications
- Chain of Custody Validation for each minute of Automatic Video Offload
- Immediate Video Playback Capable
- Accelerometer G-force Recording Triggers

Connectivity

- WiFi Connectivity
- Mass Alert Distribution - BOLO, Silver, Amber
- Cell Phone Replacement Alternative
- Unlimited VoIP WiFi Communications
- Cellular Connectivity Capable
- Text Message Capable
- Voice Command Capable
- Audio Notification Capable

Other Features

- Live Streaming Video Capable
- GPS Position Reporting
- Time, Date, GPS Location in Metadata File
- Integration with Video Mapping Software

Environmental

- Operating temperature: -10° to 40° C
- Capture minimum of 3 hours video (at lowest setting)
- Fully Rechargable in Under Two Hours
- No Electromagnetic Interference

UTILITY

© Copyright 2016 Utility, Inc. All Rights Reserved.

MULTIPLE MOUNTING OPTIONS

Merging the BodyWorn™ technology with the officer's uniform keeps it streamlined and non-threatening. This ensures that the device is beyond the easy reach of criminals and is stable when recording, to provide the optimal audio and video of an incident.

EXTERNAL VEST CARRIER

DUTY SHIRT

SAFETY VEST

FOUL WEATHER JACKET

TACTICAL VEST

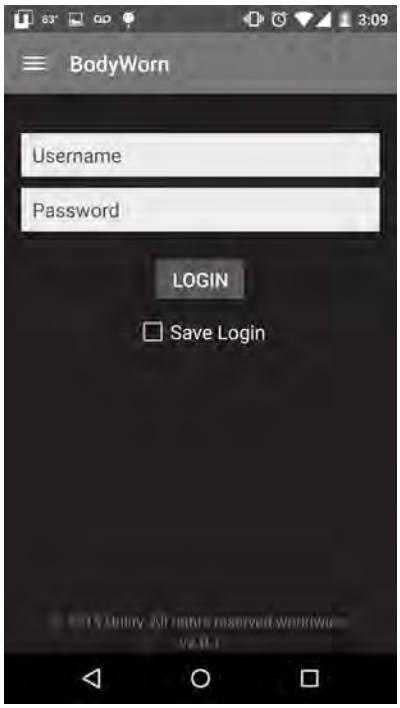
EVERYDAY MOUNTING OPTIONS

Available in a Variety of Color Options

www.bodyworn.com 404-816-0300 bodyworn@utility.com

BodyWorn User Guide

BODYWORN LOGIN

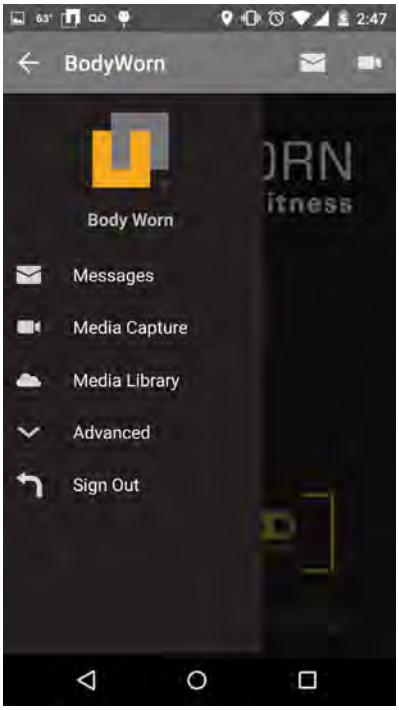


Login using the assigned username and password (same credentials as AVaiL Web) OR login via the NFC chip built into the holster.

HOMESCREEN

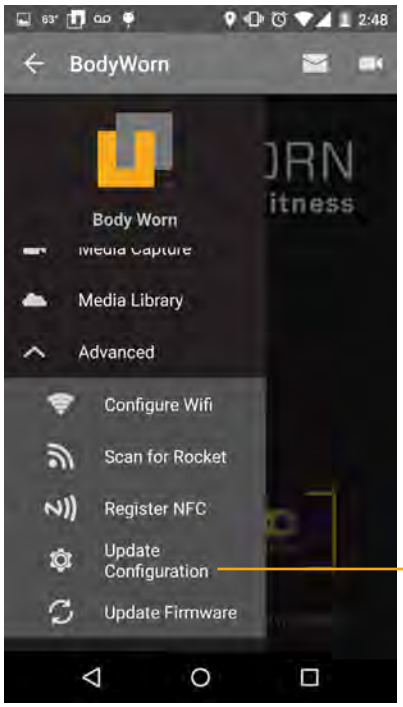
Displays on/off duty and on/off speech toggle, message icon and media icon. The user can access the **Navigation Drawer** by clicking the menu in the left-hand corner.

NAVIGATION DRAWER



Within the Navigation Drawer, the user can check messages, go to Media Capture and Media Library, access Advanced Tools and Sign Out.

ADVANCED TOOLS



ADVANCED TOOLS

CONFIGURATION UPDATES

Advanced Tools allows the user to Configure WiFi, Scan for a Rocket to gain wireless connectivity, Register an NFC chip for automatic login, Update Configuration properties and Update BodyWorn Firmware.

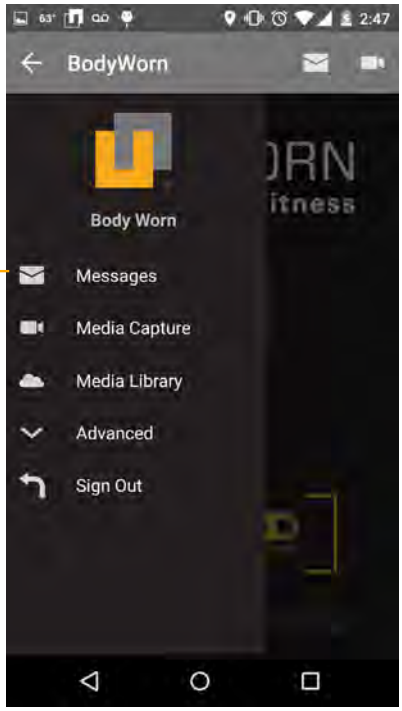
© Copyright 2015 Utility, Inc. All Rights Reserved.

BodyWorn User Guide

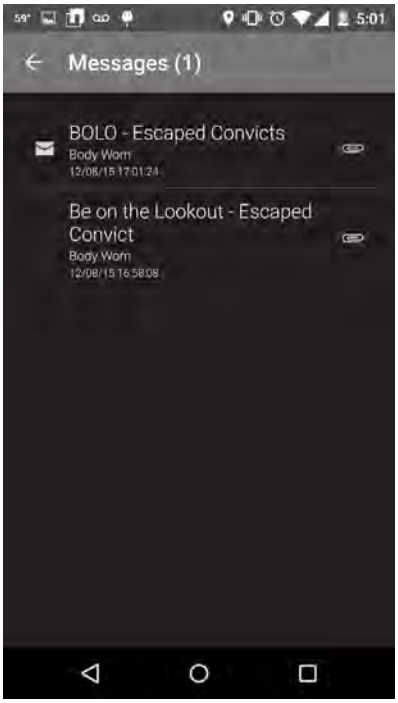
MESSAGES

View messages by clicking the envelope icon.

Messages can also be found in the Navigation Drawer.

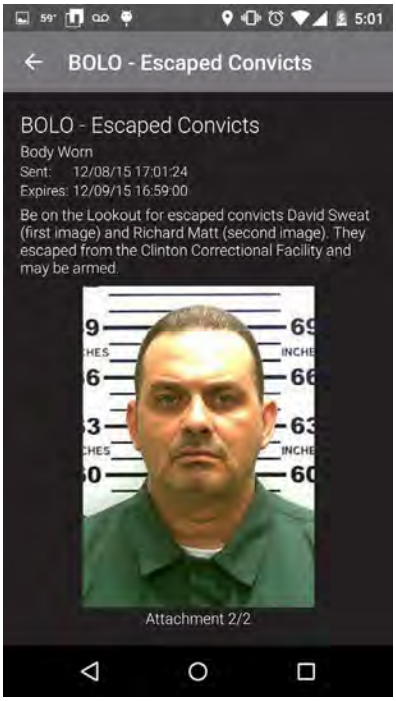


BOLO ALERTS



Messages can include BOLO alerts, Action Zone updates and more.

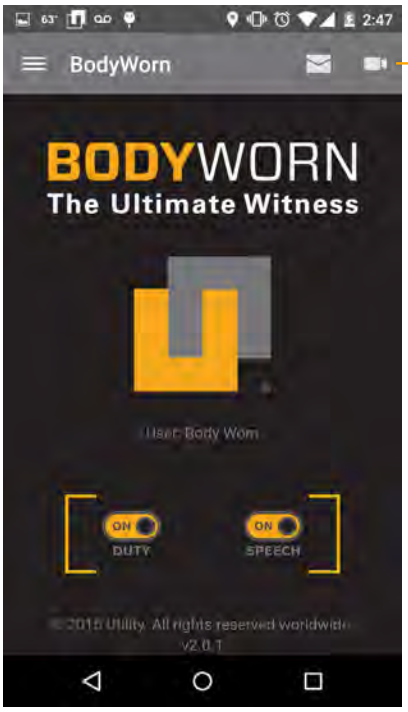
BOLOs can contain images, text, sent dates and expiration dates.



View multiple attachements by swiping the picture with their finger.

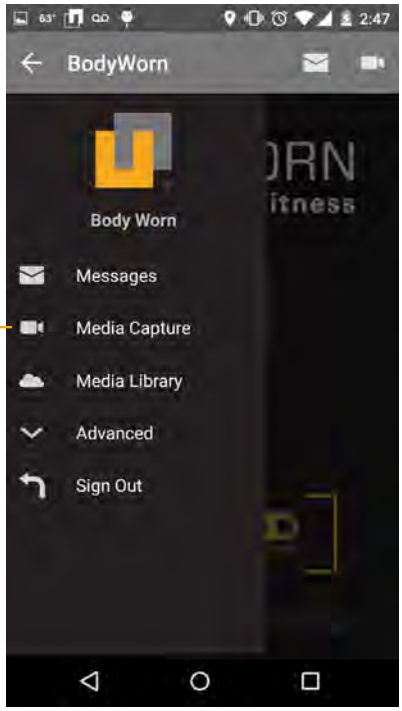
© Copyright 2015 Utility, Inc. All Rights Reserved.

MEDIA CAPTURE



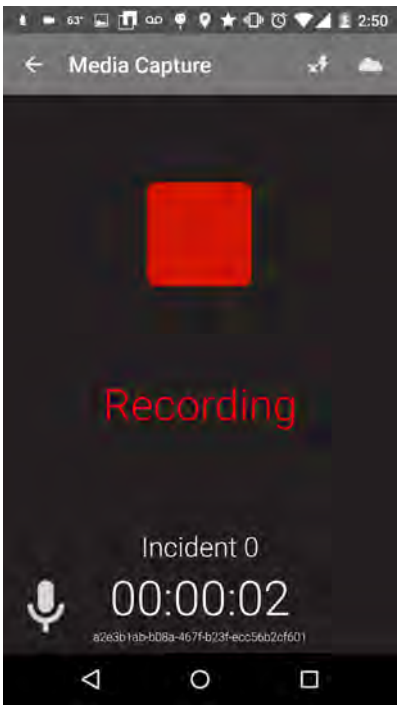
Take video or photos manually by clicking the video camera icon.

Media Capture can also be found in the Navigation Drawer.

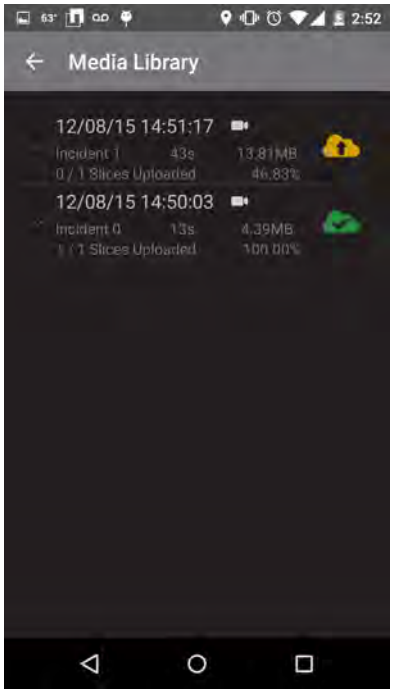


In Media Capture, the user can take pictures and record video.

Take a photo by clicking the camera icon and access the Media Library by clicking the cloud icon in the top right corner.



Stop a recording by clicking the red square and mute the recording by clicking the microphone.



Recorded media uploads can be viewed in the Media Library.

© Copyright 2015 Utility, Inc. All Rights Reserved.

PHOTO CAPTURE

Take a photo or a group of photos by clicking the camera icon.

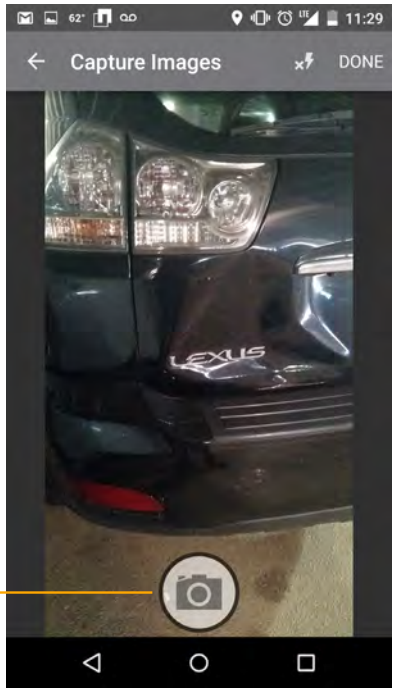
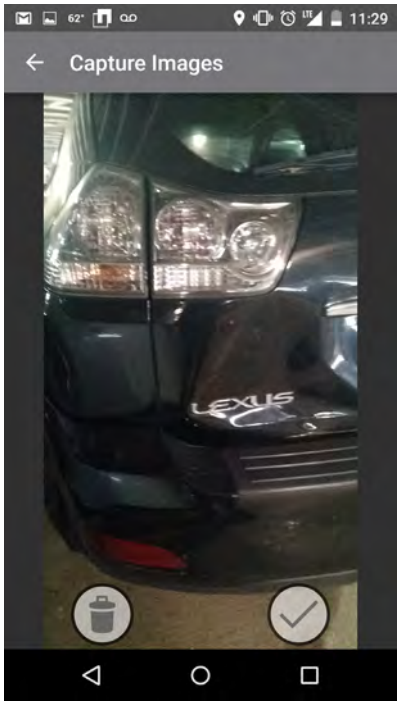


Photo Capture



Delete the photo by clicking the trashcan icon or add it to the Review Folder by clicking the check mark. Review images by clicking the back arrow.

(photos will automatically be placed in the Review Folder after 3 seconds)

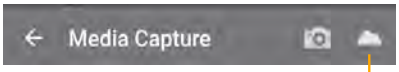
Review multiple photos by swiping left and right.

Take more photos by clicking the camera icon and save images for upload by clicking the disk icon.

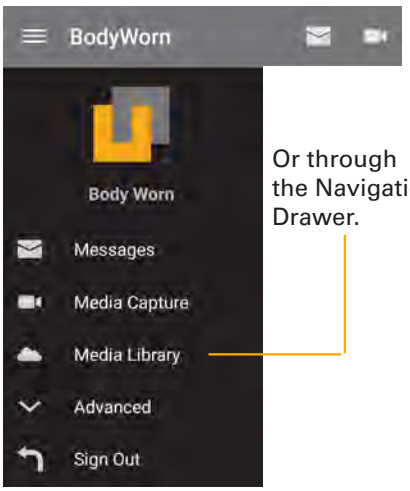
© Copyright 2015 Utility, Inc. All Rights Reserved.

BodyWorn User Guide

MEDIA LIBRARY



The Media Library can be accessed by the cloud icon in Media Capture

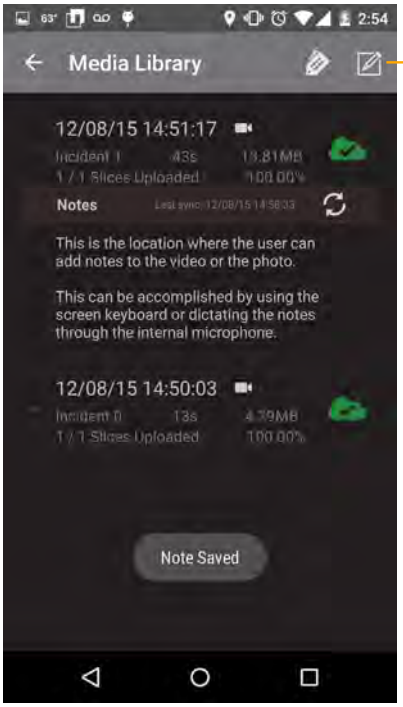


Or through the Navigation Drawer.

The media upload status is shown in the Media Library.

The green cloud icon indicates that the media is completely uploaded.

ADD NOTES



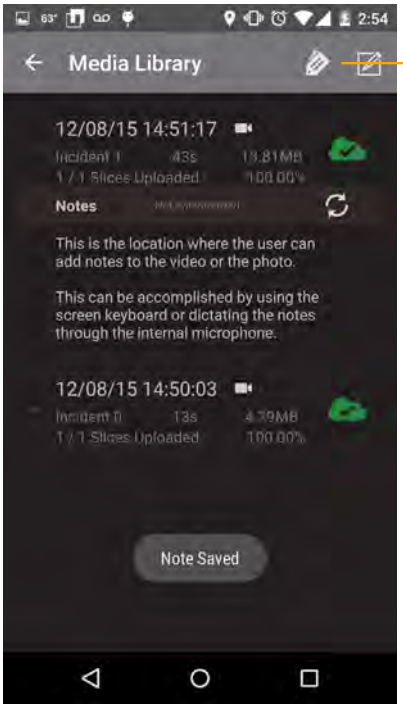
Notes can be added to media by clicking the incident and then the pencil icon in the right hand corner.

Notes must be saved before exiting the screen.

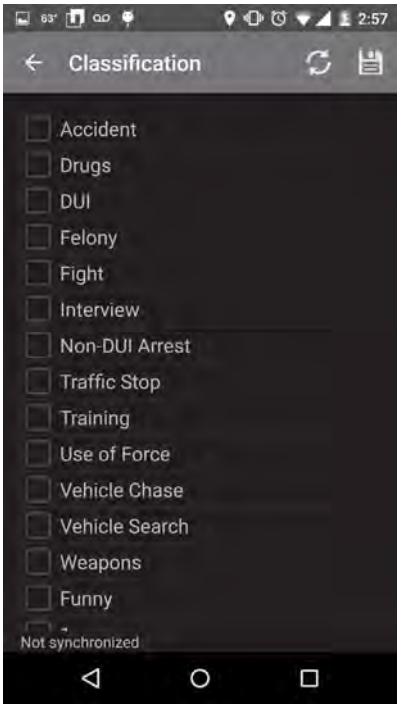
© Copyright 2015 Utility, Inc. All Rights Reserved.

BodyWorn User Guide

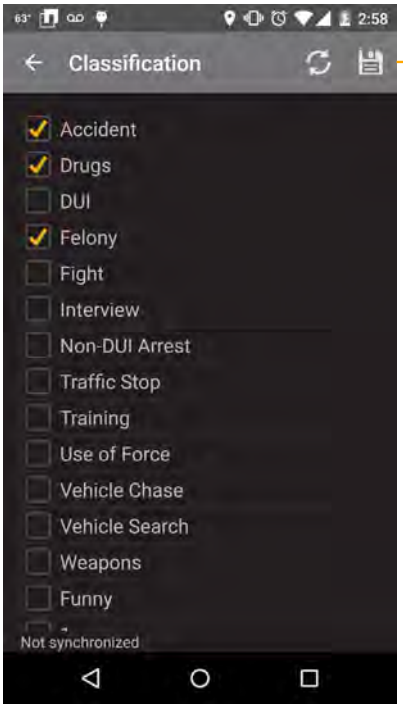
CLASSIFICATION



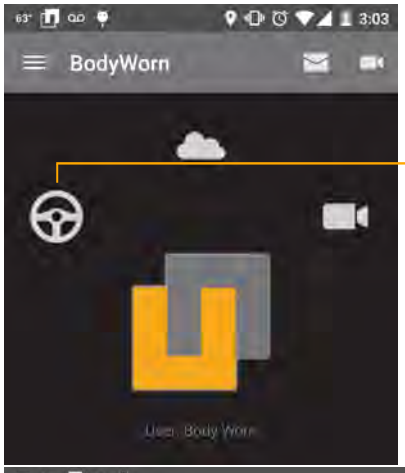
The user can classify media by clicking the incident and then the tag icon in the right hand corner.



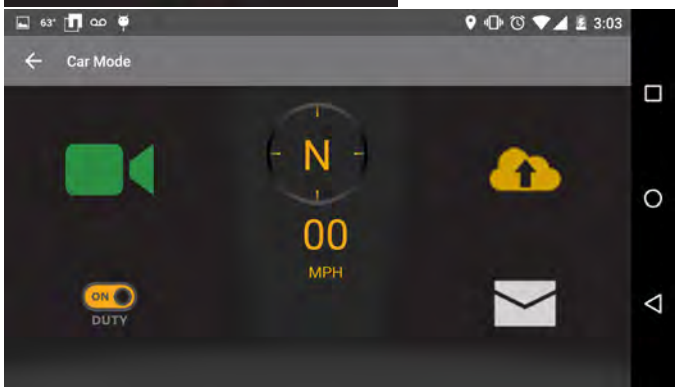
The user can choose the classifications they want to add to the incident by selecting the boxes.



Classifications must be saved before exiting the screen.



The user can access Car Mode by holding down the Utility Icon on the home screen and swipe towards the steering wheel icon.



BLUETOOTH ACTIVATION

BodyWorn can be activated through the built-in accelerometer or the connected Bluetooth device.

© Copyright 2015 Utility, Inc. All Rights Reserved.

SMARTREDACTION

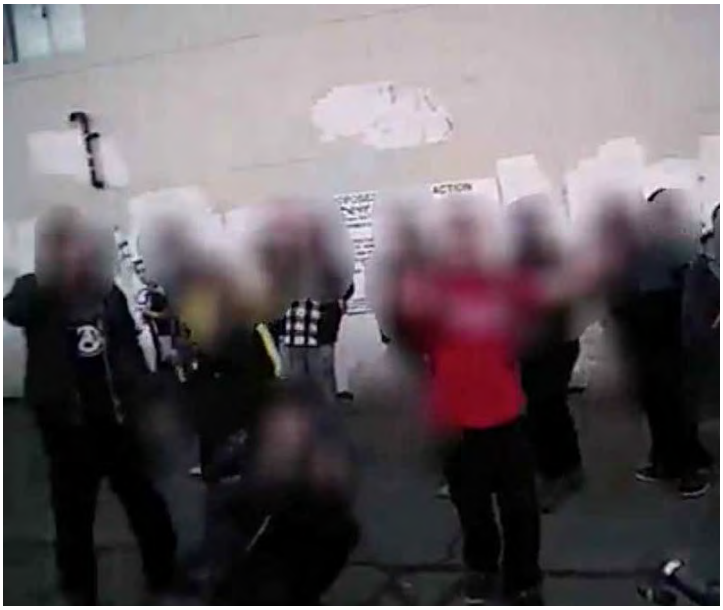
REDACT THOUSANDS OF PEOPLE IN SECONDS

As police departments equip officers with body cameras to record exchanges with the public, there has been a large increase in Public Records Requests for video evidence, such as Freedom if Information Act (FOIA), gathered by these cameras. The process of preparing videos for public dissemination, while maintaining privacy rights of those involved, has up until now been time consuming and expensive.

DEPARTMENTS CAN NOW RELIABLY & EFFICIENTLY RELEASE VIDEO FOR PUBLIC RECORDS REQUESTS IN A FRACTION OF THE TIME IT WOULD TAKE TO MANUALLY REDACT VIDEO.

UTILITY

- PROTECTS THE PRIVACY OF VICTIMS, INNOCENT BYSTANDERS, MINORS & UNDERCOVER OFFICERS
- AUTOMATICALLY IDENTIFIES, TRACKS & REDACTS
- INDUSTRY-LEADING REDACTION ACCURACY MEANS LESS TIME REVIEWING REDACTED VIDEO & LOWER COSTS
- WORKS WITH A COPY OF THE VIDEO, LEAVING THE ORIGINAL VIDEO UNTOUCHED, WHILE PROTECTING THE LEGAL EVIDENCE CHAIN OF CUSTODY
- WORKS WITH UTILITY'S BODYWORN™ & ROCKET IOT™ IN-CAR VIDEO
- INTERACTIVE TOOL WITHIN UTILITY'S AVAIL WEB™ ENTERPRISE VIDEO EVIDENCE SOFTWARE



SMARTREDACTION

CONTACT A SALES REPRESENTATIVE TODAY FOR MORE INFO.

404-816-0300 | info@utility.com | www.smartredaction.com

PATENTS: 7,768,548 B2; 6,831,556 B1; 8,781,475
PENDING PATENTS: 13 594047; 13 832517; 61 728598; 61 890570

UTILITY

© Copyright 2016 Utility, Inc. All Rights Reserved.

KNOW WHERE YOUR PEOPLE ARE, **INSTANTLY.**

A bad situation is no match for good technology. AVaiL Web™ is a secure command and control web service that provides an automatic real-time, map-based view of location and status of all mobile operations, including vehicles, personnel, and assets. AVaiL Web provides Geofence alerts, live tracking, traffic and weather overlays, asset overlays and Street Views. It's new media interface allows multiple related video and audio feeds to be played simultaneously. AVaiL Web also has live video streaming allowing dispatchers and supervisors to have complete situational awareness. It's smart. And when you use it, you'll be smart, too.

- **Scalable to thousands of vehicles**
- **GPS reporting and vehicle history**
- **GIS/ESRI data overlays**
- **Traffic and weather overlays**
- **Personal and system geofences**
- **Nested geofence polygons**
- **Geofence alerts and reports**
- **Custom device reports**
- **Satellite and street views**
- **Live tracking**
- **Video tracking and playback**
- **Live video streaming**

UTILITY

ROCKETIoT
Model X

PRODUCT FEATURES & SPECIFICATIONS

FEATURES:

- 4G LTE Internal Cellular Modem
- Supports All Major US Carriers, Dual SIM Capability
- Dual WiFi: Hotspot around the vehicle
  Access Point for high-speed offload
- Integrated Crash Sensor
- Integrated Battery Monitoring & Internal Temperature Sensor (for health monitoring)
- Optically Isolated Trigger Inputs & 1 Relay Output (5 total, 4.5V to 24V)
- Integrated Siren Trigger Interface
- Integrated On-Board Diagnostics: J1979 (ISO 15675-4), J1939 (The ISO 15675-4 was mandated in 2008 for all US cars: Is CAN interface)
- Under Voltage Warning / Shutdown
- Software Adjustable Shutdown Timer
- Integrated GPS with Antenna Detection Technology (for health monitoring)
- Remotely manage network configurations: Firewall, IPSec, Port Forwarding, Split networking, black and white list, bandwidth management

ROCKET IOT UNIT

Dimensions: 197mm (l) x 150mm (w) x 43mm (h)

Material: Cast Aluminum

Power: 9 - 24Vdc / 14W

Storage: 120GB Solid State Drive

Processor: Intel Dual Core Atom Processor, 1.33GHz

Memory: 2GB RAM, 1066 MT/s

Connectors: Color Coded, Water Tight, Locking
- 1 RED: Power and On-Board Diagnostics
- 2 DARK BLUE: 4 Ethernet (802.3af PoE 10/100Mb)
- 1 BLUE: 1Gb Ethernet
- 1 BLACK: Triggers (1 Ignition, 4 Programmable Inputs, 1 Siren, 1 Relay Output)
- 1 Radar Interface (RS-232)
- 1 USB 2.0 (optional)

RF Connectors
- 2 FME Cellular
- 2 RSPMA 2.4/5 GHz (WiFi 802.11 g/n/ac MIMO)
- 2 RSPMA 2.4/5 GHz (WiFi 802.11 g/n/ac MIMO)
- 1 SMA GPS

Environmental
- Temperature Range: -20° to 70° C
- IP-67 (submerge 1M for 30min w/ no water ingress)

Certifications
- FCC
- MIL-810G: Shock, Vibration & Temperature

IN-CAR CAMERAS

Front Camera
- 2MP Full HD
- 30 FPS at 1080p (H.264)
- 0.1 LUX Minimum Illumination for Optimal Low Light Performance
- Auto Day / Night mode
- 3.7mm Lens (Wide Angle)
- Robust Low Profile Mounting

Back Seat (Prisoner)
- 2MP Full HD
- 30 FPS at 1080p (H.264)
- 0 LUX Min Illumination
- Auto Day / Night mode
- Integrated Microphone
- 2.9mm Lens (Wide Angle)
- Robust Mounting Design

UTILITY

© Copyright 2016 Utility, Inc. All Rights Reserved.

MULTIBAND **ANTENNA**

FEATURES & SPECIFICATIONS

FEATURES:

- All-in-one Antenna:GPS, Cellular, WiFi Host & WiFi Client
- Easy to Install
- Certified for Rocket Installations
- Permanent or Temporary Options Available
- Antennas come in Black or White

SPECIFICATIONS

Frequency & Gain

- **Cable 1:** 694-894 MHz, 3 dBi & 1.7-2.7 GHz, 5 dBi
- **Cable 2:** 2.4 GHz 5 dBi; 4.9-6.0 GHz, 5 dBi
- **Cable 3:** 2.1-2.5 GHz, 5 dBi; 4.4-6.0 GHz, 5 dBi
- **Cable 4 (GPS):** 1575.42 +/- 2 MHz, LNA: 26dB 5 dBi nominal RHCP

VSWR: 2:1 max over range

Nominal Impedance: 50 ohms

Maximum Power: 10 Watts

GPS

- **Noise Figure:** 2.0 dB max, 1.7 dB typical
- **Amplifier Bias:** 2.7 to 5 VDC
- **Current:** 20 mA max, 10 mA typical

Case: 4.2"D x 3.2"H (107 mm x 81 mm) add ½" (1.3 cm) to height for magbase

Case Material: White or Black UV resistant ASA

MGW Mounting: Magnet Mount

SMW Mounting: Threaded metal stud ¾" dia. x ½"long (19 mm x 13mm) for ¼" (6mm) thick metal; supplied with gasket and nut. Other length studs available

Cables

- Cable 1: Cellular FME connector 15ft (4.5 meters)
- Cables 2 & 3: WiFi RPSMA 15ft (4.5 meters)
- Cable 4: GPS SMA 15ft (4.5 meters)

Environmental

- Temperature Range: -40° to +85° C

Certifications

- Shock & Vibration: IEEE1478, EN 61373, MIL-810G, TIA 329.2-C
- Dust/Water Ingress: SMW:IP67, MGW:IPx5

UTILITY

© Copyright 2016 Utility, Inc. All Rights Reserved.

YARD SMART WAYPOINT

PRODUCT FEATURES & SPECIFICATIONS

FEATURES:

- High Speed Video/Media Upload
- Secure Store and Forward Technology
- x86 64bit Intel Dual Core Atom Processor, 1.33GHz
- Dual WiFi MIMO
- AES 256 Encryption

SPECIFICATIONS

Dimensions: 197mm (l) x 150mm (w) x 43mm (h)

Material: Cast Aluminum

Power: 9 - 24Vdc / 14W PoE

Storage: 1 TB Solid State Drive

Connectors: Color Coded, Water Tight, Locking
- 1 RED: Power
- 2 DARK BLUE: 4 Ethernet (802.3af PoE 10/100Mb)
- 1 BLUE: 1Gb Ethernet
- 1 USB 2.0 (optional)

RF Connectors
- 2 RSPMA 2.4 GHz (WiFi 802.11 b/g/n MIMO)
- 2 RSPMA 5 GHz (WiFi 802.11 a/n/ac MIMO)

Environmental
- Temperature Range: -20° to 70° C
- IP-67 (submerge 1M for 30min w/ no water ingress)
- NEMA Weatherproof enclosure
- Shielded internal antennas
- Non-conducting fiberglass casing

Certifications
- FCC
- MIL-810G: Shock, Vibration & Temperature

UTILITY

© Copyright 2016 Utility, Inc. All Rights Reserved.

ROCKET LOCKER

PRODUCT FEATURES

FEATURES:

- Tamper-proof power and antenna connections
- Rugged composite enclosure
- Secure with MasterLock Key
- Easy to Install

Increased Security and Performance

The Rocket Locker is a secure, ruggedized housing that protects the Rocket hardware and peripherals from damage and tampering. Cable connections and hardware can only be accessed with a MasterLock™ Key.

Fully Secure

The Locker seamlessly encloses a Rocket, Booster, and Power Timer, providing a completely environment-proof encasing. Tampering is greatly reduced — no cable connection or hardware can be reached without a key.

Easy Install

The Rocket, Booster, and Power Timer are pre-mounted within the Locker itself, which is then mounted on a bracket, requiring four bolts to hold it in place. The Rocket Locker only takes up a 13"x10"x3.75" space.

UTILITY

© Copyright 2016 Utility, Inc. All Rights Reserved.

UTILITY

Generation 2 Body-Worn Cameras and the Evidence EcoSystem™

BODYWORN™

250 East Ponce de Leon Avenue, Decatur, GA 30030

www.BodyWorn.com

Letter from the Utility CEO

The purpose of this paper is to point out what is possible today in body-worn camera technology, and how it fits into the overall Evidence EcoSystem™. No specific product names are mentioned in this paper, and no specific vendor product capabilities are compared, because that was not our purpose. Generation 2 body-worn cameras can provide many benefits for Public Safety and Public Privacy Rights. Generation 1 body-worn cameras were a useful first step, but so much more is possible, practical, and cost-effective.

The "Internet of Things" (IoT) is spreading throughout Public Safety. IoT is composed of data gathering devices and sensors automatically reporting video, audio, and telemetry data over real-time IP-based wired and wireless networks to the rest of the Evidence EcoSystem™. As an example of what is possible, crime in the City of Atlanta is down 25% since 2009. Certainly the primary driver was the political leadership of Mayor Kasim Reed to get more police officers on the street. Civic leadership from the Atlanta Police Foundation, APF CEO Dave Wilkinson, and the Loudermilk family contribution of funding for new police technology such as the APD Video Integration Center was essential. I am proud to say that our company has provided some of the IoT software and technology being used by Atlanta Police today. Atlanta's tangible crime reduction results are representative of what is possible when Political, Civic, and Technology leadership come together. But Mayor Reed would likely tell you the crime rate is still too high. Technology that encourages everyone to be on their best behavior, and avoids a Situation turning into an Incident, is the best possible outcome. Generation 2 body-worn cameras are an inevitable part of Public Safety IoT.

Automatic recording triggers, real-time IP-based Internet connectivity, GPS and Motion sensors, and secure video file formats make body-worn cameras truly effective for Police Officers and for protecting Public Privacy Rights. Body-worn cameras also are a significant investment for Police Agencies and the Taxpayer. The good news is Generation 2 body-worn cameras cost no more than Generation 1 body-worn cameras, yet provide reliable data capture, Internet connectivity, and secure video storage. Police Officers, Citizens, and the Taxpayer should get the full benefit of what is practical and cost-effective today in Generation 2 body-worn cameras.

Sincerely,

Robert S. McKeeman
Chief Executive Officer
Utility

© 2014 Utility – All Rights Reserved

Table of Contents

Introduction **4**

Generation 1 Body-Worn Camera Weaknesses and Limitations **5**

Generation 2 Body-Worn Camera Advantages **6**

Generation 2 Body-Worn Camera Capabilities **8**

- Recording is triggered automatically 8
- Record in High Definition 9
- Stream Live Video 12
- Cannot be turned off during an Incident 12
- Includes integrated GPS 13
- Includes integrated 3-Axis Accelerometer 13
- Start recording all body-worn cameras within a GeoFence 13
- Upload recorded video immediately 14
- Recorded Video cannot be uploaded to YouTube and Social Media Web Sites 15
- Video file format supports metadata 16
- Distribute BOLO, Amber, Silver and other Alerts and Pictures to Bodyworns 16
- Evidence is automatically Indexed 16
- Securely Authenticate with In-Car Video using NFC 16

Incidents are not always stationary **17**

Evidence EcoSystem™ – IoT and the Future of Public Safety **18**

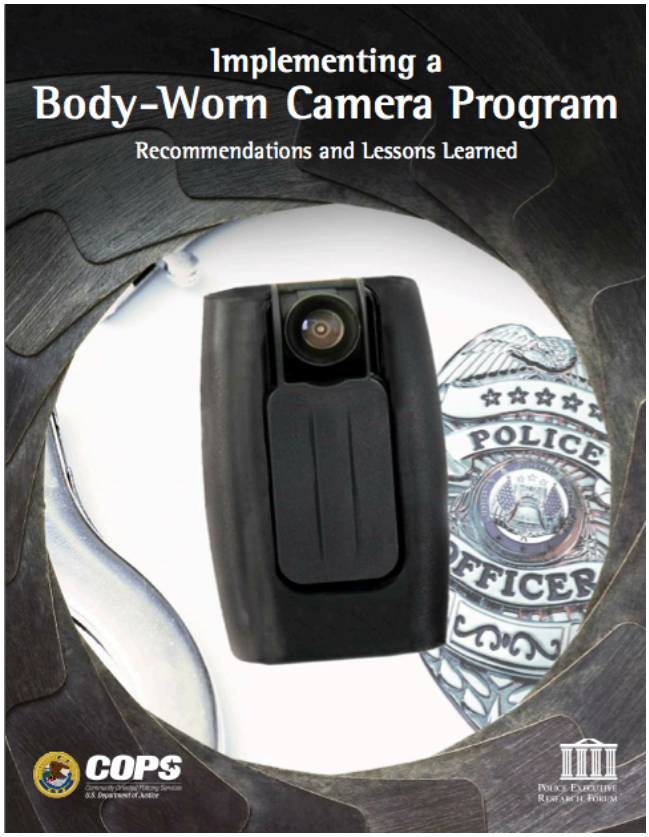
Threat to Citizen Privacy Rights – Always on "Pre-Event" Recording **20**

Conclusions **21**

© 2014 Utility – All Rights Reserved

Introduction

Utility embraces the Recommendations and Lessons Learned in the report "Implementing a Body-Worn Camera Program", jointly issued by the US Department of Justice Office of Community Oriented Policing Services, and by the Police Executive Research Forum. This report is a landmark in guiding the discussion about body-worn cameras. Our key takeaways from this report include:



- Police Actions are a matter of Public Record
- Powerful Need to Demonstrate Transparency, Openness, and Accountability
- Privacy and Trust are paramount to Community Policing
- Increasingly there are already multiple citizen video cameras at an Incident scene
- Citizens have important Privacy Rights
- Not all Citizen interaction should be recorded
- Police Officers should have Discretion with Accountability to not Record
- Maintaining the Public Trust is paramount

Underlying all these takeaways, it is imperative that body-worn video be collected reliably and stored securely. At the same time, it is important to recognize that Incidents do not necessarily stay where they start. Location and other metadata are a key part of evidence.

However, as good as the Report is, the Recommendations in this report were based upon the state of body-worn camera technology that existed in September 2013, and still exists today - what we describe as Generation 1 body-worn cameras. Generation 1 body-worn cameras have significant technology limitations that reduce their effectiveness in meeting the Report Recommendations. Generation 1 body-worn cameras in reality are not much different than GoPro®-type consumer body-worn cameras. Recording has to be manually started and can be manually stopped at any time. Video is stored in open common video file formats that can be directly uploaded to YouTube and Social Media sites. Generation 1 body-worn cameras have no Internet connectivity or internal GPS. Many Generation 1 body-worn cameras are low resolution 640 x 480 VGA – they do not even capture High Definition video like a GoPro® does. Furthermore, some Generation 1 body-worn cameras record all the time, which compromises Citizen Privacy and Officer Discretion. In contrast, Generation 2 body-worn camera recording can be started automatically as an Incident starts, can be configured so they can't be stopped manually, record at the same High Definition as consumer cell phones, leverage wireless IP-based connectivity to support real-time Situational Awareness and broadband IoT, and are

© 2014 Utility – All Rights Reserved

practical, reliable and cost-effective today. Generation 1 body-worn camera weaknesses and a description of Generation 2 body-worn camera technical advantages are described on the following pages. Generation 2 body-worn cameras will allow Police departments to realize the significant benefits that body-worn cameras can bring to Public Safety and Citizen Trust. There is no reason to accept the limitations of existing Generation 1 body-worn cameras.

Generation 1 Body-Worn Camera Weaknesses and Limitations

Current Generation 1 body-worn cameras include one or more of the following limitations:

- No automatic triggers to start recording – the Officer has to remember to manually start video recording
- The Officer can stop recording at any time for any reason by manually pressing a button
- Video is stored in a common video file format that can be uploaded directly to YouTube and Social Media web sites
- No live Video Streaming to Central Dispatch, Supervisors or Video Integration Centers
- Low-resolution video capture – 640 x 480 VGA or lower resolution that compromises citizen identification, believability of video evidence by Juries, and facial recognition technology operation. Low-resolution fuzzy video that does not clearly show what actually happened, and is not usable by facial recognition systems, is less useful.
- No connectivity with In-Car Video Recording Systems
- No integration with In-Car Video Recording systems, or with video tracks also being collected on In-Car Video Recording systems
- No ability to immediately mark and comment on body-worn video along with In-Car Video front and rear camera video tracks as part of an integrated video, audio, and metadata evidence dataset within one minute after completing recording.
- No ability for Central Dispatch to remotely start body-worn video or audio recording
- No internal GPS to report location, speed, and heading
- No internal Accelerometer for measuring G-Forces
- No ability for Central Dispatch to immediately start recording of all body-worn video cameras located within a GeoFence zone.
- Control buttons are exposed on the front of the camera
- No speech recognition to provide hands-free operation
- No audio announcements of body-worn recording capacity remaining and battery status
- No ability to download and display BOLO, Silver, Amber, and other alert text and pictures
- No audio only recording mode
- Officer has to travel to a central location to dock the body-worn to offload video
- Video remains only on the body-worn video camera until it is docked, and is at risk of being lost, damaged, or stolen before it can be uploaded
- No ability to automatically upload video wirelessly to In-Car Video Camera systems as the body-worn video is being recorded.

© 2014 Utility – All Rights Reserved

Generation 2 Body-Worn Camera Advantages

History shows technology improves every year. The "State of the Art" in September 2013 is not the State of the Art today. Body-worn cameras today do not have to suffer from Generation 1 body-worn camera limitations. Generation 2 body-worn cameras based upon proven software, hardware, and IP-based wireless connectivity are reliable, secure, and cost-effective, and are available for volume purchase immediately after the IACP Conference ends on October 28, 2014.

- Automatic triggers to start recording – without the Officer having to remember to press a manual Start Recording button.
    - Integrated with In-Car Video Recording system automated triggers such as the siren, light bar, door, weapons rack, and other automatic recording triggers. When the In-Car Video system starts recording, all body-worn cameras in the vicinity are triggered to also automatically start recording.
    - Automatically triggered to start recording when the internal accelerometer senses the Officer is running or is involved in a struggle
    - Automatically triggered to start recording when an Officer comes onto an Incident scene and another Officer's In-Car Video Camera system or body-worn camera is already recording.
- Video can be stored in a secure file format that cannot be uploaded directly to YouTube and other Social Media sites, and cannot be viewed, edited, or copied by video player software found on any Windows or Mac computer. Video and audio can only be accessed using specialized viewer software that only Police Departments have.
- Live Video can be streamed directly from the body-worn video camera to Central Dispatch, Supervisors, or to a Video Integration Center, without the body-worn video camera having to be linked to a companion device.
- Alerts from other Evidence EcoSystem™ IoT sensors and systems can be streamed real-time to the Generation 2 body-worn camera
- High Definition video recording of at least 720p that provides recognizable evidence that Police can use to identify suspects and repeat offenders, Juries can agree is compelling, and allows facial recognition technology to work effectively. Police Officers should have video recording as good as a Citizen has with an average cell phone.
- Ability for the Officer to stop recording at any time, but the body-worn camera can automatically make an audio announcement that recording is being stopped, and the audio announcement is captured as part of the video and audio before data capture actually stops. So the Officer and any nearby Citizens can have positive audio confirmation that video recording has been stopped. There does not have to be unexplained gaps in the video and audio where the video and audio just stops.
- Control buttons do not have to be exposed on the front of the body-worn video camera
- Multiple secure Control Buttons can be operated without the Officer having to look at the body-worn video camera, or take his eyes off one or more nearby Citizens
- The body-worn video camera can provide positive tactile button selection out of view of nearby Citizens

© 2014 Utility – All Rights Reserved

- Vibrations of various pulses and duration can confirm to the Officer that a body-worn camera command has been recognized and performed.
- Direct broadband IP-based data connectivity and integration with In-Car Video Recording Systems provide automatic two-way triggering and data integration
- Immediately mark and add comments to one or more body-worn videos along with In-Car Video front and rear camera video tracks in one integrated video evidence set
- Central Dispatch and Supervisors can remotely start or stop video or audio recording on the body-worn camera
- Central Dispatch can broadcast BOLO, Silver, Amber and other alerts with pictures directly to the body-worn camera screen to be viewed by Officers on the scene. Alerts can be broadcast to one body-worn camera, to all body-worn cameras within a GeoFence zone, or to every body-worn camera in the department.
- There can be an internal GPS in the body-worn video camera
- There can be an internal Accelerometer in the body-worn video camera to detect motion and acceleration such as running or a physical struggle
- Central Dispatch can immediately start recording of all body-worn video cameras located within a pre-defined or ad hoc GeoFence polygon zone.
- Central Dispatch can have a voice announcement play on all body-worn video cameras located within a pre-defined or ad hoc GeoFence polygon zone.
- Speech recognition command controls can provide hands-free operation of the body-worn video camera without the Officer having to take eyes off the Citizen
- The body-worn camera can be trained to recognize an Officer's voice, so that only the Officer can operate the body-worn video camera using voice commands.
- The body-worn video camera can make audio announcements of available recording capacity, remaining battery life, and other body-worn camera status
- The body-worn video camera can be set to audio-only recording mode
- Upload of video and audio data does not have to wait until the end of a shift or when the body-worn video camera is manually placed in an Upload docking station. Video and audio data can be immediately uploaded to In-Car Video Camera Systems, to Central Records Management systems, or to Cloud Storage. The video, audio, and metadata does not have to be at risk of being stolen, lost or compromised because it is only stored on the body-worn video camera until the end of a shift when the device is manually docked.
- The body-worn video camera can be used to send and receive secure voice and text messages when within range of an In-Car wireless communications router.

These capabilities are all representative of what the "Internet of Things" (IoT) can bring to Public Safety. Smart devices automatically reporting relevant data, so the Police Officer can focus on the situation, and his or her personal safety. Other responding Police Officers can approach an Incident with Situational Awareness of what is happening. Certainly the Police Officer should not be distracted by having to remember to manually turn on a body-worn camera. All the IoT technology included within the Evidence EcoSystem™ should be integrated to support the Police Officer and Public Safety.

Several of these capabilities warrant further explanation as described on the following pages.

© 2014 Utility – All Rights Reserved

Generation 2 Body-Worn Camera Capabilities

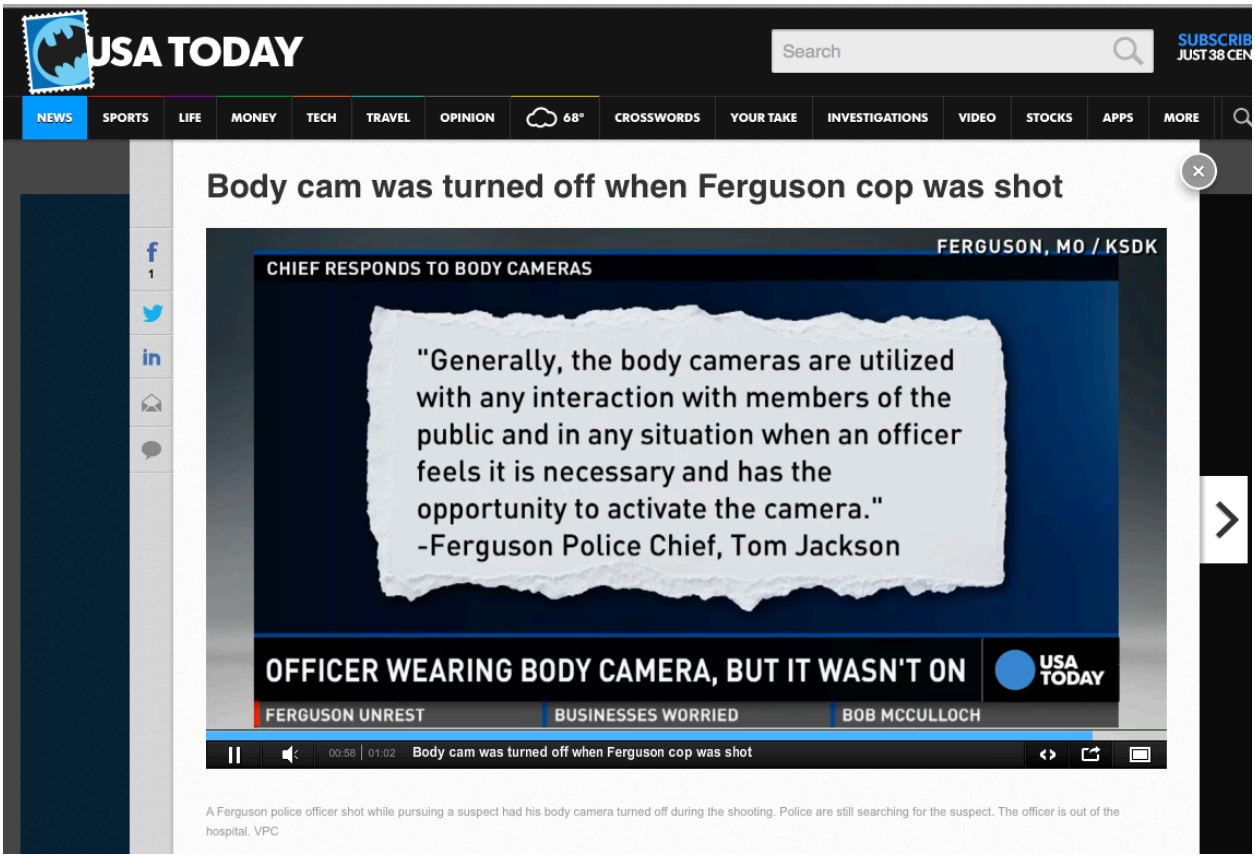
The primary Generation 2 body-worn camera advantages are real-time IP-based Internet connectivity, high-resolution video, and internal GPS. Most all Generation 2 body-worn camera capabilities flow from these three fundamental technical capabilities.

Recording is triggered automatically

Once an Incident begins, the Police Officer should focus all attention on the Incident and their personal safety, and not be distracted by having to remember to turn on their body-worn camera.

> "You want activating the camera to be a reflexive decision, not something that officers have to evaluate with each new situation. If officers have to determine what type of incident it is before recording, there are going to be a lot of situations in which a recording might have exonerated an officer, but the recording was never made." Report Page 12.

Just this past Saturday September 27, 2014, a Ferguson, Missouri police officer was wearing a body-worn camera and was shot. However, the Generation 1 body-worn camera was not turned on, so there was no video of the Incident.



http://www.usatoday.com/videos/news/2014/09/29/16415595/

© 2014 Utility – All Rights Reserved

The St. Louis County Police spokesman was quoted as saying: "he didn't know why the body camera the wounded officer was wearing was turned off during the shooting".

http://stlouis.cbslocal.com/2014/09/28/body-camera-wasnt-on-when-ferguson-officer-was-shot/

Another recent tragic example of what can happen is the San Francisco Bay Area Rapid Transit (BART) Police Officer death in January 2014. Two BART officers were investigating a robbery and entered an apartment. One BART Officer accidentally shot and killed the other BART Officer. Both Officers were wearing Generation 1 body-worn cameras. However, neither Generation 1 body-worn camera was turned on.

http://www.mercurynews.com/crime-courts/ci_25866927/da-no-charges-will-be-filed-fatal-shooting

A Generation 2 body-worn camera will activate and start recording automatically when turning on the vehicle siren or light bar at a routine traffic stop, or being dispatched to a 911 call and then opening the car door, without the Officer having to remember to do anything. All but the most routine Incidents are high risk and high stress to a Police Officer. Having to remember to turn on a body-worn camera is a distraction the Officer does not need. History shows that often the Officer does get distracted and forgets to manually turn on his or her body-worn camera.

With real-time wireless connectivity to In-Car Video Recording systems and to Central Dispatch, a body-worn camera can be automatically triggered to record at the same time the In-Car Video Recorder is automatically triggered to record. When the patrol vehicle siren or light bar is turned on, any nearby body-worn camera automatically starts recording as well. Generation 2 body-worn cameras can also be triggered by other inputs such as internal Accelerometer high G Force events resulting from running and physical struggles. The Generation 2 body-worn camera will start recording if it is not recording already. Field Supervisors, Central Dispatch, and Video Integration Center operations officers can use internet connectivity to also remotely start recording on a Generation 2 body-worn camera.

With real-time connectivity to other nearby devices, a Generation 2 body-worn camera can broadcast that an Incident is in progress, so that all other nearby Generation 2 body-worn cameras can then also start recording. The Police Officer does not have to take any manual action to start Generation 2 body-worn camera recording. Other In-Car Video systems within range of the broadcast can also start recording.

Record in High Definition

A primary takeaway from the Boston Marathon Bombing is the limited value of low-resolution video. The Boston Police and FBI were stumped because the video of the two suspected bombers was so poor that the suspects could not be identified. Facial recognition software did not work on the low-resolution images the Boston PD collected. Despite having several videos of the two primary suspects, and the efforts of photo enhancement experts, the suspect identities remained a mystery for three full days. If better quality images had been able to identify the suspects, MIT police officer Sean Collier might not have been killed.

© 2014 Utility – All Rights Reserved

FBI Press conference three days after the Bombing showing pictures of the two suspects:

Enhanced but still poor quality Suspect images from a surveillance video from a business located on Boylston Street.

© 2014 Utility – All Rights Reserved

After these FBI images were released, citizen David Green provided the following high-resolution photo taken with his iPhone 4s to the FBI. "White Cap Suspect # 2" is seen in the bottom left corner of this picture.

Because the iPhone 4s camera was much higher resolution than any other video or picture the FBI had, it was possible to zoom in on a much clearer picture of the suspect.

© 2014 Utility – All Rights Reserved

In the NY Times article by Ravy Somaiya and Jeremy Zilar published on April 18, 2013, David Green reported FBI agents stated "his picture was the best they had, because it was taken from a better camera than the others that were posted".

The Boston Marathon Bombing clearly demonstrated that low-resolution video was not able to reliably identify suspects. Police Officer body-worn cameras should have the same high-resolution video and image capabilities of the average Citizen cell phone.

Stream Live Video

Without requiring any ancillary device, Generation 2 body-worn cameras can stream live video to In-Car Video Recording systems, Supervisors, and to Central Dispatch. WiFi-enabled Generation 2 body-worn cameras can stream live Incident video from several hundred feet away to the police car or to authorized WiFi Access Point. From the police car or Access Point, the video can then be streamed to Central Dispatch or to a Supervisor vehicle for immediate display. Generation 2 body-worn cameras with cellular connectivity can stream video directly to Central Dispatch and to Supervisors in the field.

Cannot be turned off during an Incident

Generation 1 body-worn cameras are manually controlled, so they can be manually turned off at any time for any reason - good or bad. This raises the troubling potential of video not being captured on purpose. In the New Orleans officer-involved shooting of Armond Bennett in early August 2014, Generation 1 body-worn cameras were turned off deliberately. "Not only did she turn her camera off, her partner turned his off, too," Bennett Attorney Nandi Campbell stated.

http://www.wdsu.com/news/local-news/new-orleans/use-of-bodyworn-cameras-questioned-in-new-report/27903998#ixzz3EGslaFKV

Once an Incident has started, Generation 2 body-worn cameras can be configured to only stop recording when the In-Car Video Recording system is turned off, by a command from a nearby Supervisor Generation 2 body-worn camera, or remotely by Central Dispatch when it is determined the Incident is over. As the Body-Worn Camera Recommendation report points out, Officers must have Discretion and Accountability. If the body-worn camera can be manually turned off at any time with just the push of a button, there will always be a question of whether all relevant video for the Incident was captured.

A Generation 2 body-worn camera can audibly announce that it has stopped recording, so that both the Police Officer and nearby Citizens have positive audio confirmation of body-worn camera has in fact stopped recording. Furthermore, the audio announcement can be included as the last part of the Evidence recording. GPS location, date and time metadata are always recorded in a Generation 2 body-worn camera. So there is hard evidence that the recording was stopped on purpose, the Public was notified that recording was stopped, and the location and time when recording was stopped is also recorded. A Generation 2 body-worn camera can make sure there are no unexplained gaps in the video recording.

© 2014 Utility – All Rights Reserved

Includes integrated GPS

Generation 2 body-worn cameras have an internal GPS, so all video and audio is automatically tagged with GPS location metadata. Generation 1 body-worn cameras that have no GPS, or rely upon a second Bluetooth-connected device or other source of GPS location data are inherently unreliable compared to a Gen 2 body-worn device that has GPS built-in.

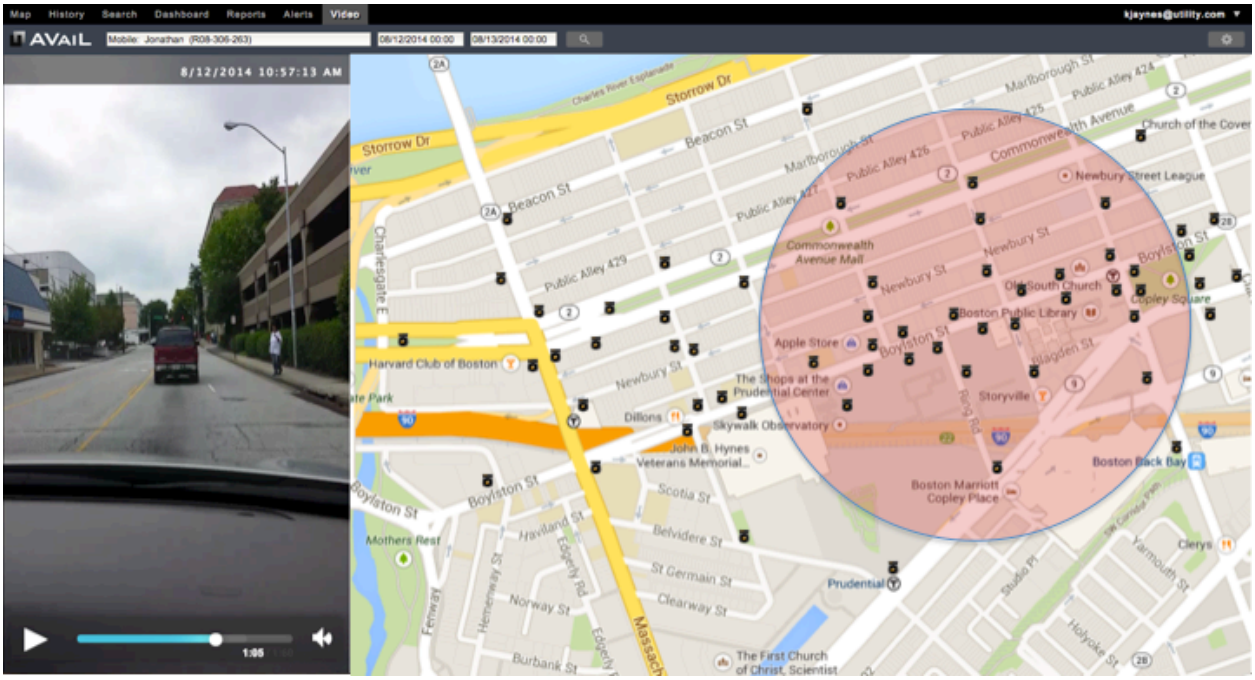
Because Incidents can change location, and can spread out once the Incident starts (Suspects take off running in different directions, the Citizen vehicle flees the scene after a stop, etc.), having direct GPS location metadata of exactly where the video was captured is important legal evidence. The Generation 2 body-worn camera moving away – i.e. the Officer moving away - from patrol car location can also be an automatic trigger to begin recording.

Includes integrated 3-Axis Accelerometer

Generation 2 body-worn cameras have an integrated 3-Axis Accelerometer that can report rapid G Force motions such as the Officer running and physical struggles. This can be another automatic trigger to start recording if the body-worn camera is not already recording.

Start recording all body-worn cameras within a GeoFence

With all Generation 2 body-worn cameras communicating GPS location to Central Dispatch on a real-time basis, it is possible to remotely start video recording on all devices within a GeoFence zone. As an example, if Boston Police had Gen 2 body-worn cameras, a Dispatcher could have drawn a GeoFence around the location of the Boston Marathon Bombing, and immediately caused all body-worn and In-Car video systems inside the GeoFence zone to start recording.



© 2014 Utility – All Rights Reserved

Furthermore, a Generation 2 body-worn camera can announce a Central Dispatch audio message such as "An Emergency is in progress – do not turn off your body-worn camera". Real-time location reporting and wireless connectivity provides First Responder Situational Awareness and Command & Control capabilities that Generation 1 body-worn cameras can never provide.

Upload recorded video immediately

Video from a Generation 2 body-worn camera can be immediately streamed to an In-Car Video Recorder or to an authorized Access Point whenever in wireless range of the vehicle, which is almost always the case. The body-worn video can be stored on the In-Car Video server along with front and back seat camera video feeds in an integrated video set. The Generation 2 body-worn video is then immediately viewable on the In-Car Video Recorder system display, and can be annotated and marked along with video from the In-Car Video front and back seat cameras. The Officer does not have to wait until the end of the shift to manually dock the body-worn camera to then be able to add notes to the body-worn camera video. If the body-worn has cellular connectivity, the video can be immediately uploaded from anywhere in cell coverage. Central CAD Dispatchers and Supervisors have the ability to view Generation 2 evidence video as it is collected and uploaded to the In-Car Video system or to "the Cloud".

Because body-worn video is uploaded immediately as it is captured, the video is not at risk of being lost, damaged, stolen, or tampered with before the end of the shift. Suspects are less likely to attempt to seize and destroy video evidence on Generation 2 body-worn cameras once they know the video is immediately uploaded as it is recorded. Once word gets around that Generation 1 body-worn video is not uploaded until the end of a shift – as word certainly will get around – bad actors will have a powerful incentive to seize and destroy the body-worn video evidence before it gets uploaded. On the plus side, Supervisors do not have to take control of Generation 2 body-worn cameras immediately after an Incident, since the video evidence is automatically uploaded as it is captured. There is no opportunity for the Officer to tamper with or lose the video evidence. Immediately uploading body-worn camera video increases Officer Safety and Public Trust. With Generation 1 body-worn cameras, video evidence is completely at risk of being tampered with or lost until the manual upload at the end of the shift – often several hours later -- is completed. Once all parties understand that video is being immediately and securely uploaded, all parties are more likely to be careful about their behavior. The best outcome is for a Situation to be defused and to never turn into an Incident. The best Incident is the one that never happens.

Once video is automatically uploaded to central storage and the Chain of Custody of the video has been validated, the video can be deleted from the Generation 2 body-worn camera just like video is automatically deleted from In-Car Video Recording systems. This immediate Chain of Custody validation process for Generation 2 body-worn cameras frees up body-worn camera video storage space. No video is permanently retained on the Generation 2 body-worn camera. So there is no reason for the body-worn video camera to be retained for an Open Records Request, and the video can't be leaked to unauthorized third parties.

© 2014 Utility – All Rights Reserved

Recorded Video cannot be uploaded to YouTube and Social Media Web Sites

Since video is not retained on a Generation 2 body-worn camera, it cannot be later uploaded to unauthorized 3rd party web sites. In addition, Generation 2 body-worn cameras do not store video in open video file formats such as .MOV and .AVI. Generation 1 body-worn cameras often store video in open, common video file formats that can be directly uploaded to YouTube and other Social Media sites, and the video can be played and copied by consumer video player software found on any Windows or Mac computer.

The January 2014 Asiana Airlines crash at the San Francisco airport is an example. A camera mounted on a firefighter helmet recorded video of a San Francisco Airport fire truck running over and killing an injured passenger who had survived the crash. The video was leaked to CNN and posted on YouTube within hours after the crash.

https://www.youtube.com/watch?v=9BHDfzKMHMo

http://www.cnn.com/2014/01/15/us/asiana-crash-new-video/

No Elected Official or Police Department wants body-worn camera video leaked to YouTube or Social Media sites. Capturing and storing video in a secure non-consumer video file format is the only sure way to prevent unauthorized postings of evidence video to YouTube and other Social Media sites, or to be shared in a way that infringes on Public Privacy Rights.

© 2014 Utility – All Rights Reserved

Video file format supports metadata

The open Generation 1 body-worn camera video file formats generally do not have a separate metadata storage capability. So metadata such as date, time, and GPS coordinates have to be overlaid on top the video image itself. This overlaying of metadata on top of the video image obscures the image behind the metadata overlay. Important evidence can be obscured.

Generation 2 body-worn cameras use a video file storage format that includes a separate metadata storage track. This separate metadata track stores time, date, GPS location, and other metadata such as 3-Axis accelerometer data indicating when and where the video was recorded, where the Officer was running, or where the Officer was involved in a struggle. The metadata track is automatically synchronized with the video and audio, so the time and location relationship of video, audio, and metadata is assured.

Distribute BOLO, Amber, Silver and other Alerts and Pictures to Bodyworns

With real-time two-way wireless connectivity and a display screen included as part of a Generation 2 body-worn camera, Central Dispatch can broadcast BOLO, Amber, Silver, or other alerts to a Generation 2 body-worn camera. Alerts are immediately available to the Police Officer. Alerts can be sent to a single body-worn camera, a group of body-worn cameras, to all body-worn cameras within a GeoFence area regardless of what groups they may belong to, or to all body-worn cameras across the Department. The alerts and pictures are displayed on the Generation 2 body-worn camera Alerts status screen.

Evidence is automatically Indexed

All evidence captured "on the fly" by Generation 2 body-worn cameras with internal GPS, Accelerometer, and real-time communications can be automatically indexed so that all evidence from all nearby Generation 2 body-worn cameras and In-Car Video recording systems are all tied to the Incident. All Incident video, audio, and metadata is searchable and available to Police Officers, Supervisors, Prosecutors, Defense Attorneys, the Courts and to the Public after appropriate Evidence Disclosure and Citizen Privacy issues are addressed. Generation 2 body-worn cameras with real-time wireless cellular broadband, WiFi, RFID, and Bluetooth connectivity to other devices and to Central Dispatch can immediately index all video, audio, and metadata evidence to the Incident.

Securely Authenticate with In-Car Video using NFC

Generation 2 body-worn cameras with a Near Field Communications (NFC) link capability can be linked to an In-Car Video system through a simple NFC chip touch process. An NFC chip in the vehicle positively identifies the vehicle. There is no need for a manual login process to "assign" a Generation 2 body-worn camera to a vehicle. Touching the Generation 2 body-worn camera with NFC reader capability to a vehicle NFC chip can automatically initiate an encrypted authentication credentials validation process and establish a secure VPN link between the Generation 2 body-worn camera and the vehicle In-Car Video Recording system.

© 2014 Utility – All Rights Reserved

Incidents are not always stationary

It is important to note that Incidents are often not stationary. An Incident may start as a traffic stop, but then turn into a suspect fleeing the scene on foot, or fleeing in their vehicle in a high-speed car chase. These types of Incidents almost always involve multiple Officers who get involved in the Incident, all on an ad hoc basis. The Evidence EcoSystem™ (described in the following pages) can engage all available Officers and all mobile and fixed location evidence-gathering devices in the vicinity of an Incident, and along the route of travel of an Incident, wherever the Incident may evolve and travel. It is never possible to predict how an Incident may evolve, or what Officers, vehicles, and other IoT evidence-gathering assets might become engaged in an Incident.

It is therefore necessary for the Evidence EcoSystem™ to be self-organizing and automatically engage all In-Car Video recording systems, Officer body-worn cameras, fixed location cameras, and other relevant IoT evidence gathering assets "on the fly" as an Incident evolves and travels from location to location. Generation 2 body-worn cameras within a designated area around an incident can all be triggered by Central Dispatch to begin collecting evidence. Furthermore, Generation 2 body-worn cameras can broadcast recording status to the Evidence EcoSystem™ so that recording is triggered automatically in all nearby Evidence EcoSystem™ devices. GPS position report metadata includes Speed and Heading, so In-Car and Officer body-worn cameras can provide the direction data necessary to activate fixed location cameras and other police vehicles along the current route of travel for the Incident.

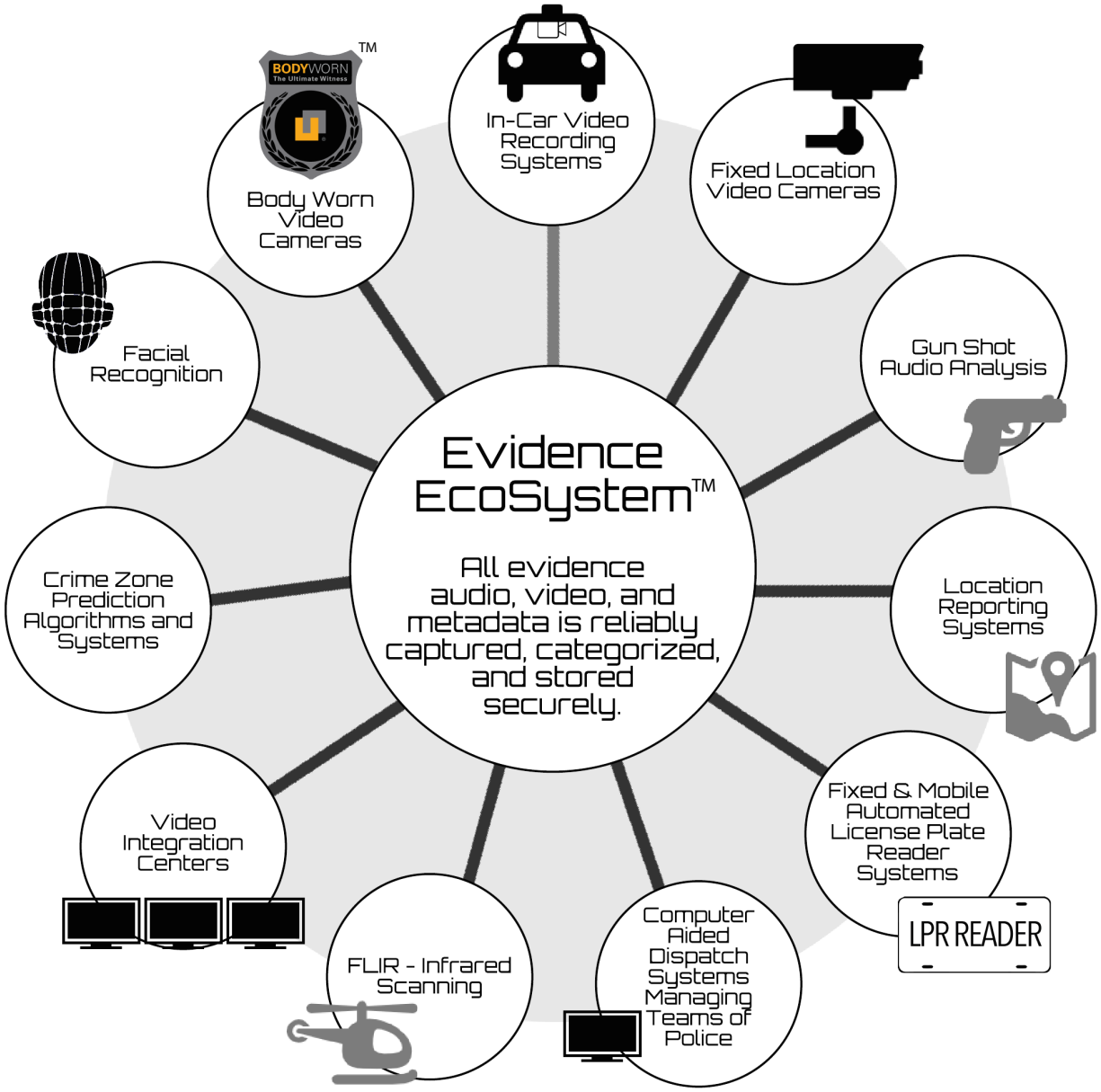
Generation 2 body-worn cameras that automatically report GPS location also provide a significant safety benefit for an Officer involved in a foot chase. It may not take long for a foot chase to take an Officer out of visual sight range of other police officers. Central Dispatch, Supervisors, Police Helicopters, and other Officers need to know where other Officers are located on a real-time basis so they have Situational Awareness so they can best assist the Officer. Real-time GPS location data of all Officers can help avoid a friendly fire situation from turning into a tragedy. If an Officer is injured during a foot chase, a Generation 2 body-worn camera reporting real-time officer location and with an emergency reporting capability could save an Officer's life.

There are many reasons why a Police organization wants the real-time location reporting data that a Generation 2 GPS enabled body-worn camera with real-time internet connectivity can provide. Incidents often do not stay where they start.

© 2014 Utility – All Rights Reserved

Evidence EcoSystem™ – IoT and the Future of Public Safety

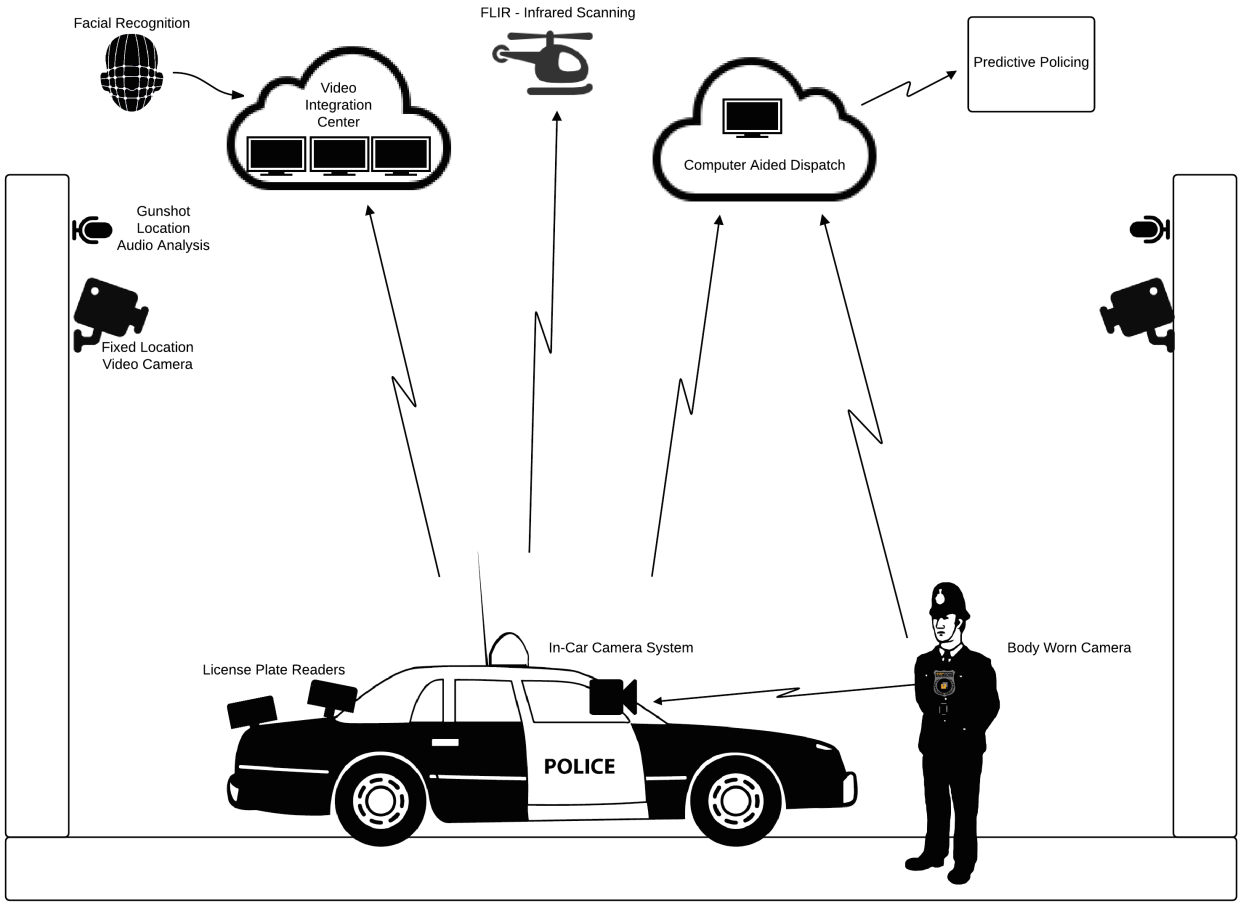
Generation 2 Bodyworn cameras are an integral part of an overall Evidence EcoSystem™. An Evidence EcoSystem™ is the real-time Internet of Things (IoT) interconnection of all evidence capturing devices, along with real-time connectivity, data analysis, and data storage involved in an Incident. An Incident is any kind of event where evidence might be collected for use in a future court case and for Public Safety.



The Evidence EcoSystem™ includes not only Generation 2 Body-worn video cameras. It also includes In-Car Video recording systems, fixed location video cameras, gun shot audio analysis and location reporting systems, fixed location and mobile Automated License Plate Reader (ALPR) systems, Central Dispatch 911 and Computer-Aided Dispatch (CAD) systems

© 2014 Utility – All Rights Reserved

managing teams of police officers, Video Integration Centers (VIC) gathering and displaying video feeds from fixed location and mobile video cameras in a region, real-time connectivity to the National Crime Information Center and other federal and state databases, crime zone prediction algorithms and systems, and video, audio, and metadata evidence storage and distribution systems to provide evidence video to Courts, Prosecutors, Defense Attorneys, Citizens involved in an Incident, and to the Public through open records requests. Evidence video, audio, and metadata in the Evidence EcoSystem™ are reliably captured, categorized, and stored securely. Central Dispatch and Field Supervisors have real-time Situational Awareness of Incident events from all data capturing devices in the vicinity of the Incident. All IoT components in the Evidence EcoSystem™ can be interconnected, and communicate video, audio, location and other metadata on a real-time basis. This integration provides reliable capture of the facts, while enhancing Officer safety and protecting Citizen Privacy Rights.



Generation 1 body-worn cameras with no connectivity to the overall Evidence EcoSystem™, where video has to be manually uploaded at the end of a shift, does have utility. But only if the Officer remembers to turn on the Generation 1 body-worn camera at the start of an Incident. Generation 1 body-worn cameras with no connectivity, and data capture reliability and video storage weaknesses, are inherently inferior to Generation 2 body-worn cameras with real-time connectivity, secure video file storage, and internal GPS technology.

© 2014 Utility – All Rights Reserved

Threat to Citizen Privacy Rights – Always on "Pre-Event" Recording

The Body-Worn Camera Recommendations report states body-worn cameras raise important questions about Citizen Privacy Rights and Trust. Privacy is the first topic mentioned in the report's "Chapter 2 - Considerations for Implementation". Determining "When to Record" was cited as the issue with the greatest Privacy implications. PERF believes "requiring officers to record every encounter with the public would sometimes undermine community members' privacy rights and damage important police-community relationships". We agree that Officer discretion is needed, and that body-worn cameras should not record at all times.

PERF further reported that very few departments have adopted a policy of recording all encounters with the Public. From Page 13 - "The more common approach is to require officers to activate their cameras when responding to calls for service and during law enforcement-related encounters and activities, such as traffic stops, arrests, searches, interrogations, and pursuits."

As this paper has shown, Generation 2 body-worn cameras can be automatically triggered to start recording when an Officer is dispatched to a call, when an In-Car Video Recording system is triggered by a siren or a light bar, when another Generation 2 body-worn camera in the vicinity starts recording, or through any number of other automatic recording triggers. In all cases, the Generation 2 body-worn camera is not recording until it is automatically triggered to record, without distracting the Officer, thus protecting Citizen Privacy Rights and supporting the PERF recommendation.

However, some Generation 1 body-worn video cameras advertise the ability to do "Pre-Event Recording". This means the body-worn camera is always recording, so that a prior 30 or 60 seconds of video can be saved once the Officer manually presses the Start Record button. A body-worn camera that is always recording is completely at odds with the PERF recommendation to not record all encounters, is a threat to Citizen Privacy Rights, and has a potential negative impact on Community Relations.

As a practical matter regarding Pre-Event Recording, in many cases the Officer is in a patrol car. Turning on the siren or light bar, or some other automatic trigger, starts the In-Car Video Recording system. Subsequently opening the police car door can trigger the Generation 2 body-worn camera to start recording. The body-worn camera in the preferred chest mount position is pointed at the car steering wheel and front dash until the Officer exits the vehicle. 30 seconds of "Pre-Event" video of the steering wheel and front dashboard of the vehicle at the start of an Incident does not provide useful evidence. Getting out of the patrol car is not the time the Officer needs to be distracted with having to remember start his body-worn camera. A Generation 2 body-worn camera can automatically start recording when the Officer opens the police car door – without the Officer having to remember to manually start anything.

© 2014 Utility – All Rights Reserved

In cases where the Officer is on foot patrol, a Call for Service from Central Dispatch can remotely start body-worn camera recording. Central Dispatch can start body-worn camera recording at any time. Voice Recognition commands, running, loud sounds, or a manual control press can also start recording. With Generation 1 body-worn cameras, if the Officer is distracted, or gets into an altercation, and does not remember to manually start the body-worn camera, or is not able to manually start recording on the Generation 1 body-worn camera, no video evidence is ever collected. The advantages of Community Policing and having a relationship with Citizens in the community will be lost when the public understands that a Generation 1 body-worn camera is always recording to capture "Pre-Event" recording.

Pre-Event Recording is useful if 30 seconds or less into an Incident, an Officer remembers he forgot to turn on his body-worn. If he remembers within 30 seconds, manually pressing the record start button on a Gen 1 body-worn will capture the start of the Incident video. But often audio is not captured during Pre-Event Recording. The far better approach for Officer safety and Public Privacy Rights is to have a Generation 2 body-worn camera that starts recording automatically based upon an Evidence EcoSystem™ IoT trigger. Human error should not prevent Incident video capture.

As the PERF report states on page 13 about Community-oriented Policing -- "Their goal, always, is to maintain an open dialogue with community members and preserve the trust in their relationships". To maintain Public Trust, Police departments should always be transparent to the Public about how public safety technology actually works.

Conclusions

The Reliability, Security, and additional capabilities of Generation 2 body-worn cameras are compelling for increasing Officer Safety and maintaining Public Trust, and will be a key part of the overall Evidence EcoSystem™. The overall goal is to have technology that encourages everyone to stay on their best behavior, so that a Situation does not turn into an Incident. The best Incident is one that never happens.

History has shown that too often the Police Officer does not remember to turn on a manually controlled Generation 1 body-worn camera. Automatic triggering of video recording is an essential part of a minimum viable body-worn camera.

Generation 2 body-worn technology is proven, reliable, and costs no more than Generation 1 body-worn cameras. Generation 2 body-worn cameras with real-time internet connectivity, high resolution cameras, secure video storage, automatic location and sensor capability such as GPS and G Force Motion Accelerometers, and real-time IoT integration into the Evidence EcoSystem™ make Generation 1 manually controlled, unconnected body-worn cameras obsolete. This paper has pointed out many compelling reasons why police departments considering body-worn camera technology should invest in Generation 2 body-worn cameras.

© 2014 Utility – All Rights Reserved

UTILITY

5 Year Total Cost of Ownership Analysis:

BODYWORN™

Typical Clip-On Body Cameras compared to Utility BodyWorn™ Video Camera

May 2016

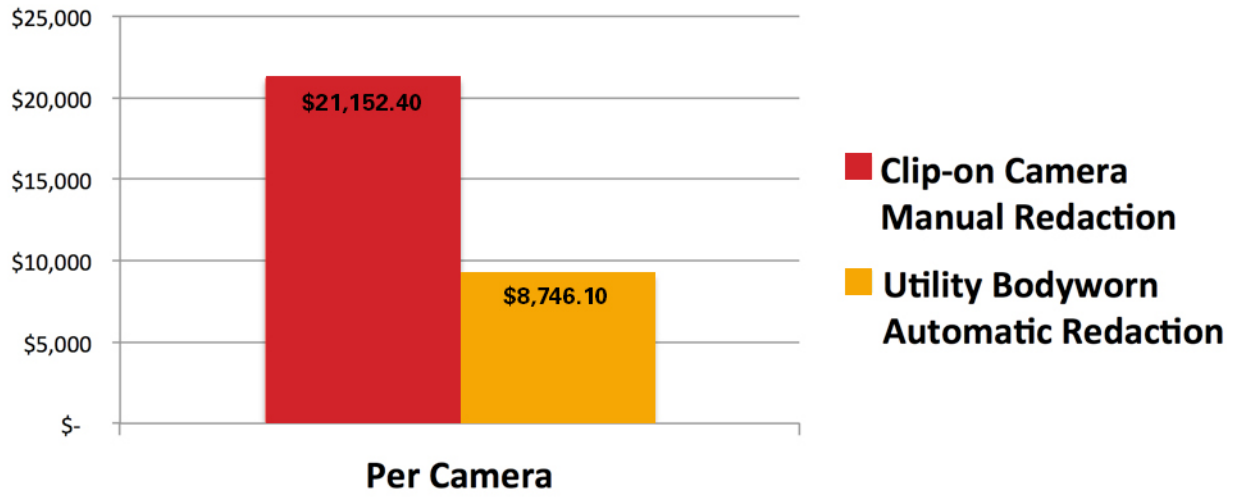
Executive Summary

Many Police Departments who have implemented body worn cameras (BWC) have been surprised to find significant additional costs. Body cameras are not simply purchased and used like a flashlight. IT support systems and staffing are required at significant additional cost to reliably store and manage video – often for years. Therefore Police Departments need to consider the Total Cost of Ownership (TCO) over 5 years. The BWC hardware itself is often far less than half the five (5) year TCO. This report provides (1) a methodology for calculating a TCO analysis, and (2) a TCO summary for two leading BWC alternatives.

Police Departments often neglect to consider the cost of Video Redaction in the BWC TCO. Redaction is obscuring faces and body parts with identifiable tattoos before video can be released for a FOIA or Press request, or before video can be shown in an open courtroom at a Trial. The staffing required to manually redact 1% of recorded video often costs more than the BWC purchase. However, a BWC with automatic video redaction software can typically avoid enough manual redaction labor hours each year to pay for the BWC.

Video storage, docking stations, training, hardware maintenance and repair, and additional software licenses for Court Officers, Prosecutors and Defense Attorneys also need to be considered in calculating a realistic TCO. Most vendors who provide cloud storage are moving to unlimited video storage as part of their total solution. Local video storage has to add the purchase cost, operations, cybersecurity, and disaster recovery staffing and support costs for local video storage servers as additional costs in their five (5) year TCO calculation.

A realistic TCO can vary dramatically as shown in the following chart.



This report shows the very compelling five (5) year TCO savings for a BWC solution that includes automatic video redaction and classification on the BWC.

© 2016 Utility – All Rights Reserved

Objective

The objective of this analysis is to provide (1) a framework for calculating the Total Cost of Ownership, and (2) document a per unit TCO comparison of Utility's BodyWorn™ video camera compared to a typical Clip-on manually operated body-worn video camera.

Background and TCO Cost Factors

The rise of BWC technology can be attributed to three primary goals: (1) Promote police accountability and transparency as a matter of public record (2) Improve high-quality public service provided by police officers, and (3) Increase the perceived legitimacy of officer-constituent interactions (Miller, Toliver and Police Executive Research Forum). Furthermore, law enforcement agencies expect BWC technology to advance proactive and preventative efforts to reduce crime (Police Executive Research Forum).

Several companies, including Utility, Inc. (Utility) have developed BWC devices that address the goals stated above. Each device addresses these goals with different types of device functionality, real-time connectivity, need for additional peripherals, and video management software capabilities. For the purpose of this analysis, commonly deployed body-worn cameras and Utility's Generation-2 BodyWorn devices are compared.

Cost is a key factor for whether a law enforcement agency will implement BWCs. However, too often Police departments fail to consider all costs that should be included in the Total Cost of Ownership (TCO) analysis. Police Departments have found TCO to be a major budget problem as hidden additional costs emerge after deployment. Costs often not fully considered during a vendor selection process include:

- Data storage – either internet cloud storage or local server video storage
- Video Management software – how to Classify, Search, Play, Export, and Purge video
- Network Infrastructure to upload video from each BWC to central video storage
- Power and Security for docking stations for BWC systems that require docking stations
- Video Redaction costs – for responding to Freedom of Information Act (FOIA), Press, and Courtroom playback of BWC videos where the privacy of bystanders, minors, victims, and police officers has to be protected
- Officer time spent classifying video – and therefore not on patrol
- Accidental deletion of un-classified video
- New officer and staff training for BWC operation and recording policy
- Re-training police officers and staff about recording policy changes

In her recent article, "Cloud Storage for Camera Data?" Julie Anderson, head of AG Strategy Group, highlighted the massive amount of data produced by video recordings. The Seattle Police Department has produced 360 terabytes of data from police car dash cams. As Police Departments also deploy BWCs on every officer, this will add an additional huge amount of

© 2016 Utility – All Rights Reserved

video data that has to be stored, secured, managed, and eventually deleted. The Anderson article cites the case of Duluth, Minnesota, where the police department spent $5,000 to purchase Body Cameras, but then struggled to support the $78,000 storage cost over a two-year period (Anderson). In another example, Minooka, Illinois recently discontinued using body-worn video cameras because the administrative burden of responding to requests for videos from attorneys and the Courts became overwhelming.

Most body-worn camera solutions include Video Management software that manages the storage, search, playback, security and retention of BWC video. Often overlooked is that stakeholders outside of the Police Department such as Court officers, Prosecutors, and Defense Attorneys also need access to BWC video. In the past video from In-Car Video systems was made available by burning and mailing CD and DVD disks of a video, which is a significant administrative burden for the Police Department. Both the Press and private citizens can often submit Freedom of Information Act (FOIA) requests for a video. This administrative burden will only increase dramatically once every officer is wearing a BWC and recording 2 hours or so of video per shift. Some BWC Video Management systems can be configured to allow stakeholders such as Courts and Prosecutors to have access to BWC Video, but often at an additional cost for software user licenses. These BWC video distribution administrative costs have to be considered in a full five (5) year TCO analysis.

BWC video typically requires redacting (fuzzing out faces and skin) before a video can be released in response to Court, Press, and Citizen FOIA requests. Video must protect the privacy of both police officers and the public, as third parties such as gang members sitting in a Jury gallery may also see the video. 30 frames per second x 60 seconds in a minute x 60 minutes in an hour totals 108,000 video frames in an hour of video. Manually redacting 108,000 video frames in an hour of video is generally a tedious and error prone process that can often take 8+ hours of staff time to redact a one-hour video. The additional staffing required to redact video can be huge. Video redaction is often the largest cost component of the five (5) year TCO for a BWC, yet is often overlooked as police departments consider BWC alternatives.

Once BWCs are deployed, video needs to be classified so that it can be found during video searches, and then purged according to a department's video retention policies. Some videos such as felonies and DUI need to be retained for years, while most other videos can be purged after the minimum retention time according to retention policy. Classifying a video is critical to avoiding the example of Fountain CO Police, where 15,000 unclassified videos that included some felony video were accidently purged and lost forever. Being able to classify video on the BWC at an Incident scene takes very little effort. On the other hand, if a police officer has to dock a BWC at the end of a shift, upload the video, and only then is able to use a Video Management system to remember and classify video (as was the case in Fountain CO), then the classification labor effort is significantly higher, accuracy suffers, and often video never gets classified. Video classification effort is a significant part of the five (5) year TCO for a BWC, and also a primary factor for reliably storing and retaining BWC video.

© 2016 Utility – All Rights Reserved

A number of police departments have found they also need to spend millions of unbudgeted dollars on networking infrastructure and power expansion to support docking stations to upload videos. All officers at the end of a shift docking their BWC and uploading video overwhelmed the data communications network at the Dallas TX Police department, to the point where no Dallas city employee could send or receive email. Charlotte-Mecklenburg Police spent over $1M in data network and power upgrades needed for BWC docking stations. These networking and power upgrade costs have to be included in the five (5) year TCO.

The security of uploading video can be compromised if a prisoner trustee is mopping floors in a non-secured room or hallway where BWC docking stations are installed. At least one BWC docking station can be rebooted at any time with a paper clip. A BWC removed from a docking station prior to upload may never upload the video to secure storage. The cost of security over docking stations is another component of five (5) year TCO that is often overlooked.

Finally, soft costs are often not included in the TCO. When deploying BWCs, officers need training to learn how to operate their new device and how to apply the department's body-worn video recording policies. Furthermore, if recording policy changes, all officers using a manually controlled BWC will need to be re-trained in how to apply the new recording policy. Recording policy change training might take months to schedule and complete. During the retraining effort, video recording policy will be applied inconsistently depending upon whether an officer has been retrained yet. Police department new hires also have to be trained. The cost of both trainer and officer class attendee time for initial deployment, plus on-going training after deployment, must be included in the five (5) year TCO.

Total Cost of Ownership Methodology

The TCO in this analysis was calculated for a 100-unit BWC deployment. This size department is thought to have the economies of scale to be representative for all 100+ officer Police departments on a per unit basis. This per BWC unit cost can therefore be applied to estimate the TCO for any 100+ unit Police Department.

In this comparison, the typical BWC and Utility are compared on the basis of three cost categories: deployment costs, direct ongoing costs, and indirect costs. Device, peripheral, storage, and software costs were aggregated from cited data sources, and represent manufactured suggested retail prices (MSRP). Redaction cost is based on effort and costs for manual and automatic video redaction as cited in Police Department RFPs, published news sources, and vendor demonstrations. Soft costs were estimated using data from Glassdoor.com salary estimates and other cited news and data sources.

© 2016 Utility – All Rights Reserved

Deployment Costs

Deployment costs are the costs most commonly associated with purchasing BWCs. These costs include the device cost as well as the cost of any peripheral devices and training for the devices. For this comparison, deployment costs are broken down into five subcategories:

1. **BWC Hardware Cost:** This is the cost of the actual body camera device. The MSRP is provided in this subcategory.
2. **Docking Station Cost:** This is the cost of any charging or data offload stations required to be purchased alongside the BWC. This cost does not include any installation, cabling, or security for Docking Station location. The MSRP is provided in this subcategory.
3. **Policy-Based Automatic Recording:** This is the cost of additional peripheral devices or software required to implement automated policy-based recording such as automatic recording triggers from police car light bars, doors, and other peripheral inputs and sensors. This cost does not evaluate how the solution operates or attempt to qualify the costs or efficacy of any limitations or concerns associated with the solution. The MSRP is provided in this subcategory.
4. **In-Field Video Review Device:** This is the cost of peripheral devices or software required to provide in-field video review, GPS location tagging, and other capabilities not provided by the BWC itself. Some BWC solutions claim capabilities that are only available through a secondary device that also has to be purchased and supported. This cost does not evaluate how the solution operates or any limitations or concerns associated with the solution. The MSRP is provided in this subcategory.
5. **Device Training**: This is the cost of training professional services provided by the vendor providing the BWC solution. This cost does not include the value of Police Officer time spent attending classes or peripheral material or location costs, which can be substantial. The MSRP for a 100-unit BWC deployment divided by 100 is provided in this subcategory. A Police Department should recognize that a BWC solution that requires an extensive policy and operational training effort will have a higher TCO.

These five categories represent the scope of this portion of the evaluation, and are considered to provide a substantial representation of the total cost of ownership associated with "deployment" costs. Other costs not explicitly stated here are not included in this evaluation.

Direct Ongoing Costs

Direct ongoing costs are the costs associated with services that are provided on an ongoing basis for general video management and storage. For this comparison, direct ongoing costs are provided in three subcategories:

1. **Video & Evidence Management Software**: This is the cost associated with providing evidence and video management software for each camera on a per month basis. This

© 2016 Utility – All Rights Reserved

cost is converted to an annual cost. This cost does not evaluate how the solution operates and any limitations or concerns associated with the solution. The MSRP is provided in this subcategory.

2. **Video Storage Cost:** This is the cost associated with storing video, either on local video data servers at the Police department or through cloud-based data storage such as Amazon AWS, Microsoft Azure, or another cloud storage provider. Some BWC solutions offer 'unlimited' data storage for a fixed fee. However, it is important to evaluate what 'unlimited' includes and does not include against departmental needs. Typically 'unlimited' requires a Police Department to have and adhere to their Video Retention Policy where data is purged according to the policy, and is therefore no longer subject to FOIA, Press, and Court requests. 'Unlimited' typically does not mean all video is stored forever. The MSRP is provided in this subcategory.
3. **Ongoing Device Support, Maintenance, and Replacement:** This is the cost associated with ongoing device technical support, device maintenance, and device replacement. The MSRP is provided in this subcategory.

These three categories provide a substantial representation of the total cost of ownership associated with "Direct On-going" costs. Other costs not explicitly stated here are not included in this evaluation.

Indirect Ongoing Costs

Indirect ongoing costs are the costs associated with products and services that are required as a result of BWC implementation on an ongoing basis. For this comparison, indirect ongoing costs are provided in three subcategories:

1. **Video Upload and Classification Labor Hours:** This is the cost associated with officer time spent uploading and classifying video during or after each shift. Using the national average for police officer salary, a cost estimate is generated by taking a percentage of that salary as it relates to the time spent by an officer uploading video and performing BWC video classification. Some solutions involve a police officer traveling to a docking station location after the end of a shift to plug the BWC into a docking station to upload video. It often takes several hours for video to be uploaded through the docking station. The police officer then has to return to the police station once again to classify the uploaded video. Based on how the classification is performed, the percentage is scaled up or down to estimate labor hour costs required to upload and classify video.
2. **Video Redaction Labor Hours**: This is the cost for redacting of BWC video to respond to Freedom of Information Act (FOIA), Press, and Court requests for a video. The privacy and visual identification of victims, minors, bystanders and police officers has to be protected before a video can be released. The staff time required to redact one hour of video is estimated from news reports and vendor solution demonstrations. The redaction labor hour cost is then scaled to an annual cost per BWC. The percentage of total hours of video that will need to be redacted is also estimated. Any software tools

© 2016 Utility – All Rights Reserved

required to perform redaction are already included in the Direct Cost for Video & Evidence Management software mentioned previously.

3. **Third Party Video Access:** This is the cost associated with Chain-of-Custody compliant evidence sharing amongst individuals within the justice system. Some vendors charge additionally for third party video access seat licenses or User Logins. It is assumed that video evidence access accounts will be provided for the Court staff, prosecution team, and defense team. This annual cost is divided by a 100 camera deployment to provide a per camera cost of additional third party video management software access.

These three categories represent the scope of this portion of the evaluation, and are considered to provide a substantial representation of the total cost of ownership associated with "indirect ongoing" costs. Other costs not explicitly stated here are not included in this evaluation.

Key Assumptions for Comparing BodyWorn™ to Alternatives

The TCO calculation methodology relies on several key assumptions. The rationale for each assumption is outlined in the following sections to allow readers of this comparison to better understand the basis of the resulting estimates.

Policy-Based Automatic Recording

It is important to note that the policy-based recording capabilities of the Utility BodyWorn™ solution are far more extensive than other BWC devices. Both BodyWorn and other BWC solutions can automatically start BWC recording when a light bar is turned on. In the case of other BWC solutions, a master control unit in the vehicle can broadcast a Recording Start message, and the BWC as a slave device will start recording. On the other hand, in the case of the Utility BodyWorn™, the BWC itself determines when to start recording based upon the status of multiple parameters, such as start recording when the police car light-bar is on, GPS speed is zero, and a police car door opens.

Utility's solution further automatically starts recording using other sensors and triggers. Sudden motion such as running or a struggle, an officer going horizontal and not responding to verbal or tactile prompts from the BWC, an officer entering a predefined geo-fence or Action zone, when an officer is dispatched to a dynamic geo-fence zone based upon a central Computer-Aided Dispatch system, or when recording start is remotely triggered by Central Dispatch. These additional automatic video recording triggers increase video recording reliability while minimizing officer distraction and potential racial bias.

Device Training

This comparison assumes that BWC device training is necessary for a successful implementation of a BWC solution. This cost assumes that for every 20 BWC units deployed, 1 day of

© 2016 Utility – All Rights Reserved

professional training will be needed from the vendor. The International Association of Chiefs of Police (IACP) includes device training in their "Acquisition of New Technology" best practices guide. Two of the three methods of training suggested are provided by the technology vendor, suggesting that device training is best provided by a vendor, and almost certainly required for successful implementation of a new technology acquisition such as a BWC (Stolting, Barrett and Kurz).

Video & Evidence Management Software

This comparison assumes that the software solution provided by typical camera solutions and Utility are equivalent in features and functionality, when they likely are not the same. In particular, if GPS location data is embedded within the video, then video can be displayed in a map-based view. Furthermore, GPS-tagged video can also be searched by location. An in-depth comparison should be conducted in order to gain a better idea of the value provided by each video and evidence management solution.

Video Storage Cost and Reliability

This comparison assumes that the unlimited storage solution provided by other vendors and Utility are equivalent, when they likely are not. Some vendors charge an additional fee for video not originating from the vendor's BWC. Cloud-based video storage can include automatic replication across multiple data centers, providing 99.999999% storage reliability. Local video storage that does not include automatic replication to remote back-up sites will be much more exposed to catastrophic video loss. An in-depth evaluation of each contract will provide insight as to the exact differences of each company's version of unlimited storage.

Ongoing Device Support, Maintenance, and Replacement

This comparison assumes that the ongoing device support, maintenance, and replacement solution provided by other vendors and Utility are equivalent, when they have differences. An in-depth evaluation of each contract will provide insight as to the exact differences and value of each company's maintenance, support, and hardware replacement policy.

Amount of Video Recorded

In order to create annual costs, assumptions on the amount of video recorded must be made. For this comparison, the amount of video that a department will collect annually per officer was based on a study conducted in Phoenix, AZ in 2011 during the early phases of body worn video rollout. The policy for recording used during this study reflects the policies adopted by many departments currently rolling out BWC programs, and should be fairly representative of the overall population of body cameras. It should be noted, however, that the amount of video recorded may be higher or lower depending on department policy and the frequency with which its officers face events that policy requires BWC video recording.

© 2016 Utility – All Rights Reserved

Based on this Phoenix study, an average officer activated their camera 414 times in a single year during which they would have had approximately 200, 10 hour shifts (assuming that they worked for 50 weeks during the year). This means that on average the camera was activated approximately 2.07 times each shift. Additionally, the mean recording time was 9.5 minutes, meaning that 414 videos would equate to approximately 65.6 hours of video recorded annually, per officer. These values are used as the basis for comparison in calculations made (Katz, Choate and Ready).

It is important to note that many RFPs, including a 2016 Phoenix body camera RFP, instruct bidders to assume a police officer will record an average of 2 hours of video per shift and approximately 200 shifts per year. This means the average police officer will record about 400 hours of video per officer per year on average. Which is more than six (6) times the volume of video recording used in this paper to calculate TCO. As an additional point of information, an NYPD body camera RFP instructed bidders to assume recording three hours of video per shift.

Redaction Costs

This comparison makes several assumptions to determine the cost of video redaction. The first assumption is that departments will redact video to fulfill FOIA, Press, and Court Officer requests for video. It is possible that some local and state governments attempt to exclude BWC footage from being subject to FOIA requests. However, this runs completely counter to 21st Century Policing guidance of transparent and accountable police operations, and will not stand up to political and public will that BWC video is a “matter of public record”. Therefore, exclusion of BWC video from public access will not be considered in this comparison.

The second major assumption required for estimating redaction costs is how much BWC footage will be collected by Police officers. As explained in the previous section, an early 2011 Phoenix pilot project showed approximately 65.6 hours of video recorded annually per officer. However, after events such as Ferguson MO, North Charleston SC, and Baltimore MD, Police departments are mandating that more types of public interaction will be recorded. Furthermore, 2015 and 2016 RFPs are mandating bidders assume 2-3 hours of video will be recorded per shift. Therefore this analysis assumes a police officer will record 2 hours per shift x 200 shifts per year on average, for a total of 400 hours of BWC video per officer per year.

The next assumption that must be made is how much of the video collected will need to be redacted. Since there is limited information on how much video actually is redacted by departments, a conservative estimate is applied in this comparison. This comparison assumes that 1% of all recorded video will need to be redacted. Therefore it is assumed that 4 hours of video will need to be redacted per officer per year.
Following the assumption of how much video will need to be redacted is how many hours of labor it will take to redact an hour of video. As a baseline, this comparison uses an estimate of 8 hours of labor to manually redact 1 hour of footage. This is supported by a study conducted in

© 2016 Utility – All Rights Reserved

Mesa, AZ where 3 videos, ranging in length from 1-2 hours, took 30.5 hours of labor to redact. Assuming the videos were 1.5 hours long on average, it would have taken 6.8 hours of labor to redact each video. While that is under the estimate being utilized, it is likely that the average video length was less than 1.5 hours, considering that the average length of a video recorded in the Phoenix study was just 9.5 minutes with 95% of BWC videos between 0 and 32 minutes long (TASER, Intl.). Further confirming this estimating factor, NYPD told new station NY1 that it would take an NYPD officer one year to redact 190 hours of pilot body-worn camera video. Assuming 1,600 hours of available work hours in a year, this equals 8.4 labor hours to redact one hour of video.

The final assumption that must be made is how much it will cost per labor hour to redact video. Recently, both Baltimore and New York have published costs for video redaction for their BWC pilot program. NYPD quoted a price of $121,000 to reimburse NYPD for redacting 190 hours of pilot video. This results in a redaction cost per hour of $636.84. Divided by 8.4 hours, the NYPD labor cost is $75.81 per hour. This estimate appeared to be high for the average police department. Currently, Las Vegas charges individuals wishing to receive BWC footage at a rate of $48 per labor hour for manual redaction. The Las Vegas rate of $48 per labor hour for an average of 8 hours to manually redact an hour of BWC video (or $384 per hour of video) is used in this comparison to determine an annual estimate of video redaction cost.

In summary, this comparison utilizes the assumption that manual redaction of video takes 8 hours per hour of video at a rate of $48 per labor hour. Additionally, this comparison assumes that officers will record 4 hours of video that will be redacted annually. These numbers may be higher or lower based on employee productivity, local cost of labor, and other factors that would be Police Department specific.

Additional Video Management Access

This comparison makes several assumptions to determine a cost for additional video management access. The first assumption is that Police Departments will provide access to Courts and Prosecutors for evidence management. It is possible that agencies would prefer to download un-redacted video evidence to share with prosecutors, judges, and other interested parties for review. However, that presents chain-of-custody and security risks that this comparison does not support.

Other assumptions were made to reflect the approximate needs of most police departments that use the vendor provided Video Management Software to share evidence with the justice system. On that assumption, an article from Evidence Magazine stated that for 2300 BWC activations, video for 62 cases existed (Lovell). This means 2.7% of all recorded video pass through from BWC activation to court cases.
Based on the same assumptions used for video redaction, an officer will activate their camera at least twice during each shift with 200 shifts each year. At this rate, a 100 officer deployment will result in 41,400 annual camera activations, meaning that there will be approximately 1,116

© 2016 Utility – All Rights Reserved

cases where BWC footage will exist. If a local government operates 51 weeks each year, this is approximately 26 cases per week. If on average the full spectrum of court judges average 2 trials per week, then 11 accounts will be required to cover all judicial account needs. Assuming that the full spectrum of lawyers can operate with similar efficiency, a prosecutor and defense account will be needed for evidence review for every two cases handled each week, an additional 22 accounts. Adjusting for intermediate rounding, this means that for a 100 unit Police officer camera deployment, 33 additional video management accounts will be needed for the Justice system. This number may be higher or lower depending on how access is granted and taken away from those involved in the judicial system. A more detailed analysis for a specific agency would be necessary to fully understand how this element plays into body camera TCO.

Video Administration

This comparison assumes that an officer using a traditional BWC system will spend 30 minutes daily offloading and classifying their video after their shift. This number was taken from a report by the Berkley, CA police chief, citing that officers in surrounding areas where BWC systems had been implemented spent an average of 2 hours each week on BWC administration, referring to offload and classification (Meehan). Assuming a substantial learning curve and 4 shifts weekly, an officer will spend 15 minutes each shift offloading video. This is 2.5% of a 10-hour shift, resulting in a labor cost of approximately 2.5% of an officer salary. According to Glassdoor.com, an American police officers make a median salary of $53,043 annually. 2.5% of this annual salary is $1,326.08, translating to a $1,326.08 classification and offload cost associated with a traditional BWC.

© 2016 Utility – All Rights Reserved

Findings

Utilizing the methodology and assumptions thus described, a total cost for each of the components listed has been derived. In this section, calculations and supporting data are included so that the comparison can be adjusted for varying data and assumptions.

Deployment Costs

Deployment costs are the cost of the device, peripheral devices, and introductory training for the device. It was found that BodyWorn by Utility costs $500.00 to purchase one BodyWorn camera. Adding a Rocket IoT router to the vehicle provides real-time 4G-LTE, WiFi, BlueTooth, and Zigbee connectivity, vehicle diagnostic interface, 120GB of storage, and various sensors and triggers connected to the light bar, siren, doors, and other switches and triggers adds $500.00. A typical camera cost $1,250.00 to purchase the body camera, docking station, vehicle lightbar BlueTooth transmitter and training. Table 1 displays the results of the calculations for the five cost components outlined in the methodology for this comparison. Costs not applicable on a per device basis assume a 100 unit camera deployment, distributed equally per camera.

Table 1: One-Time Cost Comparison Results

BodyWorn by Utility, Inc.		Cost Component	Typical Clip-On Cameras	
The BodyWorn by Utility retails at $500.	$500	**Device**	$400	Most cameras currently on the market cost around $400.
BodyWorn uploads wirelessly via WiFi and does not require a docking station.	Not Necessary	**Docking Station**	$250	A typical 6 bay docking station costs roughly $1,500.
Rocket IoT Router includes 4G-LTE connectivity, video storage, triggers and sensors.	$500	**Policy-Based Automatic Recording**	$300	Devices to enable automatic recording cost roughly $300.
The BodyWorn by Utility is equipped to review video in the field.	Built-In	**In-Field Video Review Device**	$200	In field review screen devices such as an iPod Touch start at around $200.
Utility provides training on its devices at no extra cost.	Included	**Device Training**	$100	Training services are typically offered for around $2,000 per day for a class of 20.
BodyWorn	**$1,000**	**Total**	**$1,250**	**Typical Clip-On Camera**

© 2016 Utility – All Rights Reserved

Device Training Calculation

Utility provides 1 day of training per 20 BWCs purchased. For a 100 unit camera deployment:

$$100\ cameras * \frac{1\ day\ of\ training}{20\ cameras} = 5\ days\ of\ training$$

Other vendors charge approximately $2,000 per day of training, so for an equivalent amount of training:

$$5\ days * \frac{\$2{,}000}{day} * \frac{1}{100\ cameras} = \$100\ per\ camera$$

Therefore, for a service equivalent to Utility's, other vendors would charge $100 per camera.

Direct Ongoing Costs

Direct ongoing costs are the cost of the video and evidence management software, video storage cost, and device support. Using the methodology and assumptions outlined, the total cost of direct ongoing costs for BodyWorn by Utility were $900.00 annually. Other cameras were $960 annually. Table 2 displays the calculation results for the three categories outlined under direct ongoing costs in the methodology section.

Table 2: Direct Ongoing Costs

BodyWorn by Utility, Inc.		Cost Component	Typical Clip-On Cameras	
Unlimited storage, with the AVaiL Web Video Management Platform costs $75 per month.	$900	**Video & Evidence Management Software**	$960	Unlimited storage and software usage is generally charged monthly, at a rate of $80 per month.
Unlimited storage of all evidence is included in the monthly subscription fee.	$0*	**Video Storage Cost**	$0*	Unlimited storage of video is often included, but some limitations may add cost.
Ongoing device support and maintenance is included. Replacement is included depending on contract length.	$0*	**Ongoing Device Support, Maintenance, and Replacement**	$0*	Ongoing device support and maintenance is included. Replacement is included depending on contract length.
BodyWorn	$900	**Total**	$960	**Typical Clip-On Camera**

*$0 may not meet the requirements of some departments. Further needs analysis and cost research should be conducted.

© 2016 Utility – All Rights Reserved

Indirect Ongoing Costs

Indirect ongoing costs are the cost of redaction, additional video management access, and video administration. Using the methodology and assumptions outlined, the annual indirect ongoing costs for BodyWorn by Utility were $649.22 annually. Results for typical clip-on cameras showed annual indirect ongoing costs as $3,020.48 annually. Table 3 displays the calculation results for the three categories outlined under direct ongoing costs in the methodology section.

Table 3: Indirect Ongoing Costs

BodyWorn by Utility, Inc.		Cost Component	Typical Clip-On Cameras	
Utility provides Smart Redaction, an automated system that reduces redaction to a single assurance review.	$384	**Redaction Costs**	$1,536	Manual redaction at 8 labor hours per hour of video to be redacted.
Additional Video Management Software accounts are provided at no additional fee.	$0	**Additional Video Management Access**	$158.40	Competitors charge $40 per month for additional Video Management Software accounts.
BodyWorn automatically offloads video wirelessly with limited classification automation. Full classification is completed on the device.	$265.22	**Video Administration**	$1,326.08	Video must be manually uploaded via docking station, USB cord, or Review device. Classification is manual.
BodyWorn	$649.22	**Total**	$3,020.48	**Typical Clip-On Camera**

Redaction Calculations

As stated in the Key Assumptions section, 8 labor hours is required to redact 1 hour of video manually. Labor is calculated at a rate of $48 per hour. Given that an officer will produce 4 hours of video that needs to be redacted per year, at a manual redaction productivity level, the annual redaction cost would total $1,536 per camera. Table 4 provides productivity improvement estimates, and the number of labor hours required to redact one hour of video.

© 2016 Utility – All Rights Reserved

Table 4: **Labor Hours to Redact Video**

	Smart Redaction by Utility	Manual Redaction
Estimated Labor to Video Ratio	2:1	8:1
Productivity Improvement	75%	-
Labor Hours to Redact One Hour of Video	2	8

Using the Table in 2.4:

Utility Redaction Cost

$$4\ hr\ video, annually * \frac{2\ labor\ hr}{hr\ video} * \frac{\$48}{labor\ hr} = \$384\ annually$$

Typical Assisted Redaction Cost

$$4\ hr\ video, annually * \frac{8\ labor\ hr}{hr\ video} * \frac{\$48}{labor\ hr} = \$1{,}536\ annually$$

Justice System Video Management Account Cost Calculation

As explained in the key assumptions section, a 100 unit camera deployment will require at least 33 additional video management accounts. Utility offers additional accounts for $0.00, so the calculation is not necessary. The cost of Additional Video Management Accounts for a typical solution is calculated below:

$$33\ accounts * \frac{\$40}{account * month} * \frac{12\ months}{year} * \frac{1}{100\ cameras} = \$158.40\ per\ camera$$

Video Administration Calculations

As stated in the Key Assumptions section, a docking station-based BWC camera system requires 15 minutes of video administration daily to upload and classify video out of an officer's shift. This assumes the Police Officer is not making a special trip just to dock and classify video recorded during the shift. However, if officers have to take time or get paid overtime solely to travel to a docking station location to upload and classify video, then this docking station video administration cost is seriously understated.

© 2016 Utility – All Rights Reserved

BodyWorn by Utility offers productivity benefits over a traditional BWC camera system by partially automating video classification using embedded GPS to tag video with location metadata. The remainder of classification takes place immediately on the BWC device by the officer at the scene. Additionally, video is automatically uploaded wirelessly, rather than being manually uploaded at a central base station. Typical clip-on cameras do not provide these productivity benefits. Table 5 presents data regarding the estimated productivity improvement for each system.

Table 5: **Productivity Improvements in Video Administration**

	BodyWorn by Utility	**Typical Clip-On Camera**
Estimated Productivity Improvement	80%	0%
Daily Officer Time Requirement	3 minutes	15 minutes

Using the data in Table 5 and that an officer works 4-10 hour shifts weekly:

Utility Video Administration Cost

$$3\,\text{min}\,daily * \frac{1\,hr}{60\,min} * \frac{1\,day}{10\,hr} = .5\%\,of\ time$$

$$\frac{\$53{,}043\,officer}{year} * .5\% = \$265.22\,annually$$

Typical Video Administration Cost

$$15\,\text{min}\,daily * \frac{1\,hr}{60\,min} * \frac{1\,day}{10\,hr} = 2.5\%\,of\ time$$

$$\frac{\$53{,}043\,officer}{year} * 2.5\% = \$1{,}326.08\,annually$$

© 2016 Utility – All Rights Reserved

Overall Findings

Combining the data listed above, the findings are summarized and listed below. Total up-front cost of ownership for a BodyWorn by Utility is estimated at $500.00 plus $500.00 for a Rocket IoT router. In The ongoing, annual cost of owning a BodyWorn by Utility is estimated at $649.22 annually. The total up-front cost of a typical camera is $1,265.00. The ongoing, annual cost of owning a typical camera is $3,020.48 annually. Table 6 displays the overall cost findings. Table 7 displays the lifetime cost of each device, given a 5-year life span.

Table 6: Overall Cost Findings

	BodyWorn by Utility	**Typical Clip-On Camera**
One-Time Cost	$1,000.00	$1,265.00
TOTAL One-Time	$1,000.00	$1,265.00
	BodyWorn by Utility	**Typical Clip-On Camera**
Direct Ongoing	$900.00	$960.00
Indirect Ongoing	$649.22	$3,020.48
TOTAL Ongoing	$1,780.15	$3,980.40

Table 7: 5-Year Lifetime Cost by Device

	BodyWorn by Utility	**Typical Clip On Camera**
One-Time Costs	$1,000.00	$1,250.00
Direct Annual Costs x 5 years	$4,500.00	$4,800.00
Indirect Annual Costs x 5 years	$3,246.10	$15,102.40
Lifetime Cost All Costs Considered	**$8,746.10**	**$21,152.40**

With the Utility BodyWorn solution, the Police Department gets a full vehicle wireless router that can also serve as an In-Car Video system with the simple addition of front facing and backseat IP cameras. In practice, the Rocket IoT router can serve as a wireless docking station for BodyWorn cameras that are uploading video as it is being recorded. Furthermore, all vehicle and BodyWorn video is stored in an integrated and unified Video Management system, where all vehicle and BodyWorn video related to an Incident can be displayed as multiple panels in one integrated and time synchronized view of an Incident.

© 2016 Utility – All Rights Reserved

Conclusions

Based on this comparison analysis, BodyWorn by Utility is 41.3% of the five (5) Year TCO over a typical clip-on manually operated body camera. The productivity benefits offered by Utility's technology and software reduces the five (5) year Total Cost of Ownership by $12,406.30 per camera. The savings are all in the cost savings in Video Administration and Redaction.

Departments concerned about the cost of their current BWC solution or a solution they hope to implement should conduct an independent validation of the Total Cost of Ownership analysis for their specific department. However, reducing the five (5) year Total Cost of Ownership by more than half while providing a far more capable solution can only be good for the stewardship of public resources.

© 2016 Utility – All Rights Reserved

Works Cited

Anderson, Julie. "Cloud Storage for Camera Data?" *Emergency Management*. Ed. Jim McKay. Folsom, 8 February 2016. Article.

Glassdoor.com. *Police Officer Salaries*. 23 March 2016. 28 March 2016. <https://www.glassdoor.com/Salaries/police-officer-salary-SRCH_KO0,14.htm>.

Katz, Charles M., et al. *Evaluating the Impact of Officer Worn Vody Cameras in the Phoenix Police Department*. Document. Phoenix, AZ: Arizona State University, 2014.

Las Vegas Metropolitan Police Department. *Body Worn Camera Recordings*. n.d. 28 March 2016. <http://www.lvmpd.com/Records/BodyWornCameraVideo/tabid/583/Default.aspx>.

Lovell, Steve. *Body-Worn (Video) Evidence*. January 2015. 28 March 2016. <http://www.evidencemagazine.com/index.php?option=com_content&task=view&id=1585>.

Meehan, Michael K. *Body-Worn Cameras for Police Officers*. Memo. Berkeley, CA: City of Berkeley, 2015.

Miller, Lindsay, Jessica Toliver and Police Executive Research Forum. *Implementing a Body-Worn Camera Porgram: Recommendations and Lessons Learned*. Washington, DC: Office of Community Oriented Policing Services, 2014.

Police Executive Research Forum. *Future Trends in Policing*. Washington, DC: Office of Community Oriented Policing Services, 2014.

Reaves, Brian and Andrea Burch. *Census of State and Local Law Enforcement Agencies, 2008*. Document. U.S. Department of Justice. Washington ,DC: The Bureau of Justice Statistics, 2011.

Stolting, Cpt. Sharon, Cpt. Shawn Barrett and Chief David Kurz. *Best Practices Guide, Acquisition of New Technology*. Document. Alexandria, VA: International Association of Chiefs of Police, n.d.

TASER, Intl. *End of Program Evaluation & Recommendations*. Document. Mesa, AZ: TASER, Intl., 2013.

—. *Evidence.com Pricing*. n.d. 28 March 2016. <http://www.axon.io/pricing>.

—. "Taser, Pricing & Ordering." 18 November 2015. *Charlotte Cooperative Purchasing Alliance.* 28 March 2016. <http://www.charlottealliance.org/pdf/taser-international/TASER%20International%20Pricing%20-%20Amendment%202%20Addl%20Products.pdf>.

© 2016 Utility – All Rights Reserved

Police Transparency
Versus
Video Redaction Cost and Lead-Time

SMARTREDACTION™

is the solution

250 East Ponce de Leon Avenue, Decatur, GA 30030

www.BodyWorn.com

The recent deaths of Michael Brown in Ferguson, MO, Eric Garner in Staten Island, NY, Walter Scott in North Charleston, SC, and Freddy Gray in Baltimore, MD have ignited a national controversy about police accountability and public trust in 21st Century Policing. There is an emerging consensus that police officers should wear and use body-worn video (BWV) cameras to record interactions with the public. However, body-worn cameras raise big questions about privacy rights, access to recorded video, the cost and delay of video redaction, and police accountability and transparency. This document considers these issues, and offers a technology solution to what appears to be an intractable tradeoff between police accountability and transparency, and the cost and delay of manual video redaction.

Police Accountability and Transparency

There is a rising tide of calls for better accountability and transparency of police actions. In all four deaths listed above, police officers were not wearing body-worn cameras. There is now a broad consensus that all police officers should wear body-worn cameras and record public safety interactions so there is a video audit trail of each interaction. Case studies in Rialto, California, and Mesa, Arizona, have conclusively shown that body-worn video recordings cause both police officers and the public to behave better, with significant reductions in the use of force and citizen complaints. Reliable video recordings increase accountability and transparency of police interaction with the public.

Historically, police officers have been given wide latitude and the benefit of doubt when force has been used. However, after Walter Scott was shot in the back and killed, and after Freddy Gray died from a broken neck subsequent to being transported in a police van, it appears the national consensus has shifted. The benefit of the doubt afforded to police officers when force is used is being scaled back by both the public and the legal system.

Concern about police accountability has been amplified by a growing concern about police militarization. Unfortunately, the nightly news video of Ferguson, Missouri, after the Michael Brown death looked like an Army Combat Brigade invading Iraq. Armored personnel carriers and snipers posted on rooftops around protest demonstrations unsettled public opinion. The final report of the President's Task Force on 21st Century Policing recommends moving away from

© 2015 Utility – All Rights Reserved

militarized police forces with a "Warrior" mindset, and towards a much less hostile and confrontational "Guardian" community policing approach.

It is clear that political and public opinion has fundamentally shifted towards community policing. In particular, the technology of body-worn cameras has come into the public eye as a powerful tool that can dramatically reduce Use of Force incidents and citizen complaints, and increase police accountability and transparency. In the vast majority of cases, body-worn camera video proves that police officers acted responsibly and with restraint to de-escalate situations. Many civil rights groups, legal rights organizations such as the ACLU, and the President's 21st Century Policing Task Force are calling for all police officers to wear body-worn cameras to reliably record video evidence of almost all interactions with the public. As a result of these many factors in favor of broad adoption of police body-worn cameras, it is clear that the quantity of associated video recordings will increase dramatically in the near future.

Privacy Rights

While body-worn camera video provides accountability and transparency for police interactions with the public, there are also considerable issues related to citizen privacy rights and access to copies of video recordings. In many cases victims, innocent third parties, minors, and undercover police officers will be recorded in police body-worn videos. A victim's verbal description of sexual assault or abuse will be included in some videos. These victims will be further traumatized and victimized if their description of the sexual assault is released to the public. These innocent parties should not be endangered or further traumatized by having identifiable video released to the public, where it could be posted to YouTube or social media sites.

It is also important to note that more than faces are at issue. Tattoos and other markings on the arms, legs, and other body parts can uniquely identify and expose an individual. In many cases, an individual may not be willing to talk to a police officer to provide information relevant to an investigation if there is any possibility video and/or audio will be subsequently released to the public. There are many legitimate reasons to redact video to protect the privacy rights of a victim, minor, innocent bystander, or undercover police officer.

© 2015 Utility – All Rights Reserved

Freedom of Information Act Requests

Privacy rights are important. At the same time, many states and localities have "Sunshine" laws wherein citizens and the press can request and may not be denied timely access to public records. These generally are referred to as FOIA (Freedom of Information Act) requests. The intent is all government documents and information should be available on a timely basis to citizens and the press without restriction to provide transparency and accountability of government decisions and actions.

Video recordings in many cases have been considered to be within the scope of government information that can be obtained through a FOIA request. In-Car Video Recording systems have recorded video of traffic stops, DUI, and other incidents for years. Television shows such as "Cops" are mostly playback of police In-Car dashcam videos. The public has generally become aware that police may have video of an incident. Many In-Car Videos have been released upon receipt of FOIA requests from citizens and the press – but generally only after the video has been redacted to protect the privacy of innocent bystanders, witnesses, minors, and victims.

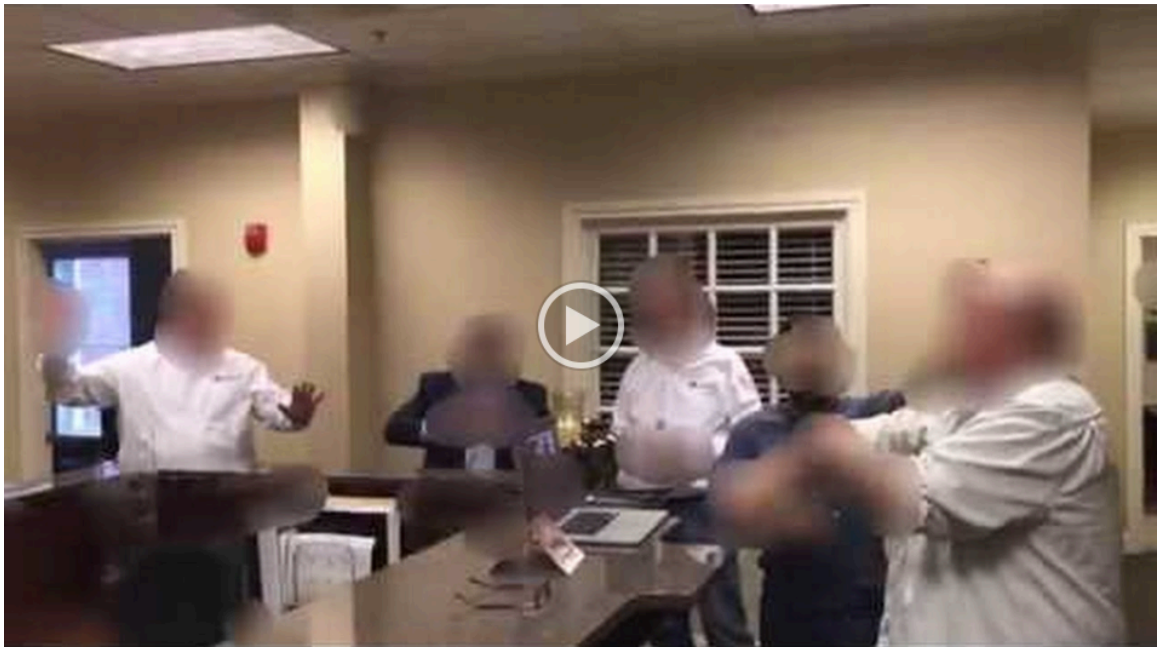
In-Car dashcam video is recorded from a police patrol car out on a public street, where there is no expectation of privacy for any actions taken in plain public view. However, police policy in many cases has been to redact this video anyway. In contrast, police body-worn cameras will often record video inside homes, businesses, and other non-public locations where there is an expectation of privacy. There will often be innocent bystanders and minors present inside homes, and will often be included in recorded video.

As police agencies equip police officers with body-worn cameras, there is an increasing expectation that every incident will have been recorded by one or more police officers. The quantity of collected video will expand dramatically. It is also completely reasonable to expect the number of FOIA requests for that greatly increased number of videos will also increase. Police departments are going to get a much higher number of FOIA requests than they have ever had in the past.

© 2015 Utility – All Rights Reserved

Video Redaction

Video redaction is a process of blurring out faces and personally identifiable markings such as body tattoos using video redacting software tools. In many cases there are several individuals shown in a video, and the face and other identifiable body parts of each person in the video has to be redacted.



Redaction protects the privacy and identity of victims, innocent bystanders, minors, and undercover police officers before video is released to the press and the public as a result of a FOIA request.

Video redaction historically has been a tedious manual process, where redacting one hour of video often requires five to ten hours of effort because video has to be manually redacted on a frame-by-frame basis. At 30 frames per second times 3,600 seconds per hour, an hour of video can have up to 108,000 individual frames that need to be redacted. In some cases, audio must also be redacted to maintain privacy or to protect the identity of undercover police officers. The redaction process has to be completed reliably, since even one un-redacted video frame – where a face is not blurred out -- might be enough to identify an individual.

© 2015 Utility – All Rights Reserved

Video redaction is a demanding manual effort that takes a lot of skilled staff time to perform. Generally, there are a limited number of staff who know how to perform video redaction, have access to video editing software tools, and are trusted parties authorized to do video redaction. Access to un-redacted video needs to be carefully controlled to prevent un-redacted videos from being leaked to YouTube or other social media websites.

As police departments roll out body-worn cameras to all police officers, it is clear that the number of recorded videos will grow dramatically. If there are many FOIA requests for a large number of video recordings within a short period of time, the redaction backlog will grow quickly. A large backlog and therefore delay in publishing redacted video can have a negative effect on the perception of police accountability and transparency. Questions will be asked about the reason for a long delay to release a redacted video. Is the delay caused by limited staff resources who can do redaction? Is there a large backlog of pending video redaction work to be performed? Or, is the police department intentionally "dragging their feet" on publishing redacted video that may not reflect favorably on the actions of one or more police officers? Given recent events, "Trust us – We are working on it" as an answer for delays in publishing redacted video is less likely to be an acceptable response. A long delay to release a video in response to a FOIA request is going to cause suspicions.

In some cases, it is possible to outsource the manual video redaction effort to a third party service. However, this can be much more expensive compared to using internal staff resources. Many police departments are allowed to charge for video redaction, but only at the lowest cost possible. A third party service obviously requires transferring the un-redacted video outside the police department to the third party service, which increases the risk the video is leaked un-redacted to unauthorized persons. The more controversial the video, the more damage a leaked un-redacted video could cause. As a result of leaked un-redacted video, an innocent bystander, witness, or an undercover Police officer could be harmed, and even have their life placed at risk.

In some cases, a trusted third party redaction service may not be available. Or the police agency may not have funds available to pay for third party manual video redaction services.

© 2015 Utility – All Rights Reserved

As a result, with the dramatic increase in the quantity of recorded video resulting from police officers adopting body-worn cameras, there are valid concerns that police departments could be overwhelmed with body-worn video FOIA requests. Police departments will certainly make a best effort to publish manually redacted video as soon as possible after a valid FOIA request is made. However, it is likely that manual video redaction work backlogs and publishing delays will increase despite the best efforts of police departments. Availability and budget for trusted and skilled manual video redaction experts to meet the increased demand for redacted body-worn videos will soon be a significant problem for many law enforcement agencies.

Legislative Efforts to limit the Release of body-worn Videos

As a result of a growing recognition of the video redaction challenges described in the preceding paragraphs, legislation is being proposed in a number of states to limit FOIA requests for police videos, or even exclude police video from the scope of information covered by "Sunshine" laws. Police agencies are asking legislators to pass laws excluding police body-worn video from the scope of allowable FOIA requests, and to deny press and citizen FOIA requests to obtain copies of police body-worn videos for incidents where body-worn video has been recorded. This is an understandable reaction to the manual video redaction staffing and funding challenge that many police departments are starting to face.

However, denying press and citizen FOIA requests for police body-worn videos runs completely counter to calls for increased police accountability and transparency. Increased police accountability and transparency is a primary reason for funding, training and equipping police officers with body-worn cameras. The public and the press knowing that police body-worn cameras should have recorded video of an incident, but the police department refusing to release the video, will likely be viewed as "stone-walling" and will damage efforts to improve public perception of police accountability and transparency.

This "stone-walling" perception will be magnified by the reality that in many cases there will be one or more citizen cell phone video recordings of the incident. The Walter Scott shooting in North Charleston, South Carolina, is a prime example. Cell phone video quality has improved to high definition 720p,

© 2015 Utility – All Rights Reserved

1080p, and even 4K resolution. A citizen cell phone video is perceived as credible and reliable in accurately showing the circumstances surrounding an incident they record.

The police department refusing to release police officer video will be perceived as not being accountable and transparent. Which is exactly the opposite and counter to a recognition that police departments need to be more accountable and transparent.

Police departments could decide to accelerate the manual redaction of high profile videos. However, selectively releasing some videos but not other videos causes further questions about police accountability and transparency.

The net result is the goal of increasing police accountability and transparency will be significantly damaged if police departments refuse to release police body-worn videos requested by the press, the ACLU, the public, and other interested parties. A shadow of doubt will be cast over the accountability and transparency of the entire policing process.

The Root Problem – Manual Redaction of Police Video

The root problem is the assumption and the past reality that video redaction is a time-consuming and expensive manual process that takes five to ten hours of skilled manual labor per hour of redacted video. However, the assumption that redacting one hour of video always requires many hours of skilled manual labor is, itself, a flawed assumption. Used to be true, but does not have to be true in the future.

Automated Video Redaction is the solution

If software algorithms and processes can be used to automatically and reliably identify and then redact faces and other identifiable body parts in police body-worn video, then many hours of skilled manual redaction labor will not be required. Automated video redaction completed in minutes by software rather than hours of skilled manual labor will dramatically reduce the cost and delay in responding to FOIA requests. Fast and reliable automated video redaction will promote police accountability and transparency.

© 2015 Utility – All Rights Reserved

It is already possible for software to blur out an entire video on a broad and indiscriminate basis. Blurring out an entire video is a brute force approach that is generally perceived as little better than refusing to release a video. No detail about anything that happened is visible, so the perception is the police department is not being accountable and transparent. However, the optimal automated redaction process should mirror how video has been manually redacted in the past. Only specific faces, tattoos on body parts, and other identifiable objects for victims, innocent bystanders, minors, and undercover police officers should be blurred out, with the rest of the video remaining clear and un-blurred.

Smart Redaction™ as part of AVaiL Web Software as a Service

Utility has already developed and is testing a beta version of automated Smart Redaction™ redaction software. The Smart Redaction software automatically identifies and blurs faces and body parts in a video. So the press, the public, a Grand Jury, and ultimately, a judge and jury, can have the facts "beyond a shadow of doubt" about what happened during an incident, while still protecting the privacy and security of victims, innocent bystanders, minors and undercover Police officers.

Furthermore, the Smart Redaction software can identify faces, body parts, and other identifiable objects as separate objects that can be selectively blurred. So a perpetrator face and body parts can remain un-blurred while the faces and identifiable body parts of victims, innocent third parties, minors, and undercover Police officers are blurred. The Smart Redaction process also provides a quality assurance review process to ensure that all objects in the video are 100% redacted. Police accountability and transparency can maximized while minimizing the cost and lead-time to publish redacted body-worn camera video.

The production version of the automated Smart Redaction software will be released before the end of 2015. The automated redaction function will be included as an update to the Utility AVaiL Web Video Management Software as a Service. All subscribers to AVaiL Web will have access to the Smart Redaction software tool at no additional cost as soon as the tool is released into production. Smart Redaction software technology can solve this video redaction cost and lead time vs. police accountability and transparency dilemma.

© 2015 Utility – All Rights Reserved

UTILITY

Eliminating Racial Bias in Recording Body-worn Videos

250 East Ponce de Leon Avenue, Decatur, GA 30030

www.BodyWorn.com

The recent events in Ferguson, MO and the death of Eric Garner in Staten Island, NY have ignited a national controversy about racial profiling, police accountability, and public trust in 21st Century Policing. There is a general consensus that police officers should wear and use body-worn video cameras. There is also clear consensus that police body-worn video cameras should not record all the time. As a result, there are big questions about when to record body-worn video, and when to stop recording body-worn video. This paper discusses how to eliminate racial bias in recording body-worn police video.

Racial Bias Academic Research

There is a solid body of academic research that shows that all human beings are biased. The book **Everyday Bias** by Howard J. Ross states "If you are human, you are biased". Mr. Ross states that bias is natural to the human mind as a survival mechanism. Overwhelmingly bias is unconscious. Humans can work to become less biased, but unconscious biases will always remain.

The book **Blind Spot – Hidden Biases of Good People** by Mahzarin Banaji and Anthony Greenwald describes hidden biases all people carry from a lifetime of exposure to cultural attitudes about age, gender, race, ethnicity, religion, social class, sexuality, disability status, and nationality. Mahzarin Banaji is the Richard Clark Cabot Professor of Social Ethics in the Department of Psychology at Harvard University. Anthony Greenwald is a Professor of Psychology at the University of Washington. Their educational web site Project Implicit https://implicit.harvard.edu/implicit/ provides information and awareness about unconscious bias. The book **Blind Spot** explores how the perceptions of social groups unconsciously influence individual judgments about character.

Understanding Prejudice

The UnderstandingPrejudice.org web site was developed in 2002 with grant funding from the National Science Foundation and McGraw Hill Higher Education. This web site includes a link to the Implicit Association Test (IAT). The IAT was developed by **Blind Spot** authors Mahzarin Banaji and Anthony Greenwald to reveal hidden "racial bias". Dateline NBC did a broadcast about

© 2014 Utility – All Rights Reserved

the Implicit Association Test on April 15, 2007, http://youtu.be/sYQVDik69Nw, so clearly the IAT is not a new concept.

The Implicit Association Test has been validated through a number of peer-reviewed academic journals over the past decade, and has been taken more than 1 million times. This 10 minute test is available on at the following internet link http://www.understandingprejudice.org/iat/ .

Everyone is Racially Biased to some degree

So it is not a matter that some people are biased, and therefore are bad, while others are not biased, and therefore good. All human beings are more or less biased on an unconscious level. Police officers are human beings like the rest of us, and each has their own set of unconscious racial bias.

Unconscious racial bias affects behavior. Police officers have to make split-second decisions where a wrong decision can be the difference between death and going home safely after the shift. So it is clear that any task that a police officer is asked to manually perform will be subject to unconscious racial bias, regardless of training or department policies and procedures.

Automatic Video Recording Start and Stop

Almost all police body-worn video cameras on the market so far are manually controlled. They are neither smart nor connected. The police officer alone decides when to manually turn the body-worn video camera on and off. As a result, manually controlled starting and stopping police body-worn video camera recording is always going to be subject to unconscious racial bias regardless of training, published policies, or the good intentions of police departments and individual police officers.

The racially unbiased alternative is to have smart connected body-worn video cameras that automatically start and stop police body-worn video recording. Software code is not human, and therefore does not have inherent racial biases. Recording can be automatically started by the In-Car Video Camera system, by entering or exiting a GeoFence zone, by a remote Supervisor who is not viewing the citizens involved in a situation, by 911 Central Dispatch, by an internal Accelerometer measuring whether a police officer is running, from body-worn

© 2014 Utility – All Rights Reserved

biometric sensors that measure an officer's heart rate, or by other local or remote automatic triggering sources. The officer does not have to be involved

in the decision to Start or Stop recording. Smart connected body-worn video recording devices can make racially un-biased video recording Start or Stop decisions. Smart and connected body-worn video cameras always follow the policy rules that are embedded in the body-worn video camera software code, are controlled by an independent third party or system, or are triggered to start or stop recording by a combination of these recording sources.

Manual Control of Video Recording

Police officers should have the ability to manually start and stop video recording. Citizen privacy rights are an important consideration, and there are times when it is appropriate to not record video or audio. However, manual recording control should be subject to technology checks and balances so that police accountability and public trust is maintained. Especially if a police officer manually turns off video recording before the end of an Incident, there should be a clear audit trail of when and why the recording was turned off. The bodyworn should have the ability to provide voice prompts that announce to all citizens in the vicinity that video recording has Started or Stopped. On the other hand, flashing red lights are intimidating, and any police officer is going to be uncomfortable with any red dot on their chest. There should be no unexplained recording gaps while an Incident is in progress. Otherwise public trust in police accountability will be lost.

Video Recording should be Automatic

Automatic recording triggers are the key to avoiding racial bias. Any body-worn video recording system that depends upon a police officer to decide and remember to turn on video recording is going to be flawed. Public trust in policing depends upon reliable, racially unbiased video recording.

A recent Consent Decree Monitor Report for the New Orleans Police Department is telling. In the period of July 1 to September 30, 2014, there were 25 incidents of major force since the deployment of body-worn cameras. In 9 cases, no body-worn camera video of the Incident was available for review.

© 2014 Utility – All Rights Reserved

http://www.nola.com/crime/index.ssf/2014/12/nopd_use_of_force_investigatio.html

The survey "American Sentiment toward Police Body-Worn Cameras" national survey showed that an overwhelming majority of the American public do not want individual police officers to determine when to record with body-worn cameras. Furthermore, 72% of Americans want body-worn cameras to start recording automatically when the police in-car video camera recording system starts recording.

http://www.reuters.com/article/2014/12/29/ga-utility-idUSnBw295065a+100+BSW20141229

Smart connected body-worn video recorders can provide policy-defined software-controlled automatic video recording that is consistent and reliable. Dumb unconnected video recorders cannot. Police departments should carefully consider the implications of purchasing dumb unconnected video recorders. A rushed short-term decision to buy could well be a bad investment, and undermine public trust in police transparency and accountability.

Police Video Recording should not be racially biased

Reliable video recording technology that encourages everyone to be on their best behavior has proven to reduce the number of Situations turning into Incidents. Eliminating the possibility of racial bias in recording or not recording an Incident increases public trust in police transparency and accountability.

As Philadelphia Police Commissioner Charles Ramsey has stated, everyone's goal should be fair and impartial policing.

© 2014 Utility – All Rights Reserved

UTILITY

Police Officer Legal Risk from a Wide Field of View in a Body-Worn Camera

250 East Ponce de Leon Avenue, Decatur, GA 30030

www.BodyWorn.com

Table of Contents

Biology of Human Eyesight 4
Video Recorder Peripheral Vision Clarity 6
A Police Officer is at a significant Visual disadvantage 6
A Police Officer will keep a primary subject in view 6
A video camera with a Wide Field of View puts an Officer at Legal Risk 7
The Legal and Financial Risks of a Wide Field of View are Significant 7
Summary - A Wide Field of View is a Legal danger to a Police Officer 7

© 2014 Utility – All Rights Reserved

Overview

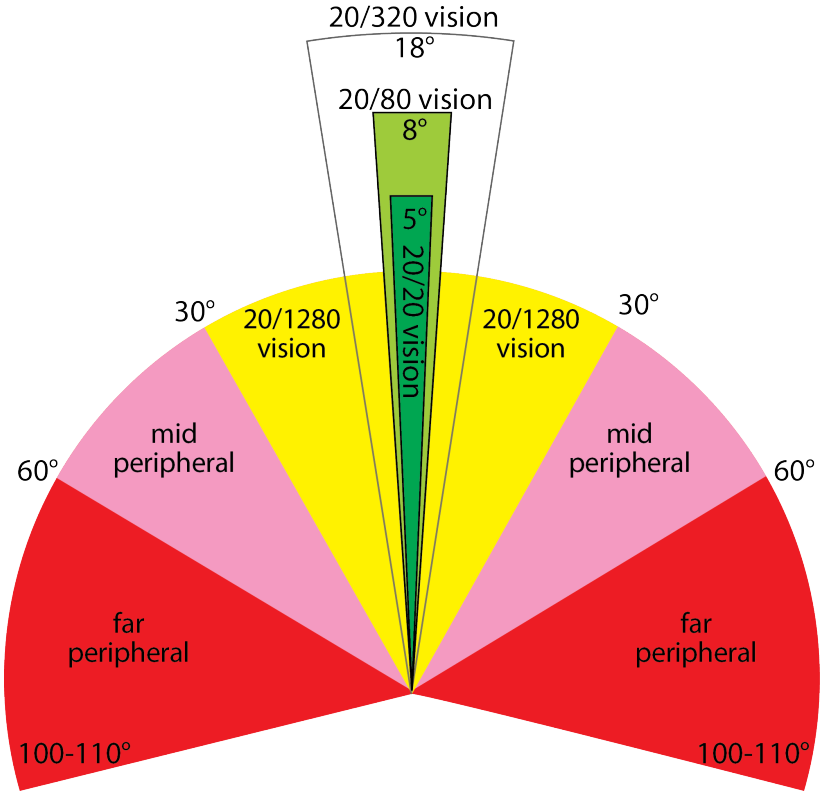
A number of recent body-worn camera Requests for Proposal have included a lockout specification of a minimum number of degrees for a body-worn video camera Field of View. In general the impression is given that the wider the field of view, the better. This paper argues that bigger is not better. Instead, a narrower field of view similar to a police officer's field of view is better. In a police officer's peripheral vision, detail is invisible. Video camera recording of peripheral vision detail is crystal clear on a video playback. A Police Officer should only be held accountable for visual detail he can actually see.

This paper draws from a number of facts about the biology of the human eye that can easily be confirmed through an internet search. The recent events in Ferguson, MO and the death of Eric Garner in Staten Island, NY have ignited a national controversy about racial profiling, police accountability, and public trust in 21st Century Policing. There is a general consensus that police officers should wear and use body-worn video cameras. However, it is critical to recognize there are fundamental differences in visual acuity between human eyesight and a video camera. A video camera with a wide field of view will record video with clear peripheral vision detail that the human eye simply cannot see. A video camera with a wide field of view puts a police officer at significant legal risk, because it can clearly record what the human eye cannot see. Police Officers should not be put at legal risk because of the biology of human eyesight.

© 2014 Utility – All Rights Reserved

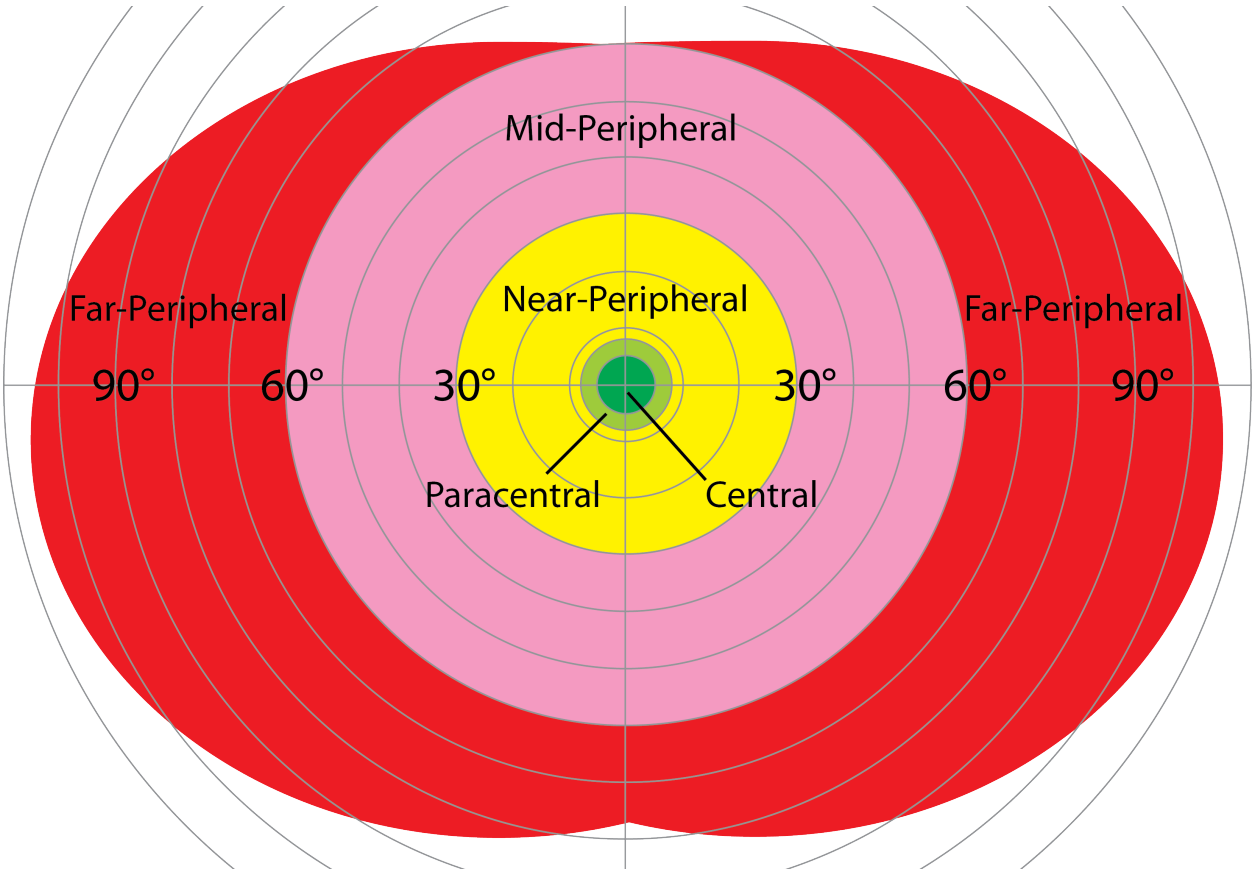
Biology of Human Eyesight

The human eye is remarkable, but it has limitations. A human being only sees detail clearly in their direct line of sight. "Foveal" Vision is where 20/20 visual acuity is possible. Foveal Vision is 1° on either side of line of sight (what you are looking at). Furthermore, **visual acuity declines by 50% for each 2.5° shift away from the center line of sight**.



The maximum effective field of view for a police officer is no more than the 18° Macular vision range — 9° on either side of the line of sight. Any event happening outside of the 18° macular range of vision is in peripheral vision. As a practical matter, no human being -- including police officers – can distinguish any detail in peripheral vision. Motion can be determined in peripheral vision, but not detail. This is easy for anyone to verify. A person looking straight ahead can see motion in their peripheral vision. But a person looking straight ahead cannot tell how many fingers a person in peripheral vision is holding up.

© 2014 Utility – All Rights Reserved



This chart is another way to depict visual clarity in central line of sight compared to peripheral vision. The area in green – where the person is looking – can see details clearly. In the Paracentral area in light green, visual acuity drops by 50%. In the yellow zone Near-Peripheral zone very little detail can be identified. In the pink Mid-Peripheral and red Far-Peripheral zones, no detail can be identified by a human eye – only motion at best. The human eye's effective field of view is less than 18°. Anyone can personally test and confirm this assertion.

The biology of why the human eye can see detail in central line of sight but not in peripheral vision has to do with the distribution of Cone and Rod cells on the eye's retina. Cone cells are more concentrated in the center of the retina, and can detect detail. Rod cells are distributed around the center of the retina, and can better detect motion and light. The details of human eye biology are beyond the scope of this paper, but information about Cone and Rod cells can be easily verified from any number of published sources.

© 2014 Utility – All Rights Reserved

Video Recorder Peripheral Vision Clarity

In very sharp contrast to the human eye, a video camera can record almost perfect clarity across the entire field of view of the video camera. Detail captured by the video camera is just as good in the outer peripheral zones as in the center of the recorded video. So a video camera can detect and record event and object detail in peripheral line of sight regions that are far, far better than a human eye could ever see.

A Police Officer is at a significant Visual disadvantage

So it is certain that a police officer cannot see peripheral detail as well as a video camera can record it. Because a police officer can only see detail for what he is looking at directly, detail about events and objects in peripheral vision areas are not clear or invisible to the police officer.

This detail recognition disadvantage is further compounded by the fact that a police officer has to make split-second life or death decisions while under extreme stress. On the other hand, a grand jury or a trial jury watch a video recording that provides clear detail across the entire field of view. The grand jury or the trial jury is not under high stress, does not have to make a split second decision, and has the luxury of being able to replay the video multiple times to look at detail. This is a luxury that a Police Officer – or any human being at the scene – does not have.

A Police Officer will keep a primary subject in view

The Tueller Drill is well known in the police world. This drill shows that an attacker with a knife who charges a police officer from 21 feet or less will be able to attack the police officer before he has time to draw his weapon and fire. So any person located within 21 feet of a Police Officer potentially could kill the Police Officer. It is therefore reasonable to expect that a Police Officer located within 21 feet of a potential aggressor is going to keep a close watch on a person who could be a lethal threat. Therefore a Police Officer is not going to recognize details of the scene in his peripheral vision. However, a video recorder will reliably capture scene detail across the video camera's entire field of view.

© 2014 Utility – All Rights Reserved

A video camera with a Wide Field of View puts an Officer at Legal Risk

As a result, a video camera with a wide field of view puts the officer at significant legal risk. The police officer has to make a split-second decision based upon what his personal eyesight can perceive. Yet the police officer's actions and reactions are subject to "after the fact" scrutiny from video recordings that provide far more peripheral scene detail than the Police Officer could ever possibly see. This puts the Police Officer at very significant legal risk of being "Monday Morning Quarterbacked" by the public, press, grand juries, supervisors, political and media commentators, prosecutors, and most importantly juries.

The Legal and Financial Risks of a Wide Field of View are Significant

The Legal and Financial Risk is significant. Beyond internal reprimands, suspensions, and getting fired, Police Officers can be and sometimes are charged with felonies up to and including homicide. Police Officers are also at risk of civil lawsuits where the standard of proof to obtain a judgment against the police officer is lower than in a criminal case. Legal defense costs are often six figure sums, even if they are eventually found not guilty. So even if a Police Officer successful defends against a criminal charge and/or a civil lawsuit, they may be ruined financially. So even a "win" is often a devastating personal financial loss.

Summary - A Wide Field of View is a Legal danger to a Police Officer

The biology of the human eye compared to a video recorder with a wide field of view puts a police officer at significant legal risk whenever there is an Incident. The solution is to have a video recorder with a field of view that is similar to a Police Officer's effective field of view. A body-worn camera field of view should be limited to less than 50°. This accounts for a police officer slightly changing his line of sight during an Incident – while always keeping the primary subject in view. Even then, the public, press, citizens, judges, and juries should recognize that detail in peripheral vision is unclear or invisible to any human being. Police Officers are human beings just like the rest of us.

© 2014 Utility – All Rights Reserved

Poll Results:

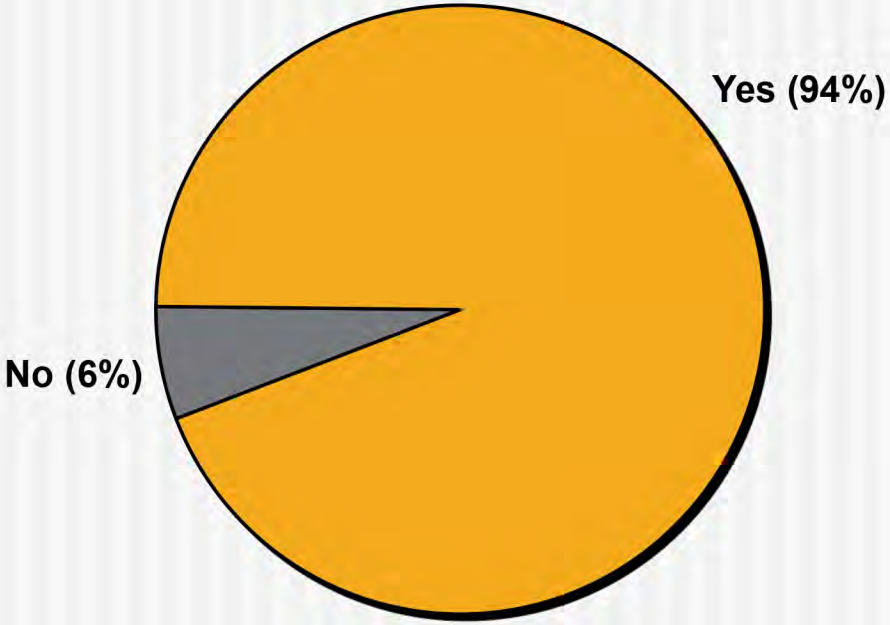
American Voters' Views on Police Body Cameras

August 2015

• Sample Size:	n=1,000 completed interviews random nationwide
• Sample:	Provided by Labels & Lists; drawn proportionally nationwide
• Eligibility:	Registered Voters
• Interview Method:	Telephone; Landline 68% / Cell 32%
• Margin of Error:	3.1%
• Interview Dates:	August 19-25, 2015
• Prepared for:	Utility, Inc.

T1: Awareness of Police Incidents -- More than nine-in-ten Americans (94%) say they have heard or read about recent "controversial incidents involving citizens… police." This near-universal awareness is remarkably high for news stories; the subject is seared into the American consciousness. High awareness stretches across every region of the country -- hitting a high of 97% in the Midwest -- across every political party and age group and is 93% for African Americans.

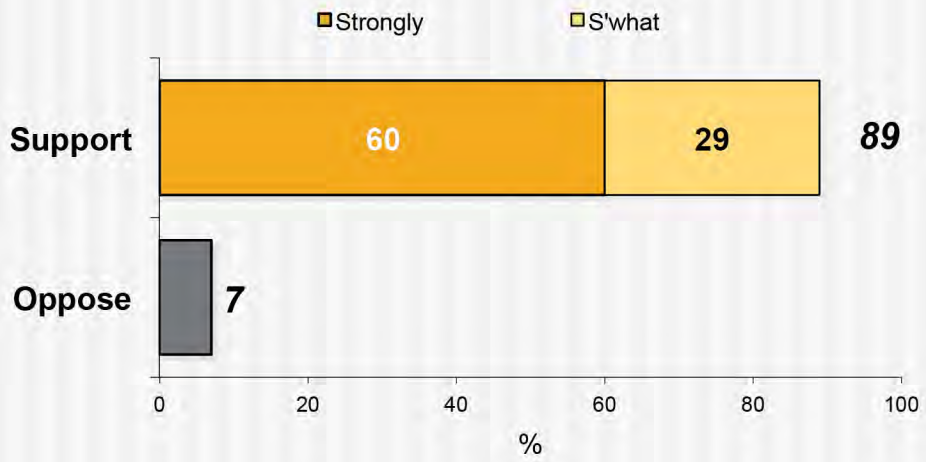
Have you heard or read anything over the past year about controversial incidents involving citizens killed or harmed by police or while in police custody?



Highest Awareness Among:	
Midwest	97%
Suburbs	97%
Age 50-64	97%
College Graduates	97%

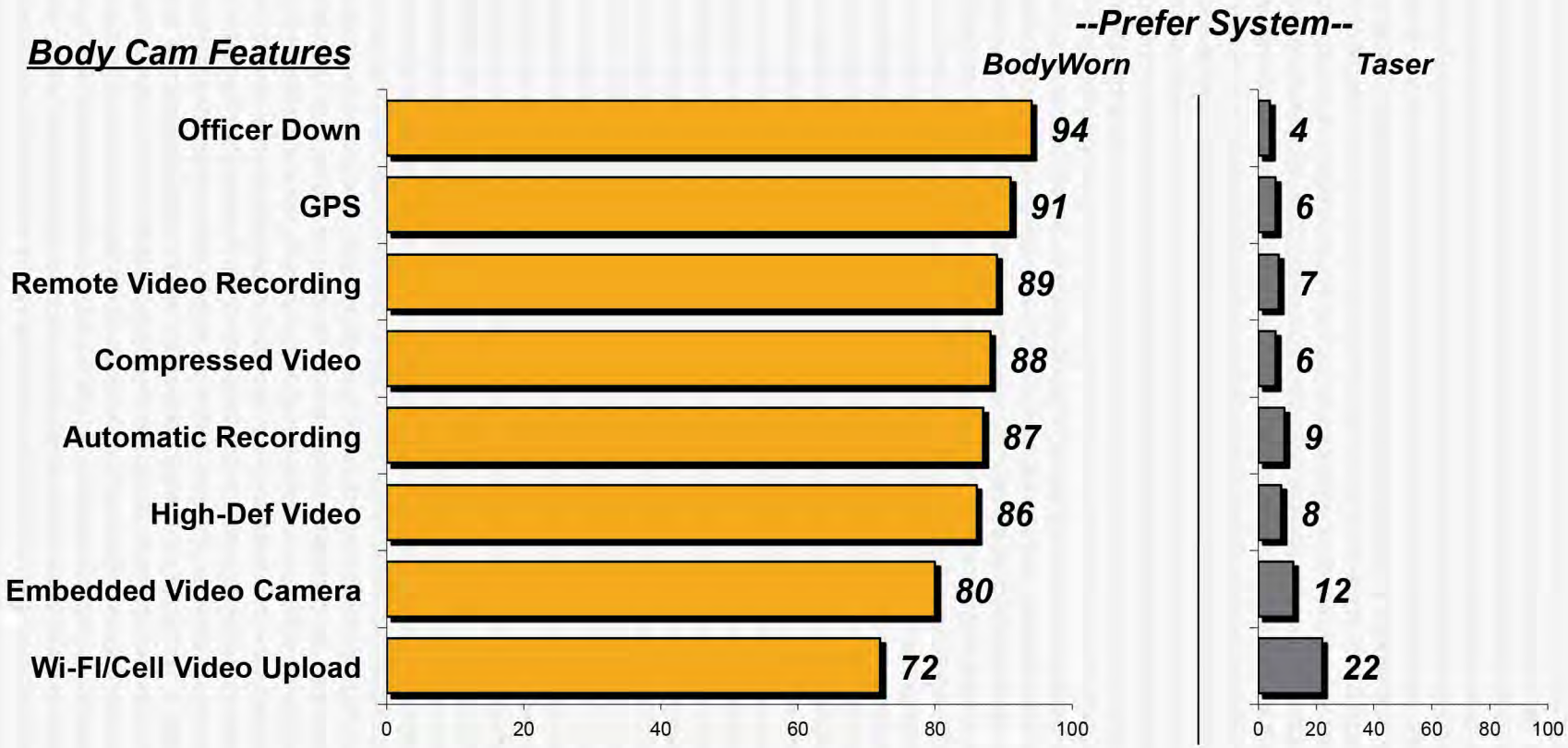
T2: Support for Police Body Cameras -- 89% of Americans support equipping police with body cameras including a three-fifths majority who "STRONGLY" support. In a rare occurrence in U.S. society today, about nine-in-ten in every party -- Democratic (91%), Republicans (88%) and Independents (90%) -- all agree in their support for police body cameras. Such unanimity creates a strong political imperative for action to equip officers quickly.

Some people have proposed that police officers be equipped with body cameras that record their interactions with citizens and criminal suspects. Do you strongly support, somewhat support, somewhat oppose or strongly oppose equipping police officers with body cameras?



	-Party-			-Race-	
	Dem	Rep	Ind	AA	Hisp
	%	%	%	%	%
Support	91	88	90	88	86
Oppose	6	9	6	7	8

T3: Best Choice of Police Body Cameras: By Features -- Americans clearly prefer the BodyWorn technology of the Smartphone camera and its software capabilities to the Taser Camera system. On eight feature dimensions, BodyWorn's capabilities are preferred in a range of 94% to 4% (Officer Down notification) to a "low" of 72% to 22% (Instant wi-fi / cell network video upload vs. End of shift camera docking video download). On average across all eight features, the BodyWorn capabilities are preferred by 86% to 9%… a 9:1 margin (see Tables 5 through 12 for details).



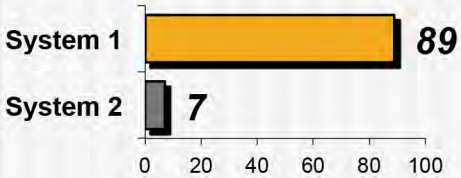
T4: Bottom Line Preference – BodyWorn vs. Taser -- When the features of each camera system are summarized, 89% of U.S. voters express a decisive preference for the BodyWorn Smartphone camera software technology. This dramatic verdict is consistent across party lines, racial groups, geographic region, gender and age. In fact, the 89% to 7% judgment in favor of the BodyWorn product is so complete and extensive it is likely to apply in near equal proportion to any electorate in America no matter how urban or rural, Democratic or Republican, minority or white, young or old.

So, in summary, if the police in your local area or state were to acquire policy body cameras, which system do you think would be better…?

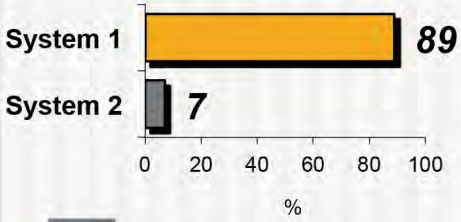
- *System #1 called the BodyWorn camera with GPS and real-time communications that can automatically start video recording, and immediately uploads videos with location data to cloud storage through a cellular or Wi-Fi connection.*

--OR—

- *System #2 camera from the Taser company has a manual on-off switch, no GPS, no communications with Central Dispatch, and stores video in the camera until the end of the shift when the officer goes back to the police station and uploads larger videos to cloud-storage.*



	-Party-			-Race-		-Density-			
	Dem	Rep	Ind	AA	Hisp	City	Sub-urbs	Small Town	Rural
	%	%	%	%	%	%	%	%	%
System 1	92	89	90	93	86	91	91	89	88
System 2	6	10	6	6	14	5	8	6	9



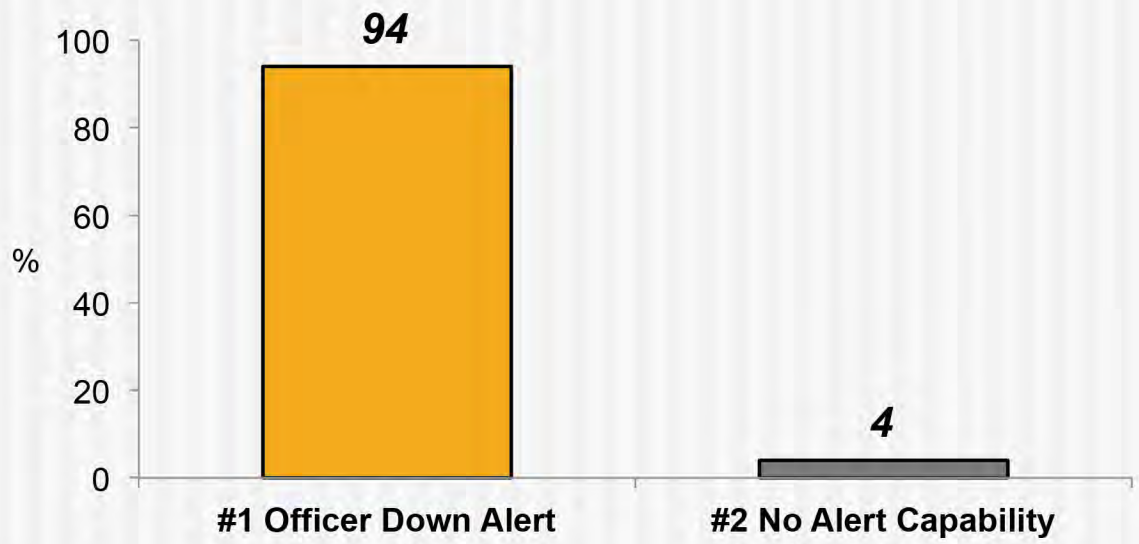
	-Region-								-Gender: By Age-					
	New Eng.	Mid. Atl.	Great Lakes	South	TX+	Mid-West	Moun tain	West Coast	-18-49-		-50-64-		-65+-	
									M	F	M	F	M	F
	%	%	%	%	%	%	%	%	%	%	%	%	%	%
System 1	90	90	88	92	90	91	79	86	91	95	80	95	84	93
System 2	8	5	7	5	9	9	14	8	8	3	13	4	10	4

T5: Specific Feature Preference: Officer Down Alert -- By 94% to 4%, U.S. voters prefer the BodyWorn capability that uses GPS to alert Central Dispatch if an officer is no longer in vertical standing position.

Which do you think is better -- #1 or #2?

System #1 uses its GPS to provide an automatic "Officer Down" emergency alert to Central Dispatch with the Officer's exact location if the Officer goes down and does not respond to voice prompts from the body camera.

System #2 is simply a camera with no GPS or "Officer Down" reporting capability.



UTILITY

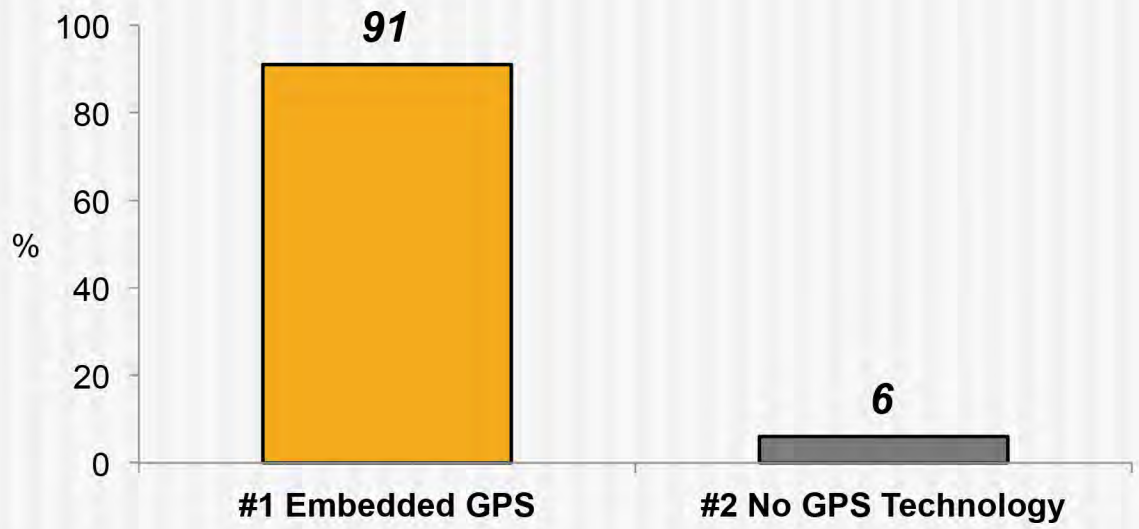
FP FREDERICKPolls

T6: Specific Feature Preference: GPS Tagging -- By 91% to 6%, Americans express a decisive verdict in favor of the BodyWorn GPS tagging system to accurately track where a video was shot over the competing system with no GPS.

Which do you think is better -- #1 or #2?

System #1 has embedded GPS so each video always accurately reports the exact location of the officer and where the video was recorded.

System #2 is simply a camera with no GPS technology so when these police camera videos are used as evidence, the location of the event must be determined using other factors.

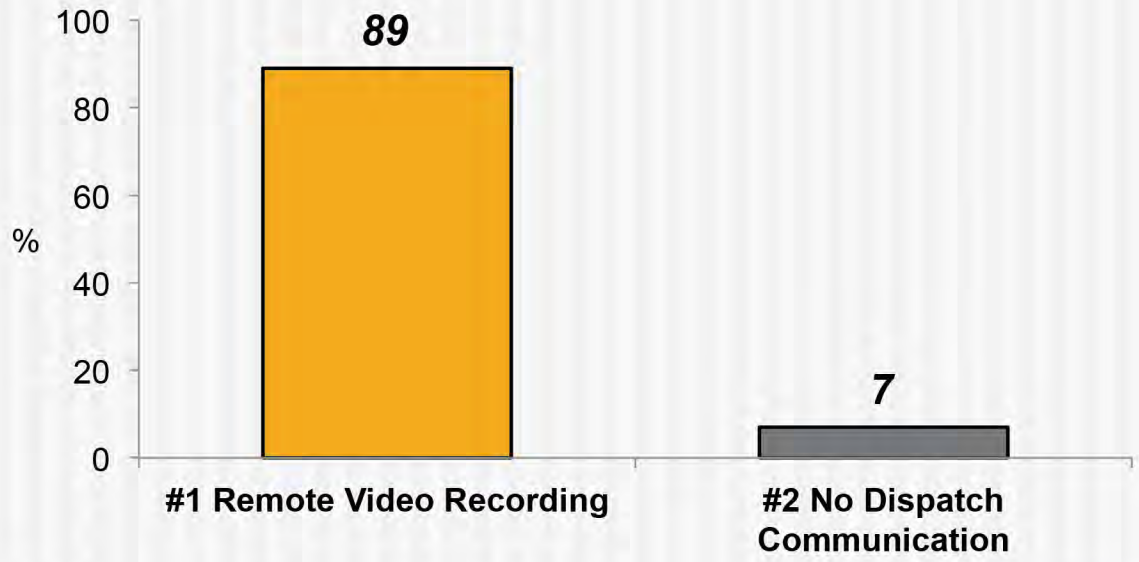


T7: Specific Feature Preference: Remote Video Recording Capability -- By 89% to 7%, the body camera system that allowed remote Central Dispatch to activate video recording on an officer's camera and send alerts to nearby cameras is seen as a benefit over the camera-only based system with no such connection.

Which do you think is better -- #1 or #2?

With System #1, during an emergency event, Police Central Dispatch can remotely start video recording and send alerts to ALL their cameras within a specified area.

System #2's Police Central Dispatch cannot communicate with the camera at all.



UTILITY

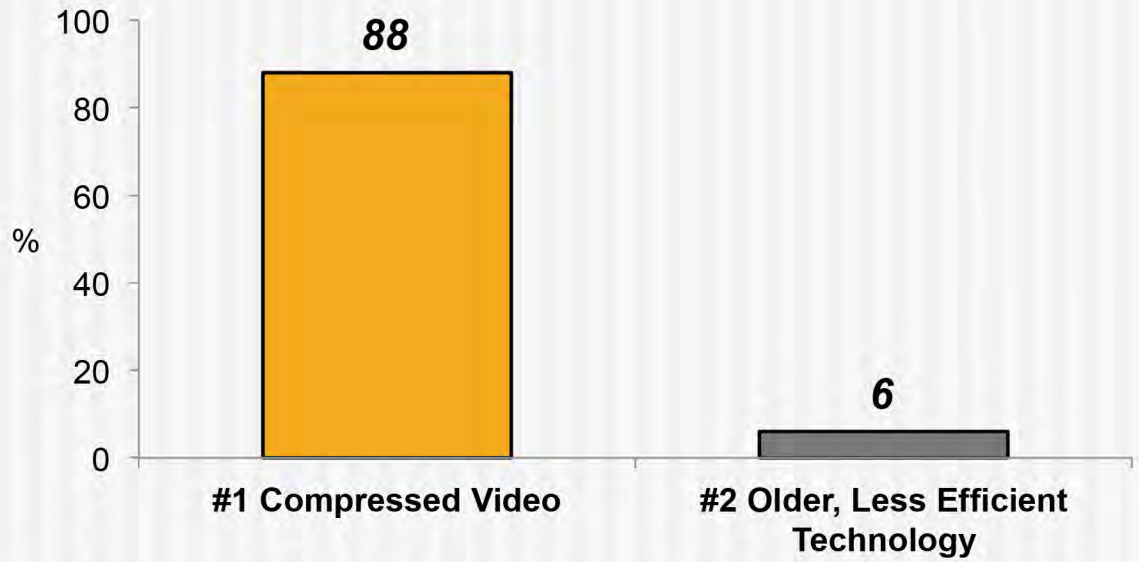
FP FREDERICKPolls

T8: Specific Feature Preference: Compressed Video -- By 88% to 6%, U.S. voters clearly support a compressed video format technology over a older less efficient system whose video files are larger and thus, cost more to store.

Which do you think is better -- #1 or #2?

System #1 uses modern video compression technology to minimize the video file size.

System #2 uses older less efficient video recording technology that results in video file sizes that are twice as large, and therefore the storage cost is also twice as much.

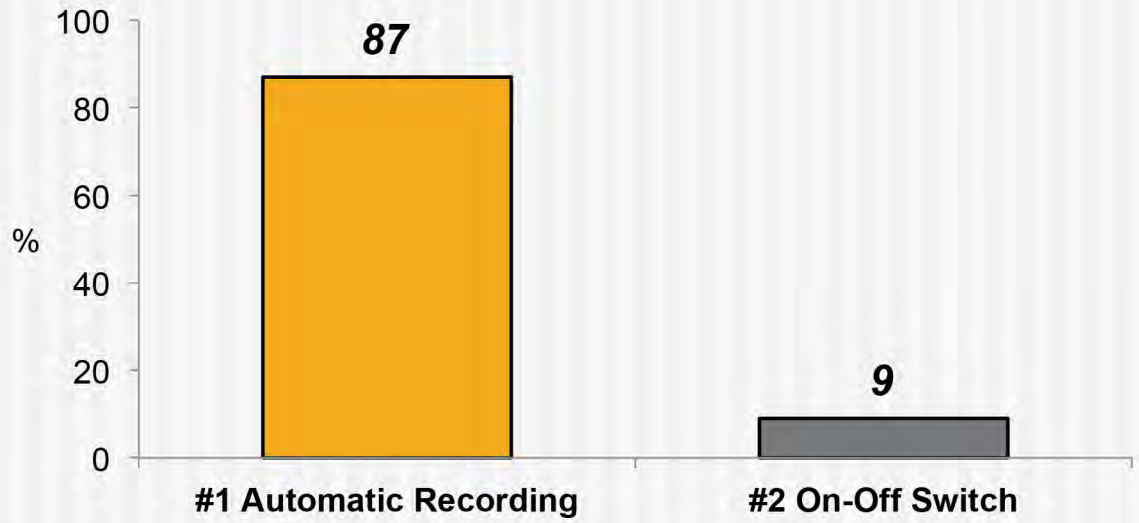


T9: Specific Feature Preference: Automatic Recording -- By 87% to 9%, the Smartphone camera system embedded in a bulletproof vest that is activated automatically when the officer's vehicle light bar goes on, the officer exits the vehicle or starts moving quickly is preferred over the Taser clip-on camera system with a manual on-off switch controlled by the officer. Again, this is a decisive verdict that mirrors overall preference for the BodyWorn system over the Taser system for a key defining feature that defines each technology. At 87% to 9%, the competition is not even close in the eyes of the American public.

Which do you think is better -- #1 or #2?

System #1 -- the body camera starts recording automatically any time an officer turns on their flashing patrol car lights, gets out of the vehicle, or starts running. The camera then continues recording until the patrol car's flashing lights are turned off.

System #2 -- the body camera has a manual on-off switch so the officer has to remember to start recording, and has control to stop recording at any time.

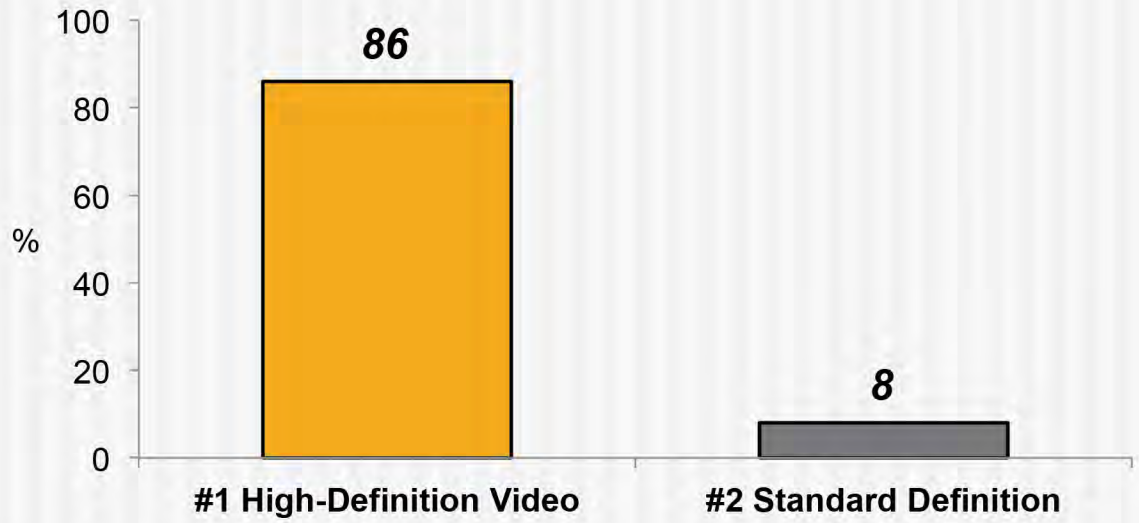


T10: Specific Feature Preference: High-Definition Video -- By 86% to 8%, American voters prefer the simple choice of high-definition video from the police body camera system over low definition. With just 6% "don't know," the choice clearly matters to voters since 94% are willing to express a preference.

Which do you think is better -- #1 or #2?

System #1's camera records in High-Definition video.

System #2's camera records in Standard Definition video.



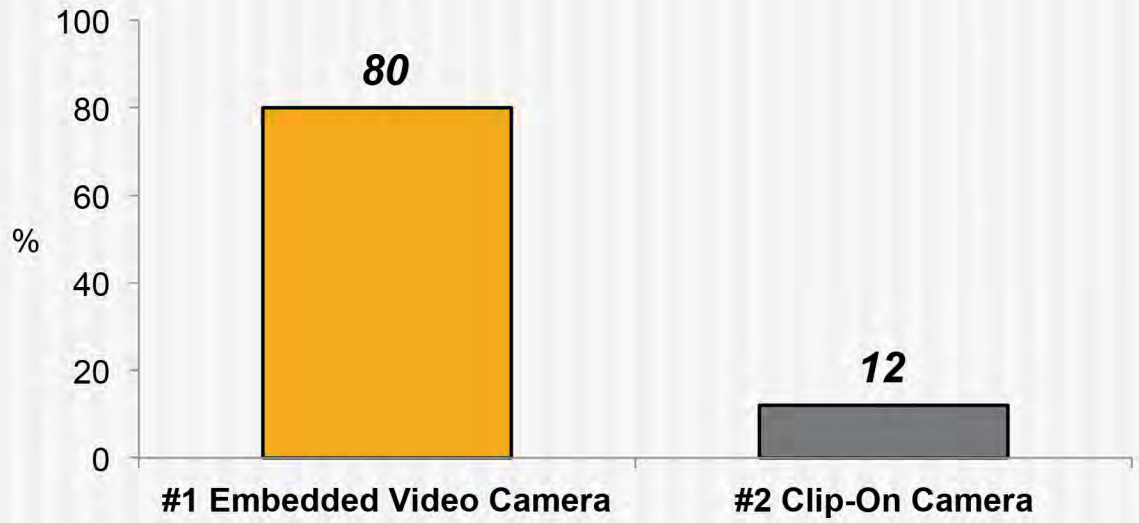
T11: Specific Feature Preference: Embedded GPS -- By 80% to 12%, a system with embedded GPS that tags video location is preferred over a less precise camera video system that has no GPS.

Next I will read you a short set of statements that describe features of two different police body camera systems. Assuming the two systems cost about the same to put in place, tell me which you think is better.

System #1 is a camera on a Smartphone that is embedded inside a bullet-proof vest the officer always wears, and cannot fall off.

System #2 is a clip-on camera about the size of a garage door opener or pager that clips onto an officer's shirt pocket, and thus, can come off when an officer runs or gets into a struggle.

Which do you think is better -- #1 or #2?

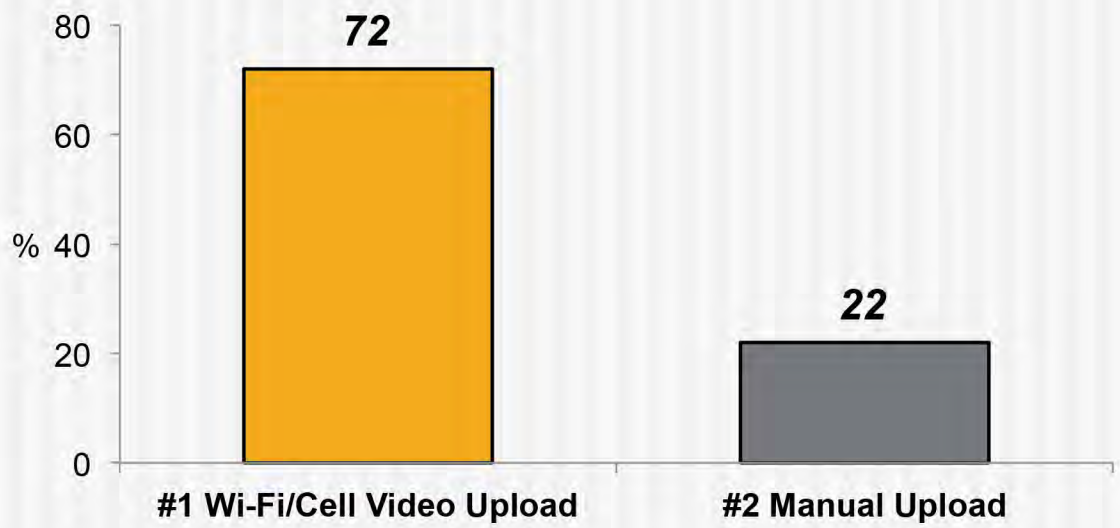


T12: Specific Feature Preference: Wi-Fi/Cell Video Upload -- By a 72% to 22% margin, American voters prefer a Smartphone-based technology that uploads videos via mobile data network capabilities over the camera system that transfers videos via computer download at the end of an officer's shift.

Which do you think is better -- #1 or #2?

System #1 -- the video from the Smartphone camera is uploaded as it is being recorded using cellular or Wi-Fi networks to a cloud-based storage system.

System #2 -- the videos are stored on the camera until after the end of the shift, when the police officer goes back to the police station and then manually docks the camera to a computer for uploading of videos to a cloud-based storage system.



More information at bodyworn.com/survey

Toplines
BodyWorn Nationwide

Actual sample:	**1000**	**1**

A. Registered to Vote.

Yes	1000	100%

1. Have you heard or read anything over the past year about controversial incidents involving citizens killed or harmed by police or while in police custody?

Yes	940	94%
No	56	6%
DK/Refused/Would not say	4	0%

2. Some people have proposed that police officers be equipped with body cameras that record their interactions with citizens and criminal suspects. Do you strongly support, somewhat support, somewhat oppose or strongly oppose equipping police officers with body cameras?

Strongly support	596	60%
Somewhat support	288	29%
Somewhat oppose	31	3%
Strongly oppose	35	3%
DK/Refused	50	5%
Total Support	884	88%
Total Oppose	66	7%

Next I will read you a short set of statements that describe features of two different police body camera systems. Assuming the two systems cost about the same to put in place, tell me which you think is better.

3. System #1 is a camera on a Smartphone that is embedded inside a bulletproof vest the officer always wears, and cannot fall off.

   System #2 is a clip-on camera about the size of a garage door opener or pager that clips onto an officer's shirt pocket, and thus, can come off when an officer runs or gets into a struggle.

   Which do you think is better?

System 1	804	80%
System 2	122	12%
DK/Refused	74	7%

4. System #1 - the body camera starts recording automatically any time an officer turns on their flashing patrol car lights, gets out of the vehicle, or starts running. The camera then continues recording until the patrol car's flashing lights are turned off.

   System #2 - the body camera has a manual on-off switch so the officer has to remember to start recording, and has control to stop recording at any time.

   Which do you think is better?

System 1	866	87%
System 2	94	9%
DK/Refused	40	4%

5. System #1 - the video from the Smartphone camera is uploaded as it is being recorded using cellular or Wi-Fi networks to a cloud-based storage system.

   System #2 - the videos are stored on the camera until after the end of the shift, when the police officer goes back to the police station and then manually docks the camera to a computer for uploading of videos to a cloud-based storage system.

   Which do you think is better?

System 1	720	72%
System 2	217	22%
DK/Refused	63	6%

---

6. System #1 has embedded GPS so each video always accurately reports the exact location of the officer and where the video was recorded.

   System #2 is simply a camera with no GPS technology so when these police camera videos are used as evidence, the location of the event must be determined using other factors.

   Which do you think is better?

System 1	908	91%
System 2	61	6%
DK/Refused	31	3%

---

7. System #1 uses modern video compression technology to minimize the video file size.

   System #2 uses older less efficient video recording technology that results in video file sizes that are twice as large, and therefore the storage cost is also twice as much.

   Which do you think is better?

System 1	882	88%
System 2	63	6%
DK/Refused	55	5%

---

8. System #1 uses its GPS to provide an automatic Officer Down emergency alert to Central Dispatch with the Officer's exact location if the Officer goes down and does not respond to voice prompts from the body camera.

   System #2 is simply a camera with no GPS or Officer Down reporting capability.

   Which do you think is better?

System 1	944	94%
System 2	40	4%
DK/Refused	16	2%

9. System #1's camera records in High Definition video.

   System #2's camera records in Standard Definition video.

   Which do you think is better?

System 1	863	86%
System 2	77	8%
DK/Refused	60	6%

10. With System #1, during an emergency event, Police Central Dispatch can remotely start video recording and send alerts to ALL their cameras within a specified area.

    System #2's Police Central Dispatch cannot communicate with the camera at all.

    Which do you think is better?

System 1	891	89%
System 2	70	7%
DK/Refused	40	4%

11. So, in summary, if the police in your local area or state were to acquire policy body cameras, which system do you think would be better?

System #1 called the BodyWorn camera with GPS and real-time communications that can automatically start video recording, and immediately uploads videos with location data to cloud storage through a cellular or Wi-Fi connection.	886	89%
System #2 camera from the Taser company has a manual on-off switch, no GPS, no communications with Central Dispatch, and stores video in the camera until the end of the shift when the officer goes back to the police station and uploads larger videos to cloud-storage.	72	7%
DK/Refused	41	4%

D1. Gender.

Male	502	50%
Female	498	50%

D2. Age.

18-29	92	9%
30-39	99	10%
40-49	141	14%
50-59	244	24%
60-64	136	14%
65-Up	257	26%
Refused	31	3%

Toplines
BodyWorn Nationwide

Actual sample:	**1000**	**6**

D3. African American/Black.

Yes	127	13%
No	828	83%
DK/Refused	45	4%

D4. Hispanic.

Yes	59	6%
No	898	90%
DK/Refused	42	4%

D5. Party ID.

Democrat	281	28%
Republican	253	25%
Independent	239	24%
Other/DK/Refused	226	23%

D6. Education Level.

0-11	37	4%
12 - High School	228	23%
Business school/some college	198	20%
College graduate	304	30%
Graduate degree	192	19%
DK/Refused	41	4%

D7. Area Live In.

Large city	188	19%
Small city/town	301	30%
Suburban area	249	25%
Rural	222	22%
DK/Refused	40	4%

Toplines
BodyWorn Nationwide

Actual sample:	**1000**	**7**
Phone		
Landline	680	68%
Cell	320	32%
Region		
New England	52	5%
Mid-Atlantic	151	15%
Great Lakes	200	20%
South	231	23%
TX-OK-AK	75	7%
Midwest	50	5%
Mountain	73	7%
West Coast	170	17%

BodyWorn Nationwide
August 2015
Job 2743

	TOTAL	---REGION---								--DENSITY--				--PARTY--				
		New Engl	Mid-Atl	Great Lakes	South	TX-OK-AK	Mid-west	Moun-tain	West Coast	City	Small Town	Sub-urbs	Rural	Dem	Rep	Ind	African Amer	Hisp
A 1	**1000**	**52**	**151**	**200**	**231**	**75**	**50**	**73**	**170**	**188**	**301**	**249**	**222**	**281**	**253**	**239**	**127**	**59**
A. Registered to Vote.																		
Yes	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
1. Have you heard or read anything over the past year about controversial incidents involving citizens killed or harmed by police or while in police custody?																		
Yes	94%	95%	96%	93%	92%	94%	97%	95%	94%	94%	93%	97%	94%	91%	95%	96%	93%	85%
No	6%	5%	4%	6%	8%	6%	3%	4%	5%	6%	6%	3%	6%	8%	5%	4%	7%	15%
DK/Refused/Would not say	0%	0%	0%	1%	0%	0%	0%	1%	1%	0%	0%	0%	0%	1%	0%	0%	0%	0%
2. Some people have proposed that police officers be equipped with body cameras that record their interactions with citizens and criminal suspects. Do you strongly support, somewhat support, somewhat oppose or strongly oppose equipping police officers with body cameras?																		
Strongly support	60%	53%	53%	61%	62%	60%	49%	63%	65%	68%	56%	59%	60%	66%	48%	65%	78%	64%
Somewhat support	29%	32%	33%	27%	27%	31%	39%	24%	27%	22%	30%	33%	30%	25%	40%	25%	10%	22%
Somewhat oppose	3%	3%	6%	4%	1%	1%	5%	2%	3%	2%	4%	3%	2%	2%	5%	4%	3%	4%
Strongly oppose	3%	5%	3%	2%	5%	1%	3%	7%	2%	3%	4%	3%	4%	4%	4%	2%	4%	4%
DK/Refused	5%	7%	5%	6%	5%	7%	3%	4%	3%	5%	7%	2%	5%	4%	3%	4%	5%	7%
Total Support	88%	85%	85%	88%	89%	91%	88%	87%	92%	90%	86%	92%	90%	91%	88%	89%	88%	85%
Total Oppose	7%	8%	9%	5%	7%	2%	8%	9%	5%	5%	7%	7%	6%	6%	9%	7%	7%	8%
Next I will read you a short set of statements that describe features of two different police body camera systems. Assuming the two systems cost about the same to put in place, tell me which you think is better.																		
3. System #1 is a camera on a Smartphone that is embedded inside a bulletproof vest the officer always wears, and cannot fall off. System #2 is a clip-on camera about the size of a garage door opener or pager that clips onto an officer's shirt pocket, and thus, can come off when an officer runs or gets into a struggle. Which do you think is better?																		
System 1	80%	82%	83%	85%	83%	80%	77%	69%	76%	82%	79%	82%	83%	82%	77%	84%	87%	86%
System 2	12%	16%	10%	10%	11%	16%	20%	16%	12%	12%	14%	10%	10%	12%	16%	10%	8%	6%
DK/Refused	7%	2%	7%	6%	7%	3%	3%	16%	12%	6%	7%	8%	7%	5%	7%	6%	5%	8%
4. System #1 - the body camera starts recording automatically any time an officer turns on their flashing patrol car lights, gets out of the vehicle, or starts running. The camera then continues recording until the patrol car's flashing lights are turned off. System #2 - the body camera has a manual on-off switch so the officer has to remember to start recording, and has control to stop recording at any time. Which do you think is better?																		
System 1	87%	90%	83%	87%	89%	87%	90%	80%	86%	88%	88%	89%	82%	87%	86%	89%	93%	92%
System 2	9%	10%	12%	9%	7%	7%	9%	16%	9%	8%	8%	7%	15%	10%	12%	7%	4%	4%
DK/Refused	4%	0%	6%	3%	4%	6%	2%	4%	5%	4%	4%	4%	3%	3%	3%	4%	3%	4%

		---REGION---								--DENSITY--				--PARTY--				
	TOTAL	New Engl	Mid-Atl	Great Lakes	South	TX-OK-AK	Mid-west	Moun-tain	West Coast	City	Small Town	Sub-urbs	Rural	Dem	Rep	Ind	**African Amer**	**Hisp**
A 2	**1000**	**52**	**151**	**200**	**231**	**75**	**50**	**73**	**170**	**188**	**301**	**249**	**222**	**281**	**253**	**239**	**127**	**59**
5. System #1 - the video from the Smartphone camera is uploaded as it is being recorded using cellular or Wi-Fi networks to a cloud-based storage system. System #2 - the videos are stored on the camera until after the end of the shift, when the police officer goes back to the police station and then manually docks the camera to a computer for uploading of videos to a cloud-based storage system. Which do you think is better?																		
System 1	72%	71%	69%	75%	76%	70%	71%	65%	70%	74%	72%	74%	70%	71%	73%	71%	67%	63%
System 2	22%	26%	26%	20%	18%	27%	25%	26%	19%	20%	22%	23%	23%	22%	24%	22%	26%	29%
DK/Refused	6%	3%	6%	5%	6%	2%	3%	9%	11%	6%	6%	2%	7%	8%	3%	6%	7%	8%
6. System #1 has embedded GPS so each video always accurately reports the exact location of the officer and where the video was recorded. System #2 is simply a camera with no GPS technology so when these police camera videos are used as evidence, the location of the event must be determined using other factors. Which do you think is better?																		
System 1	91%	89%	92%	92%	92%	89%	88%	86%	89%	91%	92%	92%	89%	89%	92%	91%	92%	85%
System 2	6%	10%	5%	4%	4%	9%	8%	10%	7%	6%	5%	6%	8%	7%	6%	7%	6%	12%
DK/Refused	3%	2%	3%	3%	3%	2%	3%	4%	4%	3%	3%	2%	3%	3%	2%	3%	2%	3%
7. System #1 uses modern video compression technology to minimize the video file size. System #2 uses older less efficient video recording technology that results in video file sizes that are twice as large, and therefore the storage cost is also twice as much. Which do you think is better?																		
System 1	88%	92%	86%	86%	91%	93%	88%	85%	87%	88%	88%	89%	90%	89%	88%	92%	87%	82%
System 2	6%	6%	8%	7%	6%	1%	10%	7%	5%	7%	6%	7%	4%	8%	6%	5%	9%	12%
DK/Refused	5%	2%	6%	7%	4%	6%	2%	8%	7%	5%	6%	4%	5%	3%	6%	4%	5%	5%
8. System #1 uses its GPS to provide an automatic Officer Down emergency alert to Central Dispatch with the Officer's exact location if the Officer goes down and does not respond to voice prompts from the body camera. System #2 is simply a camera with no GPS or Officer Down reporting capability. Which do you think is better?																		
System 1	94%	93%	95%	96%	95%	94%	95%	90%	94%	96%	95%	95%	96%	96%	94%	95%	97%	92%
System 2	4%	7%	2%	3%	3%	5%	5%	7%	5%	4%	3%	5%	3%	3%	5%	4%	2%	8%
DK/Refused	2%	0%	3%	1%	2%	1%	0%	4%	1%	0%	2%	1%	1%	1%	1%	1%	1%	0%
9. System #1's camera records in High Definition video. System #2's camera records in Standard Definition video. Which do you think is better?																		
System 1	86%	77%	83%	87%	88%	90%	90%	89%	85%	87%	88%	85%	89%	88%	85%	86%	96%	81%
System 2	8%	16%	11%	7%	6%	5%	8%	10%	5%	6%	7%	11%	6%	6%	10%	9%	4%	16%
DK/Refused	6%	7%	7%	6%	5%	5%	2%	1%	10%	7%	5%	5%	5%	7%	5%	5%	1%	3%
10. With System #1, during an emergency event, Police Central Dispatch can remotely start video recording and send alerts to ALL their cameras within a specified area. System #2's Police Central Dispatch cannot communicate with the camera at all.. Which do you think is better?																		
System 1	89%	89%	90%	91%	88%	94%	91%	86%	86%	88%	90%	89%	89%	90%	90%	88%	93%	88%
System 2	7%	11%	4%	7%	7%	5%	7%	8%	9%	8%	5%	8%	7%	6%	8%	7%	5%	12%
DK/Refused	4%	0%	7%	2%	5%	1%	2%	6%	5%	3%	5%	2%	4%	4%	2%	5%	2%	0%

		---REGION---								--DENSITY--				--PARTY--				
	TOTAL	New Engl	Mid-Atl	Great Lakes	South	TX-OK-AK	Mid-west	Moun-tain	West Coast	City	Small Town	Sub-urbs	Rural	Dem	Rep	Ind	**African Amer**	**Hisp**
A 3	**1000**	**52**	**151**	**200**	**231**	**75**	**50**	**73**	**170**	**188**	**301**	**249**	**222**	**281**	**253**	**239**	**127**	**59**
11. So, in summary, if the police in your local area or state were to acquire policy body cameras, which system do you think would be better?																		
System #1 called the BodyWorn camera with GPS and real-time communications that can automatically start video recording, and immediately uploads videos with location data to cloud storage through a cellular or Wi-Fi connection.	89%	90%	90%	88%	92%	90%	91%	79%	86%	91%	89%	91%	88%	92%	89%	90%	93%	86%
System #2 camera from the Taser company has a manual on-off switch, no GPS, no communications with Central Dispatch, and stores video in the camera until the end of the shift when the officer goes back to the police station and uploads larger videos to cloud-storage.	7%	8%	5%	7%	5%	9%	9%	14%	8%	5%	6%	8%	9%	6%	10%	6%	6%	14%
DK/Refused	4%	2%	5%	5%	3%	1%	0%	7%	6%	3%	4%	2%	3%	2%	2%	4%	1%	0%
D1. Gender.																		
Male	50%	48%	47%	51%	44%	41%	55%	58%	60%	51%	51%	51%	49%	42%	51%	57%	50%	54%
Female	50%	52%	53%	49%	56%	59%	45%	42%	40%	49%	49%	49%	51%	58%	49%	43%	50%	46%
D2. Age.																		
18-29	9%	5%	9%	11%	7%	8%	11%	9%	12%	13%	12%	11%	3%	8%	9%	9%	14%	18%
30-39	10%	13%	9%	10%	7%	13%	21%	14%	7%	13%	9%	13%	6%	8%	11%	11%	9%	8%
40-49	14%	14%	13%	14%	17%	14%	10%	17%	11%	16%	14%	13%	16%	16%	17%	11%	23%	33%
50-59	24%	23%	29%	23%	30%	19%	20%	21%	20%	23%	24%	29%	25%	27%	19%	28%	26%	18%
60-64	14%	11%	12%	16%	14%	11%	21%	8%	13%	10%	13%	14%	18%	13%	15%	15%	11%	10%
65-Up	26%	31%	26%	21%	23%	29%	17%	29%	33%	24%	27%	21%	31%	28%	29%	26%	16%	13%
Refused	3%	3%	1%	5%	3%	5%	0%	2%	3%	0%	1%	0%	1%	1%	0%	1%	1%	0%

BodyWorn Nationwide *August 2015* *Job 2743* **A 4**	**TOTAL** **1000**	***---REGION---*** New Engl **52**	Mid-Atl **151**	Great Lakes **200**	South **231**	TX-OK-AK **75**	Mid-west **50**	Moun-tain **73**	West Coast **170**	***--DENSITY--*** City **188**	Small Town **301**	Sub-urbs **249**	Rural **222**	***--PARTY--*** Dem **281**	Rep **253**	Ind **239**	**African Amer** **127**	**Hisp** **59**
D3. African American/Black.																		
Yes	13%	11%	11%	13%	20%	10%	7%	11%	8%	21%	15%	11%	6%	29%	2%	10%	100%	16%
No	83%	86%	86%	81%	75%	85%	93%	83%	88%	77%	83%	87%	92%	70%	98%	89%	0%	83%
DK/Refused	4%	3%	3%	5%	5%	5%	0%	6%	4%	3%	1%	2%	3%	1%	0%	2%	0%	1%
D4. Hispanic.																		
Yes	6%	3%	2%	2%	4%	14%	5%	6%	14%	12%	5%	6%	3%	7%	3%	6%	7%	100%
No	90%	94%	95%	93%	90%	81%	95%	90%	82%	87%	94%	92%	95%	92%	97%	93%	91%	0%
DK/Refused	4%	3%	2%	5%	5%	5%	0%	4%	4%	2%	1%	2%	2%	1%	0%	1%	2%	0%
D5. Party ID.																		
Democrat	28%	37%	37%	23%	29%	23%	17%	22%	31%	35%	32%	26%	23%	100%	0%	0%	63%	33%
Republican	25%	13%	25%	17%	28%	37%	35%	33%	24%	21%	24%	27%	33%	0%	100%	0%	5%	14%
Independent	24%	41%	24%	25%	20%	19%	30%	23%	23%	27%	26%	23%	23%	0%	0%	100%	18%	25%
Other/DK/Refused	23%	10%	14%	34%	23%	21%	18%	23%	23%	17%	19%	24%	21%	0%	0%	0%	14%	27%
D6. Education Level.																		
0-11	4%	3%	3%	5%	4%	7%	3%	1%	2%	4%	5%	1%	5%	5%	3%	4%	8%	5%
12 - High School	23%	21%	22%	27%	28%	28%	30%	16%	11%	23%	24%	16%	33%	26%	21%	25%	30%	27%
Business school/some college	20%	18%	13%	23%	19%	16%	15%	22%	27%	24%	21%	18%	20%	21%	23%	19%	21%	29%
College graduate	30%	35%	34%	29%	27%	25%	39%	33%	30%	29%	29%	40%	27%	27%	34%	32%	30%	22%
Graduate degree	19%	19%	25%	12%	19%	15%	12%	24%	25%	20%	20%	25%	14%	20%	18%	18%	11%	16%
DK/Refused	4%	3%	2%	4%	4%	9%	0%	4%	5%	1%	1%	1%	1%	1%	1%	1%	1%	0%
D7. Area Live In.																		
Large city	19%	11%	13%	15%	15%	29%	17%	27%	27%	100%	0%	0%	0%	23%	16%	21%	31%	37%
Small city/town	30%	47%	23%	35%	34%	21%	31%	28%	23%	0%	100%	0%	0%	34%	28%	32%	37%	26%
Suburban area	25%	13%	39%	24%	20%	20%	23%	20%	28%	0%	0%	100%	0%	23%	27%	24%	22%	26%
Rural	22%	24%	24%	21%	25%	22%	29%	21%	17%	0%	0%	0%	100%	18%	29%	22%	10%	12%
DK/Refused	4%	5%	1%	5%	5%	8%	0%	3%	4%	0%	0%	0%	0%	1%	1%	1%	1%	0%
Phone																		
Landline	68%	70%	71%	59%	68%	56%	66%	70%	80%	60%	67%	62%	83%	67%	77%	67%	49%	50%
Cell	32%	30%	29%	41%	32%	44%	34%	30%	20%	40%	33%	38%	17%	33%	23%	33%	51%	50%

BodyWorn Nationwide
August 2015
Job 2743

		---REGION---								--DENSITY--				--PARTY--				
	TOTAL	New Engl	Mid-Atl	Great Lakes	South	TX-OK-AK	Mid-west	Moun-tain	West Coast	City	Small Town	Sub-urbs	Rural	Dem	Rep	Ind	**African Amer**	**Hisp**
A 5	**1000**	**52**	**151**	**200**	**231**	**75**	**50**	**73**	**170**	**188**	**301**	**249**	**222**	**281**	**253**	**239**	**127**	**59**
Region																		
New England	5%	100%	0%	0%	0%	0%	0%	0%	0%	3%	8%	3%	6%	7%	3%	9%	4%	3%
Mid-Atlantic	15%	0%	100%	0%	0%	0%	0%	0%	0%	10%	12%	24%	16%	20%	15%	15%	13%	6%
Great Lakes	20%	0%	0%	100%	0%	0%	0%	0%	0%	16%	23%	19%	19%	17%	13%	21%	21%	7%
South	23%	0%	0%	0%	100%	0%	0%	0%	0%	19%	26%	19%	26%	24%	26%	20%	37%	17%
TX-OK-AK	7%	0%	0%	0%	0%	100%	0%	0%	0%	12%	5%	6%	7%	6%	11%	6%	6%	18%
Midwest	5%	0%	0%	0%	0%	0%	100%	0%	0%	4%	5%	5%	6%	3%	7%	6%	3%	4%
Mountain	7%	0%	0%	0%	0%	0%	0%	100%	0%	10%	7%	6%	7%	6%	9%	7%	6%	7%
West Coast	17%	0%	0%	0%	0%	0%	0%	0%	100%	25%	13%	19%	13%	19%	16%	16%	10%	39%

BodyWorn Nationwide *August 2015* *Job 2743*		*-GENDER-*		*--GENDER: BY AGE--*						*--EDUCATION LEVEL--*				*-SUPPORT BODY CAMERAS-*	
	TOTAL	Male	Fem	M 18-49	F 18-49	M 50-64	F 50-64	M 65+	F 65+	HS/ Less	Some Coll	Coll Grad	Grad. Degree	Strong	Some-what
B 1	**1000**	**502**	**498**	**170**	**162**	**187**	**193**	**130**	**128**	**265**	**198**	**304**	**192**	**596**	**288**
A. Registered to Vote.															
Yes	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
1. Have you heard or read anything over the past year about controversial incidents involving citizens killed or harmed by police or while in police custody?															
Yes	94%	94%	94%	96%	92%	97%	97%	89%	91%	88%	95%	97%	97%	95%	94%
No	6%	5%	6%	4%	8%	3%	3%	10%	7%	12%	5%	2%	3%	4%	6%
DK/Refused/Would not say	0%	0%	1%	0%	0%	0%	0%	1%	1%	0%	0%	0%	0%	1%	0%
2. Some people have proposed that police officers be equipped with body cameras that record their interactions with citizens and criminal suspects. Do you strongly support, somewhat support, somewhat oppose or strongly oppose equipping police officers with body cameras?															
Strongly support	60%	57%	62%	55%	59%	60%	67%	56%	62%	68%	62%	58%	49%	100%	0%
Somewhat support	29%	29%	29%	31%	25%	27%	29%	29%	32%	22%	28%	31%	36%	0%	100%
Somewhat oppose	3%	3%	3%	3%	5%	3%	2%	3%	1%	2%	3%	4%	2%	0%	0%
Strongly oppose	3%	5%	2%	5%	3%	5%	1%	6%	1%	4%	3%	3%	5%	0%	0%
DK/Refused	5%	5%	5%	5%	8%	5%	1%	6%	4%	4%	3%	5%	8%	0%	0%
Total Support	88%	86%	91%	86%	84%	87%	96%	85%	94%	90%	91%	89%	85%	100%	100%
Total Oppose	7%	9%	4%	8%	8%	8%	3%	8%	2%	6%	7%	6%	7%	0%	0%
Next I will read you a short set of statements that describe features of two different police body camera systems. Assuming the two systems cost about the same to put in place, tell me which you think is better.															
3. System #1 is a camera on a Smartphone that is embedded inside a bulletproof vest the officer always wears, and cannot fall off. System #2 is a clip-on camera about the size of a garage door opener or pager that clips onto an officer's shirt pocket, and thus, can come off when an officer runs or gets into a struggle. Which do you think is better?															
System 1	80%	77%	84%	80%	87%	80%	85%	70%	83%	85%	84%	81%	74%	86%	78%
System 2	12%	14%	10%	13%	9%	10%	10%	20%	10%	10%	9%	15%	12%	9%	16%
DK/Refused	7%	9%	6%	7%	4%	9%	5%	10%	7%	5%	6%	5%	14%	5%	7%
4. System #1 - the body camera starts recording automatically any time an officer turns on their flashing patrol car lights, gets out of the vehicle, or starts running. The camera then continues recording until the patrol car's flashing lights are turned off. System #2 - the body camera has a manual on-off switch so the officer has to remember to start recording, and has control to stop recording at any time. Which do you think is better?															
System 1	87%	82%	92%	88%	93%	79%	94%	79%	88%	88%	88%	89%	82%	92%	86%
System 2	9%	13%	6%	11%	4%	13%	5%	15%	9%	9%	9%	8%	11%	5%	11%
DK/Refused	4%	5%	3%	1%	3%	8%	1%	6%	3%	3%	3%	2%	7%	3%	3%

	TOTAL	-GENDER- Male	Fem	--GENDER: BY AGE-- M 18-49	F 18-49	M 50-64	F 50-64	M 65+	F 65+	--EDUCATION LEVEL-- HS/ Less	Some Coll	Coll Grad	Grad. Degree	-SUPPORT BODY CAMERAS- Strong	Some-what
B 2	**1000**	**502**	**498**	**170**	**162**	**187**	**193**	**130**	**128**	**265**	**198**	**304**	**192**	**596**	**288**
5. System #1 - the video from the Smartphone camera is uploaded as it is being recorded using cellular or Wi-Fi networks to a cloud-based storage system. System #2 - the videos are stored on the camera until after the end of the shift, when the police officer goes back to the police station and then manually docks the camera to a computer for uploading of videos to a cloud-based storage system. Which do you think is better?															
System 1	72%	68%	76%	79%	82%	67%	78%	57%	68%	66%	74%	76%	74%	78%	71%
System 2	22%	25%	18%	16%	16%	27%	18%	35%	22%	28%	22%	19%	18%	18%	24%
DK/Refused	6%	6%	6%	4%	2%	6%	4%	8%	11%	6%	4%	5%	7%	4%	5%
6. System #1 has embedded GPS so each video always accurately reports the exact location of the officer and where the video was recorded. System #2 is simply a camera with no GPS technology so when these police camera videos are used as evidence, the location of the event must be determined using other factors. Which do you think is better?															
System 1	91%	89%	93%	90%	94%	89%	94%	88%	92%	91%	91%	93%	89%	96%	90%
System 2	6%	8%	4%	8%	4%	8%	4%	7%	5%	6%	7%	5%	7%	3%	8%
DK/Refused	3%	4%	3%	2%	2%	3%	2%	5%	3%	3%	2%	2%	4%	1%	2%
7. System #1 uses modern video compression technology to minimize the video file size. System #2 uses older less efficient video recording technology that results in video file sizes that are twice as large, and therefore the storage cost is also twice as much. Which do you think is better?															
System 1	88%	85%	91%	90%	96%	85%	91%	83%	87%	89%	87%	92%	85%	92%	89%
System 2	6%	7%	5%	6%	3%	6%	5%	8%	8%	8%	7%	4%	7%	5%	5%
DK/Refused	5%	7%	4%	4%	1%	8%	4%	8%	5%	4%	6%	4%	9%	3%	6%
8. System #1 uses its GPS to provide an automatic Officer Down emergency alert to Central Dispatch with the Officer's exact location if the Officer goes down and does not respond to voice prompts from the body camera. System #2 is simply a camera with no GPS or Officer Down reporting capability. Which do you think is better?															
System 1	94%	93%	96%	95%	98%	93%	96%	92%	96%	97%	95%	96%	93%	98%	93%
System 2	4%	5%	3%	5%	1%	4%	4%	6%	3%	3%	4%	3%	5%	2%	5%
DK/Refused	2%	2%	1%	0%	1%	3%	0%	3%	1%	0%	1%	1%	3%	0%	2%
9. System #1's camera records in High Definition video. System #2's camera records in Standard Definition video. Which do you think is better?															
System 1	86%	84%	88%	88%	89%	85%	91%	80%	86%	89%	86%	88%	84%	92%	84%
System 2	8%	9%	7%	10%	8%	8%	5%	10%	6%	6%	8%	8%	8%	4%	11%
DK/Refused	6%	7%	5%	2%	3%	7%	4%	11%	7%	5%	6%	4%	8%	4%	5%
10. With System #1, during an emergency event, Police Central Dispatch can remotely start video recording and send alerts to ALL their cameras within a specified area. System #2's Police Central Dispatch cannot communicate with the camera at all. Which do you think is better?															
System 1	89%	85%	93%	86%	95%	84%	93%	85%	94%	90%	87%	92%	86%	93%	86%
System 2	7%	10%	4%	12%	4%	11%	4%	6%	3%	7%	10%	5%	7%	5%	9%
DK/Refused	4%	5%	3%	2%	1%	5%	3%	10%	3%	3%	3%	3%	7%	2%	5%

		-GENDER-		--GENDER: BY AGE--						--EDUCATION LEVEL--				-SUPPORT BODY CAMERAS-	
	TOTAL	Male	Fem	M 18-49	F 18-49	M 50-64	F 50-64	M 65+	F 65+	HS/ Less	Some Coll	Coll Grad	Grad. Degree	Strong	Some-what
B 3	**1000**	**502**	**498**	**170**	**162**	**187**	**193**	**130**	**128**	**265**	**198**	**304**	**192**	**596**	**288**
11. So, in summary, if the police in your local area or state were to acquire policy body cameras, which system do you think would be better?															
System #1 called the BodyWorn camera with GPS and real-time communications that can automatically start video recording, and immediately uploads videos with location data to cloud storage through a cellular or Wi-Fi connection.	89%	83%	94%	91%	95%	80%	95%	84%	93%	92%	90%	89%	88%	94%	88%
System #2 camera from the Taser company has a manual on-off switch, no GPS, no communications with Central Dispatch, and stores video in the camera until the end of the shift when the officer goes back to the police station and uploads larger videos to cloud-storage.	7%	11%	4%	8%	3%	13%	4%	10%	4%	6%	7%	7%	9%	5%	7%
DK/Refused	4%	6%	2%	1%	1%	7%	1%	6%	3%	2%	3%	4%	3%	1%	5%
D1. Gender.															
Male	50%	100%	0%	100%	0%	100%	0%	100%	0%	50%	52%	50%	50%	48%	51%
Female	50%	0%	100%	0%	100%	0%	100%	0%	100%	50%	48%	50%	50%	52%	49%
D2. Age.															
18-29	9%	10%	8%	30%	26%	0%	0%	0%	0%	6%	10%	13%	9%	8%	10%
30-39	10%	12%	8%	35%	24%	0%	0%	0%	0%	7%	6%	15%	11%	10%	9%
40-49	14%	12%	16%	35%	50%	0%	0%	0%	0%	13%	12%	12%	23%	13%	13%
50-59	24%	23%	26%	0%	0%	61%	67%	0%	0%	22%	26%	29%	22%	25%	25%
60-64	14%	15%	13%	0%	0%	39%	33%	0%	0%	15%	16%	12%	14%	15%	12%
65-Up	26%	26%	26%	0%	0%	0%	0%	100%	100%	37%	28%	19%	20%	26%	27%
Refused	3%	3%	3%	0%	0%	0%	0%	0%	0%	1%	0%	0%	1%	2%	3%

BodyWorn Nationwide *August 2015* *Job 2743*		*-GENDER-*		*--GENDER: BY AGE--*						*--EDUCATION LEVEL--*				*-SUPPORT BODY CAMERAS-*	
	TOTAL	Male	Fem	M 18-49	F 18-49	M 50-64	F 50-64	M 65+	F 65+	HS/ Less	Some Coll	Coll Grad	Grad. Degree	Strong	Some-what
B 4	**1000**	**502**	**498**	**170**	**162**	**187**	**193**	**130**	**128**	**265**	**198**	**304**	**192**	**596**	**288**
D3. African American/Black.															
Yes	13%	13%	13%	18%	17%	11%	13%	8%	8%	18%	13%	12%	7%	17%	4%
No	83%	83%	83%	81%	82%	87%	85%	87%	90%	80%	85%	86%	90%	79%	93%
DK/Refused	4%	5%	4%	1%	2%	1%	1%	5%	2%	2%	2%	1%	3%	4%	3%
D4. Hispanic.															
Yes	6%	6%	6%	11%	10%	7%	2%	1%	5%	7%	9%	4%	5%	6%	4%
No	90%	90%	90%	88%	89%	92%	96%	97%	92%	92%	90%	94%	93%	90%	92%
DK/Refused	4%	4%	5%	1%	1%	1%	2%	2%	3%	1%	1%	2%	2%	4%	3%
D5. Party ID.															
Democrat	28%	24%	32%	23%	29%	25%	34%	24%	38%	33%	30%	25%	29%	31%	24%
Republican	25%	26%	25%	29%	27%	21%	24%	32%	25%	23%	29%	29%	23%	20%	36%
Independent	24%	27%	21%	24%	19%	32%	23%	28%	21%	26%	23%	25%	23%	26%	20%
Other/DK/Refused	23%	23%	22%	23%	25%	22%	19%	16%	17%	18%	18%	22%	24%	23%	20%
D6. Education Level.															
0-11	4%	4%	3%	4%	2%	4%	2%	6%	6%	14%	0%	0%	0%	5%	2%
12 - High School	23%	22%	23%	22%	14%	22%	23%	25%	38%	86%	0%	0%	0%	25%	18%
Business school/some college	20%	20%	19%	16%	18%	24%	20%	23%	21%	0%	100%	0%	0%	21%	19%
College graduate	30%	30%	31%	37%	37%	30%	35%	24%	20%	0%	0%	100%	0%	30%	33%
Graduate degree	19%	19%	19%	22%	29%	18%	18%	19%	11%	0%	0%	0%	100%	16%	24%
DK/Refused	4%	4%	4%	0%	1%	1%	2%	3%	4%	0%	0%	0%	0%	3%	4%
D7. Area Live In.															
Large city	19%	19%	19%	23%	25%	16%	16%	19%	17%	19%	23%	18%	19%	22%	14%
Small city/town	30%	31%	29%	30%	33%	30%	29%	36%	28%	32%	32%	29%	32%	28%	31%
Suburban area	25%	25%	25%	29%	25%	30%	26%	16%	25%	15%	22%	33%	32%	24%	29%
Rural	22%	22%	23%	18%	16%	22%	28%	27%	27%	32%	23%	20%	16%	22%	23%
DK/Refused	4%	3%	5%	0%	1%	1%	1%	1%	4%	1%	0%	1%	1%	3%	2%
Phone															
Landline	68%	62%	74%	32%	49%	74%	87%	83%	88%	71%	71%	66%	63%	67%	72%
Cell	32%	38%	26%	68%	51%	26%	13%	17%	12%	29%	29%	34%	37%	33%	28%

BodyWorn Nationwide *August 2015* *Job 2743*		*-GENDER-*		*--GENDER: BY AGE--*						*--EDUCATION LEVEL--*				*-SUPPORT BODY CAMERAS-*	
	TOTAL	Male	Fem	M 18-49	F 18-49	M 50-64	F 50-64	M 65+	F 65+	HS/ Less	Some Coll	Coll Grad	Grad. Degree	Strong	Some-what
B 5	**1000**	**502**	**498**	**170**	**162**	**187**	**193**	**130**	**128**	**265**	**198**	**304**	**192**	**596**	**288**
Region															
New England	5%	5%	5%	4%	6%	5%	4%	6%	7%	5%	5%	6%	5%	5%	6%
Mid-Atlantic	15%	14%	16%	11%	18%	17%	16%	15%	16%	14%	10%	17%	20%	13%	17%
Great Lakes	20%	20%	20%	24%	18%	21%	21%	15%	18%	24%	23%	19%	12%	20%	19%
South	23%	20%	26%	18%	25%	24%	29%	18%	24%	28%	22%	20%	23%	24%	22%
TX-OK-AK	7%	6%	9%	7%	8%	4%	7%	6%	11%	10%	6%	6%	6%	8%	8%
Midwest	5%	5%	4%	7%	6%	5%	5%	4%	3%	6%	4%	6%	3%	4%	7%
Mountain	7%	8%	6%	13%	5%	4%	7%	8%	8%	5%	8%	8%	9%	8%	6%
West Coast	17%	20%	14%	16%	15%	18%	12%	28%	15%	8%	23%	17%	23%	19%	16%