

Responses to PCPA's RFI on Police Body Worn Cameras

On January 8, 2019, PCPA issued a Request for Information about police body worn cameras, also known as non-vehicle-mounted mobile video recording systems according to Pennsylvania's regulations.

Vendors were asked to provide at least the following information:

- How does your non-vehicle-mounted mobile video recording systems and technology meet Pennsylvania's published requirements?
- Have you submitted your non-vehicle-mounted mobile video recording systems to the Pennsylvania State Police for certification?
- Is your non-vehicle-mounted mobile video recording systems already certified by the Pennsylvania State Police?
- Are you offering a storage solution?
- Will you offer storage solutions bundled (no line item distinction) with the cost of each camera purchased?
- How does your storage solution meet Pennsylvania's published requirements?
- List the products and services that are already available on State Contract or PA CoStars.
- List your costs for products and services you offer.
- Will you offer a discount of those prices if multiple police departments group together to buy your products and services?

As of March 27, 2019, the Following vendors responded:

- Axon Enterprise, Inc. (Axon)
- Digital Ally, Inc
- Kustom Signals, Inc
- Municipal Emergency Services, Inc.
- WatchGuard, Inc.
- Sentinel Camera Systems

Here is How they each answered those questions.

How does your non-vehicle-mounted mobile video recording systems and technology meet Pennsylvania's published requirements?

Vendor	Response
Axon Enterprise, Inc.	List all the specifications that meet or exceed Pa's requirements
Digital Ally, Inc	Digital Ally's FirstVu HD Body Camera is in full compliance with the State of Pennsylvania's published requirements
Kustom Signals, Inc	Kustom Signals' Eyewitness Vantage meets the following published requirements.
Municipal Emergency Services, Inc	In all cases our products meet and exceed current requirements
WatchGuard, Inc	Lists all the specifications that meet or exceed Pa's requirements.
Sentinel Camera Systems	Sentinel Cameras meet or exceed all requirements.

Have you submitted your non-vehicle-mounted mobile video recording systems to the Pennsylvania State Police for certification?

Vendor	Response
Axon Enterprise, Inc.	Yes, the Axon Body 2 and the Axon Flex 2 cameras are in the list of PA State List of certified body-worn cameras
Digital Ally, Inc	Yes, Digital Ally submitted our FirstVu HD Body Camera system to the Pennsylvania State Police, and it was certified on the Pennsylvania State Bulletin.
Kustom Signals, Inc	Kustom Signals has not yet submitted the Eyewitness Vantage for certification but would be very interested in doing so.
Municipal Emergency Services, Inc	Not yet, however we would appreciate the opportunity, and are confident that with our technology, we be certified.
WatchGuard, Inc	Yes
Sentinel Camera Systems	Yes, application for certification has been submitted for consideration.

Is your non-vehicle-mounted mobile video recording systems already certified by the Pennsylvania State Police?

Vendor	Response
Axon Enterprise, Inc.	Yes, Axon Body 2 and Axon Flex 2 cameras are certified by the Pennsylvania State Police.
Digital Ally, Inc	Yes, Digital Ally submitted our FirstVu HD Body Camera system to the Pennsylvania State Police, and it was certified on the Pennsylvania State Bulletin.
Kustom Signals, Inc	Kustom Signals Eyewitness Vantage is not already certified by the Pennsylvania State Police
Municipal Emergency Services, Inc	Not yet, however we would appreciate the opportunity, and are confident that with our technology, we be certified.
WatchGuard, Inc	Yes, we are currently under contract with the Pennsylvania State Police
Sentinel Camera Systems	No, waiting for results of our application for certification

Are you offering a storage solution?

Vendor	Response
Axon Enterprise, Inc.	Yes, Axon's Body-worn cameras are paired with Axon Evidence (Evidence.com), a robust end-to-end solution that not only allows agencies to store data, it also enables new workflows for managing and sharing that data securely from anywhere
Digital Ally. Inc	Yes, Digital Ally is offering both a cloud storage solution and a local on-premise (on-site server-based) storage solution.
Kustom Signals, Inc	The Eyewitness Data Vault (EDV) file management system allows agencies to easily transfer, store and manage video files recorded by Kustom Signals' in-car video and/or body-worn video systems. EDV provides quick and easy file searching, easy playback and file duplication. Storage can be expanded locally. EDV is also compatible with Active Directory and LDAP to allow established log in credentials to be used. Kustom Signals does not currently offer a cloud-based solution.
Municipal Emergency Services, Inc	Yes, we offer multiple storage solutions as our Hydra Digital Evidence Management Software is storage agnostic. We have NAS storage which is outlined in our pricing scenario, however we would welcome the opportunity to deploy our software with your existing IT Storage infrastructure if there is potential cost savings. We offer Wasabi CJIS Certified Hot Cloud
WatchGuard, Inc	Yes. We are offering three different storage solutions, On-Premise, Hybrid, and Cloud, which are all outlined within our provided solution.
Sentinel Camera Systems	Yes

Will you offer storage solutions bundled (no line item distinction) with the cost of each camera purchased?

Vendor	Response
Axon Enterprise, Inc.	Evidence.com is licensed on a per user basis; a license is required for each camera. As a hosted application, there is no limit to the number of users your agency can add, should administrators or staff without body cameras need access to the system.
Digital Ally. Inc	Yes, Digital Ally is offering bundled storage solutions. We offer three different VuVault.com unlimited cloud storage solution bundles: the Ultimate Plan with 1-year of data retention, the Pro Plan with 180-day data retention, and the Basic Plan with 90-day data retention. Bundled discounts for the FirstVu HD Body Camera and cloud storage are listed in the Unit Price table
Kustom Signals, Inc	Kustom Signals can bundle the cost of the storage unit into the cost of each camera purchased if more than 30 cameras are purchased together
Municipal Emergency Services, Inc	Yes, we offer bundled storage solutions tied to camera cost if it is required. Many vendors have done this, and the pricing scheme ends up as misleading and many times more expensive than unbundled. We will offer both as required by specific RFP's
WatchGuard, Inc	This option is negotiable, if desired
Sentinel Camera Systems	Yes

How does your storage solution meet Pennsylvania's published requirements?

Vendor	Response
Axon Enterprise, Inc.	Evidence.com is a robust end-to-end solution that not only allows agencies to store data, it also enables new workflows for managing and sharing that data securely – from anywhere
Digital Ally, Inc	Digital Ally's VuVault.com cloud storage solution and VuVault Software storage solution are both compliant with Pennsylvania's published requirements.
Kustom Signals, Inc	Kustom Signals storage solution supports agency compliance with 18 Pa.C.S. § 5706(b)(5), the following minimum requirements that must be met for any storage of an audio recording made in accordance with 18 Pa.C.S. § 5706(b)(4), or any accompanying video recording
Municipal Emergency Services, Inc	Yes, please see below, we offer Wasabi CJIS Certified Hot Cloud Storage
WatchGuard, Inc	Each of the offered storage solutions has been designed to meet CJIS standards
Sentinel Camera Systems	Sentinel Cameras meet or exceed all requirements

Will you offer a discount of those prices if multiple police departments group together to buy your products and services?

Vendor	Response
Axon Enterprise, Inc.	Axon may consider a discount from our standard prices. Discounts will be negotiated at the individual agency level.
Digital Ally, Inc	Yes, Digital Ally will offer volume discount pricing on the Retail Unit Price List above for any State of Pennsylvania Police Department and Law Enforcement agency. Our PA COSTARS Contract and State of Pennsylvania Contract both offer our best pricing and already include a State-wide anticipated volume discount. Police Departments and Law Enforcement agencies may contact Digital Ally at any time for a quote.
Kustom Signals, Inc	Yes, Kustom Signals offers discounts on quantity purchases with the following breakdown of 6-14 units and 15+ and will honor these price breakdowns if multiple departments would like to make group purchases.
Municipal Emergency Services, Inc	Yes, we would be happy to offer discounts for multiple agencies are for larger quantities.
WatchGuard, Inc	We are open to negotiations.
Sentinel Camera Systems	Yes

List the products and services that are already available on State Contract or PA CoStars

Vendor	Response (see proposal for details)
Axon Enterprise, Inc.	Yes
Digital Ally. Inc	Yes
Kustom Signals, Inc	Yes
Municipal Emergency Services, Inc	No
WatchGuard, Inc	Yes
Sentinel Camera Systems	No

List your costs for products and services you offer.

Please see the individual responses by each vendor.

January 25, 2019

Pennsylvania Chiefs of Police Association
3905 N. Front Street
Harrisburg, PA 17110
Police Body Worn Cameras RFI

Digital Ally, Inc. is pleased to participate in the Pennsylvania Chiefs of Police Association's Request for Information for **Police Body Worn Cameras**. We believe Digital Ally, Inc. has the experience to successfully furnish State of Pennsylvania Police Departments with a high quality Body Camera system and Digital Evidence Management System.

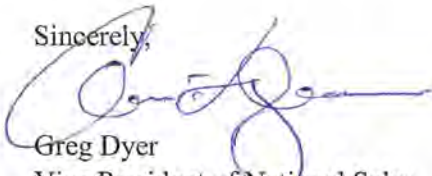
With patented automatic activation (Patents 9253452; 8781292), and an ever improving video storage model, the State of Pennsylvania Police Departments will be a step ahead in the future of policing with the assistance of our Body Camera and Digital Evidence Management solution. We believe automatic activation will prove to be an increasingly important feature to consider with the current climate of policing. With automatic activation, an officer need not worry about activating a body camera during a high-stress incident. It can instead automatically be done for him or her.

Digital Ally has been successfully involved in the implementation of a wide variety of digital In-Car Camera and Body Camera Solutions from the State Police level to the National Law Enforcement Agency level, as well as county and municipal agencies throughout the United States. Digital Ally's products are proudly represented in all 50 states and over 90 countries. We have over 50,000 camera units deployed throughout the world, while working with over 6,000 Law Enforcement agencies. Our sole business is dedicated to designing, manufacturing, and selling quality, leading edge digital video systems and related products. We understand the work, dedication, and commitments involved, and stand ready to perform all the tasks required within the scheduled time period.

With our current and future technology, no-nonsense Advanced Exchange Warranty program, and unparalleled customer service, Digital Ally will prove to be an invaluable team member with the Pennsylvania Chiefs of Police Association's Police Body Worn Cameras project.

Thank you for the opportunity to submit our information. If any of the State of Pennsylvania Police Departments would like to evaluate our systems or would like a detailed in-person presentation, we would be pleased to provide it at their convenience. Choosing a vendor for a Body Camera program is a big decision. Digital Ally stands ready to assist the State of Pennsylvania Police Departments in making this project an unparalleled success.

Sincerely,



Greg Dyer
Vice President of National Sales
Digital Ally, Inc.
9705 Loiret Blvd.
Lenexa, KS 66219
800-440-4947 (Toll-Free)

Table of Contents

Information Requested for Police Body Worn Cameras.....	3
PA COSTARS Contract Number 012-042 Price List.....	4
State of Pennsylvania Contract Number 4400014648 Price List.....	5
Digital Ally’s Retail Unit Price List.....	6
Contact Information for Digital Ally, Inc.	11
Product Information Packet for FirstVu HD Body Camera and Services	12
Product Information Packet for VuSchools Body Camera System for School Resource Officers.....	28

Information Requested

- **How does your non-vehicle-mounted mobile video recording systems and technology meet Pennsylvania's published requirements?**

Digital Ally's FirstVu HD Body Camera (non-vehicle-mounted mobile video recording system and technology) is in full compliance with the State of Pennsylvania's published requirements. Our FirstVu HD Body Camera has been approved on the Pennsylvania State Bulletin and has been tested by the Pennsylvania State Police.

- **Have you submitted your non-vehicle-mounted mobile video recording systems to the Pennsylvania State Police for certification?**

Yes, Digital Ally submitted our FirstVu HD Body Camera system (non-vehicle-mounted mobile video recording system) to the Pennsylvania State Police and it was certified on the Pennsylvania State Bulletin.

- **Is your non-vehicle-mounted mobile video recording systems already certified by the Pennsylvania State Police?**

Yes, Digital Ally's FirstVu HD Body Camera system (non-vehicle-mounted mobile video recording system) is already certified on the Pennsylvania State Bulletin by the Pennsylvania State Police.

- **Are you offering a storage solution?**

Yes, Digital Ally is offering both a cloud storage solution and a local on-premise (on-site server-based) storage solution.

- **Will you offer storage solutions bundled (no line item distinction) with the cost of each camera purchased?**

Yes, Digital Ally is offering bundled storage solutions. We offer three different VuVault.com unlimited cloud storage solution bundles: the Ultimate Plan with 1-year of data retention, the Pro Plan with 180-day data retention, and the Basic Plan with 90-day data retention. Bundled discounts for the FirstVu HD Body Camera and cloud storage are listed in the Unit Price table below.

The following bundled pricing discounts are available with our cloud storage solution bundles:

- 1) VuVault.com Ultimate Plan and FirstVu HD Body Camera Solution
 - 3-year or 5-year contract includes the FirstVu HD Body Camera at no cost
 - 1-year contract includes 50% discount on FirstVu HD Body Camera
- 2) VuVault.com Pro Plan and FirstVu HD Body Camera Solution
 - 5-year contract includes 83% discount on FirstVu HD Body Camera
 - 3-year contract includes 66% discount on FirstVu HD Body Camera
 - 1-year contract includes 39% discount on FirstVu HD Body Camera
- 3) VuVault.com Basic Plan and FirstVu HD Body Camera Solution
 - 5-year contract includes 83% discount on FirstVu HD Body Camera
 - 3-year contract includes 66% discount on FirstVu HD Body Camera
 - 1-year contract includes 33% discount on FirstVu HD Body Camera

We also offer hardware bundled pricing when our FirstVu HD Body Camera is purchased in conjunction with our In-Car Camera System, VuLink automatic activation device, and local on-premise VuVault Software solution. Our patented VuLink provides hands-free automatic activation for both the FirstVu HD Body Camera and our In-Car Camera Systems.

Volume discount pricing is also available when the hardware is purchased in large volume in conjunction with our local on-premise VuVault Software solution.

- **How does your storage solution meet Pennsylvania's published requirements?**

Digital Ally's VuVault.com cloud storage solution and VuVault Software storage solution are both compliant with Pennsylvania's published requirements.

- **List the products and services that are already available on State Contract or PA CoStars.**

Digital Ally products and services that are available on the PA COSTARS Contract Number 012-042:

<i>Product Description</i>	<i>PA COSTARS Contract Price</i>
<i>HARDWARE:</i>	
FirstVu HD Body Camera	\$505.75
Docking Station for Body Cameras	\$2,545.75
VuLink Automatic Recording Activation	\$420.75
<i>SOFTWARE AND CLOUD STORAGE OPTIONS:</i>	
VuVault Standalone Software	\$505.75
VuVault Server Software	\$1,295.00
VuVault Enterprise Software	\$1,525.75
VuVault.com Ultimate Plan	\$708 per user, per year
VuVault.com Pro Plan	\$348 per user, per year
VuVault.com Basic Plan	\$192 per user, per year
<i>EXTENDED WARRANTY:</i>	
Extended Warranty for FirstVu HD Body Camera	\$199 per device, per year
Extended Warranty for the Docking Station	\$495 per device, per year
Additional Warranty for VuLink (One Year only)	\$99 per device
<i>SERVICES AND INSTALLATION:</i>	
VuLink Installation (when installed with DVM system)	\$50 per vehicle
VuLink Installation (when installed standalone or as an add-on to existing system)	\$150 per vehicle
Professional Services Turn-Key Setup: includes onsite training, travel costs, configuration, deployment, implementation, body camera and 12-bay docking station installation	\$2,700.00

Digital Ally products and services that are available on the State of Pennsylvania Contract Number 4400014648:

<i>Product Description</i>	<i>State of Pennsylvania Contract Price</i>
<i>HARDWARE:</i>	
FirstVu HD Body Camera	\$505.75
Docking Station for Body Cameras	\$2,545.75
VuLink Automatic Recording Activation	\$420.75
<i>SOFTWARE AND CLOUD STORAGE OPTIONS:</i>	
VuVault Standalone Software	\$505.75
VuVault Server Software	\$1,295.00
VuVault Enterprise Software	\$1,525.75
VuVault.com Ultimate Plan	\$708 per user, per year
VuVault.com Pro Plan	\$348 per user, per year
VuVault.com Basic Plan	\$192 per user, per year
Administrator License for VuVault.com	\$99 per admin, per year
Share Portal for VuVault Software solution	\$399 per user, per year
Cloud Drive: Includes Block of 100GB of storage (per year)	\$63 per year
<i>EXTENDED WARRANTY:</i>	
Extended Warranty for FirstVu HD Body Camera	\$129 per device, per year
Extended Warranty for the Docking Station	\$495 per device, per year
Additional Warranty for VuLink (One Year only)	\$99 per device
<i>SERVICES AND INSTALLATION:</i>	
VuLink Installation (when installed with DVM system)	\$50 per vehicle
VuLink Installation (when installed standalone or as an add-on to existing system)	\$150 per vehicle
Professional Services Turn-Key Setup: includes onsite training, travel costs, configuration, deployment, implementation, body camera and 12-bay docking station installation	\$2,700.00
<i>BODY CAMERAS AND CLOUD STORAGE FOR SCHOOL RESOURCE OFFICERS AND SCHOOLS:</i>	
VuSchools Body Camera Kit with FirstVu HD Body Camera, Mini-Dock, choice of mounts, and cloud storage: 1 to 500 units (per Account, per Month)	\$65.80 per account, per month
VuSchools Body Camera Kit with FirstVu HD Body Camera, Mini-Dock, choice of mounts, and cloud storage: 501 to 1,000 units (per Account, per Month)	\$59.22 per account, per month
VuSchools Body Camera Kit with FirstVu HD Body Camera, Mini-Dock, choice of mounts, and cloud storage: 1,001 to 2,000 units (per Account, per Month)	\$55.31 per account, per month

- **List your costs for products and services you offer.**

Digital Ally's Retail Unit Price List for our products and services begins on the following page:

Digital Ally, Inc. FirstVu HD Body Camera System Unit Price List

To:

Pennsylvania Chiefs of Police Association
3905 N. Front Street
Harrisburg, PA 17110
Police Body Worn Cameras RFI

Date	Sales Representative	Payment Terms
1/25/2019	John Saunders Direct: 913.232.5348 Main Phone: 800-440-4947 Email: John.Saunders@digitalallyinc.com	Net30

Qty	Description	Unit Price
Body Camera System Hardware:		
1	FirstVu HD Body Camera Kit when VuVault.com Ultimate Plan 3-year or 5-year contract is purchased: includes Advanced Exchange Warranty for full term of contract (with 3-year or 5-year cloud contract)	Included at no cost
1	FirstVu HD Body Camera Kit when VuVault.com Ultimate Plan 1-year contract is purchased: includes Advanced Exchange Warranty for full term of contract (with 1-year cloud contract)	\$299.00
1	FirstVu HD Body Camera Kit when VuVault.com Pro Plan 5-year contract is purchased: includes Advanced Exchange Warranty for full term of contract (with 5-year cloud contract)	\$99.00
1	FirstVu HD Body Camera Kit when VuVault.com Pro Plan 3-year contract is purchased: includes Advanced Exchange Warranty for full term of contract (with 3-year cloud contract)	\$199.00

1	FirstVu HD Body Camera Kit when VuVault.com Pro Plan 1-year contract is purchased: includes Advanced Exchange Warranty for full term of contract (with 1-year cloud contract)	\$359.00
1	FirstVu HD Body Camera Kit when VuVault.com Basic Plan 5-year contract is purchased: includes Advanced Exchange Warranty for full term of contract (with 5-year cloud contract)	\$99.00
1	FirstVu HD Body Camera Kit when VuVault.com Basic Plan 3-year contract is purchased: includes Advanced Exchange Warranty for full term of contract (with 3-year cloud contract)	\$199.00
1	FirstVu HD Body Camera Kit when VuVault.com Basic Plan 1-year contract is purchased: includes Advanced Exchange Warranty for full term of contract (with 1-year cloud contract)	\$399.00
1	FirstVu HD Body Camera Kit includes 1-year Advanced Exchange Warranty (when purchased separately)	\$595.00
1	12-bay Docking Station for the FirstVu HD Body Camera includes 1-year Advanced Exchange Warranty	\$2,995.00

Qty	Description	Unit Price
Cloud Storage Option:		
1	VuVault.com Cloud Ultimate Plan for the FirstVu HD: with Unlimited Storage and 1-year data retention at \$59/user/month with 1-year, 3-year, or 5-year contract Includes: Unlimited Data Storage for 1 Year Advanced Exchange Warranty on hardware for full term of contract Full Software Access & Redaction Share Portal & Case Management	\$708.00 per user per year
1	VuVault.com Cloud Pro Plan for the FirstVu HD: with Unlimited Storage and 180-day data retention at \$29/user/month with 1-year, 3-year, or 5-year contract Includes: Unlimited Data Storage for 180 days Advanced Exchange Warranty on hardware for full term of Contract Full Software Access & Redaction Share Portal & Case Management	\$348.00 per user per year
1	VuVault.com Cloud Basic Plan for the FirstVu HD: with Unlimited Storage and 90-day data retention at \$16/user/month with 1-year, 3-year, or 5-year contract Includes: Unlimited Data Storage for 90 days Advanced Exchange Warranty on hardware for full term of Contract Full Software Access & Redaction Share Portal & Case Management	\$192.00 per user per year
1	VuVault.com Administrator License	\$99 per Admin per year

Qty	Description	Unit Price
Software with On-Premise Storage Option:		
1	VuVault Standalone Software	\$695.00
1	VuVault Server Software	\$1,695.00
1	VuVault Enterprise Server Software	\$1,895.00
Qty	Description	Unit Price
Services:		
1	Activation Fee	\$30.00 per device
1	Professional Services Turn-Key Setup <ul style="list-style-type: none"> • Onsite Product Setup & Configuration • Dedicated Project Manager • Weekly Project Planning Meetings • Best Practices & Implementation Planning Session • Statement of Work • System Administrator & Troubleshooting Training Session • Digital Ally Instructor Training • Implementation Document Packet • Go Live - End User Training • Go Live - Follow-up Review Session 	\$2,000.00 per location
Qty	Description	Unit Price
Optional Products and Services:		
1	VuLink: Patented body camera and in-car camera Automatic Activation Device includes 1-year Advanced Exchange Warranty	\$395.00 per vehicle
1	VuLink and Sync Cable: Patented body camera and in-car camera Automatic Activation Device includes 1-year Advanced Exchange Warranty	\$495.00 per vehicle
1	Installation of VuLink with a DVM system	\$50.00 per vehicle

1	Installation of VuLink as a standalone system or as an add-on to an existing system	\$150.00 per vehicle
1	Cloud Drive 100GB Block of Cloud Storage (for Cloud Solution only)	\$63.00 per year
1	Additional 1-year Advanced Exchange Warranty for FirstVu HD (for Local On-Premise Option only)	\$129.00 per camera per year
1	Dell Customized Server (for Local On-Premise Option only)	Customized Quote available upon request
1	Cloud Share License (Administrator only) Share Portal, Redaction, Case Management (for Local On-Premise Option only)	\$399.00 per license

- **Will you offer a discount of those prices if multiple police departments group together to buy your products and services?**

Yes, Digital Ally will offer volume discount pricing on the Retail Unit Price List above for any State of Pennsylvania Police Department and Law Enforcement agency. Our PA COSTARS Contract and State of Pennsylvania Contract both offer our best pricing and already include a State-wide anticipated volume discount. Police Departments and Law Enforcement agencies may contact Digital Ally at any time for a quote.

Contact information for a price quote:

Pennsylvania Sales Manager

John Saunders

Phone: 913.232.5348

Headquarters: 800-440-4947

Email: John.Saunders@digitalallyinc.com

Contact information for questions about Digital Ally's RFI proposal:

Bid Specialist

Nicole Leiker

Phone: 913.814.7774

Headquarters: 800-440-4947

Email: bids@digitalallyinc.com



FirstVu HD Body Camera



9705 Loiret Blvd. | Lenexa, KS 66219
800.440.4947 | 913.814.7774 | digitalallyinc.com

Table of Contents

Digital Ally, Inc. Company Information.....	3
Corporate Headquarters Location	3
Corporation Information.....	3
Contact Information	3
Company Qualifications	4
Introducing the FirstVu HD Body Camera	5
Mounting Locations	5
Included with Purchase.....	6
Upload Methods and Docking Stations	7
Specifications for Body Camera Solution.....	8
Docking Station Specifications:.....	9
Automatic Activation.....	10
VuLink Specifications	10
Available Video Management Options.....	11
VuVault.com Cloud	11
VuVault.com Unlimited Storage Cloud Plans.....	13
VuVault Local Software.....	14
Specifications for VuVault.com and VuVault.....	15
Product Support Information	16
Training	16
Warranty	16

Digital Ally, Inc. | Company Information

Corporate Headquarters Location

Digital Ally, Inc.

9705 Loiret Boulevard

Lenexa, KS 66219

w: www.digitalallyinc.com

p: 913.814.7774

toll free: 800.440.4947

f: 913.814.7775

Corporation Information

Digital Ally is a publicly held corporation traded under the symbol “DGLY”. We were incorporated in the State of Nevada on December 13, 2000. Digital Ally is overseen by a board of directors and Stanton E. Ross currently sits as the Chairman and CEO. Our company manufactures reliable, rugged, easy-to-use Body and In-Car Camera Systems for law enforcement agencies, security agencies, EMS, commercial fleets, and educational institutions.

Contact Information

Pennsylvania Sales Manager

John Saunders

p: 913.232.5348

e: John.Saunders@digitalallyinc.com

Regional Sales Director

Jeff Milligan

p: 913.814.7774

e: Jeff.Milligan@digitalallyinc.com

Bid Proposal Contact

Nicole Leiker, Bid Specialist

p: 913.814.7774

e: bids@digitalallyinc.com



Company Qualifications

Digital Ally, Inc. is committed to providing law enforcement, security agencies, EMS, commercial fleets, and educational institutions with the highest quality technology to assist in capturing digital evidence. As an industry-leader, Digital Ally designs feature-rich products that are rugged, durable and reliable. Agencies from all 50 States and more than 90 other countries rely on our products every day.

Digital Ally was established in 2004 and revolutionized mobile video by introducing a complete In-Car Camera System integrated into a rear-view mirror. This design provides a more efficient use of space in vehicles, as well as providing a user-friendly system that can be positioned so it is not distracting to users. Our In-Car Camera Systems have high quality video ranging from Enhanced D1 Resolution to full 1080p HD Resolution.

Since the introduction of our series of In-Car Camera Systems, we have expanded our product offering to include the FirstVu HD line of Body Cameras and the patented VuLink automatic activation unit. VuLink enables the automatic activation of your In-Car Camera, wireless Microphone, and Body Camera. The FirstVu HD brings all the advantages of an In-Car Camera system to the shirt pocket of every officer. It is small and lightweight, easy to operate, and allows officers to record high quality video in full 720P HD.

Digital Ally, Inc. has also developed both a dynamic, comprehensible cloud –based solution and a back office software solution for easy management, review, and archiving of recorded evidence. New products are always in the pipeline to enable our customers to stay up to date with the latest in technology.

Digital Ally's sole business is dedicated to designing, manufacturing, and selling quality leading-edge digital video systems and related products. We understand the work, dedication, and commitment it takes to provide agencies of all sizes with Digital In-Car and Body Camera solutions.

All of the video systems designed by Digital Ally, Inc. offer many important benefits such as:

- Being fully-automatic
- Simple to operate
- Enhancing officer safety
- Reducing liability
- Capturing irrefutable evidence
- A total design and support solution

Headquartered in Lenexa, Kansas, Digital Ally, Inc. is publicly traded on the NASDAQ Capital Market under symbol DGLY. We have been awarded several cooperative and statewide contracts that include GSA, NPPGov, HGACBuy, TX-DIR, MiDEAL, PA COSTARS, Purchasing Cooperative of America, and more.

With new, innovative products being designed constantly, Digital Ally, Inc. strives to offer customers the solutions they need to capture the truth in situations where it matters the most.

Introducing the FirstVu HD Body Camera



FirstVu HD

TWO-PIECE SOLUTION

FirstVu HD



The FirstVu HD two-piece model can be mounted on a variety of locations on the officer via the Klick-Fast mounting system, small or large clips, buttons, magnets, Velcro, rail and options for the lapel and tactical helmet.

Mounting Locations:

Chest



Shoulder



Lapel



Helmet



HIGH DEFINITION VIDEO & AUDIO

720p Resolution with 130° field of view

The camera captures exactly what the officer sees during the incident. HD Audio recording built into the camera.



Included with Purchase

- FirstVu HD DVR
Standard Battery Version or Extended Battery Version
- FirstVu HD Camera
11 inch cable or 48 inch cable
- Camera Cable Clamp
- Standard Battery or Extended Battery
- Battery Charger
- AC Outlet Adapter for Battery Charger
- DC Car Adapter for Battery Charger
- Charge/Data Cable
- Standard Fabric Clip Mount
- Velcro Mount
- Button Mount
- Wedge Mount Kit
- Reference User Guide



Item	Qty	Description
1	1	FirstVu HD Camera
2	1	FirstVu HD DVR
3	2	Cable, USB 2.0 Type A to Mini-B
4	1	Velcro Mount
5	1	Fabric Clip
6	1	Quick Reference Guide
7	1	Button Mount
8	1	Home Charger
9	1	Car Charger
10	2	FirstVu HD Battery
11	1	Battery Charger
12	1	Wedge Kit

Optional Accessories:

- Adjustable Mount Kit
- Spring Visor Clip
- Magnet Mount
- Motorcycle Mount Kit
- Car Mount Kit
- Head Mount Kit
- KlickFast Mount Adapter Kit
- Belt Mount Kit
- Belt Loop Holster
- Nylon Pouch
- VuLink Wireless Body Camera and In-Car Camera Link (Automatic Activation)
- FirstVu HD Docking Station

Upload Methods and Docking Stations

Docking Stations

Body Camera footage can be uploaded via USB or by using one of our Docking Stations. Choose from our 12-unit “Smart Dock” or our one-unit Mini-Dock.



12-Unit Dock
(Station Headquarters)



Mini-Dock
(Office/Desk/Home-Use/Cloud Only)



INDUSTRY’S ONLY “SMART DOCK”

Secure Timely Transfer | “Plug & Play”

Our 12-Unit Smart Docking Station has a 500GB Local Memory hard drive that allows for a faster transfer of data to local or cloud software storage. This unit also can simultaneously upload 4 hours per 12 FirstVu HD cameras within a 15-minute shift change. All of this while charging units and making updates to any configuration needed for your devices.

Dock Uploads

Upload methods include a Mini-Dock and 12-bay Docking Station for either the standard battery or extended battery

- Extended Battery Dock:
Charge the extended battery and offload video by dropping the DVR into the Docking Station
- Standard Battery Dock:
Charge both the standard batteries and offload video by dropping the DVR into the Docking Station
- Mini-Dock:
Provides all the benefits of the docking station, in a compact, single user design

Manual Uploads (with VuVault Software only)

- USB port to a computer station
 - FirstVu HD can be placed in secure mode so that it only uploads to certain IP addresses
 - Secure mode restricts access to metadata and recorded video files

Specifications for Body Camera Solution

FirstVu HD Specifications:

Video Resolution	720p (1280x720) or VGA (640x480)
Field of view	Horizontal: 95°, Vertical: 80°, Diagonal: 130°
Low Light Sensitivity	0.08 Lux (minimum); Fixed focus lens
Pre-Event Buffer	60 seconds video & audio; adjustable in one second increments
Internal Memory	32 GB secure internal memory
Encryption	H.264 codec with configurable quality settings
Secure Media Access	May be configured so only designated computers can access recordings
Covert Mode	Deactivates LEDs (vibrating confirmations and LEDs remain off)
Connection	Mini-USB for uploading recordings and charging (Docking Station optional)
Weather Rating	general water rating that is IP56 equivalent
Humidity	10 -90% RH, non-condensing. IP56 water resistant camera head
Operating Temperature	-20° to +70° C
Storage Temperature	-40° to +80° C
Weight	Camera and Cable = 0.8 oz
	Body (DVR) = 3.1 oz
Dimensions	2 5/8"(w) x 4"(h) x 5/8"(d) (Main Recorder)
	1 1/8"(w) x 1 1/2"(h) x 1.0"(d) (Camera Module)
Battery	3.7vDC 2,200mAh, Rechargeable Lithium Ion Polymer Battery, field replaceable
Quality Settings	Eight different HD or SD Quality and Frames per Second configurations
Record Time	16 hours in HD (High Quality Setting)
	54 hours in SD (Lowest Quality Setting)
Videos	Records non-proprietary AVI Videos
Metadata	Saves Date, Time Stamp, and Marks
Extended Battery	up to 16 hours Standby (or up to 96 hours with no activity)
	up to 9 hours continuous record time with pre-event enabled
Standard Battery (2 included with each FirstVu HD purchase)	up to 12 hours Standby each (or up to 48 hours each with no activity)
	up to 9 hours with both batteries (4.5 hours each) continuous record with pre-event enabled
Microphone	Internal (max. input SPL 110dB, sensitivity -42dBV)
Audio	Mono, may be muted by user Multiple configuration options
GPS	Tag GPS location during playback through VuVault GO
Made Where	Assembled in USA. Internals built in Kansas
Cloud Warranty	Advanced Exchange Warranty on hardware for full term of contract
Local Warranty	1-year Advanced Exchange included at no cost

Docking Station Specifications:

Power	
OPERATING VOLTAGE	12 VDC, $\pm 10\%$
POWER CONSUMPTION	9.6W – 24.96W
POWER ADAPTER 1	AC to DC, 12VDC / 5 A
POWER ADAPTER 2	AC to DC, 12VDC / 7.5 A
MINIMUM POWER INPUT	12 VDC, 4 A
Environmental/Mechanical	
OPERATING TEMPERATURE	-20° to +60° C
STORAGE TEMPERATURE	-40° to +85° C
RELATIVE HUMIDITY	95% @ 40° C (non-condensing)UL, CCC, BSMI
SAFETY CERTIFICATIONS	UL, CCC, BSMI
DIMENSIONS	34.6cm (13.5in.) (L) x 36.5cm (14.3in.) (W) x 15.8cm (6.3in.) (H)
WEIGHT	6.12kg (13.5 lbs)
Network	
NETWORK INTERFACE	6.12kg (13.5 lbs)
DATA TRANSFER RATE	Average >8MB/s per device upload to docking station. Up to 1GB/s from docking station to server.



Automatic Activation

VuLink: Patented Automatic Activation

Digital Ally's VuLink was the first product on the market to fully integrate in-car cameras and body worn video. The patented technology behind VuLink enables wireless automatic activation of your In-Car Camera, Wireless Microphone, and Body Camera.

VuLink Technology Features:

- View all related video feeds at the same time: Video from both your In-Car and Body Camera will sync
- Hands Free: Automatically activates Body Camera and In-Car Camera Systems
- Eliminates Distractions: Reduce incidents of user-error and the need to continuously record

Most Common VuLink Triggers:

- Emergency Lights
- G-Force or Impact Events
- Vehicle Speed
- In-Car Camera System
- Gun Lock
- Seat Belt
- Emergency Radio Switch
- Motorcycle Kickstand
- Motorcycle Handle Bar Switch
- Trunk Latch
- Fire Suppression Systems
- Doors
- GPS Zones (with In-Car Camera System)
- 12 Volt Relay



VuLink Specifications

OPERATING VOLTAGE	8-30VDC
CURRENT DRAW	250mA Maximum
MAX TRANSMIT POWER	10dBm
TRANSMIT RANGE	50ft typical
WEIGHT	55.4g (0.12 lbs.)
OPERATING TEMPERATURE	-30° to +60° C
STORAGE TEMPERATURE	-40° to +80° C
DIMENSIONS	23mm (0.9in.)(D) x 91mm (3.6in.)(W) x 61mm (2.4in.)(H)

Available Video Management Options



VuVault.com | Cloud

We at Digital Ally know how important security and flexibility are to our customers. Through proprietary hash algorithms, geographically redundant servers, and Amazon's high security standards, Digital Ally has created an evidence management and video storage solution that is extremely secure and follows CJIS standards. Our solution, VuVault.com is not only secure, it is also completely scalable so that you can adjust to incoming and outgoing officers as needed.

Overview

VuVault.com is built on the Amazon Web Services (AWS) Region application platform with a "security first" approach. The main components of the application are isolated and accessible only from the approved IP address of our portal server. User authentication and access to user data and digital media is granted solely through the portal server. Utilizing strong SSL, all web requests to the portal server and returned content are encrypted. Session-based, always changing encryption is in place for all HTML transactions and application content further obscuring any data patterns. All user and digital media activity is logged and scrutinized for malicious intent and a series of checks and balances is used to prevent unwanted activity within an account.

Customer data is isolated within our application database with steps taken at each page request to guarantee customers gain access only to their data.

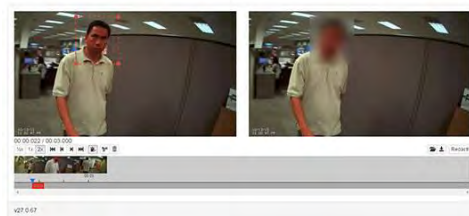


Manage Video and Cases

VuVault.com eases the burden of managing videos. There are several standard search criteria already implemented into the system, along with customizable search criteria to make finding recordings fast and easy. With case management implemented into the standard operating system, putting together case files has never been easier. Case management allows you to link all associated videos, documents, and files from your FirstVu HD and alternate outside sources into one complete case file within VuVault.com.

Redaction

Utilize our integrated redaction technology to quickly and easily redact videos. The system has intuitive automatic face suggestions as well as manual redaction capabilities. Faces, signs, license plates, shirts and other objects can all be redacted quickly and easily. Once complete the redacted video can be downloaded or shared with other users.



API Support

Digital Ally has an Application Program Interface (API) that can be utilized to connect to other vendor software. We would have to create a service contract and determine the development time needed to integrate our system with the existing systems. Digital Ally will work with the Department to determine exactly which features and information need to integrate with our systems.

Cloud Share

VuVault.com includes an extensive, secure and flexible share portal to facilitate convenient sharing of video evidence and case files with designated and credentialed third parties. This functionality can be used on a one-off basis by the issuance of one time credentials, or can be configured to allow regular and continued access by known and trusted third parties (i.e. the prosecutor and staff). These third parties will have the option, if given privileges per share, to review and/or download files in native format to solid state memory. A proprietary player is not needed to review video after it is downloaded.

Environmental Security Features

Amazon Web Services (AWS) data centers utilize innovative architectural and engineering approaches. Each data center is equipped with fire detection and suppression, power failure back-ups climate and temperature controls, and electrical and mechanical management. When a storage device reaches its end of life security measures are taken by Amazon to ensure that data is not exposed to unauthorized individuals. Amazon security platforms also host around the clock surveillance to ensure data locations are secure.

In case of failure, automated processes move data traffic away from the affected area to an alternate secure location. AWS is designed to tolerate system or hardware failures with minimal to no impact to users.

Disaster Recovery

Ensuring your data will always be protected and accessible is our number one priority; that is why we have built VuVault.com on the most trusted web service around. Amazon Web Services supplies three locations separated on the east and west coasts where all of your data will be copied and 100% secured. If one of the locations is wiped out by a natural disaster, your information will still be secured in two alternate locations states away. Any and all of the information that was flowing to that particular location will be directed to substitute locations.

VuVault.com Unlimited Storage Cloud Plans

Digital Ally has the following unlimited storage cloud plans to choose from for the FirstVu HD Body Camera:

1) VuVault.com Ultimate Plan and Body Camera Solution

Includes:

- 1-Year Unlimited Data Storage
- 1-year, 3-year, and 5-year contract plans available
 - 3 or 5-year contract includes body camera at no cost
 - 1-year contract includes 50% discount on FirstVu HD Body Camera
- Full Software Access, Redaction, Case Management, Share Portal
- Advanced Exchange Warranty on hardware for full term of contract

2) VuVault.com Pro Plan and Body Camera Solution

Includes:

- 180-day Unlimited Data Storage
- 1-year, 3-year, and 5-year contract plans available
 - 5-year contract includes 83% discount on FirstVu HD Body Camera
 - 3-year contract includes 66% discount on FirstVu HD Body Camera
 - 1-year contract includes 39% discount on FirstVu HD Body Camera
- Full Software Access, Redaction, Case Management, Share Portal
- Advanced Exchange Warranty on hardware for full term of contract

3) VuVault.com Basic Plan and Body Camera Solution

Includes:

- 90-day Unlimited Data Storage
- 1-year, 3-year, and 5-year contract plans available
 - 5-year contract includes 83% discount on FirstVu HD Body Camera
 - 3-year contract includes 66% discount on FirstVu HD Body Camera
 - 1-year contract includes 33% discount on FirstVu HD Body Camera
- Full Software Access, Redaction, Case Management, Share Portal
- Advanced Exchange Warranty on hardware for full term of contract

Cloud Drive

After the retention period expires, evidence can be transferred to the Cloud Drive for long-term storage. Cloud Drive is available in blocks of 100GB. An unlimited amount of 100GB blocks of Cloud Drive can be purchased at any time. Video that is placed in the Cloud Drive still retains the full cloud functionality available from VuVault.com. This includes redaction and the availability of all metadata.



Digital Ally recordings can be easily archived to DVD, Hard Drive, Tapes, Etc. through the user friendly VuVault Software console. The VuVault™ back office software suite enables law enforcement agencies to quickly and easily manage their digital video evidence across all of Digital Ally's products. VuVault™ is utilized for playing back, downloading, archiving, reviewing, unit configuration and management, running customizable reports and chain of custody logs as well as exporting/burning videos to DVD's for court.



With VuVault, you can also purchase the level of software that will best suit your agency. VuVault comes in Standalone, Server, and Enterprise level software options. VuVault Server and VuVault Enterprise level software come with unlimited workstation licenses.

Device and User Management

Manage all of your Digital Ally™ devices and groups through once simple back office software. VuVault administrators can configure and assign devices, set retention policies and control user and group permissions all through VuVault™

Video Evidence Reporting

Creates reports on just about anything. At the touch of a button will allow you to instantly know which officers have or haven't uploaded videos recently, identify high crime areas, and generate chain of custody reports for court. VuVault gives you the flexibility and functionality you need in a video management system.

Chain of Custody Reporting

Ensures that the exact video that was uploaded into the system is the video that is being shown to the attorneys and used in court. The original video file remains unaltered despite any notes, marks or segmentation that an officer might make to the video.

Active Directory Login

VuVault leverages Microsoft Active Directory for managing system security access and authentication. With Active Directory integration enabled, users will not need to login to VuVault once their username has been associated with an active directory group. All associated permissions for the group will be assigned automatically when logging in making VuVault incredibly easy to deploy across an agency utilizing a Microsoft server environment

Cloud Share (Optional)

Cloud Share Licenses for VuVault are available for purchase and include redaction, a portal to share video, and case management. The Share Portal is an extensive, secure and flexible portal to facilitate convenient sharing of video evidence and case files with designated and credentialed third parties. This functionality can be used on a one-off basis by the issuance of one time credentials, or can be configured to allow regular and continued access by known and trusted third parties (i.e. the prosecutor and staff). These third parties will have the option, if given privileges per share, to review and/or download files in native format to solid state memory. A proprietary player is not needed to review video after it is downloaded.

Specifications for VuVault.com and VuVault

VuVault.com Cloud Specifications

- VuVault.com cloud runs on a Virtual Machine (VM) environment and does not use a traditional SQL database.
- Local server is not required. All data will be stored in the cloud at Amazon Web Services
- Can be accessed on any computer with a modern Internet browser and a VuVault.com account.
- Amazon Web Services has a system uptime of 99.95%.

VuVault Software Specifications

- Server license
- Client license
- SQL
- Full version of VuVault required for more than 200 systems (SQL custom quote available upon request)
- Client unlimited license

VuVault Minimum Specifications

Processor	Intel® Dual Core Processor (2.00 GHz or better)
Operating System	Windows 7 or newer
Memory	4 GB
OS Hard Drive	40GB Free Space
Optical Drive	DVD+/-RW or Blu-ray Writer
Video Card	Intel® HD4000 chipset or comparable
Network Card	100 Mb Ethernet
Card Reader	USB 2.0 Card Reader

VuVault Recommended Specifications

Processor	Intel® Quad Core Processor (3.0GHz or better)
Operating System	Windows 7 or newer
Memory	8 GB or Greater (Note: >4GB of RAM will require a 64-bit OS)
OS Hard Drive	40GB Free Space
Optical Drive	DVD+/-RW or Blu-ray Writer
Video Card	Nvidia® GeForce 710M or comparable
Network Card	Gigabit Ethernet
Card Reader	USB 3.0 Card Reader

Product Support Information

Digital Ally has full-time Product Support Specialists at our corporate office in Lenexa, Kansas. Each Product Support Specialist is factory-trained on all aspects of Digital Ally's products. Our specialists also do the final testing of all software upgrades, write and upgrade manuals, etc. so they are always up to date on our latest releases.

We have Product Support Specialists on staff via telephone and email and will provide on-site assistance if necessary (additional fees may apply). At this time, our office hours are 8:00 to 5:00 Monday through Friday, Central Time Zone. Our approach to user support is simply this; do whatever is necessary to fix the problem and make the customer satisfied as quickly and efficiently as possible.

Training

Our approach to training is that it is vital to ensure that the customer understands the operation of our system and is able to fully utilize all the features available. We have also found that well trained users have much fewer problems than users who have not been trained properly. We are prepared to take whatever steps necessary to train every user, both at the time of delivery and as needed in the future.

Training will include hands-on training, quick reference guides, instructional videos available for replay, and detailed operating guides. Training will cover hardware, video management application, and software or cloud storage.

Training will be divided between end users and supervisors/administrators. Multiple sessions can be scheduled to accommodate group size and various shifts. End user training will be in a train-the-trainer format for Department personnel that will be responsible for training others and those managing/administrating the program. Supervisor/Administrator training will be for those responsible for maintaining the devices and VuVault or VuVault.com.

Warranty

An Advanced Exchange Warranty is included with VuVault.com cloud for the full term of contract. Digital Ally provides a 1-year Advanced Exchange Warranty on the FirstVu HD system with the local VuVault Software solution. The Advanced Exchange Warranty includes any defects in materials or workmanship on all system components, as well as all software upgrades not requiring hardware revisions. Additional 1-year Advanced Exchange Warranties are available for purchase with the local VuVault Software solution. The Warranty period will begin from the date of invoice.

Digital Ally's "Advanced Exchange Program" is the most revolutionary Service Policy in the industry. During our Standard Warranty Period, if the hardware has a service issue, our Technical Support Department will diagnose the problem. If we determine the problem to be a hardware issue, Digital Ally will send you a replacement module to fix the problem. Shipments reach most within 2 business days to keep down time to a minimum.

VuSchools Body Camera System

For School Resource Officers and Educators



Digital-Ally™

9705 Loiret Blvd. | Lenexa, KS 66219
800.440.4947 | 913.814.7774 | digitalallyinc.com

Table of Contents

Digital Ally, Inc. | Company Information3

Corporate Headquarters Location.....3

Corporation Information3

Contact Information.....3

Introducing the VuSchools Wall-Mount/Body Camera Solution.....4

Included with the VuSchools Body Camera System4

FirstVu HD Body Camera Specifications.....5

FirstVu HD Controls6

Cloud Software Solution7

About Amazon Web Services8

Product Support.....9

Training.....9

Warranty and Maintenance9

Digital Ally, Inc. | Company Information

Corporate Headquarters Location

Digital Ally, Inc.

9705 Loiret Boulevard

Lenexa, KS 66219

w: www.digitalallyinc.com

p: 913.814.7774

toll free: 800.440.4947

f: 913.814.7775

Corporation Information

Digital Ally is a publicly held corporation traded under the symbol “DGLY”. We were incorporated in the State of Nevada on December 13, 2000. Digital Ally is overseen by a board of directors and Stanton E. Ross currently sits as the Chairman and CEO. Our company manufactures reliable, rugged, easy to use body worn and in-car video recording systems for law enforcement agencies.

Contact Information

VuSchools Regional Sales Manager

Kevin Richard

p: 913.274.2501

e: Kevin.Richard@digitalallyinc.com

Bid Specialist

Nicole Leiker

p: 913.814.7774

e: bids@digitalallyinc.com

Introducing the VuSchools Wall-Mount/Body Camera Solution

VuSchools is a secure cloud-based video management system paired with Digital Ally's simple to operate, reliable, high definition body cameras. The FirstVu HD Wall-Mount/Body Camera Solution for School Resource Officers and educators is based on our successful FirstVu HD Body Camera for Law Enforcement. The versatile design of the camera module allows it to adapt to a solution specifically for School Resource Officers and educators.

Digital Ally understands that an unobtrusive solution, both in physical appearance and work load is a huge concern. The FirstVu HD is impact and weather resistant and utilizes secure, internal solid state memory. It includes multiple mounting locations with options for a lanyard, belt mount, and classroom wall mount for a wide view of the whole classroom. The unit is small and lightweight, weighing less than 4 ounces. The system is always on, allowing the educator or School Resource Office to perform their job, and not have the focus on the camera. The Docking Station is fully automatic, charging the battery, and uploading data to the VuSchools Cloud Portal.

Stable and tough, the solid state secure memory in the FirstVu HD is unaffected by violent motion. The simplistic design of the FirstVu HD solution puts cameras in the classroom in a safe and uncomplicated way.



Two-Piece Model with Mini-Dock

Included with the VuSchools Body Camera System

- VuSchools FirstVu HD Body Camera Kit
 - Choice between one-piece lanyard style model or two-piece model
 - 720x480 pixels video resolution
 - Audio
 - Robust form factor
 - 8 hours record time
 - Start/Stop Record Button
 - Charges overnight while offloading video
- Mini-Dock charging and downloading dock
 - View Video Feed
 - Add Notes
 - Playback recorded video
 - View storage and battery life
 - Securely Offloads Videos
 - Charges FirstVu HD camera
 - Secure Encrypted Connection



One-Piece Model



Mini-Dock

- Easy Setup
- One FirstVu HD per Mini Dock
 - Operations:
 - Apply A.C. Power
 - Connect Ethernet cable to network
 - Offload and charges FirstVu HD overnight – typically 8 hours max
- Belt Clip Mount, Lanyard Kit, Pouch, and/or Wall Mount Kit
 - The FirstVu HD one-piece model includes a lanyard style mount, magnet mount, or belt clip mount.
 - The FirstVu HD two-piece model includes a belt clip mount, lanyard style mount, or magnet mount.
 - Both the one-piece and two-piece model can be mounted on a wall with the included Wall Mount Kit
 - Both the one-piece and two-piece model can be stored in the included pouch
- VuSchools Website Service & Cloud Storage License
- VuSchools Program Turnkey Solution & Professional Services-Configuration, Set-Up, and Training
- VuSchools Program Hardware & Software Maintenance Agreement



FirstVu HD Body Camera Specifications

Camera Module	1 1/8" (w) x 1 1/2" (h) x 1.0" (d)
Main Recorder	2 5/8" (w) x 4" (h) x 5/8" (d)
Weight	3.9 oz.
Battery	Rechargeable, lithium polymer battery
Resolution	720p HD Video: 1280 x 720 .08 Lux low light/no light recording
Battery Life	8 hours consistent record time
Memory	32GB of secure, internal, solid state memory
Field of View	H = 95° V = 80° D = 130°
Encryption	H.264 Codec & Configurable Quality Settings
Rating	IPX5
Connection	Mini-USB for uploading recordings and charging
Metadata	Saves Date/Time Stamp & Marks
Pre-Records	30-sec. pre-event recording

FirstVu HD Controls

The FirstVu HD System is simple to operate. Once the DVR is turned on, the unit automatically starts pre-event recording, always capturing the last 30 seconds prior to the record button being pressed. It will only stop recording when the record button is pressed and held for approximately three seconds. Audio is always captured during pre-event and the recording. At the end of the day the FirstVu HD is docked in the included Mini-Dock, where it will automatically offload data, and charge the battery.

System Administrators can request video events from the VuSchools.com cloud portal. Each video event sends and catalogs metadata to the VuSchools.com cloud portal. Video can be reviewed and requested to be sent from the Mini-Dock to the VuSchools cloud portal on demand. If a video is not requested, it is kept for seven days. If a video is requested and uploaded to the VuSchools cloud portal, it will be kept for 30 days for review.





Cloud Software Solution

The VuSchools Cloud Portal enables educators and School Resource Officers to quickly and easily manage their digital video events. VuSchools.com is utilized for playing back video, downloading, reviewing, unit configuration and management, running customizable reports and chain of custody logs, as well as sharing portal to securely share videos with third parties.

With VuSchools.com, all cameras can simply and securely be managed. VuSchools.com includes the ability to manage video events and access the system district-wide with ease. VuSchools is built on the same Amazon Web Services platform Digital Ally uses for our Law Enforcement and Commercial customers.



Features

- Manage - View, share, and manage your digital content from any internet browser.
- Secure - All video evidence is backed up and stored securely on the cloud (Amazon Web Services).
- Easy - Automatically upload your videos straight to the cloud via the Mini-Dock.
- Accessible - Review video from anywhere you are connected to the internet.
- Smart Storyboard - Find your videos more easily from the search results.
- Universal Tagging System
- Basic Incident Management - Import documents, PDFs, and other video media into VuSchools.com
- Video Sharing - Securely share videos with third parties by way of email while maintaining chain of custody

Device & User Management

Each issued device will be connected to your VuSchools account. Simple setup by an Administrator allows for a highly capable rollout of the FirstVu HD System. Each FirstVu HD Body Camera and Mini-Dock will be assigned to an educator and/or School Resource Office to allow for easy backend management of all devices.

Chain of Custody Reporting

The exact video that is upload into the VuSchools.com cloud portal will be the same video that is viewed by an Administrator. The original video file will remain unaltered despite any notes, segmentation, or redaction that might take place. Full activity is tracked with chain of custody reporting.

Incident Management

Incident Management allows the importing of any other electronic document pertinent to the video event. This includes PDFs, Word, Pictures, etc.

About Amazon Web Services

VuSchools, is built on Amazon Web Services (AWS) Region application platform with a security first approach. The main components of the application are isolated and accessible only from the approved IP address of our portal server. User authentication and access to user data and digital media is granted solely through the portal server. Utilizing strong SSL, all web requests to the portal server and returned content are encrypted. Session-based and always changing encryption is in place for all HTML transactions and application content, further obscuring any data patterns. All user and digital media activity is logged and scrutinized for malicious intent, and a series of checks and balances is used to prevent unwanted activity within an account.

Customer data is isolated within our application database with steps taken at each page request to guarantee customers gain access only to their data.

Manage Video

VuSchools.com eases the burden of managing videos. There are several standard search criteria implemented into the system, along with customizable search criteria to make finding recordings fast and easy.

Redaction

VuSchools.com features a nearly automated redaction feature. This feature allows an Administrator to redact faces and facial features so that the video can be released as needed by the Administration. VuSchools.com also features an intuitive manual redaction tool, which allows for the redaction of audio, t-shirts, and other items as needed.

Upload Process

Uploading recordings into VuSchools.com is an easy process. Connect the FirstVu HD to the Mini-Dock with the supplied USB cable. The recorded videos will automatically upload to the Mini-Dock and will remain on the Mini-Dock until requested. All metadata will immediately upload to VuSchools.com for reporting and chain of custody purposes. Video can be reviewed and requested to be sent from the Mini-Dock to the VuSchools cloud portal on demand. If a video is not requested, it is kept for seven days. If a video is requested and uploaded to VuSchools.com, it is kept for 30 days for review. This method allows for a highly scalable solution and keeps network bandwidth to a minimum.

Environmental Security Features

Amazon Web Services (AWS) data centers utilize innovative architectural and engineering approaches. Each data center is equipped with fire detection and suppression, power failure back-ups, climate and temperature controls, and electrical and mechanical management. When a storage device reaches its end-of-life, security measures are taken by AWS to ensure that data is not exposed to unauthorized individuals. AWS security platforms also host around-the-clock surveillance to ensure data locations are secure.

In case of failure, automated processes move data traffic away from the affected area to an alternate secure location. AWS is designed to tolerate system or hardware failures with minimal to no impact to users.

Disaster Recovery

Ensuring your data will always be protected and accessible is our number one priority. This is why we have built VuSchools.com on the most trusted web service around. Amazon Web Services supplies three locations separated on the east and west coasts where all of your data will be copied and 100% secured. If one of the locations is wiped out by a natural disaster, your information will still be secured in two alternate locations states away. Any and all of the information that was streaming to that particular location will be directed to substitute locations.

Product Support

Product Support Information

Digital Ally has full-time Product Support Specialists at our corporate office in Lenexa, Kansas. Each Product Support Specialist is factory-trained on all aspects of Digital Ally's products. Our specialists also do the final testing of all software upgrades, write and upgrade manuals, etc. so they are always up to date on our latest releases.

We have Product Support Specialists on staff via telephone and email and will provide on-site assistance if necessary (additional fees may apply). At this time, our office hours are 8:00 to 5:00 Monday through Friday, Central Time Zone. Our approach to user support is simply this; do whatever is necessary to fix the problem and make the customer satisfied as quickly and efficiently as possible.

Training

Our approach to training is that it is vital to ensure that the customer understands the operation of our system and is able to fully utilize all the features available. We have also found that well trained users have much fewer problems than users who have not been trained properly. We are prepared to take whatever steps necessary to train every user, both at the time of delivery and as needed in the future.

Training will include hands-on training, quick reference guides, instructional videos available for replay, and detailed operating guides. Training will cover hardware, the video management application, and software or cloud storage.

Training will be divided between end users and supervisors/administrators. Multiple sessions can be scheduled to accommodate group size and various shifts. End user training will include train-the-trainer format for personnel that will be responsible for training others and those managing/administrating the program.

Supervisor/Administrator training will be for those responsible for maintaining the devices and VuSchools.com.

Warranty and Maintenance

Digital Ally provides a full warranty on the FirstVu HD hardware throughout the term of the contract. The warranty includes any defects in materials or workmanship on all system components as well as all software upgrades not requiring hardware revisions. The FirstVu HD System is a completely solid state device that does not require any scheduled maintenance. The warranty period will begin from the date of shipment.



Proposal for Police Body Worn Cameras

Pennsylvania Chiefs of Police Association



Pennsylvania
Chiefs of Police Association

Submitted by
WatchGuard, Inc.



WatchGuard, Inc.
415 E. Exchange Parkway, Allen, TX 75002
1.800.605.MPEG (6734)
www.watchguardvideo.com



25th of January 2019

Christopher J. Braun M.S. IT
Technology Coordinator Pennsylvania Chiefs of Police Association
3905 N. Front Street
Harrisburg, PA 17110

Reference: RFI: Police Body Worn Cameras

WatchGuard has designed and engineered a complete video solution from the ground up that completely integrates the VISTA wearable camera with the Evidence Library software. This development effort was focused on addressing and correcting a lot of issues typically associated with wearable camera deployments as well as adding innovated features and capabilities to improve quality and user experience.

VISTA sets new standards in ruggedness, overall performance, and ease of use. Unlike nearly every competing system, VISTA is constructed with industrial grade components and is manufactured in the U.S.A. It is capable of recording both High Definition and Standard Definition video, and is able to record up to 12 hours of continuous HD video.

EvidenceLibrary.com is a fully cloud hosted back office solution allowing an agency to have the application and all video storage in the cloud. EvidenceLibrary.com utilizes Microsoft Azure Government, which is an isolated version of Azure that is exclusively used by US Government Agencies and qualified vendors.

Evidence Library 4 (EL4) is an enterprise class server application supporting client connections and video sharing and a host of other features. EL4 sets a new standard for back-end capability and ease of use.

Respectfully Submitted,

Troy Montgomery
Vice President of Sales



Contact Information:

Point of Contact

Kyrié Endres, Proposal Manager

(214) 785-2608 - Direct

bids@watchguardvideo.com - Email

Company

WatchGuard, Inc.

415 E. Exchange Parkway

Allen, TX 75002-2616

(800) 605-6734 – Toll Free

(972) 423-9777 – Main

(214) 383-9661 – Fax



Table of Contents

Company Profile_____	1
Response_____	5
Body Worn Camera Solution_____	7
Pricing_____	35

COMPANY PROFILE

WatchGuard's mission is to produce the industry's best video evidence solutions for law enforcement agencies worldwide. We strive to achieve our goal and drive ROI for our customer's investment thru innovative product designs and by using the highest quality materials. We insist on excellence in all we do, leading to superior performance in our products and services.

-Steve Coffman, President

INTRODUCTION

WatchGuard was founded in 2002 and began full production of its mobile video products in September of 2005, with initial shipments beginning in October 2005. All product manufacturing is done domestically in the company's 144,000 square foot facility in Allen, Texas. The North Texas facility features an engineering laboratory, customer service installation bay, pristine production space, and a state-of-the-art training room. All engineering, assembly, and factory service is conducted in this facility.



Company Background

WatchGuard is the world's largest manufacturer of video systems for law enforcement, providing systems to over one third of all U.S. and Canadian law enforcement agencies. In the most recent industry survey by IHS, WatchGuard was again recognized by this independent research organization as the worldwide market share leader in mobile video surveillance systems.

We currently have approximately 6,500 law enforcement agencies as customers and over 77,000 of our mobile DVR systems in the field. WatchGuard has moved solidly into the number one market share position for US sales of digital police in-car video systems.

WatchGuard's commitment to innovation can be seen in the large investments we make in the Research and Development of new products. We have the largest engineering team in the industry, and have invested over \$66 million into the development of digital video systems for law enforcement. We feel that innovation of quality and technically advanced products is essential to maintaining our position in this fast paced and rapidly evolving industry.

WatchGuard produces the most advanced systems, has the most extensive track record of successful deployments, has earned a reputation for extraordinary customer support, is financially sound, and is the best positioned company to service your video needs today and for many years into the future.

The Industry's Most Significant Products

WatchGuard has been pioneering technological innovations since its inception in 2002. Over its history, WatchGuard has been first to market with many technology breakthroughs including (1) the industry's first and only completely integrated and synchronized in-car and body worn system, (2) the industry's first HD in-car video system, (3) Record-After-the-Fact functionality, (4) multiple resolution recording and (5) the industry's first direct-to-DVD in-car video system.

WatchGuard's product strategy revolves around providing premium hardware with functionality that can only be performed in hardware (versus software solutions) and video management solutions that achieve automation through integration. Our hardware roadmap includes further reduction in the size and weight of our body worn camera, continued improvement in the audio and video quality of our already industry leading cameras and microphones, increasing product longevity through improved materials and construction thereby reducing total cost of ownership for our partner agencies, tight integration with most CAD/RMS vendors, further integration, feature improvements and ease of use for our redaction software, and development of next-gen platforms for our body worn, in-car offerings and video management software that take advantage of emerging AI technologies, speech recognition abilities and facial recognition technologies.

WatchGuard continues to invest heavily in projects that bring immediate value to our partner agencies. We have one of the largest and most prolific engineering groups in the industry, and are now investing in a new corporate headquarters facility that will bring additional engineering and production capacity to the company.



Advanced Engineering

Over the past decade, WatchGuard has become the most successful company in law enforcement video. By 2010, the company grew large enough to earn the #1 market share position. Since 2010, the company has continued to grow (80% growth just in the last 36 months) and is now approximately twice the size of the second largest manufacturer.

One of the primary reasons WatchGuard has become the dominant manufacturer of law enforcement video is because of our substantial investment in research and development.

WatchGuard employs the industry's largest engineering team and has invested over \$66Re million specifically into the development of video systems for law enforcement. Our major engineering investments have resulted in numerous technological breakthroughs and patents (14 issued, 19 pending) that have enabled us to demonstrate clear technological leadership and advance the state-of-the-art.

Our current 80+ person (and growing), senior level engineering team is comprised of a wide range of expertise and experience that includes:

- System architecture
- High reliability systems design
- Image processing
- Video encoding/decoding
- Audio encode/decode
- MPEG2/MPEG4/H.264
- High speed data processing
- High speed communication
- Digital signal processing
- FPGA/CPLD designs
- User interface design
- Kernel/driver development

- File system design
- Board design and layout
- Mechanical and industrial design
- Thermal analysis
- Rigorous system validation and testing.

This incredible amount of development horsepower is focused exclusively on the capture, management and integration of law enforcement video.

As a result, WatchGuard is uniquely positioned to offer Department a combination of hardware, evidence management software, and custom development capability that is far beyond any other manufacturer.

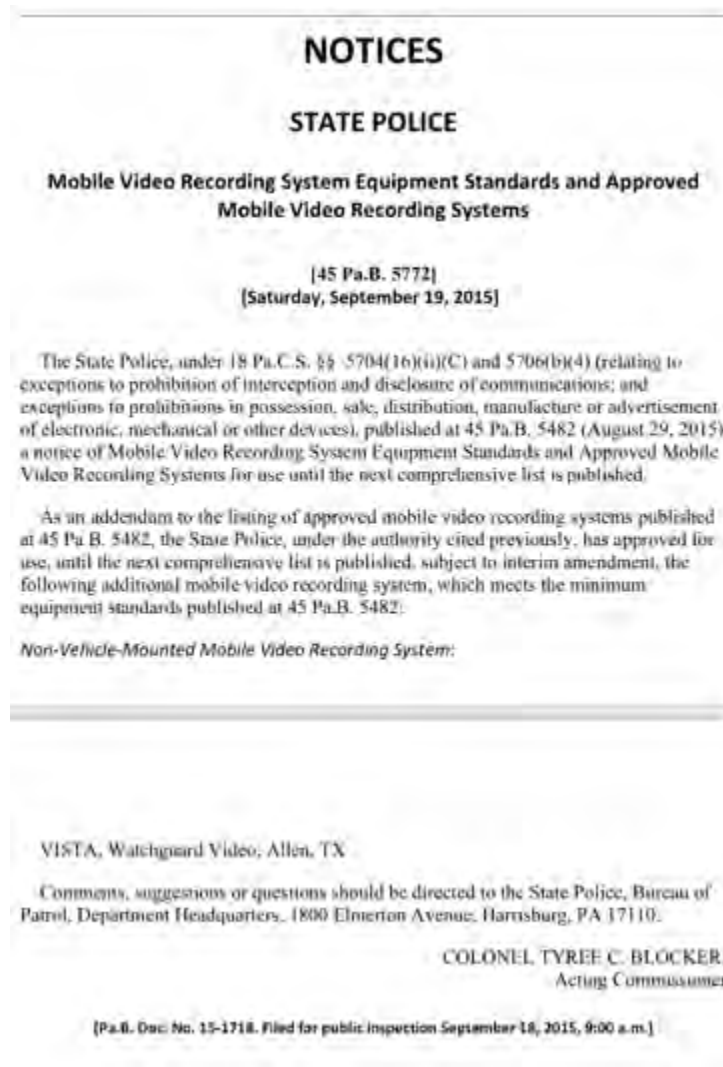
Manufactured in the U.S.A.

The company manufactures its products in its 144,000 square foot, state-of-the-art facility located in North Texas. This two story facility houses all departments including Engineering, Manufacturing, Sales, and Customer Service and it includes an impressive training room, customer installation bay, and pristine production space.

RESPONSE

How does your non-vehicle-mounted mobile video recording system and technology meet Pennsylvania's published requirements?

Our systems have been reviewed for compliance and meet the published requirements as stated below.



Have you submitted your non-vehicle-mounted mobile video recording systems to the Pennsylvania State Police for certification?

Yes.

Is your non-vehicle-mounted mobile video recording systems already certified by the Pennsylvania State Police?

Yes, we are currently under contract with the Pennsylvania State Police.

Are you offering a storage solution?

Yes. We are offering three different storage solutions, On-Premise, Hybrid, and Cloud, which are all outlined within our provided solution.

Will you offer storage solutions bundled (no line item distinction) with the cost of each camera purchased?

This option is negotiable, if desired.

How does your storage solution meet Pennsylvania's published requirements?

Each of the offered storage solutions has been designed to meet CJIS standards.

List the products or services that are already available on State Contract or PA CoStars.

Please see the attachments for our PA CoStars pricing and product listing.

Will you offer a discount of those prices if multiple police departments group together to buy your products and services?

We are open to negotiations.

SOLUTION DESCRIPTION

VISTA SOLUTION DESCRIPTION

Introduction

Over the past decade, WatchGuard Video has become the most successful company in law enforcement video. By 2010, the company grew large enough to earn the #1 market share position. Since 2010, the company has continued to grow (80% growth just in the last 36 months) and is now approximately twice the size of the second largest manufacturer.

One of the primary reasons WatchGuard Video has become the dominant manufacturer of law enforcement video is because we have invested substantially more money in research and development than any other company serving this industry. Our major engineering investments have resulted in numerous technological breakthroughs and patents (14 issued, 19 pending) that have enabled us to demonstrate clear technological leadership and advance the state-of-the-art.

Our current 80+ person, senior level engineering team is comprised electrical engineers, mechanical engineers, FPGA designers, embedded software developers, Windows software programmers, and test engineers. In addition, many of our engineers have Master level degrees or degrees in multiple disciplines (i.e. Electrical Engineering plus Computer Science).

This incredible amount of development horsepower is focused exclusively on the capture, management and integration of law enforcement video.

WatchGuard is uniquely positioned to offer Department a combination of hardware, evidence management software, and custom development capability that is far beyond any other manufacturer.

Because of the unique advantages offered by our In-Car Video products and some deficiencies in the wearable camera market, WatchGuard has spent the last three years developing the VISTA wearable camera. The goal was to incorporate some of the compelling advantages of our In-Car Video products while doing a ground up development of a wearable camera. The result is an ultra-rugged wearable camera with many first-of-a-kind features.

Since the camera itself is only part of the solution, WatchGuard did not stop there. The back-office software application is the piece that makes the cameras and the administration of the cameras and their respective video manageable. WatchGuard Video has designed and engineered a complete video server solution from the ground up that completely integrates the VISTA wearable camera with the 4RE In-Car cameras. The development effort was focused on addressing and correcting a



lot of issues typically associated with wearable camera deployments as well as adding innovative features and capabilities to improve the overall quality and user experience.

MULTIPLE CAMERA OPTIONS

The VISTA HD Wearable Camera is the system being proposed. WatchGuard engineered the VISTA solution and manufactures the product in the North Texas headquarters. VISTA is designed with complete industrial grade components and constructed with cast magnesium, polyurethane rubber and a military grade Polyetherimide resin. The camera is ultra-rugged, weatherproof, and has an operating temperature range of -40° F to +185° F. VISTA is designed to withstand years of real world use in the law enforcement environment.

WatchGuard has developed several camera options to support various department preferences and deployment scenarios. The options that are currently available are detailed below.

VISTA Extended

VISTA Extended is our original body worn camera design that was released in early 2015. It features:

- **Video Clarity and Quality** – VISTA records at 30 frames per second, and has six selectable video recording resolutions, including:
 - 720p (1280x720) – High, Medium and Low
 - 480p (864x480) – High, Medium and Low

VISTA Video Quality and File Sizes			
Setting	Resolution (pixels)	Sample Rate (megabits/second)	Average File Size Per Hour (gigabytes)
HQ-High	1280x720	5	2.32
HQ-Medium	1280x720	4	1.89
HQ-Low	1280x720	3	1.46
SQ-High	864x480	2	1.09
SQ-Medium	864x480	1.5	0.88
SQ-Low	864x480	1	0.66

WatchGuard chose 720p, not because it's the highest possible setting, but because we believe that it is the *right* setting. 720p strikes a great balance between quality and file size. To move to 1080p would significantly increase the file size of every video that is recorded as well as impact battery life by requiring more from the camera's processor.

VISTA uses H.264 High Profile (HP). The H.264 HP technology creates files that are up to 40% smaller than video captured at equivalent qualities using simpler forms of H.264.

VISTA has a 130° Horizontal field of view, and a 90° vertical field of view. The camera lens is capable of being rotated 28 degrees vertically. These angles allow the camera to have a picture covering 8.5 feet wide by 3 feet high, from 24 inches away. An example of the resulting image is below.



- **Ultra-Wide Dynamic Range** – To provide the best video in all lighting conditions, VISTA uses Ultra-Wide Dynamic Range technology. Essentially, the camera records two exposures of each frame of video at the same time: one optimized for light and one optimized for dark. The images are instantly overlaid, resulting in video that accurately represents what the human eye naturally sees. The following picture compares standard camera technology with WatchGuard's Ultra-Wide Dynamic Range camera technology. The child on the bicycle is almost invisible in the picture on the left, but can be clearly seen in the image on the right.



Video Uploading – Video can be uploaded through an individual USB transfer / charging base, or through the 8-Bay Ethernet Transfer Station. One of the weakest parts of a wearable camera is often the cable used to connect it to a PC. Cables and connectors can be prone to breaking or wearing out over the life of a camera as they are subjected to many uses and insertions. WatchGuard has designed a very rugged USB base that is used for transferring video and thus eliminated what is often the weakest piece in a wearable camera solution.



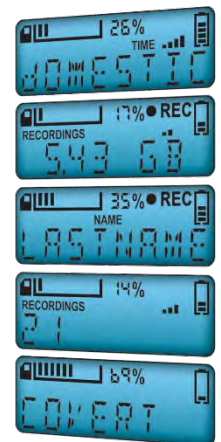
Through the individual USB base, VISTA can transfer video at a speed of 90 seconds per 1GB of data. The USB base also supports Dock and Go functionality allowing an officer to simply dock the camera and walk away. Even if the camera is off or the battery is completely drained, the USB base will power it on and initiate the file transfer.

Additionally, WatchGuard has designed an 8-Bay Transfer Station equipped with a Gigabit Ethernet port to dock and charge VISTA. This has the option of being rack mounted to allow for multiple Transfer Stations to easily be setup at a given location making it a highly scalable solution for any size agency. The Transfer Station can transfer video from 8 cameras simultaneously at up to 300Mbps.



- **Ease of Use** – VISTA was designed to be intuitive and simple to use while providing clear information as to camera status and operating condition. VISTA includes an easy one-touch operation. Simply press the button on the front of the camera to begin recording. Press the button again to end a recording.

Most other cameras use a single blinking LED light to communicate the status of storage, battery life, and recording state. The information available from this is minimal and often confusing. VISTA incorporates an LCD screen on the top of the camera to show exactly how much memory is still available, the exact battery life, how many recordings have been captured, and of course the recording state. The screen is also used to easily categorize recordings once they are stopped.



- **Record-After-The-Fact** – VISTA is designed with 32GB of storage that can be configured to constantly buffer video, even if the system is not actively recording. Depending on the video quality setting, VISTA provides the capability to go back in time from 12 hours up to 45 hours to capture critical information when it's needed. When VISTA is docked, the recorded events automatically upload to Evidence Library and the continuous video buffer stays on the device to be recorded over once it's full. If video is needed from the continuous buffer, this can easily be captured by creating a Record-After-The-Fact (RATF) event in Evidence Library while VISTA is docked. VISTA is the only wearable



camera providing the ability to go back in time and capture critical video that would not otherwise be recorded.

- **Battery Life** – VISTA includes a Lithium Polymer battery that has a stand-by life of 19 hours without pre-event or Record-After-the-Fact enabled. The approximate battery life of a single charge for our Extended Capacity VISTA allows for continuous recording of:
 - 9 Hours of recording at 720p resolution
 - 10 Hours of recording at 480p resolution

Additionally, VISTA includes intelligent standby timers to help further the actual battery life. VISTA has the ability to be configured to enter standby mode after a determined time has elapsed based on two independent options: No Movement – determined by internal accelerometers; or No Button Presses.

An upcoming item we will have available is a magnetic car charging cable that will allow officers in a car to snap the charger to the bottom of the VISTA adapter, and charge the camera while it is still operational and being worn. The cable will break away if ever forgotten to unhook when leaving the vehicle.

- **Mounting Options** – VISTA is available with a unique Chest Mount that overcomes the challenges of other mounting solutions. The Chest Mount system is designed to securely hold the camera to the uniform while keeping it very stable. It mounts the camera just below the shoulder of the Officer, rather than center mass, so that the lens is not obstructed by the user's arms when they are outstretched in front of the body.



Other mounting options include:

- Rotatable Shirt Clip
- Duty Belt Clip
- Molle Loop Mount

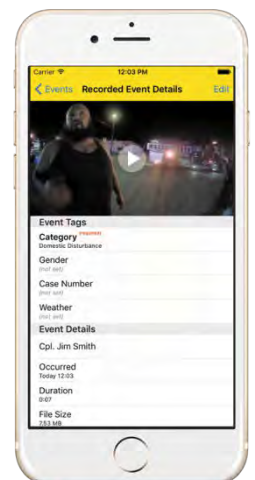
- Velcro® Plate Mount
- Klick Fast® Mount
- Tripod Mount
- RAM® Mount

VISTA WiFi

VISTA WiFi includes the same features of VISTA Extended, but adds additional functionality, including an integrated Wi-Fi radio and GPS capabilities.

VISTA WiFi is designed to add a new level of integration and functionality to 4RE, the industry's leading in-car video system, by maintaining an intelligent link to 4RE with almost no impact to VISTA's battery life. The integrated GPS receiver ensures perfect time synchronization between 4RE and VISTA.

- **Distributed Multi-Peer Recording** – This technology distributes decision-making to each camera in a multi-peer relationship. Imagine a network of cameras continually sensing the recording status of each other, acting in a peer-to-peer relationship.
 - Any camera (4RE or VISTA WiFi) can initiate a recording, and the other cameras, sensing a change in recording status, will begin recording
 - No one camera acts as a single, central controller, thus removing the single point of failure
 - A camera that initiated the group recording can move out of connectivity range without stopping the group recording in progress
 - A VISTA WiFi that's currently recording can "walk into" a group network on which it was previously associated, and the other cameras, sensing the recording status of that VISTA WiFi, will begin recording.
 - A VISTA WiFi not currently recording can "walk into" a group network on which it was previously associated, and sensing the other cameras recording, will begin recording.
- **Stand-Alone Vehicle Trigger Kit** – An upcoming release will include a Vehicle Trigger Kit that will allow VISTA to accept automatic triggers using inputs such as the emergency lights or vehicle siren, without the use of a 4RE in-car video system.
- **In-Field Viewing** – VISTA WiFi uses with SmartConnect, an optional smart phone application that will provide the officer with immediate in-field access to VISTA. Smart Connect includes the ability to:
 - Automatically and securely pairs with VISTA



- Categorize recordings
- Enter incident IDs, case number and more
- Play back recordings in HD at full frame rates
- The live viewfinder lets you see what the camera sees
- Control the VISTA camera remotely
- Change officer alert types, volume and brightness
- Toggle VISTA in or out of Covert Mode

Video from VISTA can also be reviewed with the Evidence Library Viewer application on a laptop or MDT in the police vehicle. The Evidence Library Viewer is designed to allow an officer to review video in the field while also uploading it from the VISTA camera later to the main Evidence Library database.

VISTA XLT

VISTA XLT includes the same features and functionality as VISTA Extended and VISTA WiFi, but offers additional mounting options and an extended battery life. VISTA XLT is WatchGuard's latest offering in body worn cameras.

VISTA XLT is a two-piece body-worn camera system with amazingly small, lightweight, interchangeable head and body-mounted HD cameras that allow officers to adapt to changing assignments and uniform types. Amazingly small, lightweight HD body-mounted camera is extremely comfortable to wear and easy to attach to any uniform, vest, or jacket.

Interchangeable head and body-mounted HD cameras allow officers the ability to record events from the optimal perspective using a single body camera system.



- **12+ Hour Battery Life** – VISTA XLT includes beyond full shift battery life. 12 hours of continuous HD recording allows officers to work beyond scheduled shifts without worrying about the battery keeping up. The two-piece design allows for a larger battery capacity in the DVR, extending the continuous recording life versus VISTA WiFi.

- **Head or Body Camera Options** – VISTA XLT provides a head-mounted or body-mounted HD camera. Each camera records audio and video and is connected to the DVR via a cable, which is often worn under the officer's shirt, vest or jacket. Both cameras, as well as the DVR, have a record button used to start and stop recordings.

The glasses mount snaps in to place around the forward part of the barrel on the head-mounted camera.



The magnetic mount is similar in concept to the clocking chest mount used for VISTA and VISTA WiFi, using under- and outer-shirt plates. The camera is seated in a base and held in place with two quick-release sliders. This forms the outer shirt plate. The under-shirt plate is placed under the officer's shirt.



- **Charging and Event Offloading** – VISTA XLT can charge and offload events using the VISTA USB dock or the 8 Bay Ethernet Transfer Station.

Camera Specification Comparison Table

	VISTA Extended	VISTA WiFi	VISTA XLT
Built-in Wi-Fi and GPS	No	Yes	Yes
Continuous HD Recording	11 Hours	9 Hours	12 Hours
Continuous SD Recording	12 Hours	10 Hours	13 Hours
DVR Size	3"H x 1.9"W x 1.3"D	3"H x 1.9"W x 1.3"D	3.3"H x 1.9"W x 1.3"D
DVR Weight	5.3 Ounces	5.3 Ounces	6.3 Ounces
Storage Capacity	32GB	32GB	32GB
Field of View	130°	130°	130°
Selectable Resolution	720p / 480p	720p / 480p	720p / 480p
Body-Mounted Camera Size	-	-	1.1"H x .84"W x .93"D
Head-Mounted Camera Size	-	-	.84"H x .84"W x 1.84"L
Body-Mounted Camera Weight	-	-	.5 Ounces
Head-Mounted Camera Weight	-	-	.4 Ounces

INTRODUCTION

Since the 4RE HD Digital In-Car Video System was released in 2010, it has continually been improved upon through firmware updates that have added additional features and enhanced the user experience. The latest addition to 4RE is the support for VISTA WiFi, a fully integrated body worn camera.

WatchGuard Video is pleased to present VISTA WiFi/4RE In-Car Camera System. VISTA WiFi is designed to add a new level of integration and functionality to 4RE, the industry's leading in-car video system, by maintaining an intelligent link to 4RE with almost no impact to VISTA's battery life. The integrated GPS receiver ensures perfect time synchronization between 4RE and VISTA.



Integrated in-car/body-worn offers in the market today are limited in two respects. First, many are simply one-directional, single-device recording triggers. At the most basic level, either a device outside the car (i.e. external microphone) signals the in-car video camera to begin recording, or an event in the car (i.e. light bar activation) signals a body-worn camera to begin recording. This operation is similar to using a remote control to start a recording on the DVR in your home entertainment system. It's a one-directional triggered event of a single recording device.

Secondly, even the more advanced offerings that allow connection to multiple devices (cameras) rely on a central controller to provide instruction. This would be equivalent to using a master DVR in your home entertainment system to tell other DVRs throughout your house to begin recording. It's a one-directional, one-to-many recording trigger. Building the architecture around a central controller introduces a single point of failure, should the controller lose connectivity

WatchGuard's Distributed Multi-Peer Recording technology distributes decision-making to each camera in a multi-peer relationship. Imagine a network of cameras continually sensing the recording status of each other, acting in a peer-to-peer relationship.

- Any camera (4RE or VISTA WiFi) can initiate a recording, and the other cameras, sensing a change in recording status, will begin recording
- No one camera acts as a single, central controller, thus removing the single point of failure
- A camera that initiated the group recording can move out of connectivity range without stopping the group recording in progress
- A VISTA WiFi that's currently recording can "walk into" a group network on which it was previously associated, and the other cameras, sensing the recording status of that VISTA WiFi, will begin recording.
- A VISTA WiFi not currently recording can "walk into" a group network on which it was previously associated, and sensing the other cameras recording, will begin recording.



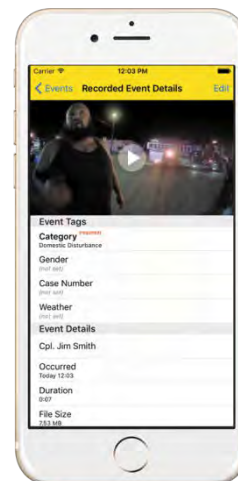
VISTA WiFi removes the need for the 4RE Wireless Microphone by providing the audio for 4RE and it is automatically activated by 4RE and can remotely activate 4RE to record. VISTA WiFi also becomes an additional camera view for 4RE and inherits the event properties of the 4RE recording such as officer name, event category, case number and more.

4RE and VISTA are the components Officers will interface with every day. 4RE is built small, lightweight, rugged, user-friendly, and requires minimal Officer interaction. The system has automotive grade components that feature a sturdy over-molded construction, which increases durability as well as occupant safety. Further adding to the robustness of the system, all vital connections are locking connectors that have been thoroughly tested in this environment.

VISTA is designed with industrial grade components, and constructed of cast magnesium, an ultra-hard military-grade resin and polyurethane rubber. Together the components and construction provide an extremely wide operating range of -40°F - +185°F in an ultra-rugged design to meet the demands of law enforcement.

In addition to working with 4RE, VISTA WiFi will also work with SmartConnect, an optional smart phone application that will provide the officer with immediate in-field access to VISTA.

- Automatically and securely pairs with VISTA
- Categorize recordings
- Enter incident IDs, case number and more
- Play back recordings in HD at full frame rates
- The live viewfinder lets you see what the camera sees
- Control the VISTA camera remotely
- Change officer alert types, volume and brightness
- Toggle VISTA in or out of Covert Mode



EVIDENCE LIBRARY 4 EVIDENCE MANAGEMENT SOFTWARE

The Department's current solution, Evidence Library 4 Web (EL4), utilizes Microsoft SQL Server databases, and can be hosted on premise on agency servers, or deployed as a hybrid solution.

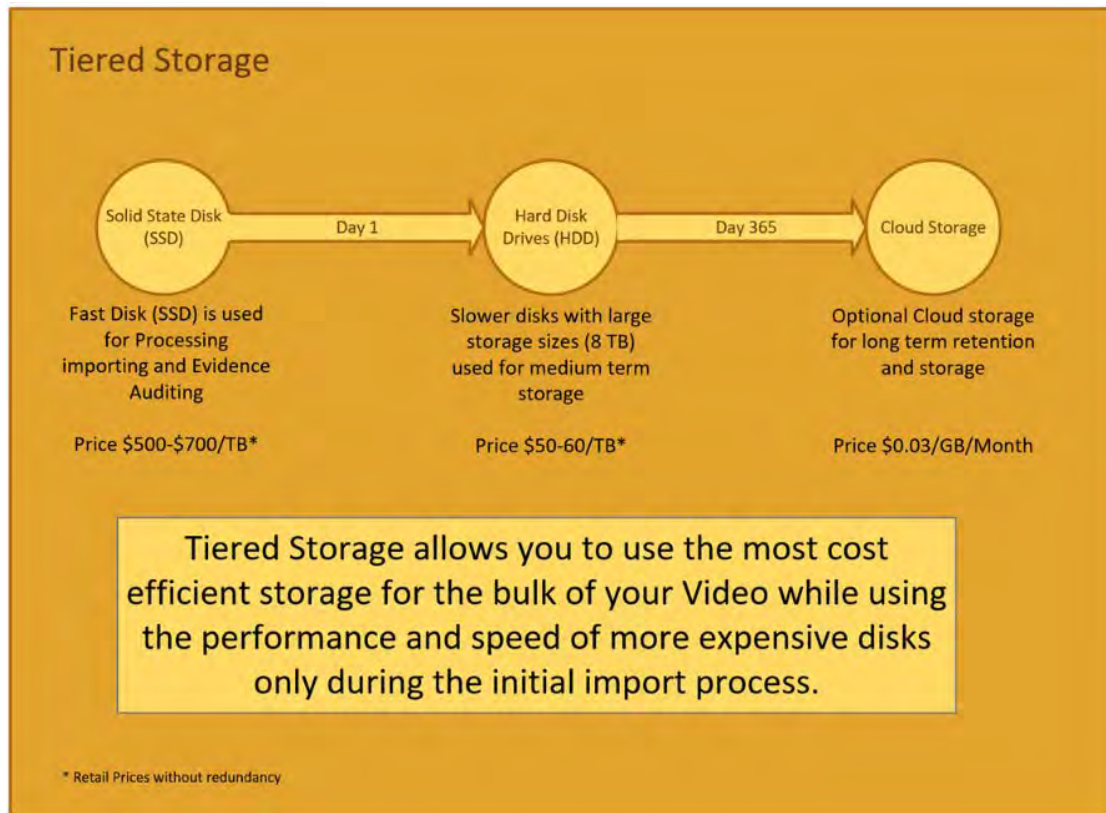
EL4 provides advanced file management, a graphical search engine, the ability to share important evidence, and a feature-rich media player, which is all accessible from a convenient Web Client. WatchGuard engineers designed this software from the ground up to have all of the functionality, features, and the customization options necessary to ensure that law enforcement agencies have a tool they can use to protect, search, copy, share, and create reports for their video evidence.

Evidence Library is primarily based on the Microsoft technology. Using the building blocks of Microsoft Windows Server, Microsoft SQL Server and Active Directory provide for seamless integration in to your existing infrastructure. The primary interface is a modern web browser making deployments fast and easy.

We propose the department utilize the servers already in use for either On-Premise storage or Hybrid. The storage solution that was purchased in 2016 and 2017 includes a large amount of storage and is also expandable at a fraction of the cost of cloud storage.

Storage options include:

- **On Premise Storage** – An on-site storage solution allows video to move rapidly from the cameras to the storage device. The movement of large amounts of video from hundreds of cameras can be complete in minutes instead of hours. This frees up cameras to be used for multiple shifts, which means the Department could purchase fewer cameras, docking stations and transfer bays.
- **Hybrid Storage** – The EL4 hybrid model offers a combination of both on premise storage and cloud storage. This will allow the agency to store video on premise for a defined period of time and then have video moved to the Cloud for long-term storage. This provides the cost efficiency of on premise storage during the time when most access to video is needed while also providing the benefits of CLOUD-SHARE and Cloud storage for long-term retention and archiving.



Hybrid Solution

A hybrid On Site / Cloud storage solution offers a best of both worlds deployment scenario. A hybrid solution provides the Department with the same benefits of an on-site solution, which includes:

- 1) Fastest possible video offload speeds
- 2) Quickest access to video

It also allows the Department to have video stored on premise during the time period when quick access to video is needed (generally right after an important incident has occurred), and then it automatically moves video to a secure CJIS compliant Cloud where it can live out its long-term storage requirements. A hybrid solution also requires considerably less hardware to be purchased and maintained locally than an on-site solution.

This solution works well for an agency that is comfortable with Cloud storage. It can be setup to use an existing Cloud storage agreement, or with a new agreement.

Cloud storage support is currently limited to two types, Microsoft Azure Public and Microsoft Azure Government.

Microsoft Azure Government is an isolated version of Azure that is exclusively used by US Government Agencies and qualified vendors. Microsoft has signed CJIS agreements with multiple states and has committed to maintain strict standards of compliance.

WatchGuard Video is a Microsoft Managed Service Provider for Azure Government and can sell services to our customers if they do not already have Azure Government contracts.

When available, WatchGuard Video will recommend the use of Microsoft Azure for cloud storage. The cloud platform is designed to meet US government demands, including:

- Physical and logical network-isolated instance of Azure
- Dedicated to US government with all data, applications, and hardware residing in the continental United States
- Broad range of compliance certifications critical to US government
- US datacenters located more than 500 miles apart, providing true geographic redundancy
- Support for hybrid scenarios, as well as a vast array of services, programming languages, and tools

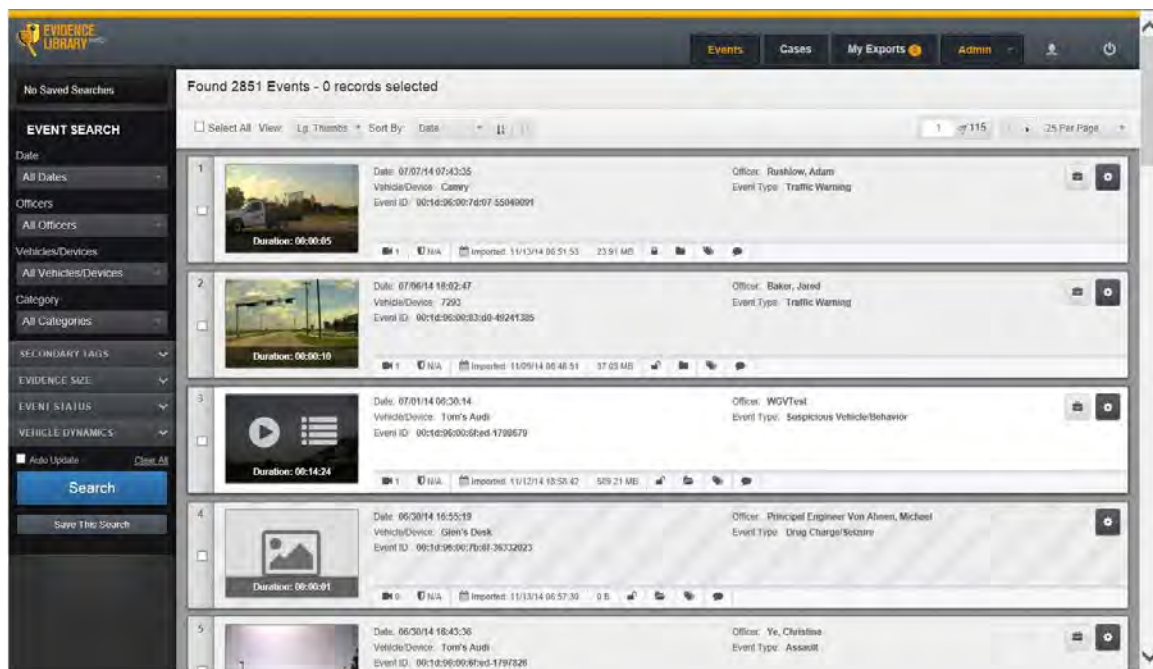
Data centers are located in Iowa and Virginia with redundant data stored at both locations. All servers hosted in the Azure datacenter will be setup so that their disks are globally redundant (exist in both datacenters). In the event of a disaster, the VMs can be recovered in a 24-hour period. All video storage in Azure blobs is also globally redundant with three copies kept in each datacenter. In the event a datacenter is unavailable, all naming references will transition to the redundant datacenter.

Azure Express Route is a private link to either Azure service that increases bandwidth and reduces network latency. It is not required for either solution but is recommended when large volumes of data are going to be sent to Azure.

FEATURES AND FUNCTIONALITY

The Interface

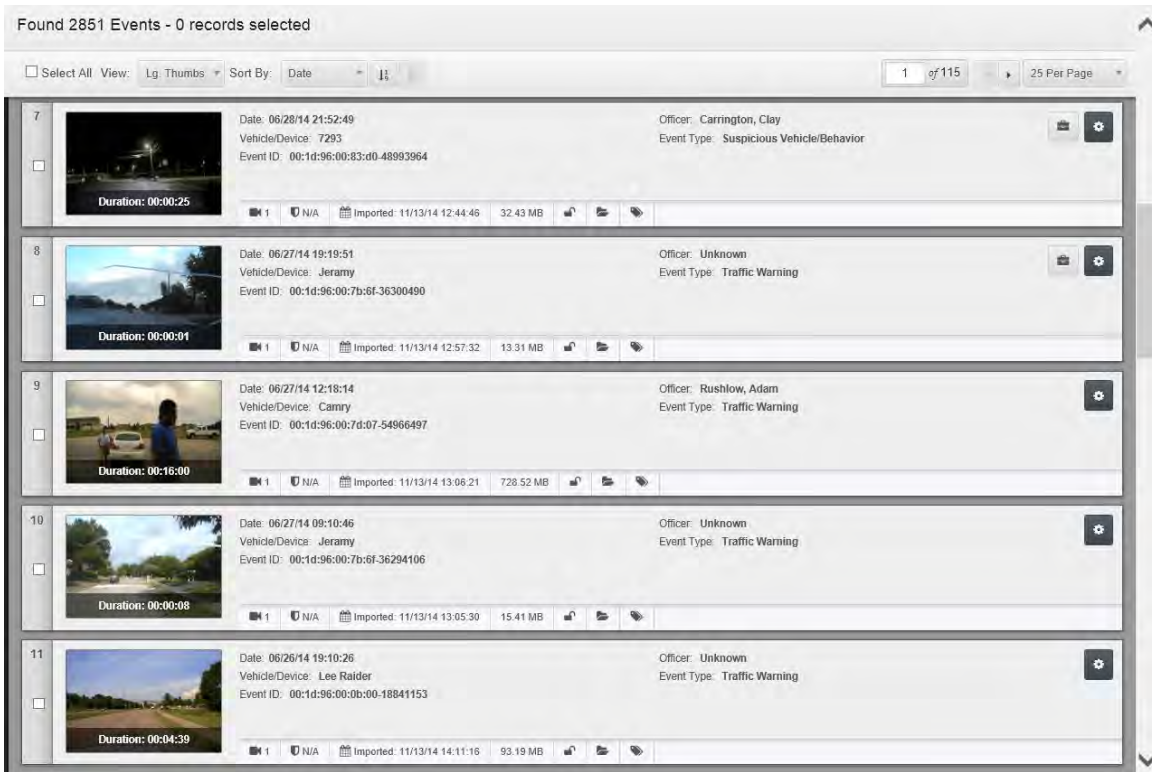
Evidence Library uses a very intuitive graphical and tabbed interface. This interface allows the user to easily toggle between the available functions of EL4, including Events, Cases, Exports, and Admin functions.



Events Tab

The Events tab provides a view of the Recorded Events in EL4 from both VISTA and 4RE. When an officer uses both VISTA and 4RE on the same incident, EL4 automatically links the recordings together based on 4RE and VISTA recordings that have the same officer name and a date and time overlap. With the introduction of VISTA WiFi, the recordings will be linked together through the synchronization in the vehicle as VISTA becomes part of the 4RE system. As a further level of integration, EL4 will also support simultaneous playback allowing for multiple camera streams to be played back in synchronization so the user can watch both the 4RE video and VISTA video at the same time.

From the Events Tab, important information from each event is displayed on this screen including, a thumbnail image from the event, Date/Time, Vehicle/Device, Event ID, Officer Name, and Event Type. Additionally, the user can see other key pieces of information at a glance such as the date the event was imported, the number of camera views, the size of the event, secondary Event Tags like Case Number, and notes. From here, events can easily be played, exported or added to a case.



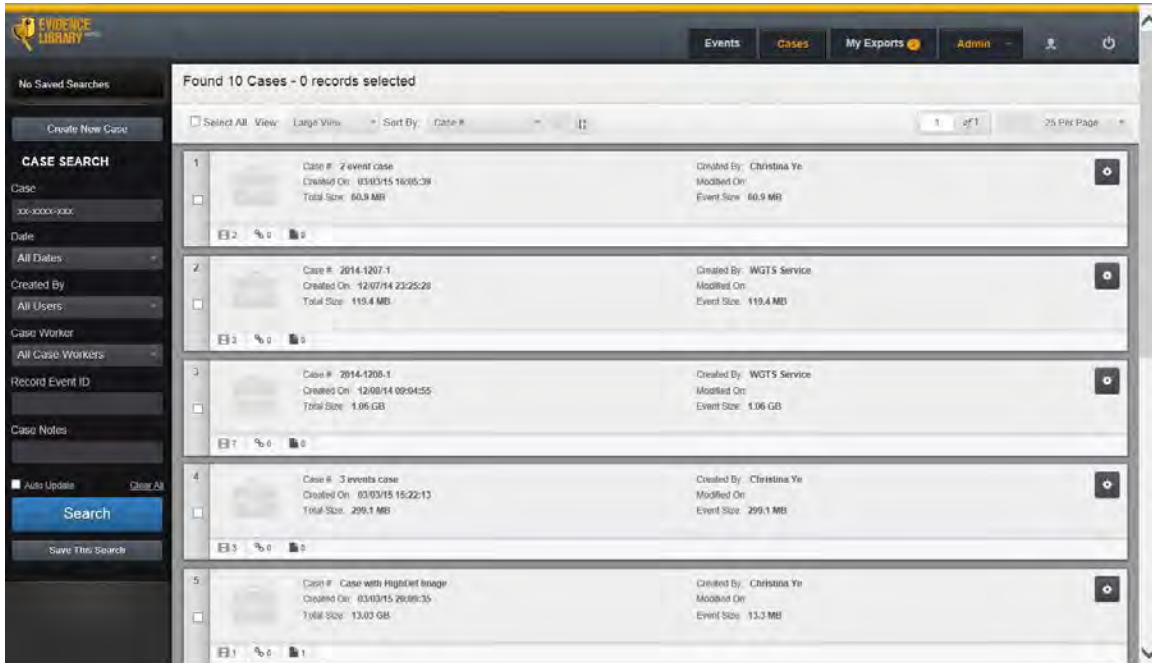
Found 2851 Events - 0 records selected

Select All View: Lg Thumbs Sort By: Date 1 of 115 25 Per Page

Event ID	Date	Vehicle/Device	Officer	Event Type	Duration	Imported	Size
00:1d:96:00:83:d0-48993964	06/28/14 21:52:49	7293	Carrington, Clay	Suspicious Vehicle/Behavior	00:00:25	11/13/14 12:44:46	32.43 MB
00:1d:96:00:7b:6f-36300490	06/27/14 19:19:51	Jeramy	Unknown	Traffic Warning	00:00:01	11/13/14 12:57:32	13.31 MB
00:1d:96:00:7d:07-54966497	06/27/14 12:18:14	Camry	Rushlow, Adam	Traffic Warning	00:16:00	11/13/14 13:06:21	728.52 MB
00:1d:96:00:7b:6f-36294106	06/27/14 09:10:46	Jeramy	Unknown	Traffic Warning	00:00:08	11/13/14 13:05:30	15.41 MB
00:1d:96:00:0b:00-18841153	06/26/14 19:10:26	Lee Raider	Unknown	Traffic Warning	00:04:39	11/13/14 14:11:16	93.19 MB

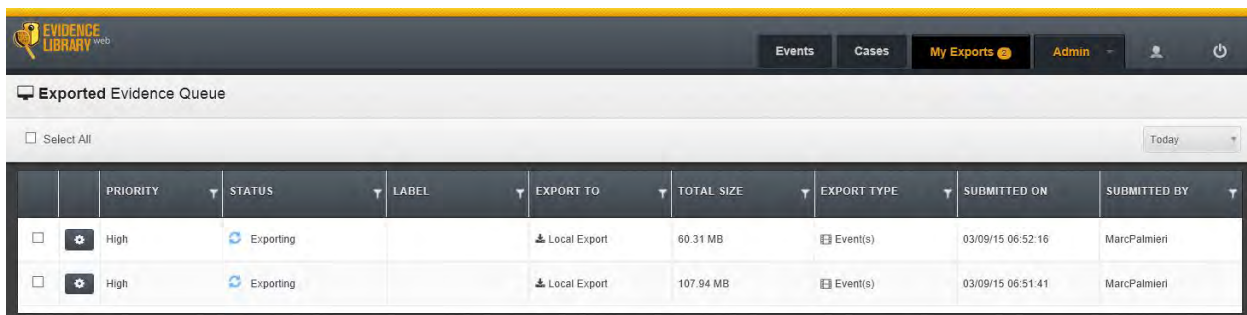
Cases Tab

EL4 includes the ability to perform Case Management, which allows the ability for case “container” creation and content management. With this feature, users may associate one or more VISTA or 4RE recordings with a case, as well as other general user files such as: PDFs, spreadsheets, reports, videos from 3rd party systems, audio recordings, still pictures, drawings, etc. Cases can be further managed by adding users as Case Workers with specific sets of permissions for that case.



My Exports Tab

“My Exports” allows a user to see and manage their exports and since EL4 includes a Web Client, this can be done from any computer on the network that the user has access to. The “My Exports” view can easily be sorted and filtered so it can be easily managed.



	PRIORITY	STATUS	LABEL	EXPORT TO	TOTAL SIZE	EXPORT TYPE	SUBMITTED ON	SUBMITTED BY
<input type="checkbox"/>	High	Exporting		Local Export	60.31 MB	Event(s)	03/09/15 06:52:16	Marc Palmieri
<input type="checkbox"/>	High	Exporting		Local Export	107.94 MB	Event(s)	03/09/15 06:51:41	Marc Palmieri

Kiosk Mode

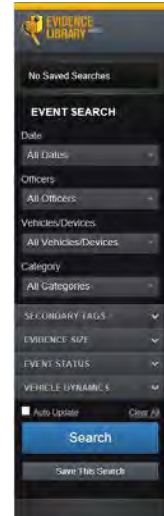
Kiosk mode allows for VISTAs to easily be used in a pooled camera environment where an officer is allowed to use any available camera rather than having a camera assigned to them. For Little Rock Police Department, this means, not as many body worn cameras would need to be purchased.

From the Kiosk (this is a feature of EL4 that is designed to run in a web browser on a network PC), the officer simply selects their name from a dropdown list and then chooses VISTA Checkout. The Kiosk will then determine the best VISTA for the officer based on the following criteria: fully charged battery and all events transferred. The Kiosk then displays the location of the assigned VISTA (Transfer Station and Slot number) and that VISTA will begin to beep and the LCD screen will illuminate and display the officer's name making it easy to identify.



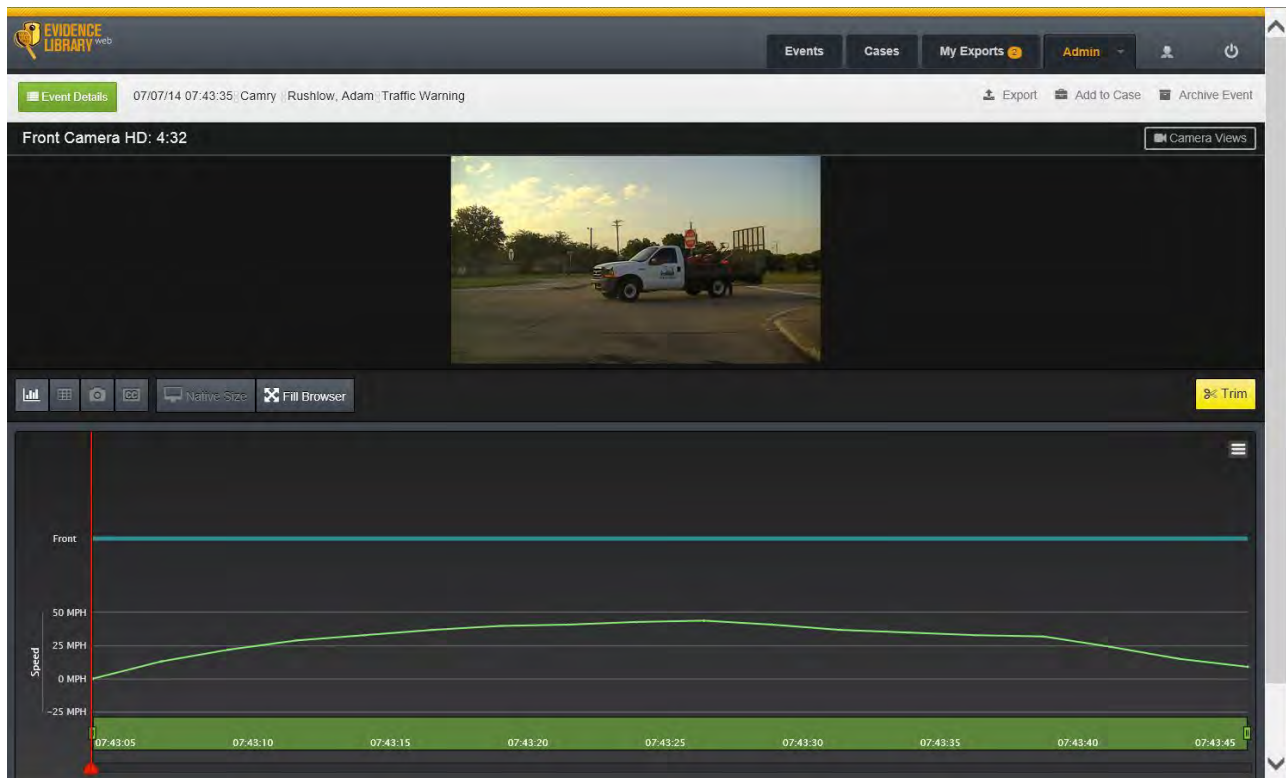
Graphical Search Engine

Searches are performed live on the Search bar, which can be simple or complex in nature, allowing all types of searches to be performed from the same area without leaving the main Records Events screen. The ability to perform complex searches on the Search bar allows for building and saving complex searches using multiple fields, with both specific values or across ranges in a graphical environment. For example, a search could easily be created to find any recordings in the last 60 days tagged as “Traffic” or “Other”, with a radar target speed of 55 MPH or higher, that occurred within 1.25 miles of a specific GPS location.



Media Player with Timeline Graphing

The built-in media player includes a graphical display of the dynamic metadata. Users can visually spot when lights, siren, or brakes were activated during the event timeline or view the patrol speed graph to quickly find moments of interest. Snapshot and copy/export functions are built into the player, including the ability to burn DVDs or convert file formats along with the ability to trim video.



Convenient Export Video Player

Evidence Library makes it easy to share video with attorneys and prepare videos for court. An embedded player can be included during file export, which enables any PC to play the video files without the need to install software prior to playing the video.

CLOUD-SHARE

In addition to the traditional method of exporting video to a disk or other device to then be shared, EL4 includes the ability to share Events and Cases by publishing the information to the Cloud in a Microsoft Azure CJIS certified data center through CLOUD-SHARE. A link with permissions and expiration dates can then be shared with the appropriate individuals. Links can be sent with one of the following permissions:

- Access allowed to anyone with the link.
- Access allowed with a secure access code
- Access only allowed to a registered user

The ability to use CLOUD-SHARE is a permission that must be assigned to EL4 users and parameters, such as how long the information can be made available for and e-mail addresses and domains allowed for sharing, are administratively controlled. After information has been shared, sharing permission can later be revoked if necessary.

With EL4, WatchGuard has developed a locally hosted solution with the ability to share via a secure hosted cloud solution. This offers the benefits of an on premise deployment while providing cloud based sharing for your critical video without the need to store everything in the cloud. This solution avoids the high reoccurring costs of storing everything in the cloud when only a small percentage of video is needed for easy sharing and distribution. On average we find that agencies typically share 5% or less of the total amount of video they accumulate.

Admin Tab

The Admin Tab provides access to Administrator function such as, Fleet Management, Security Management and Evidence Management with Email Notification for Storage Alerts.

Fleet Management – This section of the client is where all of the VISTA Cameras and 4RE DVRs are provisioned and settings are applied. Evidence Library supports a very capable Fleet Management section that includes group level configurations, automatic configuration updates to VISTA Cameras when docked and 4RE DVRs wirelessly or manually by USB, and firmware upgrades that are automatically sent to the VISTA Cameras when docked and the 4RE DVRs wirelessly or manually by USB. Fleet Management is also where all the various policy and system settings for VISTA and 4RE are configured including Event Categorization. Fleet Management consists of four major parts:

- Department Information
 - These settings include Department Name, Units of Measure, The IP address of the Application Server, and the Admin Password that is used in 4RE.

➤ All Devices

- This is the section that will hold all of the device information for the Department's VISTA and 4RE systems. After a device is created, it may then be assigned to a configuration, which is a set of unique settings that will be applied to all the devices assigned to the configuration.
- Once a device is in your Fleet, upon its first upload it will then begin to track its current firmware version and current configuration status. Any out-of-date devices or devices that are not assigned to any configurations will be noted on the list of devices.

➤ All Officers

- The All Officers section will show a global list of all the users who have either the "VISTA/4RE Officer" or "VISTA/4RE Officer and Supervisor" claims. It will also show what Configurations the Officers are assigned to. Essentially, any configuration that an Officer is assigned to means that this Officer's name will appear in the list of Officer Names when checking out a VISTA Camera or logging into the 4RE DVR. From this screen, multiple Officers may be selected and quickly assigned to an existing configuration.

➤ Configurations

- A configuration is a set of VISTA and 4RE policies and settings.
- A configuration contains a unique set of devices assigned to it.
- Multiple configurations may be created.
- Within a configuration lies 4 different sections:
 1. Assigned Devices
 2. Assigned Officers
 3. Recording Properties - All of the Recording settings for VISTA and 4RE are configured in this area. Recording properties affect camera resolution, Pre-Event time, Recording Reminder Alerts, Record-After-The-Fact, and additional criteria.
 4. Device Behavior - The final area of the configuration is Device Behavior. This is where most policy and power settings are made such as Sleep timers and Automatic Off timers.

➤ Event Tag Configuration

- Here the Department may designate which Event Categories should be prompted on VISTA after the Officer stops the recording. Event Category options are often times things like, Warning, Citation, DUI, Arrest, or whatever else may be applicable to the department. In addition to helping

with searching video, Evidence Retention policies can also be tied to Event Category.

- Additional Event Tags may be created for the sole purpose of back office use, and therefore not applied on the VISTA camera. The information for these tags can be entered in EL4 after video has uploaded. Creating and editing the Event Tags is done globally using either a wizard or by manually creating them. Event tags may be any of the following formats:
 1. List of answers
 2. Alphanumeric input
 3. Numeric input
- There is no limit as to how many tags may be created.

Security Management – The Security Management module of EL4 houses all of the user information, permissions and group level security settings. Users of the system must include any person who will be logging into the Web Client or operating a VISTA or 4RE system. After the users are entered into the system (Active Directory integration available) User Groups are created that give a specific set of permissions, or claims. Users are then added into User Groups based on the level of access to the system needed. Based upon the Department's desire for certain users to perform certain tasks, groups may be dynamically created for nearly any circumstance the Department envisions.

Claim Name	What Action The Claim Allows																			
	Login	Search for Unrestricted Record Events	Review and Play Unrestricted Record Events	Mark a Record Event as Restricted	Search for Restricted Record Events	Review and Play Restricted Record Events	Un-Restrict a Record Event	Edit Record Event Properties	Import Record Events via US Transfer	Export Record Events	Setup Users, Groups and Permission Levels	Restore Record Event Data	Evidence Management Access	Audit Log Review	Ability to Archive to Online Storage	Granted In-Car Supervisor Permissions	Create and Manage Case Archives	Allows the Viewing of Case Archives	Grants Access to Watch Commander	
User	Yes	My	My																	
Enhanced Search		All																		
Enhanced Search and Review		All	All																	
Enable Restricted Access				Yes*																
Search and Review Restricted Events				Yes*	Yes	Yes	Yes													
Edit Record Event Properties								Yes*												
Import									Yes											
Export										Yes*	Yes*									
User Security Management											Yes									
Fleet Management											Yes									
Archive Restore												Yes								
Evidence Management													Yes							
Review Detailed Audit														Yes						
In-Car Officer															Yes					
In-Car Officer and Supervisor															Yes	Yes				
Case Management																	Yes	Yes		
Case Worker																	My	My		
Enhanced Case Worker																		Yes		
Live Video Streaming																			Yes	
Administrator	Yes	All	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	

* = Assumes other claims have allowed you access to the given event.

Evidence Management – Rules are created in this section of EL4 that determine how long video is kept before it is either deleted or archived. This section leverages the Event Category that was selected at the time of the recording or later identified in the client. For each Event Category listed, the Department is allowed to specify an action that is performed and at what interval it is performed. Both the retention period and the action performed on the event are choices left up to the Department.

The next configuration related to Data Cleanup is how the Department wants the Data Cleanup procedure to run. It may be set to run on a schedule automatically or manually at times initiated by a user with Evidence Management permissions. Regardless of when and how it runs, Data Cleanup will run through the entire list of retention rules and perform the actions necessary across the entire solution.

System Specifications for Evidence Library	
System	Minimum Requirement
Application / Database	64-bit Hardware Windows Server 2008 R2 64-bit, Windows Server 2012 R2 Microsoft SQL Server 2008 R2 Standard, 2012 Standard, 2014 Std. Virtual Server Support VMware vSphere Hypervisor (ESXi) Microsoft Hyper-V
Client Operating System	Windows 7 64-bit Windows 8.1 Windows 10 Windows Editions: Professional, Ultimate Member of Active Directory Domain
Client Hardware	1.7GHz Dual Core comparable or faster processor 4GB RAM or more 160MB of available hard-disk space DVD-RW drive One available USB 2.0 port Super VGA (1,024x768) or higher-resolution video adapter
Wireless Network	802.11n Compatible 5.2GHz (Recommended) or 2.4GHz band Available 40MHz channel WPA2-AES Encryption (128 bits) using PSK
Network	100Mb/1Gb Ethernet Available RFC 1918 (private) address space Sufficient bandwidth to transport data from Upload Server (if used)
Database Server Storage (Separate from Application Server)	Operating System – Mirrored 2x500GB SATA 7,200 RPM drives SQL Storage – Raid 5 3x500GB SATA 7,200 RPM drives Global Spare – 500GB SATA 7,200 RPM drive
Application Server Storage	Operating System – Mirrored 2x128GB SSD drives SQL Storage on Application Server – RAID 5 3x480GB SSD Drives Video Storage – Raid 5 3x (or more*) 4TB SATA 7,200 RPM drives Global Spare – 4TB SATA 7,200 RPM drive

EvidenceLibrary.com

EvidenceLibrary.com is a fully cloud hosted back office solution allowing an agency to have the application and all video storage in the cloud. EvidenceLibrary.com is a future release, that we expect to be available for deployment mid Q4, 2018.

EvidenceLibrary.com utilizes Microsoft Azure Government, which is an isolated version of Azure that is exclusively used by US Government Agencies and qualified vendors. Microsoft has signed CJIS agreements with multiple states and has committed to maintain strict standards of compliance.

WatchGuard is a Microsoft Managed Service Provider for Azure Government and can sell services to our customers if they do not already have Azure Government contracts. The cloud platform is designed to meet US government demands, including:

- Physical and logical network-isolated instance of Azure
- Dedicated to US government with all data, applications, and hardware residing in the continental United States
- Broad range of compliance certifications critical to US government
- US datacenters located more than 500 miles apart, providing true geographic redundancy
- Support for hybrid scenarios, as well as a vast array of services, programming languages, and tools

Data centers are located in Iowa and Virginia with redundant data stored at both locations. All servers hosted in the Azure datacenter will be setup so that their disks are globally redundant (exist in both datacenters). In the event of a disaster, the VMs can be recovered in a 24-hour period. All video storage in Azure blobs is also globally redundant with three copies kept in each datacenter. In the event a datacenter is unavailable, all naming references will transition to the redundant datacenter.

EvidenceLibrary.com offers two separate storage plans:

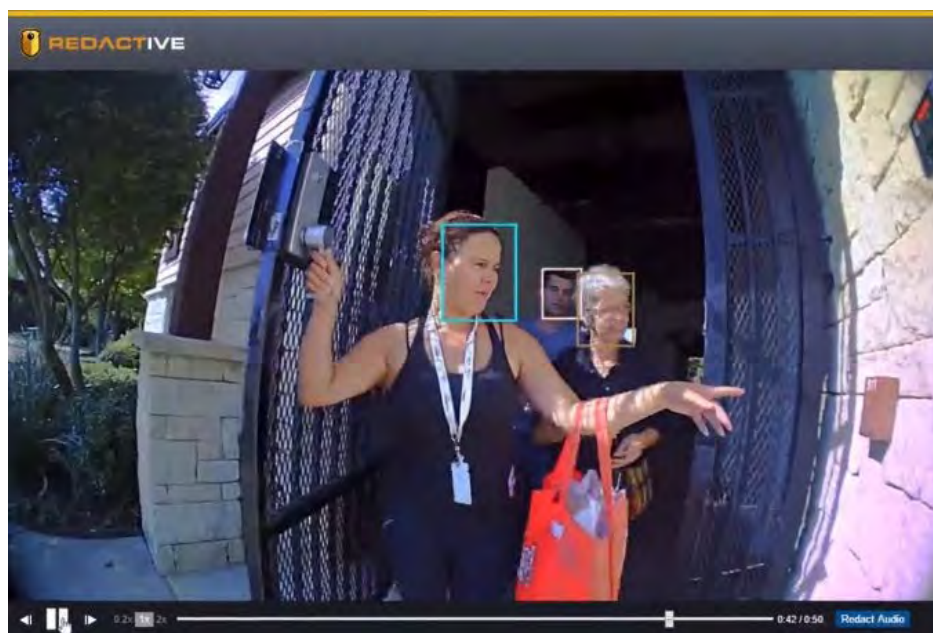
- **Better than Unlimited Plan** – Store an unlimited amount of HD and SD video recordings. The agency will receive unlimited storage for the published price if the data retention policy does not exceed one year for non-evidentiary recordings or 10 years for evidentiary recordings (evidentiary recordings are defined as recordings associated with a case).
 - Includes Unlimited Users – Everyone in the agency can access video evidence. No per user fees. EvidenceLibrary.com is not charged by the number of user accessing the system. It's charged by the number of devices. So, an agency may set up an unlimited number of users (i.e. administrators, supervisors, evidence technicians, officers, etc.) without incurring additional cost.

- Unlimited Sharing – Share video evidence with anyone who has an email address. No user account or fee required. EvidenceLibrary.com users will make use of CLOUD-SHARE to share evidence without service level or number of shares limitations.
 - Credit or Cash Rebate – Receive cash back or credit for using storage management best practices. When the actual data usage across all devices averaged over the year is less than 700GB per device, the agency will receive a rebate at the end of each contract year equal to 36¢ per GB for the year for each GB under 700GBs per device that is actually used. The agency gets to decide if the rebate is in the form of cash or credit.
- **Actual Usage Plan** – As inferred in the name, customers pay for total storage used per month. This plan does include unlimited users.

REDACTIVE Redaction Software

Redaction capabilities are provided by REDACTIVE, the solution currently being utilized by LRPD. Video files are imported in to REDACTIVE and then modified versions are saved. The original file will remain unaltered. REDACTIVE includes:

- Automated Face Detection
 - REDACTIVE quickly scans the entire video clip first, automatically detecting faces, so the user spends much less time manually performing the task
- Forward and Backward Object Scanning
 - Select any object at any point in the video clip and REDACTIVE will automatically scan forward and backward to find it, allowing the user to redact the object before or after the selection point – or throughout the entire clip.
- Simple, Selective Audio Muting
 - Select, preview and redact any portion of the audio track simply by highlighting the area with a click and drag of a mouse.





COSTARS - 12 PRICE LIST - WatchGuard Video

4RE In-Car Video System		MSRP	Contract
4RE-200-GPS-ZSL	4RE In-Car Camera System. Includes GPS, High definition Zero Sightline (720P) forward facing camera, Infrared color cabin camera, DVR, integrated 200GB automotive grade hard drive, 16GB USB removable thumb drive, cabin microphone, 900 MHz Hi Fidelity wireless microphone, hardware & cabling, 1 yr. warranty. Includes Evidence Library Express software.	5,990.00	4,783.00
4RE-64S-GPS-MTR	4RE Motorcycle Camera System. Includes GPS, Waterproof Display, Waterproof standard definition camera, DVR, integrated 64GB solid state hard drive, 16GB USB removable thumb drive, 900MHz Hi Fidelity wireless microphone, Wireless Microphone Lapel Microphone, hardware & cabling and One (1) Year Factory Warranty. Includes Evidence Library Express software.	6,270.00	5,295.00
4RE-200-VIS-INT	4RE High Definition In-Car Video System with Integrated VISTA Wi-Fi Includes: Zero Sightline HD Front Camera, Separate Back Seat Camera, VISTA HD Wi-Fi Integrated Wearable Camera, VISTA HD Wi-Fi Charging / Transfer Base, 4RE, VISTA, Smart PoE Switch (Connects the 4RE In-Car Video System to the VISTA HD Wi-Fi Wearable Camera in the vehicle) Integrated GPS, Crash detection, DVR with integrated 200GB, automotive grade hard drive, 16GB USB drive, 4.3" touch screen remote display control panel, Cabin microphone, All mounting hardware and cabling, One (1) Year Factory Warranty. Includes Evidence Library Express software.	6,995.00	5,495.00
4RE-200-INT-001	4RE Interview Room Solution, One Camera Package - Choice of: traditional dome security camera with integrated microphone, covert motion sensor hidden camera, and covert pinhole camera, DVR with integrated 200GB hard drive, 16GB removable USB flash drive, mounting hardware and cabling, Easy-On wall switch, and Watch Commander Live Video Streaming software.	5,990.00	4,995.00
4RE-200-INT-002	4RE Interview Room Solution, Two Camera Package - Choice of two cameras: traditional dome security camera with integrated microphone, covert motion sensor hidden camera, and covert pinhole camera, DVR with integrated 200GB hard drive, 16GB removable USB flash drive, mounting hardware and cabling, Easy-On wall switch, and Watch Commander Live Video Streaming software.	6,230.00	5,195.00
4RE-WRL-KIT-05G	Upgrade 4RE to wireless upload capability 802.11n 5GHz. Requires Evidence Library 3 software or higher	250.00	199.00
4RE ELITE	Upgrade 4RE DVR to Elite version supporting up to 6 cameras	345.00	275.00
4RE ZOOM UPGRADE	Upgrade front camera to HD zoom camera	250.00	199.00
4RE PANORAMIC UPGRADE	Upgrade front camera to the Panoramic camera	250.00	199.00
DUAL MIC UPGRADE	Upgrade to dual Hi-Fi wireless microphones	985.00	785.00
In-Car Hardware Warranty		MSRP	Contract
WAR-4RE-CAR-2ND	Warranty, 4RE, In-Car, 2nd Year (Months 13-24)	125.00	100.00
WAR-4RE-CAR-3RD	Warranty, 4RE, In-Car, 3rd Year (Months 25-36)	250.00	200.00
WAR-4RE-CAR-4TH	Warranty, 4RE, In-Car, 4th Year (Months 37-48)	410.00	325.00
WAR-4RE-CAR-5TH	Warranty, 4RE, In-Car, 5th Year (Months 49-60)	565.00	450.00
Evidence Library 4 Software		MSRP	Contract
SFW-ELX-KIT-100	Evidence Library Express Software	-	-
KEY-EL4-SRV-001	Evidence Library 4 Web Server Site License	1,250.00	1,000.00
KEY-EL4-DEV-001	Evidence Library 4 Web 4RE In-Car Device License	190.00	150.00
KEY-EL4-DEV-002	Evidence Library 4 Web VISTA Device License	190.00	150.00
KEY-EL4-DEV-003	Evidence Library 4 Web 4RE Combo-Discount Device License Key	95.00	75.00
KEY-EL4-DEV-004	Evidence Library 4 Web VISTA Combo-Discount Device License Key	95.00	75.00
SFW-EL4-CLD-BAS	Evidence Library 4 Web CLOUD-SHARE - Basic Includes 24 shares per device. Included with Evidence Library Software Maintenance.	-	-
SFW-EL4-CLD-FUL	Evidence Library 4 Web CLOUD-SHARE - Full Included 48 shares per device. Optional upgrade.	55.00	45.00
SFW-EL4-CLD-EXT	Evidence Library 4 Web CLOUD SHARE - Extended Includes 72 shares per device. Optional upgrade.	125.00	100.00
SFW-MOB-APP-001	VISTA Mobile Companion (ELX/EL4 No Maintenance Plan)	95.00	75.00
SFW-WCM-LIC-FEE	Watch Commander License Fee (per car)	275.00	250.00



COSTARS - 12 PRICE LIST - WatchGuard Video

SFW-WCM-KIT-100	Watch Commander Live Video Streaming Application	2,900.00	2,500.00
SFW-SQL-SRV-012	Software, SQL Server 2012, w/5 CAL	520.00	415.00
SFW-WIN-SRV-012	Software, Windows Server 2012, w/5C CAL	965.00	770.00
SFW-SQL-CAL-R21	Software CAL, SQL Server 2008, R2, 1 CAL	115.00	90.00
SFW-SQL-CAL-R25	Software CAL, SQL Server 2008, R2, 5 CALs	515.00	410.00
Evidence Library Software Warranty		MSRP	Contract
SFW-MNT-EL4-001	Software Maintenance, Evidence Library, 1st Yr (Months 1-12)	190.00	150.00
SFW-MNT-EL4-002	Software Maintenance, Evidence Library, 2nd Yr (Months 13-24)	190.00	150.00
SFW-MNT-EL4-003	Software Maintenance, Evidence Library, 3rd Yr (Months 25-36)	190.00	150.00
SFW-MNT-EL4-004	Software Maintenance, Evidence Library, 4th Yr (Months 37-48)	190.00	150.00
SFW-MNT-EL4-005	Software Maintenance, Evidence Library, 5th Yr (Months 49-60)	190.00	150.00
Additional Options		MSRP	Contract
USB-DRV-101-16G	4RE, USB 2.0 Thumb Drive, Rubberized, 16GB	50.00	39.00
USB--DRV-100-32G	4RE, USB 2.0 Thumb Drive, Rubberized, 32GB	90.00	70.00
CAM-AUX-SNY-SPR	Camera Assy, Auxiliary, Gimble Bracket Assy, 4RE	245.00	195.00
KEY-4RE-MBL-001	4RE, Mobile App License Key	65.00	50.00
HDW-ETH-SWT-001	4RE, Power Over Ethernet / Gigabit 4-port Switch (required when including both WiFi and Mobile App)	190.00	150.00
MIC-WRL-DTC-400	Hi-Fi Microphone Desktop Charger Kit 1 (Cradle, and AC Charger)	125.00	99.00
SVC-4RE-ONS-300	4RE, On-Site Service, Access Point Installation	1,250.00	1,000.00
SVC-4RE-ONS-400	4RE System Setup, Configuration, Testing and Training (per site)	3,125.00	2,500.00
SVC-4RE-INS-100	4RE System Installation, In-Car (Per Unit Charge)	QUOTED	QUOTED
SVC-VID-REM-100	Video System Removal (Per Unit Charge)	QUOTED	QUOTED
SVC-SIT-SUR-001	Site Survey, 4RE Wireless Discovery and Examination	4,375.00	3,500.00
MIC-WRL-TRN-400	Transmitter, Hi-Fi Microphone (additional)	435.00	345.00



COSTARS - 12 PRICE LIST - WatchGuard Video

Cables		MSRP	Contract
MIC-CBN-100-07F	Cabin Microphone - 7'	35.00	25.00
MIC-CBN-EXT-12F	Cabin Microphone Extension Cable - 12'	15.00	10.00
CAB-ETH-STR-10F	Cable Assembly, Straight Ethernet, CAT5e, 10'	15.00	10.00
CAB-ETH-STR-25F	Cable Assembly, Straight Ethernet, CAT5e, 25'	15.00	10.00
CAB-HDM-4RE-15F	4RE, Cable, HDMI/Mini, Display ONLY, Straight, 15'	25.00	19.00
CAB-HDM-4RE-15F	4RE, Cable, HDMI/Mini, Display ONLY, Straight, 15'	25.00	19.00
CAB-FWD-STR-15F	4RE, Cable, HDMI, Front Cam, Straight, 15'	25.00	19.00
CAB-ZSL-STR-15F	4RE, Cable, HDMI, ZSL, Straight, 15'	35.00	25.00
CAB-BST-STR-16F	4RE, Cable, HDMI, Port 2, Backseat Camera, 2-Pin Connect, Straight, 16'	40.00	30.00
CAB-EXT-MMB-15F	Cable Assy, 4RE, Extension, 15', male Molex/BNC, WardMay/Aux Camera	25.00	19.00
CAB-AUX-STR-03F	4RE, Cable, HDMI, Port 2, Dual, Auxiliary Camera, Straight, 3'	35.00	25.00
CAB-AUX-2PN-18I	Cable Assy, Auxiliary Camera (JCC), 4RE Short 18" (2 pin Molex Male)	35.00	25.00
CAB-MHD-STR-15F	CABLE, 4RE, M-HDMI STR to HDMI STR, 15' (HD Mini Zoom)	35.00	25.00
CAB-RIA-100-SRY	Radar Interface Cable for Stalker, Y-Cable, 10'	95.00	75.00
CAB-RIA-101-DG1	Radar Interface Cable for Decatur Genesis I, 12'	95.00	75.00
CAB-RIA-102-KSE	Radar Interface Cable for Kustom Eagle, 12'	95.00	75.00
CAB-RIA-102-KSR	Radar Interface Cable for Kustom Raptor RP-1, 12'	95.00	75.00
CAB-RIA-103-MPH	Radar Interface Cable, MPH Bee 3, Decatur Genesis II, 9 Pin D-Sub, 12'	95.00	75.00
CAB-RIA-104-DG2	Radar Interface Cable for Decatur Genesis II, 7mm LEMO, 12'	95.00	75.00
Brackets		MSRP	Contract
BRK-4RE-FPK-02I	Bracket Kit, 4RE, DVR, Console Faceplate, 2"	45.00	35.00
BRK-4RE-DVR-100	Bracket Kit, 4RE, DVR, Universal	95.00	75.00
BRK-MRU-200-099	Bracket, 4RE DVR, Mounting Shelf Kit, Ford Crown Victoria 1999-2009	95.00	75.00
BRK-4RE-OHD-101	Bracket Kit, 4RE, Display, Chevy Tahoe, 2007+	95.00	75.00
BRK-4RE-OHD-100	Bracket Kit, 4RE, Display, Ford Crown Vic, 2005(b)+	95.00	75.00
BRK-4RE-OHD-103	Bracket Kit, 4RE, Display, Dodge Charger, 2006-2010	95.00	75.00
BRK-4RE-OHD-104	Bracket Kit, 4RE, Display, Universal Visor Post	95.00	75.00
BRK-4RE-OHM-100	Bracket Kit, 4RE, Overhead Multi, Crown Vic (All), Expedition 03-06	95.00	75.00
BRK-4RE-OHM-101	Bracket Kit, 4RE, Overhead Multi, Headliner Clip, Expedition 07-11+	95.00	75.00
BRK-ANT-NMO-001	4RE, WiFi Vehicle Antenna Mount, NMO, Drill 3/4" Hole, 17' long	95.00	75.00
Servers and Storage Hard Drives		MSRP	Contract
HDW-4RE-SRV-001	Tower Server, Intel i7 3.40 GHz, 8GB RAM, 4x2TB SATA 7,200 RPM drives, 5.5TB usable video storage, Windows 7 Pro 64-bit, SQL Server 2008 R2 (1CAL), 3-Year full service (on-site or reimbursed) warranty.	4,360.00	3,481.00
HDW-4RE-SRV-002	Tower Server, Intel i7 3.40 GHz, 8GB RAM, 4x3TB SATA 7,200 RPM drives, 7.8TB usable video storage, Windows 7 Pro 64-bit, SQL Server 2008 R2 (1CAL), 3-Year full service (on-site or reimbursed) warranty.	4,800.00	3,832.00
HDW-4RE-SRV-102	Server, 4RE, 16 HDD, 3U, 6-15 Concurrent Cars, 5CAL, Gen 3 (3U rack mount, 16 SATA hard drive bays, plus 2 X 128GB SSD 6Gbps drives for the OS Partition, SAS backplane, dual 1200W power supplies, Intel XEON E5-1620 V3 3.5 Ghz 4 Core 8 Thread, 8GB (2x4GB), 1.2 V, DDR4 2133 ECC, LSI 9361-4I 12GB RAID SAS, PCIE 3.0, Microsoft Windows Server 2012 R2 64-Bit, Microsoft SQL Server 2012 Standard (5 CALs), 3 Year full service (on-site or reimbursed) warranty.	9,690.00	7,750.00
HDW-4RE-SRV-201	Server, 4RE, 3U, 16-35 Concurrent Cars, 5CAL (3U rack mount, 16 SATA hard drive bays, plus 2 X 128GB SSD 6Gbps drives for the OS Partition, SAS backplane, dual 1200W power supplies, SM X10SRI-F, Intel C612 Chipset, up to 1TB ECC 3DS RAM, PCI-E 3.0, Intel XEON E5-2620 V3 2.4 Ghz 6 Core 12 Thread, 32GB (4x8GB), 1.2 V, DDR4 PC4-1700, LSI 9361-4I 12GB RAID SAS, PCIE 3.0, Microsoft Windows Server 2012 R2 64-Bit, Microsoft SQL Server 2012 Standard (5 CALs), 3 Year full service (on-site or reimbursed) warranty.	11,065.00	8,850.00
HDW-4RE-HDD-4TB	Hard Drive, Server, 4TB, 7,200, 64MB cache 4RE	400.00	300.00
HDW-4RE-HDD-6TB	Hard Drive, Server, 6TB, 7200RPM, 4RE Enterprise Class	550.00	425.00
HDW-4RE-JBD-012	Storage, JBOD Enclosure, 12-bay, 2U, includes SAS Cable	3,220.00	2,575.00
HDW-4RE-JBD-016	Storage, JBOD Enclosure, 16-bay, 3U, includes SAS Cable	3,655.00	2,925.00
HDW-4RE-JBD-024	Storage, JBOD Enclosure, 24-bay, 4U, includes SAS Cable	4,190.00	3,350.00



COSTARS - 12 PRICE LIST - WatchGuard Video

HDW-4RE-JBD-044	Storage, JBOD Enclosure, 4RE, 44-bay 4U, Included SAS Cable	6,220.00	4,975.00
HDW-4RE-RBT-DVD	Primera Bravo 4101 DVD±/CD-R	3,745.00	2,990.00
HDW-4RE-RBT-BLU	Primera Bravo 4101-Blu DVD±/CD-R/BD-R	4,990.00	3,984.00
WAR-SRV-RCK-5YR	Warranty, Rack Server, Full Service On Site, 5-Year (Months 37-60)	1,470.00	1,175.00
Access Point		MSRP	Contract
WAP-BLD-05G-001	4RE, WiFi Access Point, 802.11n, 5GHz, Sector (includes PoE)	315.00	233.00



COSTARS - 12 PRICE LIST - WatchGuard Video

DV-1 In-Car Video System		MSRP	Contract
DV1-EOH-GPS	DV-1, Overhead System. Includes: Overhead Recorder Unit, Combination Front/Cabin Camera, Cabin Microphone, Hardware & Cabling, Lifetime Firmware Upgrades, One (1) Year Factory Warranty, Wireless Microphone Kit, Leather Holster, 10 Pack DVD+RW Evidence Discs, Fleet Manager Utility, DVD Manager Utility	6,240.00	4,920.00
DV1-EMD-GPS	DV-1, Modular System. Includes: Modular Recording Unit, Remote Display Control Panel, Combination Front/Cabin Camera, Cabin Microphone, Hardware & Cabling, Lifetime Firmware Upgrades, One (1) Year Factory Warranty, Wireless Microphone Kit, Leather Holster, 10 Pack DVD+RW Evidence Discs, Fleet Manager Utility, DVD Manager Utility	6,685.00	5,264.00
In-Car Hardware Warranty		MSRP	Contract
WAR-EXT-PUR-2YR	2 Year Extended Factory Warranty (Months 13 to 24)	315.00	250.00
WAR-EXT-PUR-3YR	3 Year Extended Factory Warranty (Months 13 to 36)	700.00	560.00
WAR-EXT-PUR-4YR	4 Year Extended Factory Warranty (Months 13 to 48)	1,185.00	945.00
WAR-EXT-PUR-5YR	5 Year Extended Factory Warranty, DV-1 (Months 13 to 60)	1,790.00	1,430.00
Additional Options		MSRP	Contract
CAM-AUX-SNY-SPR	Camera Assy, Auxiliary, Gimble Bracket Assy, 4RE	245.00	195.00
HDW-SYS-DCS-100	WatchGuard DVD Copy Station PC with preloaded software	2,370.00	1,892.00
PWR-UPS-INT-200	DV-1, iUPS (Intelligent Uninterruptible Power Supply)	190.00	150.00
DVD-EVI-MED-021	DV-1, Disc, Non-Labeled DVD+RW Blank Media	5.00	0.77
DVD-EVI-MED-011	DV-1, Non-Serialized DVD+RW Red Evidence Label Media	5.00	0.99
DVD-EVI-MED-001	DV-1, Serialized DVD+RW Red Evidence Label Disc Media	5.00	1.25
SVC-DV1-INS-100	DV-1 System Installation (Per Unit Charge)	440.00	350.00
MIC-WRL-TRN-400	Transmitter, Hi-Fi Microphone VERSION 2	435.00	345.00
MIC-WRL-DTC-400	Hi-Fi Microphone Desktop Charger Kit 1 (Cradle, and AC Charger)	125.00	99.00
Brackets		MSRP	Contract
BRK-CRC-103-008	Bracket, Installation Kit, Ford Interceptor SUV (Explorer), 2012	190.00	150.00
BRK-CRC-103-009	Bracket, Installation Kit, Ford Sedan (Taurus), 2012+ Interceptor	190.00	150.00
BRK-CRC-111-009	Bracket, Mounting Kit, DV-1 OH, Ford F-150, 2009+	120.00	95.00
BRK-CRC-109-013	Bracket, Mounting Kit, DV-1 OH, Dodge 1500, 2013	120.00	95.00
BRK-CRC-100-012	Bracket, Mounting Kit, DV-1 OH, Chevy Caprice 2014+	160.00	125.00
BRK-CRH-101-006	Bracket, Ceiling Mount Kit, Chevy Impala 2006-2012 (Remove Headliner)	120.00	95.00
BRK-VPM-101-006	Chevy Impala 2006-2009 (with Console)	60.00	45.00
BRK-CRC-103-008	Chevy Tahoe (2015+), Silverado, 2500, Suburban, Sierra (2014+)	220.00	175.00
BRK-VAC-107-004	Chevy Tahoe (with AC Controls) 2004-2006	160.00	124.00
BRK-CRC-107-007	Bracket, Ceiling Mount Kit, Chevy Tahoe PPV 2007-2013 (Remove Console) Ticket Light Included	220.00	175.00
BRK-VPM-107-099	Visor Post Bracket, Chevy Tahoe/Silverado/2500 Truck 1999-2006	60.00	45.00
BRK-VPM-116-006	Chevy Trail Blazer 2006-07	60.00	45.00
BRK-CRC-106-006	Bracket, Ceiling Mount Kit, Dodge Charger 2006-2010	100.00	75.00
BRK-VPM-105-005	Visor Post Bracket, Dodge Durango 2005-2008	60.00	45.00
BRK-VPM-102-003	Dodge Intrepid 2003	60.00	45.00
BRK-VPM-109-006	Dodge Ram 1500 Pickup 2006	120.00	95.00
BRK-VRC-109-000	Dodge Ram 1500 Pickup 2006 (Remove Console)	120.00	95.00
BRK-VRC-109-013	Dodge Ram 1500 Pickup 2009+ (Remove Console)	160.00	125.00
BRK-VPM-100-099	Visor Post Bracket, Ford Crown Victoria 1999-2005(A)	60.00	45.00
BRK-VPM-100-005	Visor Post Bracket, Ford Crown Victoria 2005(B)-2011	60.00	45.00
BRK-VPM-103-001	Ford Expedition 2001-2002	60.00	45.00
BRK-VPM-103-003	Visor Post Bracket, Ford Expedition 2003-2007	60.00	45.00
BRK-VWC-103-000	Visor Post Bracket, Ford Expedition 2006-2007 (with Console)	60.00	45.00
BRK-CRC-103-007	Bracket, Ceiling Mount Kit, Ford Expedition 2007-2012 (Remove Console) Ticket Light Included	220.00	175.00
BRK-VPM-104-000	Ford Explorer 2000	120.00	95.00
BRK-VPM-104-001	Ford Explorer 2001-2002	120.00	95.00
BRK-VPM-104-003	Ford Explorer 2003-2004	120.00	95.00



COSTARS - 12 PRICE LIST - WatchGuard Video

BRK-VPM-104-005	Visor Post Bracket, Ford Explorer 2005-2007	120.00	95.00
BRK-VPM-104-008	Visor Post Bracket, Ford Explorer 2008-2009, (Remove Console) Ticket Light Included	260.00	205.00
BRK-VPM-111-001	Visor Post Bracket, Ford F-150 Pickup 2001	60.00	45.00
BRK-VPM-111-006	Visor Post Bracket, Ford F-150 Pickup 2006	60.00	45.00
BRK-CRC-111-007	Ford F-150 SuperCrew Pickup 2007-08 (Remove Console)	160.00	125.00
BRK-CRC-111-009	Ford F-150 Pickup 2009-2014 (Remove Console)	160.00	125.00
BRK-VPM-112-006	Ford F-250 Pickup 2006-2009	120.00	95.00
BRK-VPM-114-006	Ford Van E150/E350 2006	60.00	45.00
BRK-RDM-100-06I	Bracket, Modular Remote Display Mount, Rigid - 6"	50.00	39.00
BRK-RDM-100-09I	Modular Remote Display Mount, Rigid - 9"	60.00	45.00
BRK-RDM-100-12I	Modular Remote Display Mount, Rigid - 12"	60.00	45.00
BRK-RDM-200-10I	Modular Remote Display Mount, Flex - 10"	60.00	45.00
BRK-RDM-200-12I	Modular Remote Display Mount, Flex - 12"	60.00	45.00
BRK-RDM-200-14I	Modular Remote Display Mount, Flex - 14"	60.00	45.00
BRK-RDM-RAM-100	Modular Remote Display Mount, Headliner (RAM Mount)	160.00	125.00
BRK-VFS-100-005	Modular Remote Display Visor Post Kit, Ford Crown Victoria 2005-2009 (with Fire Suppression System)	200.00	159.00
BRK-MRU-100-000	Bracket, Modular Recording Unit Base Mounting Plate	35.00	25.00
BRK-MRU-200-099	Bracket, 4RE DVR, Mounting Shelf Kit, Ford Crown Victoria 1999-2009	100.00	79.00



COSTARS - 12 PRICE LIST - WatchGuard Video

VISTA Wearable Camera System		MSRP	Contract
VIS-STD-KIT-001	VISTA Standard Capacity Wearable Camera System. Capable of High Definition (720P) video recording for 6 continuous hours (standard definition recording also available). Includes a transfer/charging base, mounting hardware, One (1) Year Factory Warranty, and Evidence Library Express software.	995.00	795.00
VIS-EXT-KIT-001	VISTA Extended Capacity Wearable Camera System. Capable of High Definition (720P) video recording for 9 continuous hours (standard definition recording also available). Includes a transfer/charging base, mounting hardware, One (1) Year Factory Warranty, and Evidence Library Express software.	1,120.00	895.00
VIS-EXT-WIF-001	VISTA HD, WiFi Extended Wearable Camera (Camera Only)	1,250.00	995.00
VIS-CHG-WIF-BSE	VISTA HD, WiFi Charging Radio Base Station	250.00	200.00
HDW-ETH-SWT-005	4RE, VISTA HD WiFi, Smart PoE Switch	245.00	195.00
SFW-MOB-APP-001	VISTA Mobile Companion (ELX/EL4 No Maintenance)	95.00	75.00
SFW-MOB-APP-002	VISTA Mobile Companion (EL4 w/Maintenance)	Included	Included
VIS-CHG-DTC-001	VISTA USB Charge and Upload Docking Base	120.00	95.00
VIS-MNT-KIT-002	VISTA HD Locking Chest Mount without Straps	80.00	60.00
VIS-BLT-CLP-001	VISTA HD Duty Belt Clip	25.00	20.00
VIS-BLT-CLP-100	VISTA HD Shirt Clip with Slider	40.00	30.00
VIS-MNT-MOL-001	VISTA HD, Molle Vest Adapter Clip	\$25.00	\$20.00
VIS-MNT-TRI-001	VISTA HD, Tripod Mount Base Adapter	\$45.00	\$35.00
VIS-MNT-VEL-001	VISTA HD, Velcro Backing Plate (with Hook/Loop Velcro Set uninstalled)	\$25.00	\$20.00
VIS-MNT-KLK-001	VISTA HD, "Klick Fast" Mount Adapter	\$45.00	\$35.00
VIS-MNT-RAM-001	VISTA HD, Ram Mount Kit	\$45.00	\$35.00
VIS-MNT-RAM-002	VISTA HD, Suction Cup RAM Mount Kit, 6" Arm	\$155.00	\$125.00
VIS-USB-HUB-001	VISTA HD 7 Port USB Hub	40.00	30.00
VIS-VTS-DTC-001	VISTA HD 8 Bay Ethernet Transfer Station	1,870.00	1,495.00
VIS-WRL-BAT-100	VISTA HD Extended Battery, LI-ION, 3.6V 4050mAH	55.00	40.00
VIS-WRL-BAT-001	VISTA HD Standard Batter, LI-ION, 3.6V 2700mAH	40.00	30.00
WAR-VIS-CAM-1ST	VISTA HD Warranty, Standard 1st Year	-	-
WAR-VIS-CAM-NOF	VISTA HD No Fault Warranty, Years 1-3	475.00	380.00

BID ITEM WORKBOOK**COSTARS-12 Emergency Responder Loose Supplies****BID ITEM SHEET****BIDDERS/CONTRACTORS LEGAL NAME**

Enforcement Video, LLC

PRICING

The Bidder may offer any type of discount, mark-up, or other pricing structure such as multiple discounts for different lines of products, or different price lists, or different classes of Purchasers, or different prices for different quantities of products. Please reference Subsection 6.b. of the Special Terms and Conditions for further guidance.

After Contract award, a Contractor may offer, either on its own initiative or at a Purchaser's request, additional discounts, reduced mark-ups, customized lists, or discounted prices for any purchase within the scope of the Contract, even if such discounts, mark-ups, or discounted prices were not included in the bid prices.

The Bid Item Workbook should contain a separate Bid Item Sheet for each manufacturer's price list or cost sheet.

MANUFACTURER:

Enforcement Video, LLC

PRICING STANDARD: (Check that which is applicable.)

____ Catalog or Manufacturer's/Distributor's Most Recently Published Price List Less % of Discount
____ Suppliers Cost Plus % of Mark-up
____ x Custom List including Net Prices

PRICE LIST IDENTIFICATION:**CATALOG OR PRICE LIST NAME:** COSTARS - 12 Price List**IDENTIFICATION NO. (IF APPLICABLE):** _____**EFFECTIVE DATE:** _____

27-Sep-13

CLASS OF PURCHASER: All Purchasers

(i.e. All Purchasers or separate lines for specific classes, such as Educational Purchasers and Non-educational Purchasers.)

WatchGuard Video		
Law Enforcement / Public Safety Equipment and Supplies		
Part Number	Description	Net Price
DV1-EOH	DV-1 5TH Generation Overhead In-Car Video System	4,895.00
DV1-EMD	DV-1 5TH Generation Modular In-Car Video System	5,250.00
4RE-STD-GPS	4RE HD In-Car Video System	4,790.00
4RE-64S-GPS-MTR	4RE HD Motorcycle Video System	5,295.00
4RE-200-VIS-INT	4RE HD In-Car Video System w/Integrated VISTA WiFi	5,495.00
4RE-200-INT-001	4RE Interview Room Solution, One Camera Package	4,995.00
4RE-200-INT-002	4RE Interview Room Solution, Two Camera Package	5,195.00
KEY-EL4-SRV-001	Evidence Library 4 Web Server Site License	1,000.00
KEY-EL4-DEV-001	Evidence Library 4 Web 4RE In-Car Device License	150.00
KEY-EL4-DEV-002	Evidence Library 4 Web VISTA Device License	150.00
KEY-EL4-DEV-003	Evidence Library 4 Web 4RE Combo-Discount Device License Key	75.00
KEY-EL4-DEV-004	Evidence Library 4 Web VISTA Combo-Discount Device License Key	75.00
SFW-WCM-LIC-FEE	Watch Commander License Fee (per car)	250.00
SFW-WCM-KIT-100	Watch Commander Software Installation Disc w/ Case and Document	2,500.00
VST-STD-KIT-001	VISTA HD Standard Capacity Wearable Camera	795.00
VST-EXT-KIT-001	VISTA HD Extended Capacity Wearable Camera	895.00
VIS-EXT-WIF-001	VISTA HD, WiFi Extended Wearable Camera (Camera Only)	995.00
KEY-WGV-RED-001	Software, REDACTIVE(sm), Single Seat License	3,995.00
WAR-WGR-MNT-001	Software Maintenance, REDACTIVE(sm), 1st Year (Months 1-12)	785.00
WAR-WGR-MNT-002	Software Maintenance, REDACTIVE(sm), 2nd Year (Months 13-24)	785.00
WAR-WGR-MNT-003	Software Maintenance, REDACTIVE(sm), 3rd Year (Months 25-36)	785.00
WAR-WGR-MNT-3YR	Software Maintenance, REDACTIVE(sm), 3-Year Bundle (Months 1-36)	2,250.00
WAR-WGR-MNT-ADD	Software Maintenance, REDACTIVE(sm) +1 Extended Addiitonal Year	785.00



9652 Loiret Blvd.
Lenexa, KS 66219
800.458.7866

Contact: David Nicholl and Rod Smith

Due: Friday, January 25, 2019 at 4:00PM

Request for Information Police Body Worn Cameras





9652 Loiret Blvd TEL: 800.458.7866
Lenexa, KS 66219-2406 913.492.1400
www.KustomSignals.com FAX: 913.492.1703

January 24, 2019

Christopher J. Braun M.S. IT
Technology Coordinator Pennsylvania Chiefs of Police Association
3905 N. Front Street
Harrisburg, PA 17110

SUBJECT: Request for Information Police Body Worn Cameras
DUE DATE: Friday, January 25, 2019 at 4:00PM

Dear Mr. Braun:

Kustom Signals, Inc. has been serving the needs of law enforcement agencies for more than 50 years. We appreciate the opportunity and look forward to working with the Pennsylvania Chiefs of Police Association (PCPA) in cooperation with the Local Technology Workgroup (LTW) of the Pennsylvania Commission on Crime and Delinquency (PCCD). Kustom Signals is offering our state-of-the-art Eyewitness Vantage which will add significant value to your law enforcement program and enhance traffic safety, officer safety, and public safety.

We strive to be the worldwide leader in speed enforcement, the most trusted provider of video evidence solutions and the recognized leader in customer satisfaction. Our history of innovation, commitment to quality, customer loyalty, and focus on service has forged Kustom Signals' identity, and as a direct result we are serving our third generation of officers. We are dedicated to working hard for our customers and are positioned to meet the requirements in the enclosed proposal. Supporting a spirit of cooperation to guarantee your needs are met earns not only your business, but more importantly, your trust.

Our highly qualified team, consisting of Video Product Manager David Nicholl and Domestic Sales Manager Rod Smith, is available to answer questions. Please feel free to contact David at 800-458-7866 extension 3008 and/or Rod at 1-800-458-7866 extension 913-302-8487.

Kustom Signals is well known as an established leader in the law enforcement community and we look forward to sharing our industry experience and robust product offerings with the PCPA.

Sincerely,

A handwritten signature in blue ink that reads 'Chris N. Abel'.

Chris Abel, President

cc: David Nicholl, Video Product Manager
Rod Smith, Domestic Sales Manager

Your Trusted Partner in Law Enforcement

Information Requested

How does your non-vehicle-mounted mobile video recording systems and technology meet Pennsylvania's published requirements?

Kustom Signals' Eyewitness Vantage meets the following published requirements:

The design of the non-vehicle-mounted mobile video recording system must use technology which includes a camera with date/time stamp capability, a microphone and a recording device, enclosed in secure protective enclosure(s). It may also contain controls, a monitor, GPS, wireless transceiver components and other electronic components. The non-vehicle-mounted mobile video recording system must be powered from a battery internal to the protective enclosure and must be weatherproof. The internal battery may be integral to the unit or removable. It is permissible to have an external battery to extend the operating life of the system. The non-vehicle-mounted mobile video recording system must have a minimum record time of 2 continuous hours. The system must operate over the following temperature range: -4°F to 122°F (-20°C to 50°C).

Camera

The camera component must have the following features:

- A. Must be color video.
- B. Minimum of 640 x 480 pixel resolution.
- C. Minimum of 68 degrees field of view.
- D. Minimum of 30 frames per second.
- E. Minimum sensitivity rating of 3.4 lux or lower. Unit may use Infrared LED illumination to obtain lower than 3.4 lux equivalent.
- F. Camera does not have to be in the same enclosure as the recorder. Can be connected to the recorder either by cable or wireless connection.

Recorder

The recorder component must have the following features:

- A. Enclosed in a secure housing protected from physical damage.
- B. Date/time recording index.
- C. Minimum of 4 gigabytes of nonremovable solid state memory, 4 gigabytes removable media or a combination of both removable and nonremovable memory.
- D. Editing and record-over protection.

System Control

The system must:

- A. Be capable of recording audio and video simultaneously, but may also provide the user with the option to record video only or audio only.
- B. Provide the user with the capability to manually turn the power on and off as necessary.

Wireless Link (optional)

The unit may use a wireless link to connect the camera to the recorder, recorder to another device, combination camera/recorder to another device or be used to download the evidence.

The wireless link must have the following features:

- A. Use a secure digital connection.
- B. Wireless link can be used to play back a locally stored event on the recorder or store the media to a remote location such as secure Cloud storage.
- C. FCC Type acceptable under 47 CFR Part 15 (relating to radio frequency devices).

Eyewitness Vantage is a one-piece body-worn camera that provides one-handed, glove-friendly start and stop record functionality. The large start/stop slider is centrally located and is spring loaded to provide tactile feedback so the officer has confidence the camera is in or out of record mode.

Notification LED's provide battery status, record status and file transfer activity. These LED's can be blacked out for officer safety.

Vantage includes the following features:

- Configurable high and standard definition resolution at 1080p at 30 fps; 720p at 60 fps; 720p at 30 fps; and D1 (480p) at 30 fps all using MPEG4 h.264 file format
- 120 degree wide-angle lens without the peripheral distortion found on other body-worn cameras
- Non-removable 32GB compact flash storage
- Configurable pre-event recording (up to 30 seconds for all resolution options)
- Battery life – Standard battery provides 48 hours of operation in Power Save mode - up to 4 hours continuous use in Standby mode. Extended provides 96 hours of operation in Power Save mode - up to 8 hours continuous use in Standby mode.
- Storage capacity (on internal 32GB solid state storage) – up to 6 hours 1080p/30, up to 6 hours 720/60, up to 14 hours 720p/30, up to 17 hours 480p
- Configurable audio mute button
- Configurable bookmark button
- GPS location tagging with incident/bookmarking button (track officer location and incidents during playback in back office software)
- Configurable day/night mode for even better low-light performance
- Configurable infrared illuminators (optional) to see in the dark
- Configurable “beep” and/or “buzz” record status notification
- LEDs provide status of battery capacity, internal media capacity, file transfers, low media, record, and audio mute

The Vantage ships with a rugged spring clip designed to withstand rigorous law enforcement work environments. The clip rotates 360 degrees allowing for flexible uniform mounting locations. An optional magnetic mount is available that allows the camera to be mounted anywhere on the uniform shirt. No modifications will be needed to the current uniform. Should additional mounting options be desired, an interface to Peter Jones' Klickfast mounts is also under development. Please refer to this link for more information: <http://www.peterjonesilg.co.uk/equipment-cameras/index.html>.

Each Vantage comes standard with a docking station for charging and downloading files to the file management system. Multi-docks are available to facilitate larger installations – multiple cameras can be simultaneously transferring files and recharging their internal batteries.

Please refer to the attached product specification sheet at the end of this document for additional product information.

Have you submitted your non-vehicle-mounted mobile video recording systems to the Pennsylvania State Police for certification?

Kustom Signals has not yet submitted the Eyewitness Vantage for certification, but would be very interested in doing so.

Is your non-vehicle-mounted mobile video recording system already certified by the Pennsylvania State Police?

Kustom Signals Eyewitness Vantage is not already certified by the Pennsylvania State Police.

Are you offering a storage solution?

The Eyewitness Data Vault (EDV) file management system allows agencies to easily transfer, store and manage video files recorded by Kustom Signals' in-car video and/or body-worn video systems. EDV provides quick and easy file searching, easy playback and file duplication. Storage can be expanded locally. EDV is also compatible with Active Directory and LDAP to allow established log in credentials to be used. Kustom Signals does not currently offer a cloud-based solution.

When comparing local storage to cloud storage for the video files, Kustom Signals believes you will find pros and cons to each option. Cloud storage takes the responsibility of maintaining the storage off the agency, but it also comes at a cost that can be significantly higher than purchasing and maintaining storage on-site. Further, to end a cloud storage agreement, there can be fees to retrieve video back from the provider, and files retrieved may not include any of the history of what happened with that file. A local storage option is something that the agency owns and has full control over. In the event the agency moved to another body camera provider after several years, the critical evidence and all its history would still be contained on the database maintained and located on hardware owned by the agency. For these reasons, we believe local storage from the on-set is currently the most cost effective solution.

Please refer to the attached product specification sheet for Eyewitness Data Vault Back Office Software at the end of this document for additional product information.

Will you offer storage solutions bundled (no line item distinction) with the cost of each camera purchased?

Kustom Signals can bundle the cost of the storage unit into the cost of the each camera purchased if more than 30 cameras are purchased together.

How does your storage solution meet Pennsylvania's published requirements?

Kustom Signals storage solution supports agency compliance with 18 Pa.C.S. § 5706(b)(5), the following minimum requirements that must be met for any storage of an audio recording made in accordance with 18 Pa.C.S. § 5706(b)(4), or any accompanying video recording:

A. Camera system

1. While worn by the officer, a camera system shall be considered a physically secure location.
2. Upon removal from the officer's body, the camera system shall be maintained in a physically secure location in accordance with CJIS Policy standards.
3. If a camera system is located in a criminal justice conveyance, it shall be considered located in a physically secure location. If the camera or hard drive is removed from the criminal justice conveyance, it shall conform with the CJIS Policy. A criminal justice conveyance is any enclosed mobile vehicle used for the purposes of criminal justice activities with the capability to comply, during operational periods. A physically secure location, as stated in section 5.9.1 of the CJIS Policy (relating to physically secure location) is as follows:

A physically secure location is a facility, a criminal justice conveyance, or an area, room or a group of rooms within a facility, with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control, State Identification Bureau control, FBI CJIS security addendum, or a combination thereof, and shall consist of the following:

- a. Security perimeter—area that is posted, separated and secured.
- b. Physical access authorizations—list of authorized personnel.
- c. Physical access control—control all physical access points (AP).
- d. Access control for transmission medium—control physical access to information systems, distribution and lines.
- e. Access control for display medium—not visible to unauthorized personnel.
- f. Monitoring physical access—monitor and respond to security incidents.
- g. Visitor control—authenticate and escort visitors.
- h. The agency shall authorize and control information system-related items entering and exiting the physically secure location (delivery and removal).

B. Data transfer or downloading the data

1. If accomplished through a wireless connection, agencies shall meet the CJIS Policy requirements, as stated in section 5.13.1.1 (relating to 802.11 wireless protocols).
Note: Wired Equivalent Privacy and Wi-Fi Protected Access cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for Federal Information Processing Standard (FIPS) 140-2 and may not be used.
2. Agencies shall implement the following controls for all agency-managed wireless APs with access to an agency's network that processes unencrypted CJI:
 - a. Perform validation testing to ensure rogue APs do not exist in the 802.11 wireless local area network and to fully understand the wireless network security posture.
 - b. Maintain a complete inventory of all APs and 802.11 wireless devices.

- c. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
 - d. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.
 - e. Enable user authentication and encryption mechanisms for the management interface of the AP.
 - f. f. Ensure that all APs have strong administrative passwords and ensure all passwords are changed in accordance with section 5.6.2.1 of the CJIS Policy (relating to standard authenticators), as follows:
 - (1) Be a minimum length of eight characters on all systems.
 - (2) Not be a dictionary word or proper name.
 - (3) Not be the same as the user ID.
 - (4) Expire within a maximum of 90 calendar days.
 - (5) Not be identical to the previous ten passwords.
 - (6) Not be transmitted in the clear, outside the secure location.
 - (7) Not be displayed when entered.
 - g. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.
 - h. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, and the like) or services.
 - i. Enable all security features of the wireless product, including the cryptographic authentication, firewall and other available privacy features.
 - j. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
 - k. Ensure that the ad-hoc mode has been disabled.
 - l. Disable all nonessential management protocols on the APs.
 - m. Ensure all management access and authentication occurs through FIPS-compliant secure protocols (for example, SFTP, HTTPS, SNMP over TLS, and the like). Disable non-FIPS-compliant secure access to the management interface.
 - n. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum, logs shall be reviewed monthly.
 - o. Insulate, virtually (for example, virtual local area network and access control lists) or physically (for example, firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.
 - p. When disposing of APs that will no longer be used by the agency, clear AP configuration to prevent disclosure of network configuration, keys, passwords, and the like.
3. 3. If the data is manually downloaded by an individual or retained outside of a physically secure location, it will need to be encrypted at rest and in transit, per sections 5.10.1.2.1 and 5.10.1.2.2 of the CJIS Policy (relating to encryption for CJI in transit; and encryption for CJI at rest).

C. Storage of the data

Storage of data on location, if considered a physically secure location, shall be treated the same as all CJI at the location. Storage offsite, or in the cloud, shall meet all the requirements of the CJIS Policy for encryption while in transit and at rest, if applicable. If encryption is not used at rest, any person with access to the data or systems storing the data shall be properly vetted with a fingerprint-based background check and Security Awareness Training, and required agreements shall be maintained.

1. As stated in section 5.10.1.2.1 of the CJIS Policy: When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit strength to protect CJI.
2. As stated in section 5.10.1.2.2 of the CJIS Policy: When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption. When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.

D. Reviewing and release of data

1. Data from the camera system shall only be reviewed by authorized personnel; that is, personnel that have been cleared through a fingerprint-based background check, have received Security Awareness Training and have signed the appropriate agreements, if applicable. If required, the Management Control Agreement for local government IT, or The Security Addendum for private contractors, shall be completed and on file.
2. Prior to the release of data from the camera system, the data shall be reviewed and any areas containing CJI shall be removed or rendered unintelligible. Any data received from CLEAN or the National Crime Information Center in either video or audio format, or both, shall be removed or rendered unintelligible prior to release to any unauthorized or unintended personnel.

E. Retention of data

Data shall be stored for 60 days unless needed for prosecution, courts, litigation, appeals or other operational needs.

F. Destruction of data

The data, or the data storage devices that are to be destroyed, shall be destroyed in compliance with the CJIS Policy, and a written destruction procedure that complies with the CJIS Policy shall be maintained at the agency. As stated in section 5.8.3 of the CJIS Policy (relating to digital media sanitization and disposal): The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

List the products and services that are already available on State Contract or PA CoStars.

Kustom Signals has a contract in place with PA CoStars that includes the following equipment:

- Eyewitness HD In-Car Video System Basic Package w/tablet controller
- Eyewitness HD In-Car Video System Basic Package with MDC interface
- Eyewitness HD In-Car Video System Bundled w/tablet controller
- Eyewitness HD In-Car Video System Bundled with MDC interface
- Vantage Body Worn Video Camera with Standard Battery
- Vantage Body Worn Video Camera with Extended Battery
- Eyewitness Data Vault LITE Back Office Video File Management Software License (CRS 4299)
- Eyewitness Data Vault HQ Video File Management Software License (CRS 4324)
- Eyewitness Data Vault (EDV) Precinct Video File Management Software License (CRS 4325)
- EDV 12000 - includes a workstation with 12TB storage (CRS 4300)
- EDV 24000 - includes a workstation and server w/24TB integrated RAID storage (CRS 4301)
- EDV 32000 includes a workstation and server w/32TB integrated RAID storage (CRS 4302)
- EDV 40000 includes a workstation and server w/40TB integrated RAID storage (CRS 4303)
- EDV 72000 includes a workstation and server w/72TB integrated RAID storage (CRS 4304)
- EDV 96000 includes a workstation and server w/96TB integrated RAID storage (CRS 4305)
- EDV 120000 includes a workstation and server w/120TB integrated RAID storage (CRS 4306)
- EDV Viewing Workstation (CRS 4308)
- EDV Extended Software Support Per Year (CRS 4326)
- Wireless Access Point Kit - Ubiquiti
- Wireless Access Point Accessory Kit (1 kit per site supports up to 6 A/Ps)
- Field Application Engineer (FAE) Time:
 - Includes one day of on-site installation services for service, installation, testing and training
- SMART 650 Speed Awareness Trailer
- SMART 650+ Speed Awareness Trailer
- SMART 800 Speed Awareness Trailer
- SMART 800+ Speed Awareness Trailer
- SMART 850 Speed Awareness Trailer
- SMART 850+ Speed Awareness Trailer
- SMART VMS Model I Speed Awareness Trailer
- SMART VMS Model II Speed Awareness Trailer
- SMART VMS Model III Speed Awareness Trailer
- SMART VMS HT Speed Awareness Trailer
- SMART 275 Pole-Mounted Speed Awareness Display
- SMART 350 Pole-Mounted Speed Awareness Display
- SMART 375 Pole-Mounted Speed Awareness Display
- SMART 400 Pole-Mounted Speed Awareness Display
- SMART 450 Pole-Mounted Speed Awareness Display
- SMART 475 Pole-Mounted Speed Awareness Display
- Tracker

Falcon HR Hand-Held Stationary Radar with Fastest and Carrying Case
 Falcon HR Hand-Held Moving/Stationary Radar with Fastest, 7" Dash Mount & Bracket, and Carrying Case
 Falcon HR Hand-Held Moving/Stationary Radar with Fastest, Same Direction Mode, 7" Dash Mount & Bracket
 and Carrying Case
 Golden Eagle II Dash-mounted Dual KA Band Radar
 Directional Golden Eagle II Dash-mounted Dual KA Band Radar
 Raptor Dash-mounted Single K Band Radar
 Raptor Dash-mounted Dual K Band Radar
 Raptor Dash-mounted Single KA Band Radar
 Raptor Dash-mounted Dual KA Band Radar
 Eagle 3 Dash-mounted Single Ka-band antenna
 Eagle 3 Dash-mounted Dual Ka-band antenna

Will you offer a discount of those prices if multiple police departments group together to buy your products and services?

Yes, Kustom Signals offers discounts on quantity purchases with the following breakdown of 6-14 units and 15+ and will honor these price breakdowns if multiple departments would like to make group purchases.

Our standard price breakdown follows:

Internal Part Number	Description	List Price	1-5 Selling Price	6-14 Selling Price	15+ Selling Price
8000	Vantage, Standard Battery, 32GB	\$ 844	\$ 675	\$ 635	\$ 595
8001	Vantage, Extended Battery, 32GB	\$ 931	\$ 745	\$ 700	\$ 655

Other Relevant Information

History of Kustom Signals

Kustom Signals, Inc. has been dedicated to serving the public safety equipment needs of law enforcement for more than 50 years. We strive to be the **worldwide leader in speed enforcement, the most trusted provider of video evidence solutions and the recognized leader in customer satisfaction**. Our vast array of durable and reliable products positions us to be the Village of Schaumburg's (Village) complete traffic safety equipment source.

Kustom Signals' innovative accomplishments have been marked by the following industry firsts:

- 1970-First Digital Readout Radar (TR6)
- 1972-First Moving Radar (MR7)
- 1975-First Handheld K-band Radar (HR-8)
- 1975-First Two-window Microprocessor Based Radar (KR-11)
- 1976-First Statistical Package (STATPACK for KR-11)
- 1978-First Moving K-band Handheld Radar (HR-12)
- 1979-First Instant-On Function (KR-10)
- 1985-First All-Direction Mode Radar with Stopwatch Mode (H.A.W.K.)
- 1988-First Speed Monitoring Awareness Radar Trailer (SMART)
- 1988-First Patrol Car Video System with Temperature-Controlled Vault (Eyewitness)
- 1990-First LIDAR with Heads-Up-Display (ProLaser)
- 1990-First LIDAR with Continuous Tracking History (ProLaser)
- 1990-First LIDAR with Settable Range (ProLaser)
- 1992-First In-Car Video System with Auto Zoom (Eyewitness)
- 1992-First In-Car Video System with Wireless Microphone Record Activation (Eyewitness)
- 1994-First Three-Window Time/Distance/Speed Computer (Tracker)
- 1994-First Digital Signal Processing based Radar with Fastest Vehicle Mode (EAGLE)
- 1994-First Digital Signal Processing based Radar with Multi-band Antennas (EAGLE)
- 1994-First Digital Signal Processing based Radar with Wireless Remote Control (EAGLE)
- 1996-First Speed Monitoring Trailer with Free-Flow Statistics Method (SMART)
- 1996-First Speed Monitoring Trailer with Violator Alert (SMART)
- 1998-First Digital Signal Processing based Radar with TruTrak Speedometer Input (EAGLE)
- 1998-First Covert, Pole-Mounted Traffic Statistics Gathering Device (StealthStat)
- 1999-First LIDAR with Selectable Environmental Mode (ProLaser III)
- 2002-First Digital In-Car Video Offering Multiple Recording Media Options (Digital Eyewitness)
- 2004-First Digital In-Car Video that Offered Multiple Compression Options and Multiple File Transfer Options (Eyewitness NXT)
- 2004-First In-Car Video Offering Dual Control for MDC and Dedicated Controller (Eyewitness NXT)

- 2006-First Binocular Style Speed Enforcement Laser (Pro-Lite+)
- 2006-First Traffic Lidar to be Powered with AA Batteries
- 2007-First Handheld K-band Planar Array Antenna (Falcon HR)
- 2007-First Traffic Safety Video Lidar with Moving Operation (LASERwitness)
- 2008-First Two-Piece Radar with a Graphical Display (Raptor)
- 2008-First Radar with Target Tracking Bar - DuraTrak™ (Raptor)
- 2006-First two-piece radar with K-band Planar Array Antenna (Raptor)
- 2010-First Four Camera Simultaneous Recording Video, Offering 30 fps and 720x480 Resolution on all Four Channels (G3 Vision)
- 2010-First Digital In-car Video System Utilizing Windows Internet Explorer as MDC User Interface – No Client Application Installed on MDC (G3 Vision)
- 2010-First to Offer a Look-back Buffer on Two Channels (G3 Vision)
- 2011-First Traffic Lidar with Recalled Events Database (ProLaser 4)
- 2011-First Traffic Lidar to be Powered by AA, USB, or 12 VDC Power (ProLaser 4)
- 2013-First Video Laser with AutoTrak™ Automatic Zoom (LaserCam 4)
- 2015-First In-Car Video with Tablet-like User Interface (Eyewitness HD)
- 2015-First In-Car Video with Dedicated Controller Using (essentially) the Same GUI as the MDC Interface (Eyewitness HD)
- 2016-First Body Worn Camera to Offer Pre-Event, GPS, Audio Mute, Bookmarking, Day/Night Mode, and IR LEDs All In One Package (Eyewitness Vantage)

Financial Stability

Founded in 1965 in rural southeastern Kansas, Kustom Signals has grown into a global enterprise. Our history, integrity, collaboration and dedication have enabled Kustom Signals to prosper and the associates, leaders and owners are committed to the company's ongoing business expansion.

Kustom Signals is a wholly owned subsidiary of MPD, Inc. and proudly participates in an Employee Stock Ownership Plan. Earnings from the business continue to be reinvested in product development, operational improvements, productivity tools and key staff additions. We anticipate solid earnings and growth for the foreseeable future.

We have the productive capacity as well as the financial strength and management expertise to successfully deliver what you need. Additionally, we are aligned with strong and successful suppliers who are not only key to our success in product development and manufacturing, but have sufficient capacity to grow with us. Kustom Signals is here to stay.

Customer Service Support

One number...a bundle of services. Kustom Signals' Factory Service Center, which is located in Chanute, Kansas, repairs every product manufactured by Kustom Signals. Additionally, we make it our goal to provide superior support to each and every one of our customers.

After initial implementation is complete, product support (in warranty as well as out of warranty) is structured so the Village receives the necessary assistance from our Factory Service Manager and Kustom Signals' Factory Service Center. In addition to our Factory Service Center support, Regional Sales Manager Jeff Williams and Account Manager Sonya Schoneman are also available to provide assistance as needed.

Kustom Signals' commitment continues long after the sale. Through our extensive service offerings, we link you directly with dedicated and experienced technicians who perform comprehensive diagnostics and resolution for your vehicle and traffic safety equipment needs. Technical support specialists are accessible at our factory through our toll-free telephone number, (800) 835-0156, between 7:00 a.m. and 6:00 p.m. Central Time, Monday through Friday. The type of support needed may vary, as will the person that should be contacted. The sales team will always help connect you to the right support specialist, or you can also visit our website at www.kustomsignals.com, go to the Service & Support drop-down menu, and select Customer Service Contacts. This provides a list of contact information for various parts of our service business. Each support specialist has a minimum of two years of experience as a production technician or service technician, providing a high level of product expertise.

Commitment to Providing Quality Products

The Village can be assured that Kustom Signals' executive-level management will be made aware of potential problems and involved in the resolution. Our commitment to providing top-of-the-line products enhances serviceability. In the event a problem is encountered, the strategy for the resolution begins at the top of our organization. Each week a teleconference is held to review weekly reports received from District Managers and Account Managers.

The purpose of this meeting is to prepare operations for upcoming orders and to discuss potential as well as existing customer concerns. To be proactive in handling potential issues as well as addressing any outstanding issues, action plans are formulated before the meeting is adjourned. Through these meetings and timely follow-up, our top executives are kept informed of concerns directly affecting agencies and can implement the necessary corrective and preventive measures.

By preventing and/or correcting issues related to quality, service, cost and delivery schedules, in a timely manner, Kustom Signals' customers can expect to purchase higher quality products at lower prices. Customer service is a key element of our success. The organization, infrastructure, and supporting processes are focused on ensuring exceptional customer satisfaction for every customer. Kustom Signals spares no effort to ensure a customer's satisfaction is fully met regarding product and service quality, because you are our #1 priority.

Trust Kustom Signals

- **History and Tradition:** Kustom Signals has been serving the public safety equipment needs of law enforcement agencies for more than 50 years. We are proud that three generations of officers have had access to our products. With the most experience in the industry, our solutions meet the needs of more than 17,000 customers across the United States and in 60 foreign countries. Each day Kustom Signals strives for excellence in everything we do.
- **Consistency:** The heritage and reputation of Kustom Signals have been built on a solid Midwestern work ethic. Law enforcement is our only business. We design, assemble, and support our products with Kustom Signals employees, not contractors. In this way, we maintain the quality that our customers have come to expect.

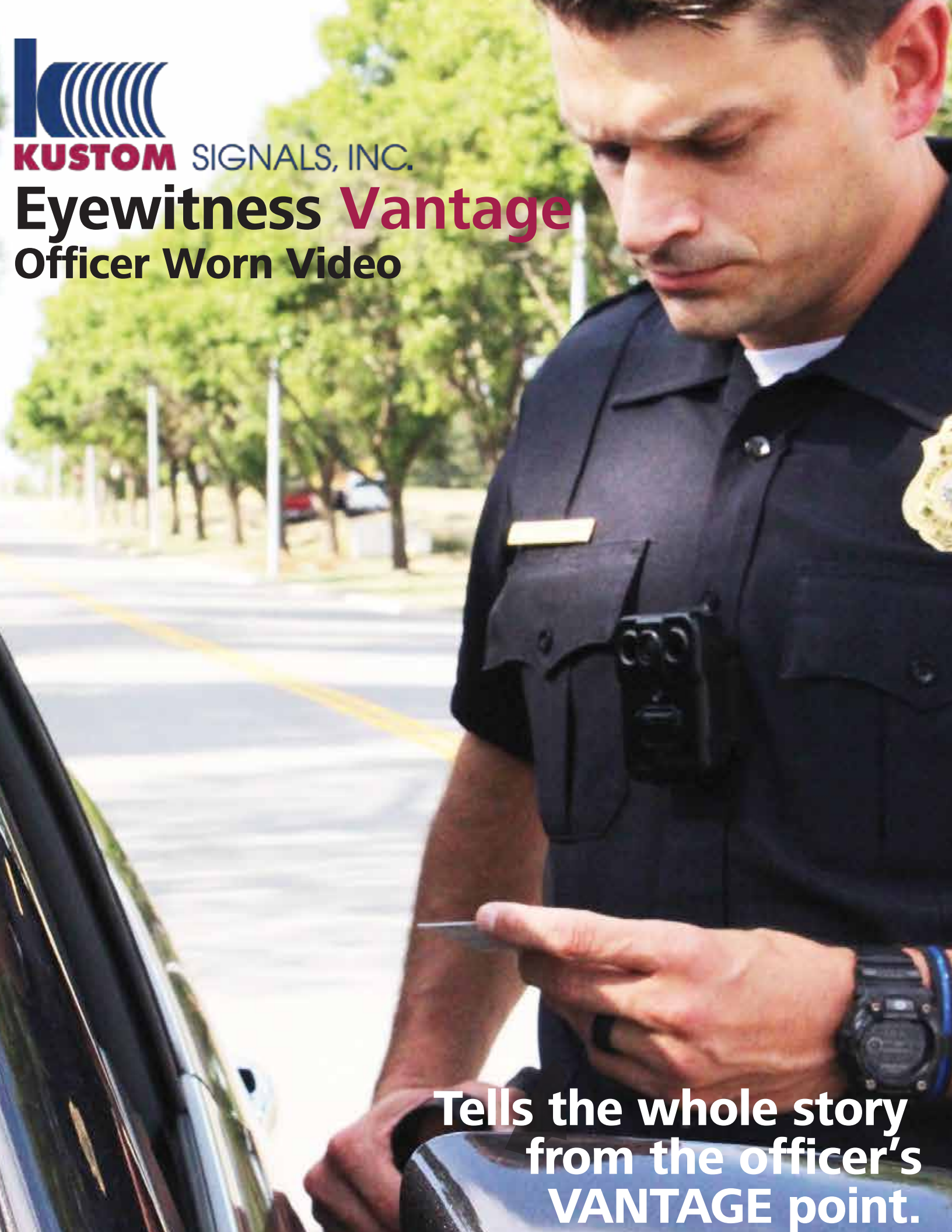
- **Versatility:** Designing and marketing traffic speed radar, lidar, in-car video systems and mobile roadside speed monitoring trailers/displays positions Kustom Signals to be a one-stop-shop for agencies. Our products have been specifically designed for the law enforcement industry, taking into consideration the harsh environment they will encounter. You can feel confident in our products – our team would not sell a product that each of us would not use ourselves.
- **Financial Stability and Support:** Kustom Signals is financially sound and continues to be a strong and growing company. Our long-standing history proves our stability, followed by the fact that officers trust our systems.
- **Customer Focus:** As a full-service solutions provider, Kustom Signals provides product breadth, advanced technology and personalized service support. Our success in the law enforcement industry is because we focus on quality awareness and customer satisfaction.
- **Robust Solutions:** Kustom Signals takes pride in knowing that our solutions are customizable and will help enhance officer safety, ensure accountability and reduce liability.

Kustom Signals is proud to be your trusted partner in delivering critical law enforcement solutions.

Attachments

Please refer to the following product information sheets for:

- Eyewitness Vantage
- Eyewitness Data Vault



KUSTOM SIGNALS, INC.

Eyewitness Vantage **Officer Worn Video**

**Tells the whole story
from the officer's
VANTAGE point.**

Eyewitness Vantage

Officer Worn Video



Vantage offers true HD video, excellent quality low light recording and wireless file transfer to Kustom's new Eyewitness HD in-car system*.

Available with extended battery for up to 9 hours of record time.

Overview

- Excellent low light performance:
 - Matches what the officer sees
 - Configure with day/night mode for even better low light performance
 - Optional IR LEDs for capturing video in total darkness (Agency configurable)
- Select the resolution/storage combination that is best for your agency: 1080p/30 fps, 720p/60 fps, 720p/30 fps, D1 (480p/30 fps)
- Simple, glove friendly operation allows officers to focus on important tasks
- Wide-angle done right: 120° - capture details others may miss with minimal distortion
- Docking station for convenient dock-and-go file transfers and battery charging



Preferred Features Made Standard

- Pre-event recording (configurable up to 30 seconds)
- GPS - store coordinates with bookmark, support for geo-searches and synchronized clocks
- Configurable audio mute button if needed to comply with privacy laws
- Bookmark button identifies important events saving time during review

File Security/Authentication

- Recording media is non-removable
- File access requires a secure FTP Ethernet connection between the Vantage docking station and EDV/EDV Lite
- MD5 hash is calculated for each file on the camera before transfer
- MD5 is calculated again after transfer and compared against the original MD5 value. Only if there is a match is the file allowed to be ingested into the database and purged from the camera
- Each file's original MD5 value stays with the file for its life on the database. All subsequent MD5 calculations are compared against the original value calculated by the camera to confirm authenticity



Simple operation



HD 1080p
HD 720p
SD 480p



4.5 hours (standard)
9 hours (extended)



Highly configurable



32GB secure storage



Yardarm Holster Aware™



Field of view



Rugged



GPS



Pre-event recording



Bookmarking



Audio mute



WiFi

Multiple recording resolutions

Excellent low-light capability

Superior file integrity

Specifications

Resolution:	Selectable - 1080p/30 fps, 720p/60 fps, 720p/30 fps, D1 (480p/30 fps)
Battery Life:	
Standard:	Up to 4.5 hours SD video, up to 4 hours HD video 720p;
Extended:	Up to 9 hours SD video, up to 8 hours HD video 720p
Power Save Mode:	Standard: 48 hours; Extended: 96 hours
Internal Storage:	32GB
Record Capacity:	Up to 6 hours 1080p/30 fps, up to 6 hours 720p/60, up to 14 hours 720p/30, up to 17 hours 480p
Weight:	4.4 oz (125 g), standard battery; 6 oz (169 g) extended battery excludes clip: 0.5 oz (17 g)
IP64 compatible:	Protection from dust and water
Drop Test:	Complies with MIL STD 810G
Indicators:	Battery level, file transfer status, record status, audio mute, low media
Warranty:	One year



Excellent depth-of-field - objects near and far are crisp and clear

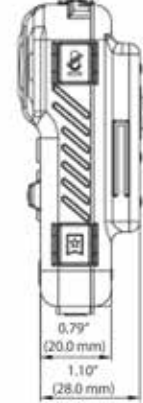
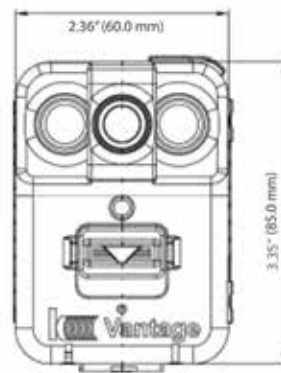


Redacted for privacy*

*Future Enhancement Options

- Redaction and cloud storage through Eyewitness Data Vault back-office software
- Wireless file transfer to Eyewitness HD in-car video system means officers don't have to turn camera in at end of shift
- Vantage files inherit the associated ICV file's stop and hold classifications = no more classifying files back at the station
- Automatic file association between Vantage and Eyewitness HD for easier/time-saving search and simultaneous playback
- Bi-directional record triggering. EyewitnessHD record activations will trigger Vantage recordings (and vice versa)
- Peer to peer record triggering – our design limits record activations to paired cameras only. This avoids the unwanted triggering of other cameras that can happen with systems that broadcast a record trigger to any camera within range
- Interface with Yardarm Holster Aware sensor - unholstering a weapon will automatically start a recording.

Dimensions



Standard: 0.79"
(20.0mm) deep
Extended Battery 1.10"
(28.0mm) deep

Options

- Up to 9 hours record time with extended battery
- Mag-mount (used in lieu of supplied spring-clip)
- Multi-dock (supports six cameras - multiple multi-docks can be connected together to support larger fleets)
- File Management Software - see Eyewitness Data Vault and Eyewitness Data Vault Lite
- Extended warranty
- In car charging kit
- Play Vantage files in the car
- Wired transfer to Eyewitness HD

Yardarm Holster Aware*

- Unholstering a weapon automatically starts a recording
- No officer interaction needed to capture critical events
- Officer attention remains on the event, not the camera
- Attain multiple angles of the situation when configured with two-camera triggering



Vantage File Transfer Options

Stand-Alone

Wired docking station in office for downloading and charging. This can also function as an in-car charger/download station.



- OR -



Eyewitness Data Vault (EDV) or Eyewitness Data Vault Lite

Multi-Dock:
Insert up to 6 cameras for charging and downloading. Connect additional multi-docks together for larger fleets.

With Eyewitness HD*



In-car docking station for syncing, wired downloading to Eyewitness HD and charging.



Eyewitness HD DVR



- or -



Optional wireless* transfer allows camera to stay on officer.



Transfer all files to EDV or EDV Lite. EDV supports manual, wired or wireless transfer from Eyewitness HD. EDV Lite supports only manual transfers.

Eyewitness Data Vault *Lite*

- Ideal file management solution for smaller installations of Kustom video systems that utilize manual file transfer
- Offers the same intuitive look and feel as Eyewitness Data Vault, and retains an impressive list of features: ingest, search, play, burn and file export
- Comprehensive Admin option includes items such as User Management to control which features are accessible to each user
- Economical, customer-installable on your PC
- Included with your Vantage purchase (1 per agency)



EDV Features

EDV *Lite*

EDV

• Customer installable	●	
• Intuitive user interface	●	●
• Simple and advance searches	●	●
• Easy DVD burning	●	●
• Comprehensive audit reports	●	●
• Multiple file retention times		●
• Supports multiple sites (networked clients)		●
• Supports multiple asset types		●
• Supports wired/wireless file transfer		●
• Supports MS Active Directory		●
• Web interface for remote viewing		●
• Fleet Management		●

Intuitive, secure file management

Eyewitness Data Vault is a powerful digital video management solution that automatically and securely manages digital assets locally or across a network. It is configurable and scalable to fit virtually any environment.

Configurable

- Highly scalable - supports small & large installations - expand storage locally
- Flexible storage policy based on officer name, car number, file classification, etc. - Improves file management and resource efficiency
- Highly configurable user and user group management - determine which features within the program and the web interface are accessible to users/groups



Convenient

- Intuitive, user friendly interface simplifies learning and enables efficient use
- Compatible with Active Directory and LDAP - easily integrates with established login credentials
- Quick export from Results screen saves time
- Ingest groups of files (i.e. photos) together and link to a case number
- Easily burn multiple copies of a file
- Include reports and associated files with burned copies

- Manage evidence from all Kustom Signals' digital in-car, motorcycle and body worn video, as well as digital evidence from non-proprietary sources



- Playback timeline - easily cue video to any event (trigger, bookmark)

Secure

- Highly configurable rights management - determine who sees what
- Automatic file integrity checks (MD5) ensures authenticity
- Comprehensive audit reports track and validate chain of custody

Additional Features

- Easy DVD/Blu-Ray burning (Include video file(s), audit report, associated files)
- Powerful search features improve the efficiency and accuracy of searches
- Dashboard application for convenient monitoring of system services/storage
- Web Interface - allows authorized officers to search and play files from web browser

Highly scalable

Easy to use

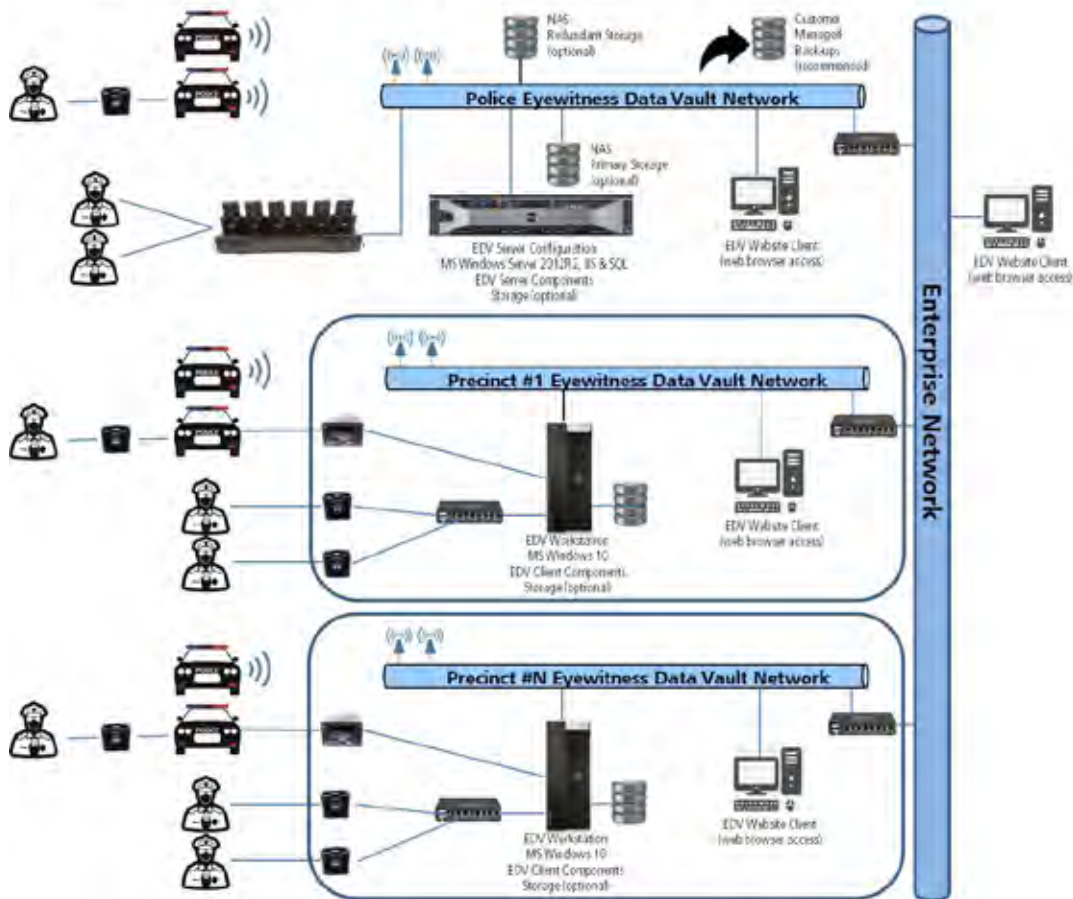
Secure user management

Eyewitness Data Vault

Digital Asset Management System



Eyewitness Data Vault Network Diagram Example



Future Enhancements

- Cloud Storage option
- A/V redaction tool
- Multi-camera synchronized playback



Eyewitness Vault - Data Sheet - USA Eng - Print - 09/2018

Eyewitness Data Vault *Lite*

- Ideal file management solution for smaller installations of Kustom video systems that utilize manual file transfer
- Offers the same intuitive look and feel as Eyewitness Data Vault, and retains an impressive list of features: ingest, search, play, burn and file export
- Comprehensive Admin option includes items such as User Management to control which features are accessible to each user
- Economical, customer-installable on your PC

EDV Features

	EDV <i>Lite</i>	EDV	EDV 3.0
• Customer installable	●		
• Intuitive user interface	●	●	●
• Simple and advance searches	●	●	●
• Easy DVD burning	●	●	●
• Comprehensive audit reports	●	●	●
• Multiple file retention times		●	●
• Supports multiple sites (networked clients)		●	●
• Supports multiple asset types		●	●
• Supports wired/wireless file transfer		●	●
• Supports MS Active Directory		●	●
• Web interface for remote viewing		●	●
• Fleet Management		●	●
• Cloud storage			●
• A/V redaction tool			●
• Multi-camera synchronized playback			●

Municipal Emergency Services, Inc.
Response for:

Request For Information Police
Body Worn Cameras
Pennsylvania Chiefs of Police
Association

25 January 2019

Municipal Emergency Services & Lawmen Supply
Contact: Mark Windover VP/General Manager
203-304-4121
7 Poverty Rd.
Southbury, CT 06488
Fax:203-264-3325
mwindover@mesfire.com

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

Mr. Christopher J. Braun M.S. IT
Technology Coordinator
Pennsylvania Chiefs of Police Association
3905 N. Front Street
Harrisburg, PA 17110

25 January 2019

Re: Request For Information Police Body Worn Cameras

Dear Mr. Braun;

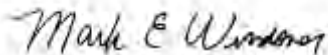
This is to respectfully submit our proposal for the Request For Information Police Body Worn Cameras on behalf of Municipal Emergency Services, Inc. (MES). Our team looks forward to working with you on this exciting project.

The following pages will respond to your statement of work requirements and will provide further background on our company, our project approach, our technology and our ability to satisfactorily meet the needs of Pennsylvania Chiefs of Police Association for your Body Worn Camera program. Most Body camera programs consist of 3 key elements Hardware, Storage and Software. We will offer an extremely unique approach to all aspects of the mission:

- 1) We will provide a robust Body Worn Camera with a full 2-year warranty on all hardware.
- 2) **Unlike most in the industry, MES does not build the mission around making money on storage whether in the cloud or on-premise.** For this program, we are offering Wasabi storage, however the SW is very flexible and can quickly adapt to whatever storage strategy you prefer.
- 3) Our team will provide world class service, with local training and program support, technical support that is led by the developers that wrote every line of the Software code, and a corporate commitment from MES that is unparalleled.

I am the authorized signatory of all technology programs for MES.

All the best,



Mark E Windover
VP/General Manager
Municipal Emergency Services, Inc.

Mark Windover
VP/GM
7 Poverty Rd. Suite 85H
Southbury, CT 06488
203-560-6010
mwindover@mesfire.com

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

Executive Summary

The following response is presented by Municipal Emergency Services (MES) in conjunction with its subsidiary Lawmen Supply, Inc (LSC) and VisioLogix (formerly HD Protech). Our team has the combination of experience in the Public Safety marketplace with best in class solutions that meet and exceed the requirements listed in the Pennsylvania Chiefs of Police Association Request For Information Police Body Worn Cameras. We anticipate that our solution will provide an excellent value for easy to deploy and manage Body Worn Cameras, in an unmatched operational environment.



MES and LSC have 45 years of combined experience in Public Safety. MES is a leading supplier to the Public Safety trades while LSC is a leading Police Safety Products Supplier with 375 Public Safety professionals across the country with an average of 25+ years of experience in the trades.

We are also proud to have as our partners, Transcend, based in Columbia, MD providing world class BWC hardware and VisioLogix, as a key technology provider for the Hydra Mission and Video Management software tool. VisioLogix is an MBE, WBE, and HUB company, from Houston, TX representing over 50% of the goods and services outlined in this proposal.

If you prefer cloud storage, we are offering a safe, CJIS Certified, economical and flexible Cloud Storage option via Wasabi Cloud Storage. Wasabi was started by the founders of Carbonite and has quickly become an outstanding source for secure and fair cloud storage.



The Municipal Emergency Services team has thoughtfully reviewed your requirements and have architected a hardware, software, and services solution that is effective, scalable, easy to administer, and will provide outstanding short and long term value for the Pennsylvania Chiefs of Police Association.

Current State of the BWC Industry



- Agencies have been pressured into costly long-term cloud contracts with ***NO WAY OUT.***
- Microsoft or Amazon Cloud solutions are generally 2X the cost of using your own IT infrastructure or Wasabi Cloud Storage.
- Opportunity to save thousands of dollars by using your current IT infrastructure or via Wasabi Cloud Storage, with **COMPLETE FLEXIBILITY ON THE BACK END SHOULD YOU DECIDE TO MOVE YOUR DATA.**
- MES/Lawmen will help you design the ideal BWC storage solution that will save you money today and over the long term either in your own environment or with Wasabi.
- **We are so committed to your success that we will help you design your own on-premise solution with your own infrastructure, we will sell you on-premise storage, or we will provide Wasabi Storage.**

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

Questions Related to RFI

- 1) *How does your non-vehicle-mounted mobile video recording systems and technology meet Pennsylvania's published requirements?***

In all cases our products meet and exceed current requirements. Please see the response below to the specific requirements.

- 2) *Have you submitted your non-vehicle-mounted mobile video recording systems to the Pennsylvania State Police for certification?***

We have not yet, but would appreciate the opportunity, we are confident that with our technology, we will have a meaningful addition to the certified companies and products with new and exciting technology.

- 3) *Is your non-vehicle-mounted mobile video recording systems already certified by the Pennsylvania State Police?***

Not yet, however we would appreciate the opportunity, and are confident that with our technology, we be certified.

- 4) *Are you offering a storage solution?***

Yes, we offer multiple storage solutions as our Hydra Digital Evidence Management Software is storage agnostic. We have NAS storage which is outlined in our pricing scenario, however we would welcome the opportunity to deploy our software with your existing IT Storage infrastructure if there is potential cost savings. We offer Wasabi CJIS Certified Hot Cloud Storage at simple pricing of \$5.99/TB per month, no long term commitment required.

- 5) *Will you offer storage solutions bundled (no line item distinction) with the cost of each camera purchased?***

Yes, we offer bundled storage solutions tied to camera cost if it is required. Many vendors have done this and the pricing scheme ends up as misleading and many times more expensive than unbundled. We will offer both as required by specific RFP's.

- 6) *How does your storage solution meet Pennsylvania's published requirements?***

Yes, please see below, we offer Wasabi CJIS Certified Hot Cloud Storage.

- 7) *List the products and services that are already available on State Contract or PA CoStars.***

Our Company is a CoStar vendor but the proscribed BWC items are not yet on CoStars. We are however an NPPGov GPO National Purchasing contract and our prices reflect these discounts.

Request For Information Police Body Worn Cameras Pennsylvania Chiefs of Police Association

8) *List your costs for products and services you offer.*

Product	Contract Category	Description	Model #	Net Price
Body Worn Camera	Category 1 Public Safety Video Cameras	64GB Internal memory DrivePro Body 30 Body Camera with a 2 year Warranty.	TS64GDPB30A	\$299.00
Body Worn Camera	Category 1 Public Safety Video Cameras	Docking Station for DrivePro Body cameras (30) with a 2 year Warranty.	TS-DPD6N	\$599.00
Body Worn Camera	Category 1 Public Safety Video Cameras	Description: 16TB, Network attached storage (NAS), DPB Control center with a 2 year Warranty.	TS-DBN1-16T	\$1,299.00
Body Worn Camera	Category 1 Public Safety Video Cameras	The Visiologix CITE A1 is a multi-functional, multi-purpose Law Enforcement tool that has a wide array of uses. The unit can be used as a standalone video recorder. An officer can use the CITE A1 to record 1080p quality video, photograph crime scenes, and record audio statements. CITE A1 records up to 7 hours of video at 1080P (over 13 hours at D1), over 250 hours of audio, and over 10,000 photos based on the internal 32GB storage card. Standard contents include: The Kit includes: Visiologix CITE A1 Camera, Standard Clip, Docking Base, USB Cable and CITE Configuration Tool for downloading videos and making configuration changes. Camera Dimension: 120x73x25mm (4.72"x2.87"x0.98"). Weight: 274g (8.8 oz). Includes 1 Year Warranty	007-1000	\$599.00
Body Worn Camera	Category 1 Public Safety Video Cameras	The Visiologix Z2 is a multi-functional, multi-purpose Law Enforcement tool that has a wide array of uses. The unit can be used as a standalone video recorder. An officer can use the CITE Z2 to record 1080p quality video, photograph crime scenes, and record audio statements. CITE Z2 records up to 8 hours of video at 1080P (approximately 16 hours at D1) based on the internal 32GB storage card. Standard contents include: The Kit includes: Visiologix CITE Z2 Camera, Standard Clip, Docking Base, DSM1 Mount, USB Cable and CITE Configuration Tool for downloading videos and making configuration changes. Camera Dimension: 85x55x23mm (3.35"x2.2"x0.9"). Weight: 140g (4.5 oz). Includes 1 Year Warranty	008-1000	\$349.00
Body Worn Camera	Category 1 Public Safety Video Cameras	CITE Camera M1G3 Intelligent Docking Station for use with EMS Standard/Enterprise Software. The docking station provides eight-port USB transfer and charging capability allowing for up to 4 hours to charge the camera. Web Interface provide easy configuration. Standard 1 Year Warranty. This model only requires a Gigabit network and 110/220V Power source.	518-1000	\$1,499.00
Body Worn Camera	Category 1 Public Safety Video Cameras	Body Worn Video Camera – includes 1080p Video, Still camera, voice recorder with automatic and program infrared to work in complete darkness. Includes a GPS transponder for location services, and a 32GB storage card which can capture up to 14 hours of video, 500 hours of audio, or over 20,000 photos. Package includes Long and Short Clip, Power Charger, DC Cable, USB Cable, and a camera software utility tool for downloading videos and making configuration changes.	004-1000	\$399.05
Body Worn Camera Video Management Software Annual Fee	Category 2 Data Management Software	Body Worn Video Camera software tool for managing the video output, the chain of video evidence, with the ability to attach records to each video file, which can be virtually any file type including audio, video, pdf, xls, doc, ppt etc. Key tool for managing the BWC asset at the agency level and managing security and full WAN/LAN capability.	SAS-1002	\$249.00
004-1000 Annual Support and Maintenance	Category 6 Services	Year 2 and beyond Product support for the Body Camera 004-1000 priced per body camera	004-1001	\$97.16
BWC Specialized NAS Server	Category 3 Data Storage and Upload Services	4 Bay NAS Server Capable of deploying up to 16TB of raw storage via 4 drives with 4TB Each	BWC NAS-16	\$2,226.00
Professional Installation Support	Category 6 Services	Day rate for Engineering support for remote install	151201-1000	\$2,499.00
Specialized Phone Support (Per Incident)	Category 6 Services	Dedicated phone support for remote access into agency PC or server priced per incident	151201-1008	\$345.45

9) *Will you offer a discount of those prices if multiple police departments group together to buy your products and services?*

Yes, we would be happy to offer discounts for multiple agencies are for larger quantities.

7 Poverty Road, 85H Bennett Square, Southbury, CT 06488 Phone: 203-304-4121

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

Response to Requirements

The following will respond to the requirements set forth in the RFI. While MES sells many different Body Worn Cameras that meet and exceed the requirements listed, we are focusing our remarks on our leading product today the Transcend DPB30 IP67 64GB Body Worn Camera.

Date/time stamp capability

The DPB30 has a date/time and GPS stamp capability that provides embedded stamping on every frame of video or still photo captured by the device. The image delivered looks like this and is an immutable element of the file once produced.



Microphone and a recording device, enclosed in secure protective enclosure(s).

The DPB30 has an IP67 enclosure that has been drop tested following the MIL-STD-810G 516.6-Transit Drop Testing protocols.

It may also contain controls, a monitor, GPS, wireless transceiver components and other electronic components.

The DPB30 has a free smartphone application that allows the user to control, monitor, provide GPS connectivity, as well as a secure wifi streaming (BWC to phone) capability.



**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

The non-vehicle-mounted mobile video recording system must be powered from a battery internal to the protective enclosure and must be weatherproof. The internal battery may be integral to the unit or removable. It is permissible to have an external battery to extend the operating life of the system.

The non-vehicle-mounted mobile video recording system must have a minimum record time of 2 continuous hours.

The DPB30 has a 3120mAh non-removable battery in an IP67 enclosure. The battery provides for up to 12 hours of continuous video. A USB cable is included with each camera which provides for recharging either from a DC source or external USB driven battery.

The system must operate over the following temperature range: -4°F to 122°F (-20°C to 50°C).

The DPB30 has an operating temperature range of -20°C (-4°F) ~ 65°C (149°F).

Camera

The camera component must have the following features:

- A. Must be color video.*
- B. Minimum of 640 x 480 pixel resolution.*
- C. Minimum of 68 degrees field of view.*
- D. Minimum of 30 frames per second.*
- E. Minimum sensitivity rating of 3.4 lux or lower. Unit may use Infrared LED illumination to obtain lower than 3.4 lux equivalent.*
- F. Camera does not have to be in the same enclosure as the recorder. Can be connected to the recorder either by cable or wireless connection.*

The DPB30 provides the following:

- A) Full color video in standard operation
- B) Delivers 480P, 720P, up to 1080P resolution
- C) Operates has a 130° Field of View
- D) 30 Frames per second delivered at all resolutions
- E) Operates down to <1 Lux and has an Infrared illumination tool for less light.
- F) The DPB30 has the camera and recorder in the same enclosure, however we have a unit that has an external camera.

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

Recorder

The recorder component must have the following features:

- A. Enclosed in a secure housing protected from physical damage.*
- B. Date/time recording index.*
- C. Minimum of 4 gigabytes of nonremovable solid state memory, 4 gigabytes removable media or a combination of both removable and nonremovable memory.*
- D. Editing and record-over protection.*

The DPB30 provides the following:

- A) IP 67 Mil Spec enclosure.
- B) Date and Time stamp embedded in each frame of the video and still photos.
- C) 64GB of non-removable memory
- D) All cameras are password protected to prevent editing and record-over protection.

System Control

The system must:

- A. Be capable of recording audio and video simultaneously, but may also provide the user with the option to record video only or audio only.*
- B. Provide the user with the capability to manually turn the power on and off as necessary.*

The DPB30 provides the following:

- A) Simultaneous and synchronized audio and visual recording with the option to mute audio with a touch of a button and can toggle back on from a muted state.
- B) Camera turns off/on with the touch of a single button.



**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

Wireless Link (optional)

The unit may use a wireless link to connect the camera to the recorder, recorder to another device, combination camera/recorder to another device or be used to download the evidence. The wireless link must have the following features:

- A. Use a secure digital connection.*
- B. Wireless link can be used to play back a locally stored event on the recorder or store the media to a remote location such as secure Cloud storage.*
- C. FCC Type acceptable under 47 CFR Part 15 (relating to radio frequency devices).*

The DPB30 has a free smartphone application that allows the user to control, monitor, provide GPS connectivity, as well as a secure wifi streaming (BWC to phone) capability. It is recommended that the unit be charged with data uploaded via the 6 port docking station outlined below. All DPB30 cameras and accessories are certified by; CE, FCC, BSMI, NCC, and MIC.

Law Enforcement Officer Camera System Data Handling Requirements

A. Camera system

- 1. While worn by the officer, a camera system shall be considered a physically secure location.*

The DPB30 has multiple secure mounting options to secure the device to the operator. A recent Police Magazine article indicated that 58% of officers surveyed indicated that their BWC unit had fallen off. MES and Transcend have taken great care in created a sturdy and stable environment to properly secure the devices to the officers. The DPB30 has multiple mounting options with its secure heavy-duty clip solution. There are also magnetic, molle, and Velcro mounting solutions as well.



**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

2. Upon removal from the officer's body, the camera system shall be maintained in a physically secure location in accordance with CJIS Policy standards.

Per the description above, we highly recommend the use of the proscribed docking station in a secure agency location to ensure proper CJIS security protocols. All data is moved through the system via the Hydra Digital Evidence Management software (DEMS) via encrypted protocols. Please see schematic in our Technology Summary.

6 Port Docking Station



B. Data transfer or downloading the data

The DPB30 has non-removable media storage which allows only the secure offloading of data. Also, the memory card is 64GB eMMC (embedded multimedia card) which is soldered on the board, therefore there is no memory card you can simply pop out and plug in to another device. In the event the camera is stolen or gets in the wrong hands, you cannot access the data without a password. All data transfers are done via secure communication using HTTPS and all data transferred are secured using 256-bit encrypted communication with 2048-bit root keys.

C. Storage of the data

Storage of data on location, if considered a physically secure location, shall be treated the same as all CJI at the location.

The MES BWC solution with the Hydra DEMS is storage agnostic. Many agencies have chosen to deploy via a cloud environment which in our case is CJIS secured via Wasabi Hot Cloud Storage (Please see attached schematic). Many BWC companies will force agencies into 3-5 year inflexible cloud contracts to lock up their business. We would much rather earn the business every year with great service and let the agency decide for themselves. 90% of the time agencies have the on-premise storage resources already in place which is where the mission should begin. If over time substantial infrastructure investment is required then consider making the call between insourced (on-premise) or outsourced (cloud) storage solutions.

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

D. Reviewing and release of data

1. Data from the camera system shall only be reviewed by authorized personnel; that is, personnel that have been cleared through a fingerprint-based background check, have received Security Awareness Training and have signed the appropriate agreements, if applicable. If required, the Management Control Agreement for local government IT, or The Security Addendum for private contractors, shall be completed and on file.

The MES BWC solution with the Hydra DEMS provides for RBAC (Role Based Access Controls) which provide a full spectrum of personnel access authorization protocols. Please see our technology description for further details.

2. Prior to the release of data from the camera system, the data shall be reviewed and any areas containing CJI shall be removed or rendered unintelligible. Any data received from CLEAN or the National Crime Information Center in either video or audio format, or both, shall be removed or rendered unintelligible prior to release to any unauthorized or unintended personnel.

The MES BWC solution with the Hydra DEMS provides for a deletion mechanism that is complete and tracked via an extensive logging system throughout the process. Please see our technology description for further details.

E. Retention of data

Data shall be stored for 60 days unless needed for prosecution, courts, litigation, appeals or other operational needs.

The MES BWC solution with the Hydra DEMS provides for an unlimited number of retention schedules so a 60 day retention is standard. Please see our technology description for further details.

F. Destruction of data

The MES BWC solution with the Hydra DEMS provides for a deletion mechanism that is complete and tracked via an extensive logging system throughout the process. Please see our technology description for further details.

Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association

Technology Description

BWC – Digital Evidence Management and Storage Solution

The Body Worn Camera mission is centered around 4 key components; 1) Hardware, 2) Software, 3) Application Assurance, and 4) Storage. Our software is the foundational element of the entire ecosystem as it allows many different types of BWC hardware, while accommodating on-premise, Cloud, or Hybrid storage.

1) Hardware

We are delivering best in class IP-67 SHD hardware that has been tested in the toughest of environments and real field punishment. Our goal is to make the camera itself incidental to the mission with a care free ownership experience with an extremely quick training requirement.

2) Software

Our globally deployed C-3 Sentinel client software has been adapted onto a Web version called Hydra. As before, the interface is elegant with simple to follow steps for a secure and efficient operational and administrative experience. This software is not only hardware agnostic, it can be used in virtually any storage environment. Hydra makes CJIS compliance a breeze with its RBAC administrative control protocols.







3) Application Assurance

Hydra Application infrastructure is deployed via Microsoft Azure Government Cloud Services. This provides the highest level of security for the application which includes all of the file metadata and supporting infrastructure for the object storage in Wasabi. This secures all of the web hosting aspects of the Hydra software suite as well.

4) Storage

Our docking station and DrivePro™ Body Control Center provides 16TB of data storage per 2 6-bay docks at the local center level which provides additional speedy back up for immediate review and an excellent redundancy for your on-premise storage. Our Hydra Software is completely storage agnostic so you are able to continue to deploy whatever storage array you prefer and move data at any time to either additional on-premise resources, cloud storage options, or a hybrid, 100% your call.

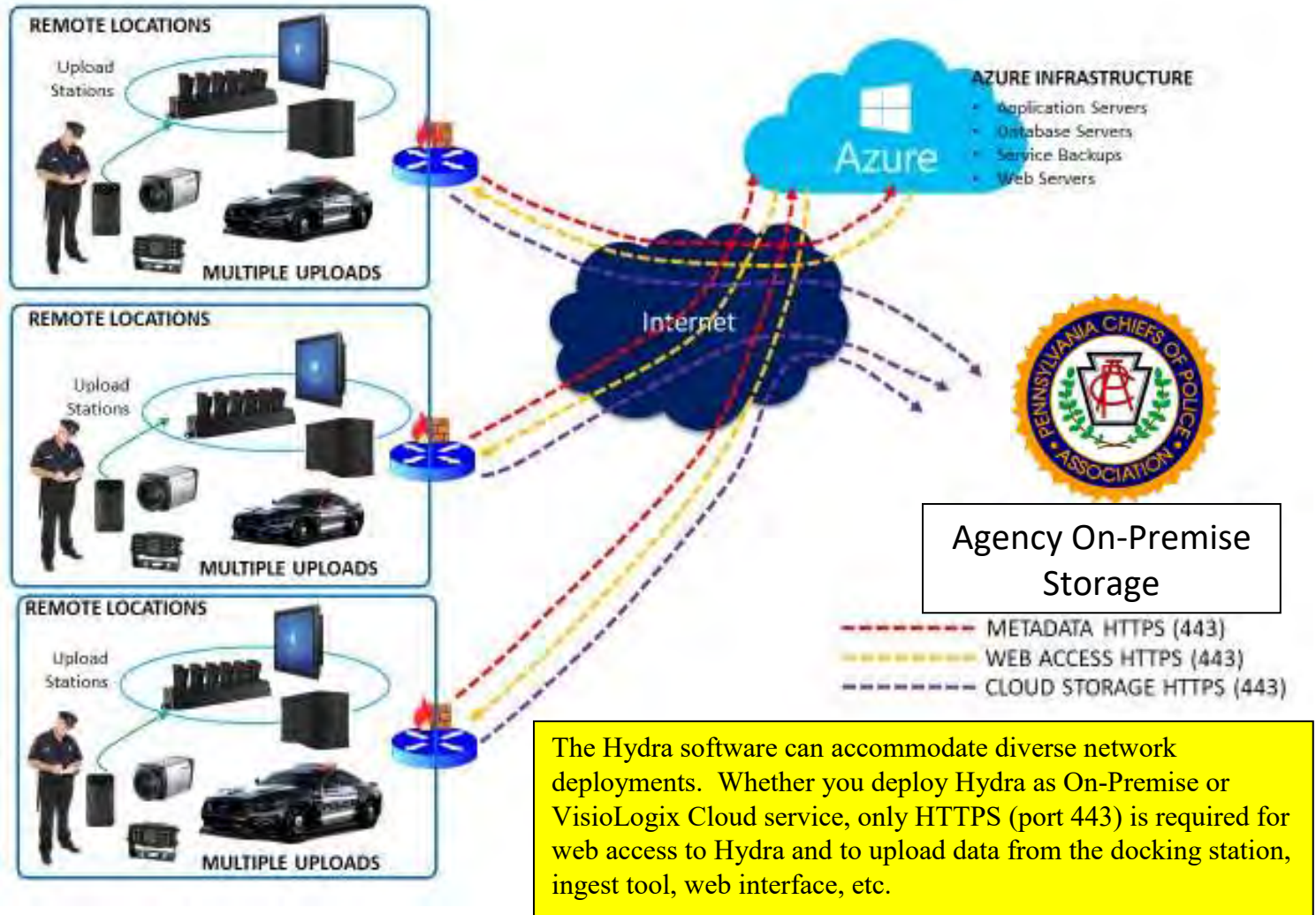
Our all-star line-up:

Software	Application	Hardware	Storage
			
			On-Premise provisioned at the docking station level or on the Cloud VisioLogix Hydra Software is agnostic to storage preference.

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

On Premise Storage Schema for Pennsylvania Chiefs of Police Association

Data is uploaded from the camera to the local redundant DrivePro™ Body Control Center at the docking center level, data is then sent to the Hydra DEMS application is delivered and managed via the Microsoft Azure application layer. All Data is then uploaded from remote locations via the internet to your secure on-premise storage.



**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

DEMS Mission Schema for Pennsylvania Chiefs of Police Association

The VisioLogix BWC program is an easy to deploy and efficient way to manage this critical mission. It starts with the camera being taken from the intelligent docking station. No sign out is required unless the assets are shared. The easy to use DPB30 Camera gets deployed to the field and captures video, pictures, etc. While in the field, the operator is able to review the captured case data on an MDT.

Outlined in Step #3 is our EMS Mobile Client Software which (if authorized by the administrator) allows the operator to review and annotate captured files via the light weight client software that can be installed on the MDT. The operator is able to add key metadata elements including case #, the address, the event classification, along with any video clips that the operator would like to make to help support the case.

All of this data is saved to the camera for each file and is then uploaded at the docking station at the end of shift or whenever the operator chooses to upload their data. The data is then immediately uploaded to the Hydra Database in the Wasabi hot storage cloud.



**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

Solution Overview

The MES/Lawmen Body Worn Camera solution provides a comprehensive solution that will provide best in class BWC hardware, and managed data storage, along with an industry leading Mission Management software solution.



The primary camera proposed is an IP-67 waterproof heavy duty camera that is a full featured camera that offers a WiFi and Bluetooth connection and a free App which allows the officer to review videos prior to downloading to the system. The camera the unit delivers a 130° field of view with a 3120 mA battery delivering up to 12 hours of video at standard definition with 24+ hours of standby.

An important element of our proposed solution is a GPS module. The Transcend DPB30 camera has a GPS module that delivers location to all video files captured. When combined with the vehicle MDT GPS, provides an added dimension to the data delivered. There is also low light capability which allows the camera to operate down to less than 1 Lux and has an infrared capability that captures up to 10ft at low or no light situations.

Triggering the Drive ProBody Body Team Sync for Mutual Aid

When a team is created and Bluetooth is turned on, when Camera #1 is activated, all surrounding connected team member Cameras are triggered and activated to support Camera #1.

Team Sync



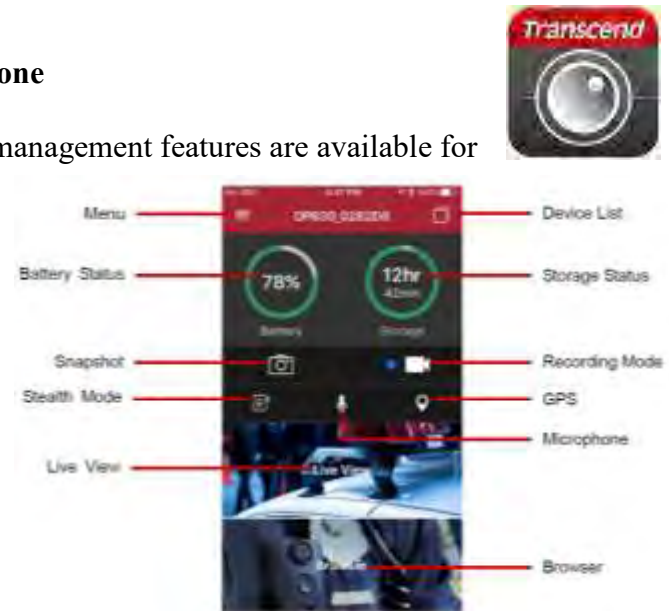
**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

DrivePro Body App for any Android or IOS Smartphone

Simply download the free app for your phone and many management features are available for your mission.

Once the camera is paired, you are able to see exactly how much battery and storage remain and are able to live view via BlueTooth and WiFi.

Operators are able to see live view from the video camera from up to 25ft. Browsing and reviewing files is also possible via the app.



Docking Station

The Docking Station allows you to securely ingest camera data from multiple locations. With the capability to throttle bandwidth, the docking station will never saturate a slow Internet connection. This solution provides a cost and time effective answer for ingesting camera data and returning cameras to the field faster.



DrivePro™ Body Control Center

Transcend's DrivePro Body Control Center is a digital evidence management system designed specifically to work with the TS-DPD6N networked docking station. With up to 16TB storage capacity, this secure, centralized server can store more than 4,000 hours of 1080P video recordings. All data transfers are done via secure communication using HTTPS and all data transferred are secured using 256-bit encrypted communication with 2048-bit root keys. We have estimated the following for potential storage requirements.



While the hardware is critical, we firmly believe that it is our software that sets us apart

Request For Information Police Body Worn Cameras Pennsylvania Chiefs of Police Association

Software Solution

We at MES/Lawmen firmly believe that the software component of a body worn camera is the most critical from managing evidentiary files, to managing user access, and file management issues, the software is what an agency lives with every day. The hardware on the road becomes incidental to the mission, it's the software that will enable PCPA to operate efficiently and effectively.

Video Evidence Management Software – The Hydra Mission Management and Video software tool is a highly intuitive software package that allows administrators to provide for solid management of the Dash Camera and Body Worn Camera assets, while providing the necessary tools to regulate and assign access to files and functions. The system was designed with the end game of providing solid legal ground for the control and management of the video, photo, and audio files captured by your cameras.

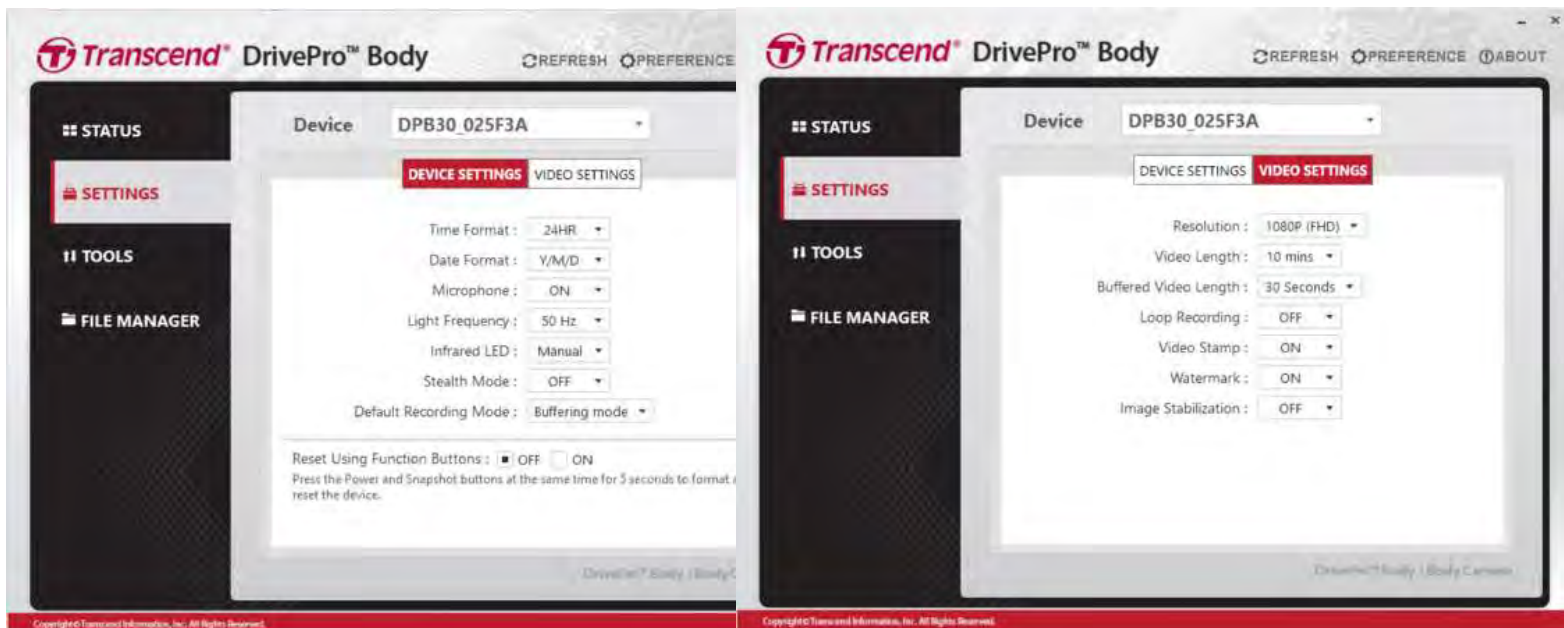
It is understood that policies surrounding the Body Worn Camera mission will continue to evolve over time. The Lawmen/VisioLogix mission management and video software solution provides for complete flexibility as it relates to many key policy issues including; retention, file access, chain of evidence and many other issues.

To further explain the capabilities of the software, we have divided the Body Worn Camera mission into 8 steps from assigning the camera to the eventual transfer of evidentiary files.

Step #1 Managing the Camera asset

A critical task of any large-scale Body Worn Camera as proposed for RPD is the management of the camera asset. We offer a very convenient tool that allows administrators to perform a wide variety of tasks while maintaining a well-managed inventory of cameras and users.

The Drive Pro Tool Box allows administrators to easily assign an identical camera profile to all of the cameras in the mission. The Admin is able to set all camera settings and to assign cameras to an individual officer. Agency Administrators truly appreciate the convenience and elegance of this tool.



Request For Information Police Body Worn Cameras Pennsylvania Chiefs of Police Association

#2 Deploy in Field

When an officer commences video capture, they simply push the record button to capture video of an event, at which time a programmable audible/haptic response of a beep or a buzz emitted from the device. To complete the recording, the officer then pushes the record button and then 2 beeps or buzzes will be emitted from the device indicating that the video was completed. While the officer is recording the event, a red light indicates that the event is being recorded, if desired. An officer may review the video via the smartphone app, but will not be able to remove or alter any of the captured video data.



#3 Classify Critical Evidence

One of the keys to efficient management of the body camera video file assets is to create and execute an effective retention policy and methodology. The C3 Sentinel software provides a tool for agencies to effectively and efficiently remove unnecessary files in a consistent and fair way. The software has a classification system that will automatically assign times and dates for unnecessary files to be purged from the video file storage system in order to properly manage volume and the inherit costs and complexity associated with managing large volumes of data.

The classification of a video file can be made at the mission software level and is able to be assigned to the video files at the camera level following a recorded event. This will streamline the check in administrative process. These classifications not only allow for retention length, they can assign specific users levels that can review these events, and important can route events to different storage locations if desired.

☰
Settings

⏪
Classifications

Classification	Code	Primary	Mobile	RBAC	Retention Policy
Arson	AR-0912	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	30 Day
Assault-NoWeapon	ANW-101	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	6 Month
Assault-Weapon	AW-123	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	6 Month
Auto Accident	AA-200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	60 Day
Auto Arson	AA-100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	60 Day
Auto Theft	AT-1231	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	60 Day
Bank Fraud	BF-882	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Sergeant Role	1 Year
Burglary	BR-1221	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	90 Day
Domestic Violence	DV-100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	No Security	90 Day
DWI	DWI-010	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	90 Day
Felony 1	DM-090	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Officer Role	30 Day
Homicide	HC-919	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Detective Role	1 Year
Parking Violation	PVX-100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	90 Day
Robbery	RB-1921	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	6 Month
Runaway	RXX-100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	6 Month
Stolen Property	SPX-100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	90 Day
Suicide	SSX-100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	1 Year
Traffic Violation	TR-100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	6 Month

☒ Primary Classification
☒ Mobile Classification
 Classification Name

 Classification Code

 RBAC, Security

☒ Enable Retention Policy

☐ Enable Aging Policy

 Storage Device

Save
Reset
Delete

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

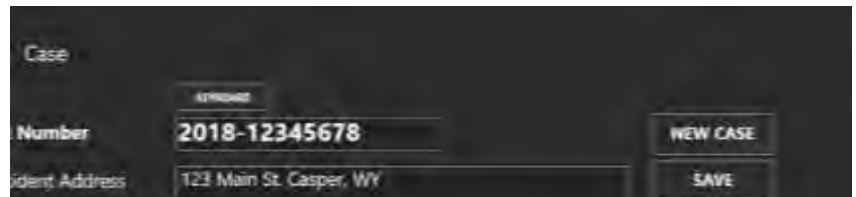
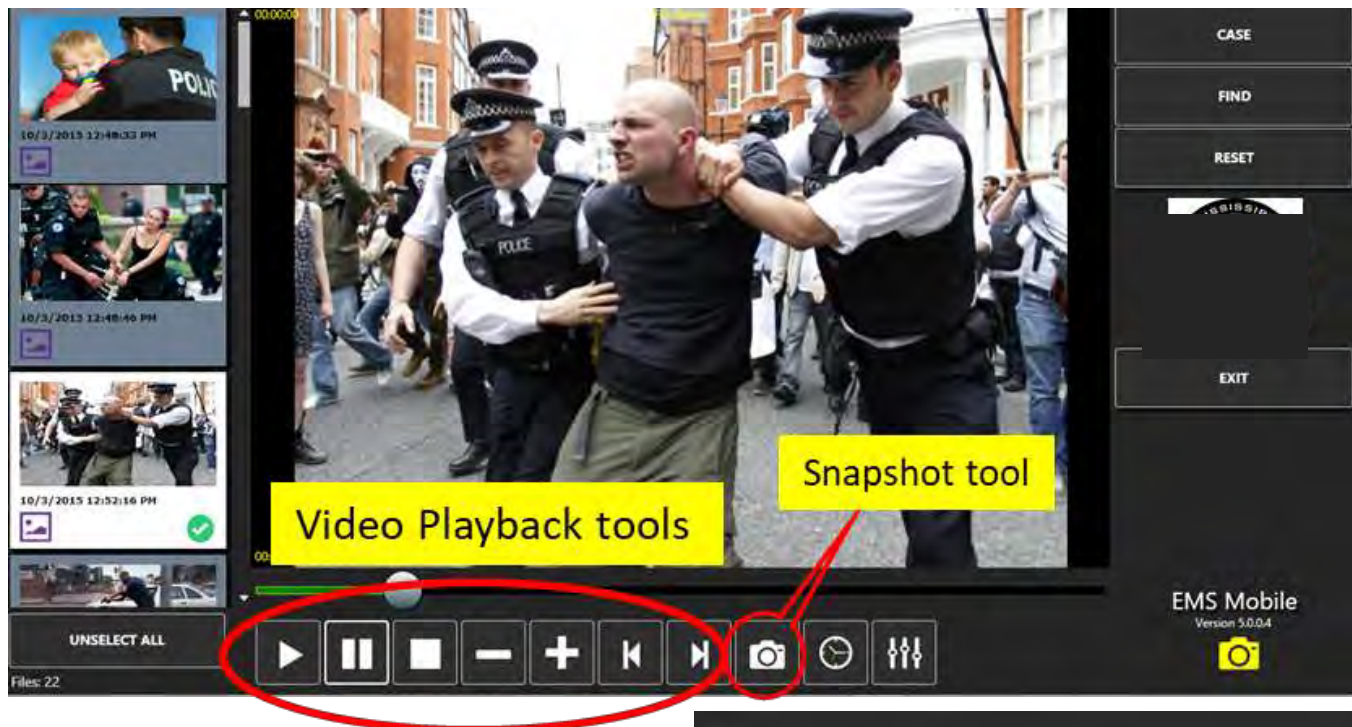
#4 Review and Annotate Files in the field via the MDT

EMS Mobile Client software can be installed on the MDT allowing officers to securely review BWC files (without downloading), and add notes and metadata which can include case#, ticket#, and critical event classification information that are attached automatically to the files to be downloaded from the cameras.

This tool allows the officer the opportunity to review video, tag pertinent sections, attach additional reports of virtually every file type, and to take snapshots of elements of the video for evidentiary management.

The field review of files allows the operators to make the best possible notes while the event is still fresh in their mind to “do once at once”. All of the notes and metadata are added to the file and stored in the camera until the operator comes to the shop to securely download. If the file has been properly coded, there is little that the officer must do once the camera is docked.

The Mobile Client on the MDT is extremely convenient and easy to use.



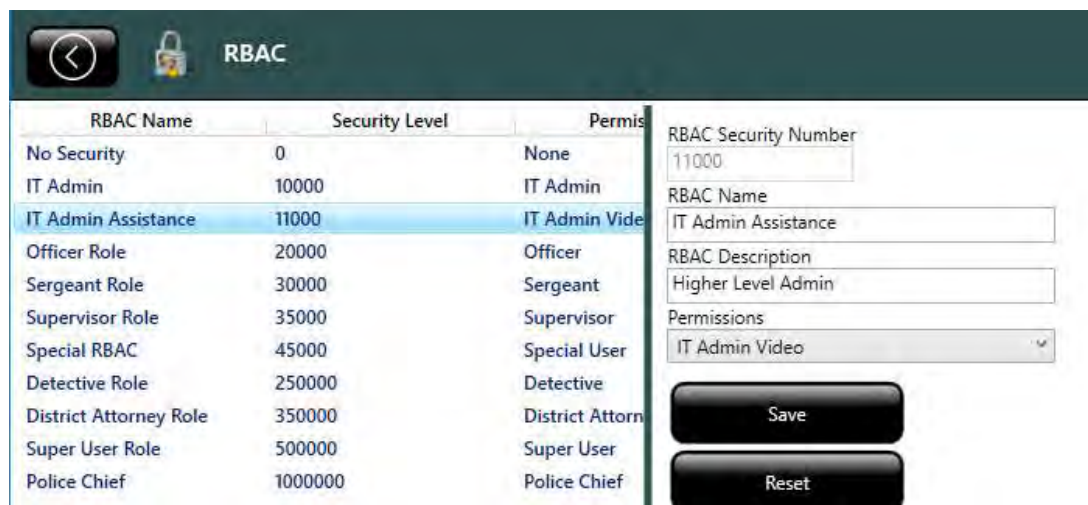
- Deploys RBAC permission standards
- Unlimited number of Permission Groups.
- 33 Key System Activities as permissions.
- Completely controls access to the system.

Request For Information Police Body Worn Cameras Pennsylvania Chiefs of Police Association

RBAC System access protocols

The Hydra system was pressure tested with the British Home Office with some of the strictest of RBACs (Rules Based Access Controls) in the world. Our system was designed with this in mind so we are able to manage roles in a wide range of ways.

The first level of group permissions is at the full RBAC level which assigns an infinite number of permissions level for your agency. In this case, the chief is at the highest level of 10000000, the next highest level is at 500000 at the Super User level. This allows the agency to classify the most sensitive of files at whichever level is most convenient and to allow the most defensible allocation of access to those who need it.



RBAC Name	Security Level	Permissions
No Security	0	None
IT Admin	10000	IT Admin
IT Admin Assistance	11000	IT Admin Video
Officer Role	20000	Officer
Sergeant Role	30000	Sergeant
Supervisor Role	35000	Supervisor
Special RBAC	45000	Special User
Detective Role	250000	Detective
District Attorney Role	350000	District Attorney
Super User Role	500000	Super User
Police Chief	1000000	Police Chief

RBAC Security Number: 11000

RBAC Name: IT Admin Assistance

RBAC Description: Higher Level Admin

Permissions: IT Admin Video

Save

Reset

RBAC at the rank level is also critical. This provides an efficient and consistent application of the access control discipline in a hierarchical and chain of command manner. In your case, the Commander would get a higher permissions level than the officer. This is all definable at the agency level.



RBAC Name	Security Level	Permissions	Accounts
No Security	0	None	0
IT Admin	10000	IT Admin	0
IT Admin Assistance	11000	IT Admin Video	0
Officer Role	20000	Officer	1
Sergeant Role	30000	Sergeant	1
Supervisor Role	35000	Supervisor	1
Special RBAC	45000	Special User	0
Detective Role	250000	Detective	0
District Attorney Role	350000	District Attorney	0
Super User Role	500000	Super User	4
Police Chief	1000000	Police Chief	0
TEST PROFILE	5000000	Test	0

RBAC Security Number: 500000

RBAC Name: Patrol Commander

Description: Super Supervisor

Permissions: Super User

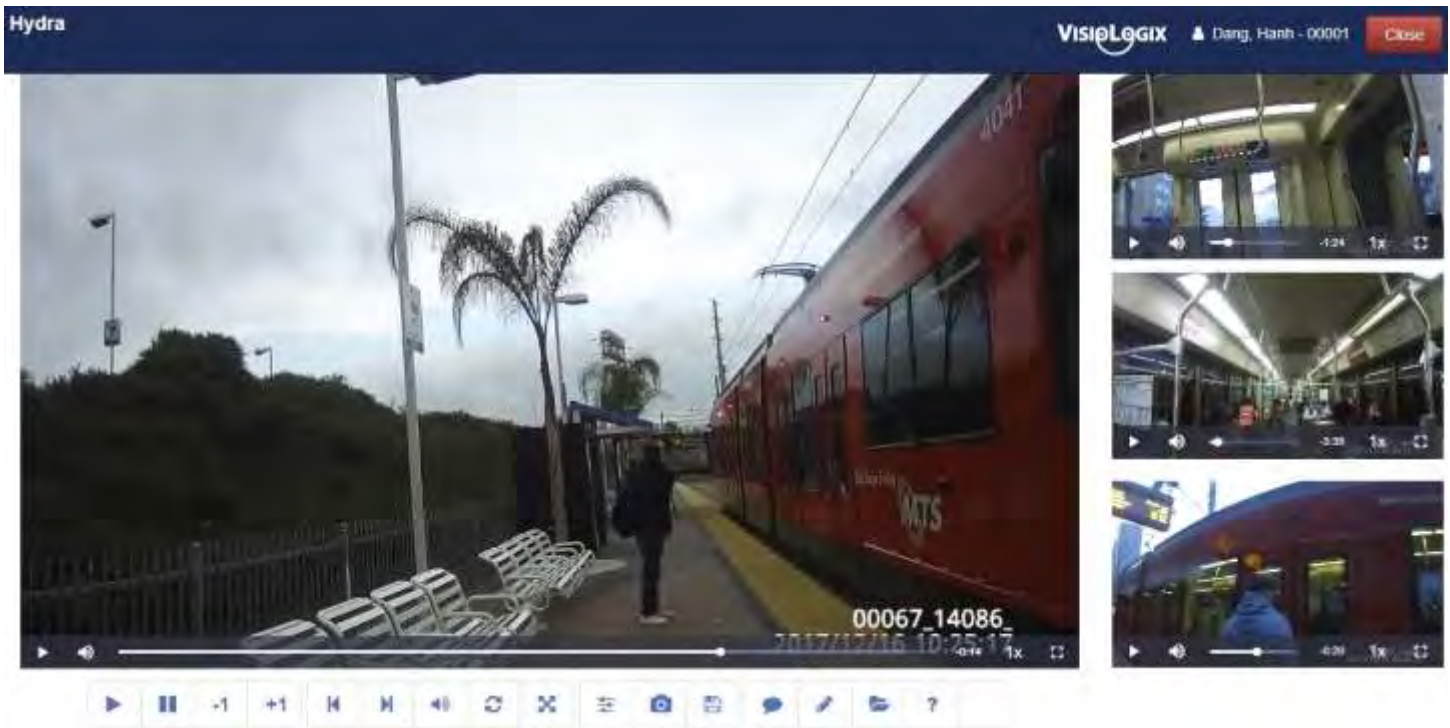
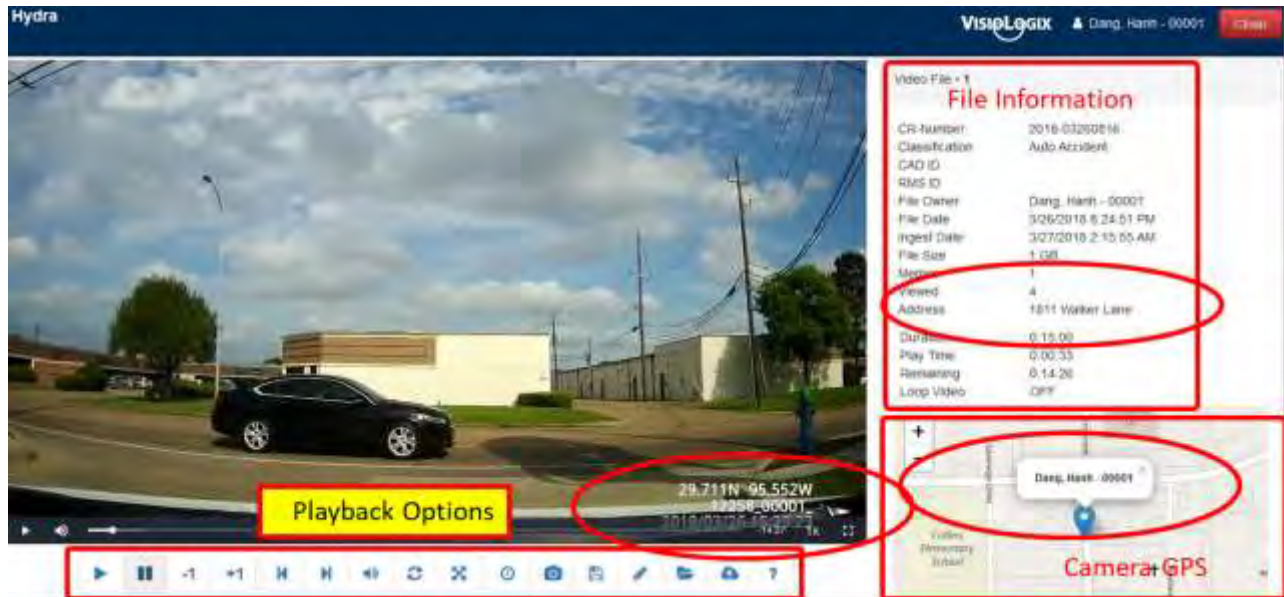
Save

Reset

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

#7 Review and Manage Files

The VisioLogix VEMS has a thoughtful and easy to use file review system with easy search with Boolean operators as well as an array of tools for viewing, classifying, annotating and redacting files. The interface is simple.



Request For Information Police Body Worn Cameras Pennsylvania Chiefs of Police Association

#8 Data Security

All files ingested in to the system are assigned a SHA2 hash code unique to the file. The hash code for each file is stored with the file metadata in the database. The system will automatically alert if the file has been tampered with. The figure to the right is an example of how the hashing files look as well as the structure of the metadata.

File Owner	Windover, Mark - 902
Original Name	ICV_20180509114520.mpg
File Name	83ee2ed7-2d62-4ac1-8ce0-c0f55ada0d84.MP4
File Time	5/9/2018 1:02:35 PM
Ingest Time	5/9/2018 2:02:35 PM
Last View	5/9/2018 2:03:10 PM
View Count	1
Duration	00:00:07
File Size	1.3 MB
Camera ID	107.77.223.139

In compliance with the IACP recommendation, all video captured has a digital signature applied via the camera check out process. When an officer checks out their camera and inputs their PIN, all files that are captured on the camera, will have the officers badge number (or other designation as determined by the agency) embedded directly to the files.

There are a number of critical safeguards in our solution that prevent deletion of files; 1) Camera memory is embedded and not removable, 2) Video, Audio, and Photo files can be reviewed at the camera level with no opportunity to delete or change files in any way, 3) Once the files have been downloaded into the system, the Mission Management Video system assigns file management access at the administrator level, 4) Only personnel assigned by the administrator (we recommend only 1 or 2) are able to manually delete files.

The C3 Sentinel Software suite has an easy to use administrative function (see Step #6 above) that assigns user access by individual or group. The system has the ability to use Microsoft Active Directory as a means to allow for authentication at the user level. Password strength is completely programmable at the administrator level with 8 system parameters.

Hydra | Dashboard | Settings | Reports | Alerts | Accounts | Help

VisioLogix

SYSTEM SETTINGS

Category	Description	Value
ENV - CUSTOMER	Customer Account Name	VisioLogix Corporation
ENV - CUSTOMER	Account Logo URL Reference	http://visio.logix.com/content/uploads/2018/02/visio_logix_2018.png
ENV - CUSTOMER	Logo Image Height	50
ENV - CUSTOMER	Logo Image Width	100
ENV - ADDRESS	Default Account Address	6100 Corporate Drive, Suite 234
ENV - ADDRESS	Default Agency Address City	Houston
ENV - ADDRESS	Default Address State	Texas
ENV - ADDRESS	Default Postal Code	77039
ENV - MISC	Port Display for Case Number	Case Number
ENV - RETAIN	Retention service enabled	True
ENV - RETAIN	Run Retention Date	True
ENV - RETAIN	Time of day to run retention agent (HH:MM)	01:30
ENV - RETAIN	Erasure status unlocks after n days	True
ENV - RETAIN	Min days to delete unerase files	120
ENV - RETAIN	Frequency - day of the week (S-D)	1
ENV - RETAIN	Retention - File Purge Check Period Days	30
ENV - PWD	Enable Password Restrictions	True
ENV - PWD	Minimum pass length	8
ENV - PWD	Requires uppercase letter	True
ENV - PWD	Requires a number	True
ENV - PWD	Not be same as user Login ID	True
ENV - PWD	Password must contain special characters (REGEX)	False
ENV - SECURITY	Enable 2 Factor Authentication	True
ENV - SECURITY	Allow User Access to Reset PWD	True

Description

Minimum password length

Value

8

Default Type: INT

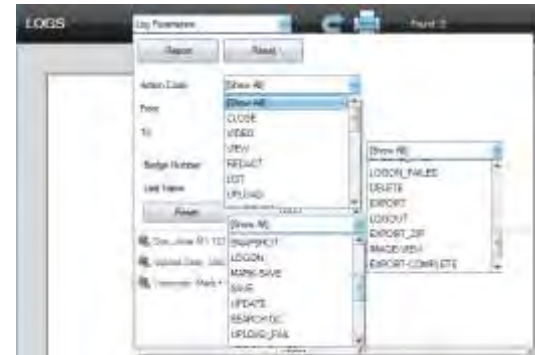
Save Cancel

Request For Information Police Body Worn Cameras Pennsylvania Chiefs of Police Association

Logging and Control Capabilities

The Hydra software has a thorough logging methodology that allows administrators and supervisors to have complete transparency into all aspects of the DEMS operation. The report logs 20 different account activities as it relates to system access. There is also an extensive SQL reporting feature that provides a complete look at all account, camera, evidence and file activities.

The Hydra software suite also has complete logging at the user, PC, and camera level. Every call on the system is completely tracked to manage user activity on the system. This is a critical element of maintenance of evidentiary integrity. Since the software supports SQL Reports, anyone with SQL Reports knowledge will be able to produce additional reports as needed. For example, PCPA can set up an SQL Report server to centralize all reports created by the IT Department.



ACCOUNT ACTIVITY

0000 Admin, IT
11/29/2014 2:37:04 PM / 7/7/2015 11:25:39 AM

0. 6/8/2015 7:32:36 PM Action Code: LOGON
Domain: ME SFIRE Machine: ME S-LPT-21426S Machine account: mwindover
IP: 10.100.10.187 Machine ID: 3691-1B0D-B7BD-570B-4570-B7B4-12DE-02AA
Admin, IT [0000]/ admin

1. 6/8/2015 7:42:09 PM Action Code: LIST
Domain: ME SFIRE Machine: ME S-LPT-21426S
IP: 10.100.10.187 Machine ID: 3691-1B0D-B7BD-570B-4570-B7B4-12DE-02AA
List Accounts

2. 6/8/2015 7:45:44 PM Action Code: LOG
Domain: ME SFIRE Machine: ME S-LPT-21426S
IP: 10.100.10.187 Machine ID: 3691-1B0D-B7BD-570B-4570-B7B4-12DE-02AA
Admin, IT [0000]



**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

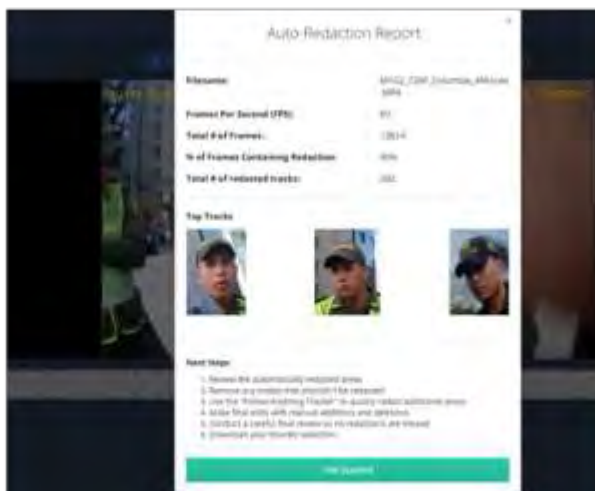
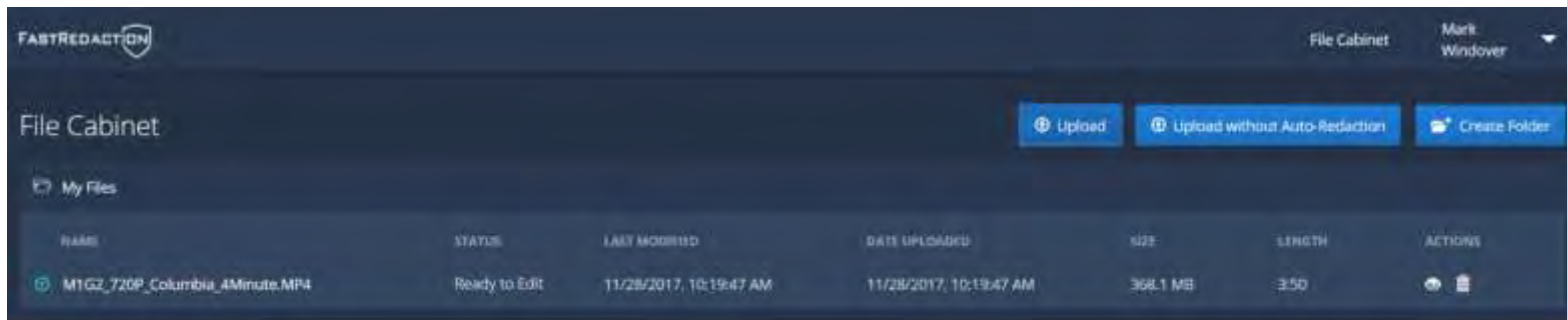
Request For Information Police Body Worn Cameras Pennsylvania Chiefs of Police Association

Redaction Capabilities

We are recommending obtaining a seat license for Fast Redaction, which is a robust and easy to use Web based redaction tool. It is extremely easy to deploy this software in any number of locations via the web. Every file is placed in a secure cloud based CJIS secure environment.

Fast Redaction has industry leading algorithms that have been used in major agencies like Cleveland, OH PD and New Haven PD and is quickly being adapted by agencies all over the country. The VisioLogix DEMS solution will provide a simple web interface for working within Fast Redaction's CJIS compliant cloud environment. The figure below outlines the end product which easily and automatically blurs face and other key identifying features like license plates without human intervention.

Here is the web interface for use with any video sources of data.



**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

Wasabi Cloud Storage

Wasabi features a highly parallelized system architecture that delivers breakthrough performance. A fully compliant Amazon S3 API protects and extends previous investments and gives customers a choice in storage management applications and backup tool



Strong Security Systems and Practices Safeguard Customer Data

Wasabi hot cloud storage is engineered for extreme data durability, integrity and security. The service is built and managed according to security best practices and standards, and is designed to comply with a range of industry and government regulations including HIPAA, HITECH, FINRA, MiFID, CJIS and FERPA.

Wasabi takes a “defense-in-depth” approach to security to protect against the widest range of threats. We ensure the physical security of our data centers; employ strong authentication and authorization controls for all cloud compute, storage and networking infrastructure; and encrypt data at rest and in transit to safeguard confidential data.



Physical Security

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

Secure Network Architecture

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

Immediate Access to Data

Wasabi doesn't play games with Hot or Cold archived data. With Wasabi all stored data is Hot and always immediately accessible at the highest speeds in the industry.

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

Data Privacy and Security

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

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

Data Durability, Protection, and Redundancy

Wasabi hot cloud storage is engineered for extreme data durability and integrity. Wasabi provides eleven 9s (99.999999999%) object durability, protecting data against hardware failures and media errors. In addition, Wasabi supports an optional data immutability capability that protects data against administrative mishaps or malicious attacks.

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

All data has $2N + 1$ redundancy, which means there are two parallel arrays with the same exact architecture and the two arrays are integrated together and communicating which workloads are where for protection purposes. If something happens to one array, you have another adjacent array in constant communication which can pick up right where the other one may have failed.

Wasabi 2N+1 Redundancy



Absolute Flexibility

Unlike all other Public Cloud Providers, Wasabi allows you complete access to all of your data with the ability to migrate any or all of your data to another source whether it be local or another cloud provider. After all...your data is always your data.



Summary

Wasabi is engineered to meet stringent data security and privacy requirements. The service is built and managed according to security best practices and standards, and employs a defense-in-depth approach to protect against a wide array of threats. We ensure the physical security of our data centers, implement strong authentication and access controls to safeguard infrastructure and services, and encrypt data at rest and in transit to protect privacy and prevent unauthorized disclosure.

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

Company Background- Organization and Experience

Municipal Emergency Services is one of the largest providers of Public Safety goods and services in the United States with well over 25,000 customers across the country. Our 375 people manage a business that is in excess of \$227M (2016 Revenue) and have delivered some of the largest public safety programs in the US in the police, fire and EMS trades.

MES and its Law Enforcement business, Lawmen Supply Company, have 45 years of combined experience in Public Safety. MES is a leading supplier to the Public Safety trades while LSC is a leading Police Supplier with our 375 Public Safety professionals across the country with an average of 25+ years of experience in the trades.

Listed below are key contact reference names for BWC programs built and deployed by MES and VisioLogix, technology provider for your solution. The most important element of the solution is the software and that has been pressure tested in large deployments on a scale with the PCPA BWC program as described.

Customer	Vendor	Contact Name:	Address:	Phone:	Email:	Camera Count
Rochester Police Department	MES and HD Protech/VisioLogix	Lt. Mike Perkowski	185 Exchange St. Rochester, NY 14614	585-428-8831	mp0963@cityofrochester.gov	508
Chinese Police in Shenzhen	HD Protech/VisioLogix	Rita Wang	Win-Win Development Technology Co Floor 4, Plant 112, Jindi Industrial Zone, Futian District, Shenzhen, China.	Cell: +86 181 2707 3684	wangr@sector2dev.com	12,000
ALSI-ASIA-PAGE Ltd.	VisioLogix leading project.	Alexandr Ponomarev	Head of Security Solutions Department 34a, Zhandosov st, Almaty, Kazakhstan	Phone: +77272971016 Mob: +77019077131	Alexander.Ponomarev@alsi.kz	2,000
Allied Universal Protection Services	MES and HD Protech/VisioLogix	Mr. Mark Meredith, General Manager	10680 Trenea Street, Suite 450 San Diego, CA 92131	(858) 322-6206 Direct	Mark.Merideth@aus.com	85
Atlantic County (NJ) Department of Corrections	MES and HD Protech/VisioLogix	Lt. Bruce Carber	5060 Atlantic Ave. Mays Landing NJ. 08330	609-909-7577	carber_bruce@aclink.org	48

Regarding our relevant experience, VisioLogix, the lead technology BWC and Video Management Software provider for the proposal, has experience with a number of large agency deployments over the past 4 ½ years. Key expertise in integration of hardware and the VisioLogix, C3 Sentinel Mission Management software. The recap of agencies and size of deployment is as follows:

Installation of Units by Size of Deployment

up to 5 BWC Units	6 - 100 BWC Units	101 - 500 BWC Units	501 - 1000 BWC Units	1000+ BWC Units
51 agencies	68 agencies	18 agencies	4 agencies	4 agencies

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

The following is a portion of our reference list, please feel free to call anyone on the list.

Reference List

Rochester Police Department MES/Lawmen and VisioLogix Services complete 2/28/17
Lt. Michael Perkowski Michael.Perkowski@CityofRochester.Gov
Research & Evaluation Section
185 Exchange Blvd
Rochester, NY 14614
Phone: 585-428-8831

Allied Universal Protection Services MES/Lawmen and VisioLogix
Mark Merideth Mark.Merideth@aus.com
General Manager
Allied Universal Security
10680 Treena Street, Suite 450
San Diego, CA 92131

Atlantic County (NJ) Department of Corrections
Lt. Bruce Carber carber_bruce@aclink.org
Training Unit Supervisor
Atlantic County Dept. Public Safety
5060 Atlantic Ave.
Mayslanding NJ. 08330
609-909-7577

Greenwich Township Police Dept. MES/Lawmen and VisioLogix Services complete 2016
Captain Kevin Nastasi knastasi@greenwichpd.com
421 W. Broad St.
Gibbstown, N.J. 08027
Desk 856-423-6576
Office 856-423-4206

Win-Win Development Tech. for the Chinese Police VisioLogix leading project.

Rita Wang wangr@sector2dev.com
8/F Building B1 Block Five
Honghualing Industrial Park
Taoyuan Street Nanshan District, Shenzhen, China
Cell: +86 181 2707 3684

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

Rochester (NY) Police Department

Our largest US reference customer is Rochester Police Department with over 500 BWC's deployed. Rochester is a complex organization with 8 remote locations and a myriad of security protocols. The MES/VisioLogix team worked closely with RPD to establish a robust and high performance BWC mission. When the entire industry was heading to a Cloud Based environment, RPD took the more challenging and significantly less expensive approach of using its own storage infrastructure. RPD has also collaborated with our development teams to create a best in class software and operating environment that has translated nicely from just a BWC environment into a full digital evidence management platform.



Chinese Police

VisioLogix has managed a challenging installation of over 12,000 BWC's and a highly complex and distant operation. With a solid software foundation, VisioLogix was able to navigate through the numerous roadblocks of a foreign operating environment. This project has helped VisioLogix to scale at the highest levels. The SQL database was successfully pressure tested with 12,000 cameras and even more users. This project has helped the organization to establish protocols for managing the largest of customers.

Kazakhstan Police

VisioLogix has managed a similar large program with the police in Kazakhstan. This deployment features in excess of 2,000 Body Cameras across a fast-moving environment. The main challenge that VisioLogix has faced is that the software is required to manage multiple different body worn cameras. Meeting this challenge has helped the VisioLogix team to create a hardware agnostic environment which is unique in the industry.

January 30, 2019

ATTN: Christopher J. Braun
Pennsylvania Chiefs of Police Association
3905 N. Front Street,
Harrisburg, PA 17110

Dear Mr. Braun:

Axon Enterprise, Inc. (Axon) is pleased to submit the enclosed proposal for a body-worn camera solution to the Pennsylvania Chiefs of Police Association (PCPA) and the State of Pennsylvania. This proposal describes Axon's top-tier body-worn camera program.

The system you select should meet your objectives to provide a solution to purchase implement an effective body-worn camera solution for Pennsylvania's over 30,000 sworn officers working in over 1200 police departments. Axon is the leading provider of law enforcement technology; our primary purpose is to help you achieve your goals and advance the efforts of public safety agencies through technology wherever possible.

Our comprehensive body-worn camera program offers rugged and reliable cameras, the **Axon Body 2** and **Axon Flex 2**, with numerous mounting possibilities. Axon's body-worn camera systems also extend beyond hardware, consolidating all Axon-captured evidence in Evidence.com, Axon's cloud-based and CJIS-compliant digital evidence management software (DEMS).

Some additional benefits you can receive as an Axon partner today are:

- Regular hardware refreshes
- Expert deployment, training, and support
- A Dock & Walk workflow
- Evidence.com DEMS and native data management tools
- Axon View and Axon Capture mobile applications
- Monthly software upgrades
- Unlimited cloud-based storage
- Immediate video access
- Proven CAD/RMS integrations



17800 N 85TH STREET
SCOTTSDALE, ARIZONA 85255

AXON.COM

Axon has developed, expanded, and enhanced its technology over time to build a fully integrated platform with direct input from law enforcement agencies around the world. To date, we've partnered with over 7,500 agencies to deliver industry-leading digital evidence capture solutions and our offerings will only get stronger as we continue developing new products and features to meet the evolving needs of the law enforcement and public safety community.

If you have any questions regarding our proposal, pricing or products, please contact our Proposal Manager, Debashree Nag at 425.589.1963 or dnag@axon.com. Thank you for your consideration; we look forward to continued conversation with the PCPA.

Sincerely,

Robert Driscoll

VP, Associate General Counsel

Axon Enterprise, Inc.

REQUEST FOR INFORMATION POLICE BODY WORN CAMERAS PENNSYLVANIA CHIEFS OF POLICE ASSOCIATION

Submitted by:

Axon Enterprise, Inc.



**17800 North 85th Street
Scottsdale, AZ 85255
800.978.2737
January 30, 2019**

TABLE OF CONTENTS

INFORMATION REQUESTED.....	1
----------------------------	---

INFORMATION REQUESTED

The information requested includes the manufactures, vendors or resellers of specific products and services that meet Pennsylvania Laws, standards and regulations that allow them to develop the necessary polices required. In addition, cost and discounted price are requested. Please provide at least the following information:

- **How does your non-vehicle-mounted mobile video recording systems and technology meet Pennsylvania's published requirements?**

The **Axon Body 2** is a self-contained audio-visual body-worn camera unit with no external wires. We offer numerous mounting options, some optimized for security (Z-Bracket, Molle, and Magnet mounts) and others built for versatility (Shirt pocket, Clip, and Velcro mounts). Mounts can accommodate uniforms, belts, outerwear including jackets, and tactical and SWAT vests (without any alteration).

The Axon Body 2 was designed specifically for law enforcement use in tactical policing situations. Activation of event recording is simple and accessible, making it easy for officers to operate the device in high-stress situations. Recordings are initiated with a single "Event Button" located on the front of the device, so an officer can easily reach it with one hand.



The Axon Body 2 mounted on an officer's chest

Features & Benefits

- **HD Video:** The industry's best low-light video records in 1080p HD
- **Full-shift Battery:** Lasts for a full shift (over 12 hours)
- **Configurable Pre-Event Buffer:** Capture up to 2 minutes before an event
- **Dual-Channel Audio:** Camera records two audio channels
- **Axon Signal Wireless Activation:** Cameras start recording automatically based on pre-defined triggers
- **Optional Mute:** Disable audio in the field to support dual-party consent
- **Mobile Application:** Tag and replay videos from the field with Axon View
- **RapidLock Mounts:** Versatile mounts are designed for versatility and comfort, while keep the camera steady

Technical Specifications

- **Field of View:** 143 Degrees
- **Recording Capacity:** Up to 70 Hours Depending on Resolution
- **Video Quality:** 30 frames per second; resolution spanning 480p - 1080p
- **Battery:** Rechargeable lithium-ion polymer battery (3000 mAH capacity)
- **Weather Resistance:** IEC 60529 IP67 (dust, water); MIL-STD-810G (Salt fog)
- **Humidity:** 95% non-condensing
- **Operating Temperature:** -4 °F To 122 °F [-20 °C To 50 °C]
- **Drop Test:** 6 Feet – camera is housed in high-impact polymer
- **Dimensions:** 3.42 in x 2.76 in x 1.01 in (slightly larger than a pack of cards)
- **Weight:** 5.0 oz.

The **Axon Flex 2** is a point-of-view camera that provides multiple options for wearing the camera to suit your officers' needs in the field. The 120° field of view lens captures events as experienced by the wearer.

The camera is connected to a controller, which houses the battery, with one cable. The Axon Flex 2 camera can be mounted on Oakley Flak Jacket® glasses, ball caps, uniform collars and epaulettes, a lowrider headband, on a vest, and motorcycle and SWAT helmets.



Officer in the field using the Axon Flex 2 camera with the Oakley Flak Jacket® mount

Axon Flex 2 Features & Benefits

- **HD Video:** The industry's best low-light video records in 1080p HD
- **Full-shift Battery:** Lasts for over 12 hours covering an entire shift
- **Configurable Pre-Event Buffer:** Capture up to 2 minutes before an event
- **Dual-Channel Audio:** Camera records two audio channels
- **Axon Signal Wireless Activation:** Cameras start recording automatically based on pre-defined triggers
- **Optional Mute:** Disable audio in the field to support dual-party consent
- **Mobile Application:** Tag and replay videos with the Axon View mobile app
- **RapidLock Mounts:** The system uses versatile mounts designed for versatility and comfort, while keep the camera steady

Technical Specifications

- **Field of View:** 120 degrees
 - **Recording Capacity:** Up to 70 Hours depending on resolution
 - **Video Quality:** 30 frames per second; resolution spanning 480p - 1080p
 - **Battery:** Rechargeable lithium-ion polymer battery (3600 mAH capacity)
 - **Weather Resistance:** IEC 60529 IP54 (dust, rain); MIL-STD-810G (Salt fog)
 - **Humidity:** 95% non-condensing
 - **Operating Temperature:** -4° F to 122° F [-20° C to 50° C]
 - **Drop Test:** Up to 6 feet – devices are housed in high-impact polymer
 - **Dimensions:** Controller: (D1) 0.94 in, (D2) 1.14 in, (W) 2.45 in, (H) 3.0 in;
Camera: (L) 2.9 in, (H) 0.75 in, (W) 0.74 in
 - **Weight:** Controller: 4.4 oz., Camera: 0.88 oz.
- **Have you submitted your non-vehicle-mounted mobile video recording systems to the Pennsylvania State Police for certification?**

Yes, the Axon Body 2 and the Axon Flex 2 cameras are in the list of PA State List of certified body-worn cameras.

- **Is your non-vehicle-mounted mobile video recording systems already certified by the Pennsylvania State Police?**

Yes, Axon Body 2 and Axon Flex 2 cameras are certified by the Pennsylvania State Police.

- **Are you offering a storage solution?**

Yes, Axon's Body-worn cameras are paired with Axon Evidence (**Evidence.com**), a robust end-to-end solution that not only allows agencies to store data, it also enables new workflows for managing and sharing that data securely from anywhere.

Officers and command staff can upload content from Axon and TASER devices or other systems easily, manage it simply with search and retrieval features, and then collaborate effortlessly with prosecutors and other partners by using powerful sharing features. When storage needs increase, the cloud-based system allows agencies to scale instantly and cost-effectively.

Many agencies today are taking advantage of our unlimited data offering to best protect the agency from escalating costs over the course of a program.

- **Will you offer storage solutions bundled (no line item distinction) with the cost of each camera purchased?**

Evidence.com is licensed on a per user basis; a license is required for each camera. As a hosted application, there is no limit to the number of users your agency can add, should administrators or staff without body cameras need access to the system.

A license is what allows a user to access either Basic or Pro Evidence.com features. License counters appear on the administrator's view of the Dashboard, and the Roles page to help you keep track of your licenses. Users in the Lite tier do not count toward your agency's total licenses.

Basic Tier

The Basic tier is the lower of the two paid tiers on Evidence.com. Basic tier users are people who need to upload and manage their digital evidence, but do not need access to advanced features such as automated redaction and group monitoring.

Pro Tier

The Pro tier is the higher of the two paid tiers on Evidence.com. Pro tier users are people who need access to advanced features, such as automated redaction, group monitoring, agency analytics and reports, and human transcription services, among others.

Licenses Tiers

✓ indicates functionality included in the cost per license. Costs for additional features are indicated on a per license basis.

Evidence.com License Tier Features	BASIC	PRO
Secure File Storage	✓	✓
File & Case Sharing	✓	✓
Video Clips & Markers	✓	✓
Custom User Roles & Categories	✓	✓
Automatic File Deletion Schedules	✓	✓
Bulk Reassign, Share, Edit	✓	✓
Single Sign-On (SSO)	✓	✓
Video Redaction		✓
Group Monitoring		✓
Agency Usage Reports		✓
Advanced Device Analytics		✓
Human Paid Transcription		✓
Multicam Playback		✓
Restricted Evidence		✓
Axon Citizen 1:1		✓
Redaction Studio		✓

Evidence.com License Tier Features	BASIC	PRO
Included Storage	Includes 10 GB of storage for non-Axon Fleet video	Includes 30GB of Storage for non-Axon Fleet video

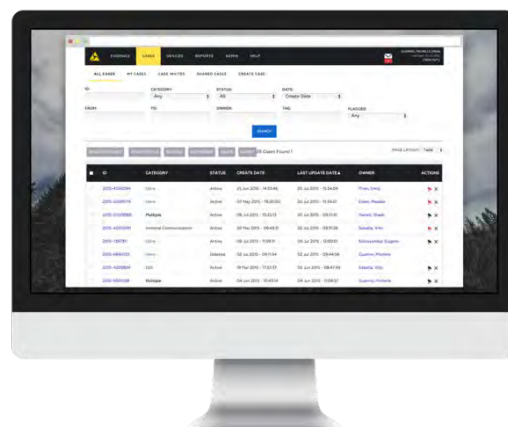
- **How does your storage solution meet Pennsylvania's published requirements?**

Evidence.com is a robust end-to-end solution that not only allows agencies to store data, it also enables new workflows for managing and sharing that data securely - from anywhere.

A SCALABLE SOLUTION

Officers and command staff can upload content from Axon and TASER devices or other systems easily, manage it simply with search and retrieval features, and then collaborate effortlessly with prosecutors and other partners by using powerful sharing features. When storage needs increase, the cloud-based system allows agencies to scale instantly and cost-effectively.

Many agencies today are taking advantage of our unlimited data offering to best protect the agency from escalating costs over the course of a program.



Control Access with Roles and Permissions

Each Evidence.com user is assigned a role. Roles determine a user's permissions, which control levels of access to features and functions in Evidence.com. Information access via Evidence.com is controlled through a robust "Access Control System" managed by the Administrator and that features comprehensive audit trails. Access to information is governed by the agency-defined access control system built into Evidence.com.

Access is controlled according to:

- Pre-defined roles
- Pre-defined individuals (i.e., who has access to what data feed)
- User account-specific passwords

Active Directory

Evidence.com can interface with a federated **Active Directory** to support user login with their agency credentials. Using the industry-standard SAML protocol, officers no longer need to juggle multiple usernames and passwords. With Active Directory

federation, Evidence.com uses the agency's network to authenticate users. Agency credentials are never sent to Evidence.com. This means that if a user changes their password on Active Directory they will log in with that new password.

Simplified Evidence Categorization

Evidence.com uses category types to organized stored video, simplifying the search process for your agency users. All categories are set by your agency to reflect your policies and desired structure. This categorization also facilitates database management by automatically ensuring that only relevant evidence is retained in the system. Every event that is captured and uploaded to Evidence.com can be assigned a category to determine how long it is retained in the system. Proper categorization is important to ensure that incidents remain in the system for the appropriate amount of time. Categories include policy settings for evidence retention and restricted access for especially sensitive evidence.

Evidence Retention Policies

Storage Set-Up Options and Automatic Deletion

For proper management, agencies must create a set of agency-specific Categories large enough to properly segregate evidence by type for retention-setting and search functionality. This list should not be so large that it becomes an impediment to efficient field use by users. Categories can be edited or added later within Evidence.com by users with appropriate access. The category assigned to a video file determines the retention policy associated with that piece of evidence. The evidence retention policy determines:

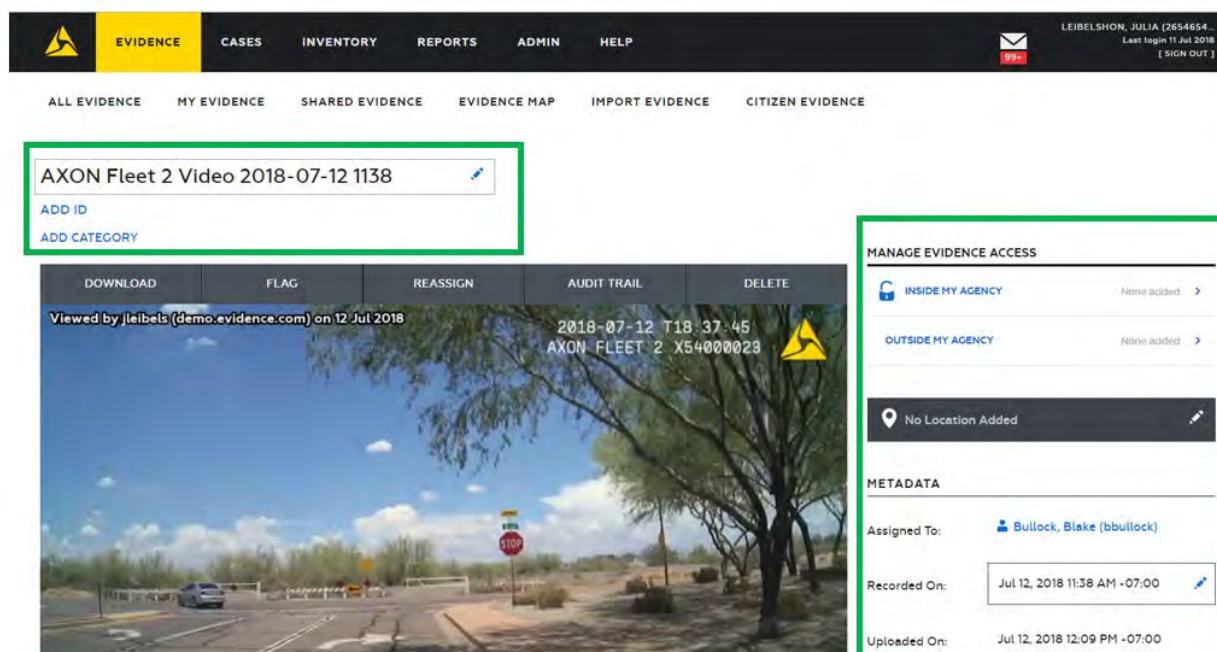
1. Whether the system will initiate automatic deletion of evidence assigned to the category.
2. How long the system waits before initiating the deletion of evidence that is not included in a case. Axon video deletions are based on the recording date. Deletion of all other evidence is based on the upload date.

Remorse Periods for Retrieving Deleted Files

To protect against accidental deletions, administrators can recover files up to 7 days after they are queued for deletion. This policy applies to evidence only. Cases are never deleted automatically. Evidence included in a case is exempt from deletion until it is removed from the case. If evidence is in multiple categories, the longest retention time will be used. This 7-day remorse/recovery period and approval workflow is designed to protect evidence and chain of custody. After the remorse period, the file is expunged.

Managing Your Digital Evidence

Evidence.com was designed to provide users with easy, straightforward ways to review and manage digital evidence. Once a user has located the desired file, he or she can perform the following actions (all actions will be recorded in the evidentiary audit log).



- **Edit Title and ID**
- **Add or Remove Tags** – Tags are labels that can be applied to evidence. Tags can be added to evidence for easy locating in the future. Evidence searches allow users to filter the search results by tags.
- **Edit Location** – The specified location for evidence determines where the pin representing the evidence appears on evidence maps.
- **Add, Edit and Delete Notes** – Notes can be posted about evidence. In addition to the text of the note, Evidence.com shows the author of the note and the date and time that the note was created and updated.

Users can also perform the following actions as part of the streamlined search process:

- **Edit Description** – Descriptions of the evidence can be added or edited.
- **Edit Recorded Date and Time**
- **Download Evidence File** – Data can be exported to external media such as CD-ROMS, flash drives, and external hard drives.
- **Flag or UnFlag Evidence** – Evidence can be flagged to make it easy to find in the future. Evidence searches allow users to filter the search results by the flag status of evidence.

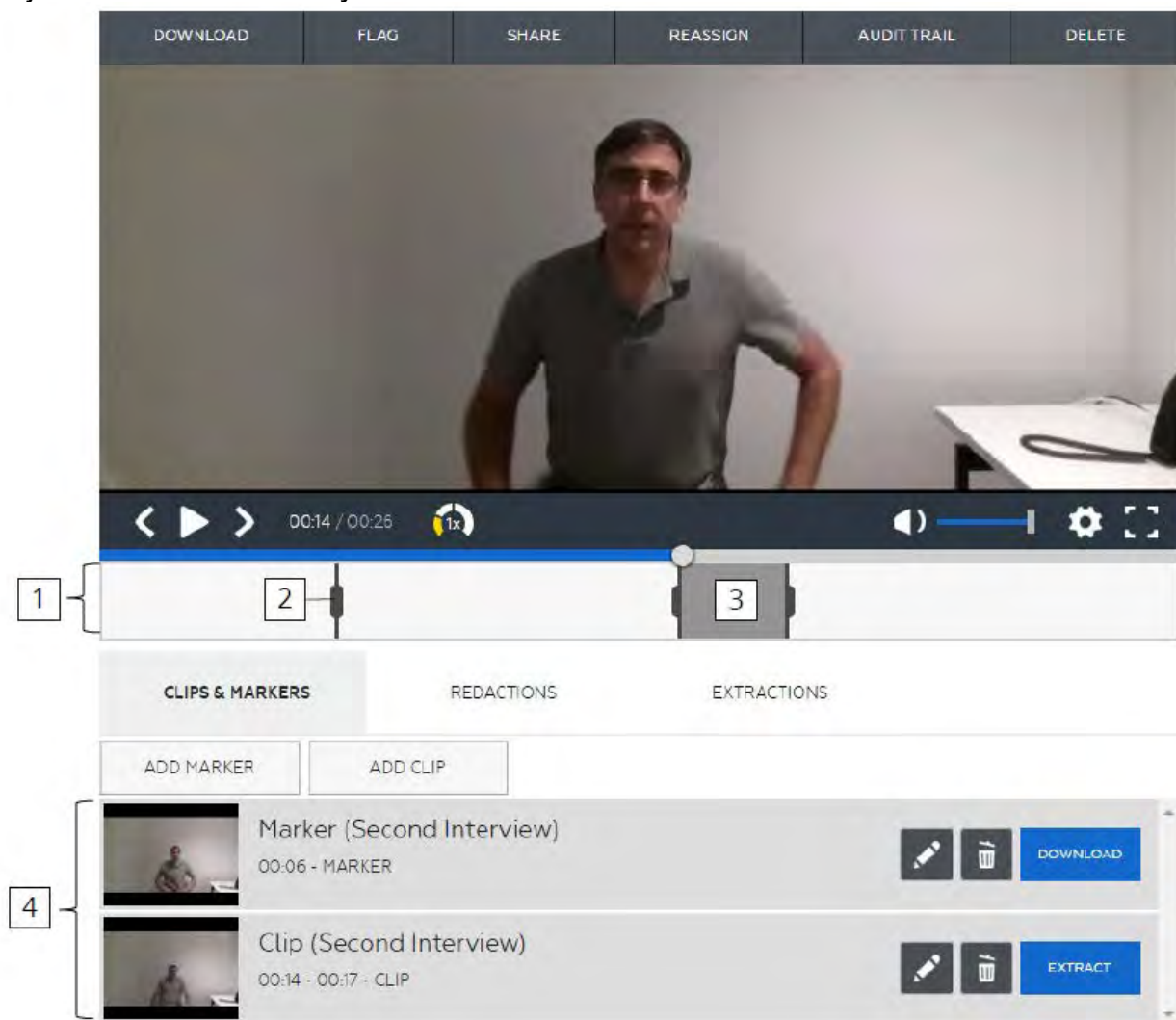
- **Add to or Remove Evidence from a Case** – Users can add or remove evidence to one or more cases.
- **Reassign Evidence** – Users can assign evidence to a user. The user to whom the evidence is assigned becomes the owner of the evidence.
- **View Evidence Audit Trail**
- **Delete Evidence** – Users can manually initiate the deletion of an evidence file. Deleted evidence is added to a deletion queue for 7 days. This helps prevent deleting evidence unintentionally.
- **Restore Deleted Evidence** – If evidence has a status of Queued for Deletion, users can restore the evidence, which removes it from the deletion queue.
- **Assign and Un-Assign Categories** – For evidence that is not assigned to a case, changing the categories that the evidence is assigned to may change the scheduled deletion date. If the scheduled deletion date has already passed, the evidence will be added to the deletion queue.
- **Extend Retention Period** – If evidence is scheduled for deletion, users can extend how long the system retains the evidence before adding it to the deletion queue. The period of time that the retention is extended is equal to the length of the retention policy currently in effect for the evidence. The category assigned to the evidence determines the retention policy. If more than one category is assigned to evidence, the longest retention policy is applied.

Working with Video and Audio Evidence

- **Play, Pause, Rewind, and Fast Forward**
- **View Source** - For video uploaded from an Axon device managed by an Evidence.com agency, the View Evidence page lists the evidence source on the right side of the page. The serial number and model of the recording device are listed.
- **Show and Hide Clock**
- **Rotate the Video** - Users can rotate the video player image 90, 180, or 270 degrees clockwise. This feature is for convenience while viewing a video only. For example, the camera itself may have been on its side or upside down while recording. The rotation does not affect the original video file and is not saved in any way.
- **Markers** - Users can use markers to indicate key moments or highlight important aspects of a video or audio evidence file. For video markers only, users can download markers as image files. Prior to downloading the marker, users can specify options such as whether the title and description appear on the downloaded image. Users can control whether the scrub bar, located below the video image, shows red icons for each marker.
- A **clip** is a continuous segment of an evidence file that you can define. You can create a clip for any segment of an evidence file and assign the clip a title and description. For example, if a 10-minute video includes a 30-second segment that captures important actions and audio, you can create a clip for the important segment.

Marker and Clip Controls

The following image highlights the main Evidence.com video player interface and each major feature available to your users.



Marker and Clip Controls	
1 — Timeline	3 — Clip handles
2 — Marker handle	4 — Markers and clips list

- **Magnify Zone** - Users can use the zone magnification tool to zoom in on a portion of a frame as needed to view details in the video. Users have the option of converting a magnified zone into a marker.
- **Show and Hide Thumbnails** - Thumbnails provide an easy way to preview parts of a video. They appear at the bottom of the video image. Users can move the mouse pointer across them to see each thumbnail.

- **View Video Frame by Frame** - Below the video player, the frame-by-frame scrub bar appears. Each segment of the bar represents a video frame. Use the frame-by-frame features as needed:
 - To preview frames
 - To navigate quickly to a specific frame, and;
 - To skip backwards or forwards

Video Redaction Capabilities*

Evidence.com provides the ability to redact what can be seen and heard in video evidence files. The redaction tools enable you to create redacted versions of video evidence files without affecting the original file.

A *redaction* is a set of information that tells Evidence.com what to redact in a video. You can create a redaction with either Evidence.com redaction tool:

- Manual redaction
- Assisted redaction featuring Smart Tracker technology

When you have completed creating or editing a redaction, you can extract a redacted video. You can create and maintain many redactions for each video evidence file. This enables you to create different redacted videos for different audiences or different purposes.

An extracted video is a video evidence file that Evidence.com creates from a clip or a redaction. Evidence.com never alters the original video evidence file when you create a clip or a redaction.

The clips and redactions features complement each other. If you have a long video and need to share a redacted segment, it is recommended that you first create a clip, extract a video from the clip, and then redact the extracted video.

Redacting a Single Video: The process of redaction involves placing one or more masks in the video. Users can specify precisely which video frame a redaction mask applies to. The redaction mask types are the following:

- **Vector** – Redacts a portion of video frames, in a shape, color, and opacity specified by the user.
- **Blackout mask** — Replaces video frames with a solid black frame.
- **Filter mask** — Obscures entire video frames with either a blur filter, an outline distortion filter, or a segmentation filter.
- **Audio mask** — Remove audio from the frames to which user applies the mask.
- **Skin Blurring** — When using this feature, the user selects the level of skin blurring. Then, during processing, the redaction algorithm searches for skin tones throughout the video and blurs them to the selected level.

Pennsylvania Chiefs of Police Association
Request For Information for Police Body Worn Cameras

Users will also have the option of redacting audio for the duration of a video mask.

Bulk Video Redaction: Public disclosure and FOIA requests can be time consuming, especially when large volumes of videos must be reviewed and potentially redacted. To aid with these large requests, the Bulk Redaction feature allows you to queue video evidence for bulk redaction.

Evidence.com will redact the videos and bundle them into a file. We will email with a link to download this file when it's ready. This link will be active for 3 days.

ORDER SUMMARY

Evidence - 3 files
Request Date - 27 Jul 2015 - 12:22:43 (GMT-0700)
Estimated File Size - 16.95 MB

DOWNLOAD FORMAT

☐ ZIP
☒ ISO

BLUR LEVEL

☐ LOW
☒ MEDIUM
☐ HIGH

AUDIO

☒ MUTE AUDIO

Bulk redaction creates a copy of the original video and a blur filter over the entire video. It can also remove audio for the duration of that copy as well. The blur over the entire video allows requestors to see what happened in the video without potentially revealing personally identifiable details such as faces, addresses, or license plates. This presents an opportunity for agencies to fulfill mass public disclosure requests in the least amount of time.

*Video Redaction is a feature available with Pro licenses (not available with Basic licenses).

- **List the products and services that are already available on State Contract or PA CoStars.**

Axon Enterprise, Inc. is on PA CoStars with the following product groups:

- Electroshock Weapons & Accessories
- Duty Belts, Holsters & Pouches
- Body and Vehicle Cams

- **List your costs for products and services you offer.**

Please find our prices of products and services listed under Appendix A.

- **Will you offer a discount of those prices if multiple police departments group together to buy your products and services?**

Axon may consider a discount from our standard prices. Discounts will be negotiated at the individual agency level.

APPENDICES

- A. Axon Camera Agency Pricing_2019
- B. Axon Body 2 Specifications
- C. Axon Flex 2 Specifications
- D. Axon Interview Specifications
- E. Axon Fleet Specifications
- F. Axon Signal Specifications
- G. Evidence.com Specifications
- H. Evidence.com for Prosecutors Specifications
- I. Evidence Sync Specifications
- J. Axon View Mobile Application Specifications
- K. Axon Citizen Product Card



17800 N. 85th St. Scottsdale, AZ 85255-6311

800.978.2737 Toll Free • 480.991.0791 Fax

www.axon.com • Sales@axon.com

2019 Law Enforcement Agency Pricing – Axon Systems

Axon Flex 2 Camera Hardware and Accessories

Model	Product Description	Agency Price
11528	Axon Flex 2 Camera (online)	\$449.00 ea.
11529	Axon Flex 2 Camera (offline)	\$649.00 ea.
11532	Axon Flex 2 Controller	\$250.00 ea.
11544	Oakley Flak Jacket Kit, Axon Flex 2	\$164.00 ea.
71037	Low Rider Headband, Axon Flex 2	\$29.00 ea.
11545	Collar Mount, Axon Flex 2	\$41.00 ea.
11554	Clip, Oakley, Axon Flex 2	\$23.00 ea.
11546	Epaulette Mount, Axon Flex 2	\$30.50 ea.
11547	Ballcap Mount, Axon Flex 2	\$29.00 ea.
11555	Mount, Ballistics Vest, Axon Flex 2	\$31.00 ea.
11548	Universal Helmet Mount, Axon Flex 2	\$27.00 ea.
11549	Tactical SWAT Kit with ARC Rail, Axon Flex 2	\$65.00 ea.
11533	Cable, Coiled, Straight to Right Angle, 48", Axon Flex 2	\$17.50 ea.
11534	USB Sync Cable, Axon Flex 2	\$10.50 ea.
73082	Wall Wart	\$14.95 ea.

Axon Body 2 Camera Hardware and Accessories

Model	Product Description	Agency Price
74001	Axon Body 2 Camera System (online)	\$499.00 ea.
74004	Axon Body 2 Camera System (offline)	\$699.00 ea.
74006	Axon Body 2 Battery Pack	\$39.00 ea.
11553	USB Sync Cable	\$10.00 ea.

Axon Body 2 Camera and Flex 2 Controller Mounts **

Model	Product Description	Agency Price
74018	Z-Bracket, Men's, Axon RapidLock	\$29.95 ea.
74019	Z-Bracket, Women's Axon RapidLock	\$29.95 ea.
74020	Magnet, Flexible, Axon RapidLock	\$29.95 ea.
74021	Magnet, Outerwear, Axon RapidLock	\$29.95 ea.
74022	Small Pocket, 4" (10.1 cm), Axon RapidLock	\$29.95 ea.
74023	Large Pocket, 6" (15.2 cm), Axon RapidLock	\$29.95 ea.
71026	Reinforced Flexible Magnet Mount, Axon RapidLock	\$29.90 ea.
71038	Reinforced Flexible Magnet Mount, Back Plate	\$13.00 ea.
74028	Wing Clip Mount, Axon RapidLock	\$29.95 ea.
11507	MOLLE Mount, Single, Axon RapidLock	\$29.95 ea.
11508	MOLLE Mount, Double, Axon RapidLock	\$39.95 ea.
11509	Belt Clip Mount, Axon RapidLock	\$29.95 ea.

** Two mounts are included (a la carte) for \$0; \$29.95 for each additional mount.

Axon Signal Hardware & Services

Model	Product Description	Agency Price
70112	Axon Signal Vehicle unit (1 per car/motor)	\$279.00 ea.
Service	Axon Signal Vehicle unit installation and/or training	Variable
70116	Axon Signal Performance Power Magazine (SPPM)	\$100.00 ea.
varies	Axon Signal Sidearm	\$10 per user per month (60-month term required)



Axon Dock Hardware

Model	Product Description	Agency Price
11536	1-bay + Core Axon Dock for Axon Flex 2	\$375.00 ea.
11537	6-bay + Core Axon Dock for Axon Flex 2	\$1,495.00 ea.
11538	1-bay for Axon Flex 2	\$99.00 ea.
11539	6-bay for Axon Flex 2	\$1,195.00 ea.
11541	1-bay T&E Dock for Axon Flex 2	\$0
11542	6-bay T&E Dock for Axon Flex 2	\$0
74009	1-bay + Core Axon Dock for Axon Body 2	\$375.00 ea.
74008	6-bay + Core Axon Dock for Axon Body 2	\$1,495.00 ea.
74011	1-bay for Axon Body 2	\$75.00 ea.
74010	6-bay for Axon Body 2	\$1,195.00 ea.
70027	Axon Dock Core, compatible with all 1-bays and 6-bays	\$300.00 ea.
70033	Wall mount, Axon Dock	\$42.00 ea.
70040	Desk plate, Axon Dock	\$35.00 ea.

Customer Care Extended Warranty

Model	Product Description	Agency Price
85070	TASER Assurance Plan Axon Body 2 annual payment	\$240.00 ea.
85054	TASER Assurance Plan Axon Flex 2 annual payment	\$348.00 ea.
87026	TASER Assurance Plan Axon Dock 6-Bay annual payment	\$336.00 ea.
80118	2-Year Extended Warranty Axon Flex 2 Camera	\$299.95 ea.
87029	2-year Extended Warranty Axon Body 2 camera	\$199.95 ea.
87030	2-year Extended Warranty Axon Dock for Axon Body 2, single bay + core	\$129.90 ea.
87031	2-year Extended Warranty Axon Dock for Axon Body 2, 6-bay + core	\$499.90 ea.
80124	2-year Extended Warranty Axon Dock for Axon Flex 2, single bay + core	\$129.90 ea.
80125	2-year Extended Warranty Axon Dock for Axon Flex 2, 6-bay + core	\$499.90 ea.

Axon Evidence (Evidence.com) Services

Model	Product Description	Agency Price
87001	Basic Axon Evidence license: 1 year	\$180.00 ea.
89001	Pro Axon Evidence license: 1 year	\$468.00 ea.
80022	Pro Axon Evidence License Annual Payment	\$468.00 ea.
85100	Axon Evidence integration license, annual payment	\$180.00 ea.
85123	Axon Evidence Unlimited Plan annual payment*	\$948.00 ea.
85130	Officer Safety Plan annual payment**	\$1,308.00 ea.
85035	Axon Evidence storage (GB): 1 year	\$0.75 ea.

* This license tier is only available for 3-year or 5-year terms

** This license tier is only available for 5-year terms.

*** Axon Evidence storage not included with the Basic Package. A-la-carte storage is required.



Axon Professional Services

Model	Product Description	Agency Price
n/a	Basic remote support	Free
85055	Axon Full Service	\$17,000 ea.
85144	Axon Starter	\$2,750 ea.
85146	Axon 1-Day Service	\$2,000 ea.

Axon may change pricing or product offerings at any point in time. The committed pricing is based on each Axon Quote provided to the Agency.

Freight Policy Freight is the responsibility of the purchaser. All taxes, duties and customs, where applicable, are the responsibilities of the customer.

Pricing Pricing for Law Enforcement/Correctional Agencies Only. Must be a sworn law enforcement officer to purchase.

Order Lead Time 4 to 6 weeks ARO. **ALL SALES ARE FINAL.**

For delivery status or information on how to place an order, call our sales department at 800-978-2737, fax: 480-991-0791

Axon Enterprise, Inc.'s Sales Terms and Conditions for Direct Sales to End User Purchasers apply to all sales and are available at <http://www.axon.com/sales-terms-and-conditions>.

Flak Jacket is a trademark of Oakley, Inc.

▲, ▲ AXON, Axon, Axon Body 2, Axon Evidence, Axon Flex, Axon Flex 2, Axon Fleet, Axon Signal, Axon Signal Sidearm, Axon Signal Vehicle, and TASER are trademarks of Axon Enterprise, Inc., some of which registered in the US and other countries. For more information, visit www.axon.com/legal. All rights reserved. © 2019 Axon Enterprise, Inc.



YOU'RE JOB ISN'T ALWAYS PRETTY.

Come rain, shine, blood or sweat—our products will be there, toughing it out alongside you. Because when it comes to safety, security, and your agency, looks don't matter – reliability does.



800-978-2737 axon.com/body2

AXON BODY 2 FEATURES AND BENEFITS

RETINA HD VIDEO: The industry's best low-light video now records in HD.

FULL-SHIFT BATTERY: 12+ hours

PRE-EVENT BUFFER: Configure your pre-event buffer time to capture up to 2 minutes before an event.

WIRELESS ACTIVATION: Axon Signal reports events, like when you open the car door or activate the light bar, so your camera can detect them and start recording.

OPTIONAL MUTE: Ability to disable audio in the field to support dual party consent.

IN-FIELD TAGGING: Add a marker to important points in your video.

UNMATCHED DURABILITY: Built to withstand extreme weather and brutal conditions.

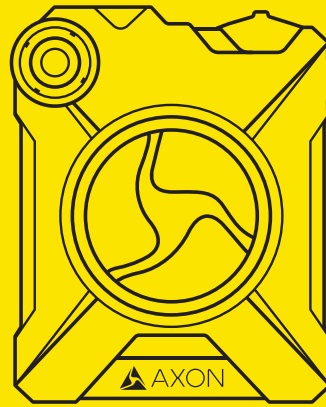
RAPIDLOCK MOUNTS: Versatile mounts keep the camera steady during tough situations.

MOBILE APP: Stream, tag, and replay videos right on your phone with Axon View.

MULTI-CAM COMPATIBILITY: Review up to four videos, including Axon Body 2, Axon Flex 2 and Axon Fleet footage, on one screen through Evidence.com.



APP AVAILABLE FOR
APPLE AND ANDROID



AXON BODY 2 SPECIFICATIONS

VIDEO RESOLUTION: Configurable up to 1080p

WEATHER RESISTANCE: IP67 (IEC 60529)

CORROSION RESISTANCE: MIL-STD-810G
METHOD 509.5 (SALT FOG)

FIELD OF VIEW: 143 degrees

OPERATING TEMPERATURE: -4 °F to 122 °F
-20 °C to 50 °C

DROP TEST: 6 Feet

HUMIDITY: 95% non-condensing

WARRANTY: 1 year from date of receipt with
extended full five-year warranty options

RECORDING CAPACITY: Up to 70 hours
depending on resolution

Android is a trademark of Google, Inc., iOS is a trademark of Cisco Technology, Inc., and Apple, the Apple logo, iPhone, iPad and iPod touch are trademarks of Apple, Inc. The Android robot is reproduced or modified from work created and shared by Google and used according to terms described in the Creative Commons 3.0 Attribution License. Wi-Fi is a trademark of the Wi-Fi Alliance.

▲, ▲ AXON, Axon, Axon View, Axon Body 2, Axon Flex 2, and Evidence.com are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information, visit www.axon.com/legal. All rights reserved. © 2017 Axon Enterprise, Inc.



GAIN A NEW PERSPECTIVE

THE LEADING POINT-OF-VIEW CAMERA, EVOLVED

Unmatched Durability | Best-in-Class Image Quality | Optimum Wearability

Gain a new perspective with the Axon Flex 2 camera. It brings point-of-view video to the next level, boasting a rugged industrial design, new mounts, and advanced capabilities like unlimited HD and a 120-degree field of view. Plus, it belongs to the growing Axon network of devices and apps that work together so you can focus on what matters - your job, not your technology.

AXON FLEX 2 FEATURES AND BENEFITS

BEST-IN-CLASS IMAGE QUALITY: The leading point-of-view camera now records in HD.

DUAL-CHANNEL AUDIO: Reduce ambient noise for improved sound quality.

WIDER FIELD OF VIEW: Capture more at the scene with a 120-degree field of view.

FULL-SHIFT BATTERY: Lasts for 12 hours of battery.

PRE-EVENT BUFFER: Configure your pre-event buffer time to capture up to 2 minutes before an event.

ENHANCED MOUNTS: Designed for versatility and optimum comfort.

UNMATCHED DURABILITY: Built to endure extreme field and weather conditions.

WIRELESS ACTIVATION: Axon Signal reports events, like when you open the car door or activate the light bar, so your camera can detect them and start recording.

MOBILE COMPATIBILITY: Stream, tag, and replay footage right on your phone with the Axon View app.

EVIDENCE.COM INTEGRATION: Easily manage, retrieve, and share videos online.

MULTI-CAM COMPATIBILITY: Review up to four videos, including Axon Flex 2, Axon Body 2 and Axon Fleet footage, on one screen through Evidence.com.



APP AVAILABLE FOR
APPLE AND ANDROID

AXON FLEX 2 SPECIFICATIONS

WEATHER RESISTANCE IEC 60529 IP54 (dust, rain); MIL-STD-810G (Salt fog)

HOUSING High-impact polymer

FIELD OF VIEW 120 degrees

OPERATING TEMPERATURE -4 °F TO 122 °F [-20 °C TO 50 °C]

DROP TEST 6 feet

VIDEO MPEG-4 (MP4); H.264

HUMIDITY 95% non-condensing


WARRANTY 1 year from date of receipt

RECORD TIME Up to 70 hours depending on resolution

ENCRYPTION 256-bit AES

Apple and  are trademarks of Apple Inc. and  and Android are trademarks of Google Inc.

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

 AXON, Axon, Axon View, Axon Body 2, Axon Flex 2, and Evidence.com are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information, visit www.axon.com/legal. All rights reserved. © 2017 Axon Enterprise, Inc.

MPC0250 REV F





CAPTURE AND PROTECT YOUR VIDEO INTERVIEW EVIDENCE

Axon Interview allows agencies to capture video of witness and suspect interviews, tag it with descriptive metadata, and automatically transfer it to Evidence.com. Featuring world-class security and large-agency support, it is a full interview room video solution that provides critical, defensible evidence for the prosecution.

PROTECT THE TRUTH

A full video record of the interrogation process helps protect officers against claims of abuse, coercion, and perjury.

INCREASE CONVICTION RATES

Interview room video provides stronger evidence for the prosecution, leading to fewer pre-trial motions and improved evidentiary record on appeal.

SECURE YOUR INTERVIEWS

Data is encrypted, and the system includes automated audit trail capabilities for tracking chain of custody.

CUSTOMIZE YOUR DEPLOYMENT

Axon Interview works for any-sized agency with support for multiple simultaneous interviews, decentralized monitoring and remote camera sites.

ELIMINATE DATA SILOS

Completed interviews are securely stored and managed alongside all other types of digital evidence at your department. All interview metadata is retained on the Evidence.com platform for efficient search and retrieval.

AXON INTERVIEW FEATURES & BENEFITS

REDUNDANT RECORDING: Ensure the confession is captured every time.

24/7 BUFFERING OPTION: Capture forgotten interviews and let nothing slip through the cracks.

METADATA MANAGEMENT: Flexible customer-defined metadata.

PRE AND POST-EVENT RECORDING: Customize pre and post-event windows of up to 7 minutes.

TOUCH-SCREEN SOFTWARE: Quickly enter metadata with high accuracy.

HIGH-DEFINITION: Produce industry-leading audio and video for the prosecution.

MASKING: Preserve attorney-client privileges without sacrificing video continuity.

MOTION-BASED TRIGGER: Supports DWI/DUI rooms for when officers' hands are full.

AXON INTERVIEW SPECIFICATIONS

TAMPER-PROOF TECHNOLOGY SHA-2 hashing algorithm and chain of custody including standard reports

VIDEO ENCODING H.264 baseline and main profile (MPEG-4 part 10/AVC), streaming compliant

CAMERA SECURITY HTTPS encrypted communication to the camera, IEEE 802.1x network access control

SUPPORTED PROTOCOLS IPv4/v6, FTP, CIFS/SMB, SMTP, Bonjour, UPnP

POE SUPPORT Power over ethernet IEEE 802.3af/802.3at type 1

COVERT OR OVERT CAMERAS Support for either style of camera to best fit your needs



Axon Fleet 2

THE NEXT GENERATION OF IN-CAR HITS THE ROAD



| TAKE YOUR VIDEO TO THE NEXT LEVEL

Offload Anywhere | Plug & Play Functionality | Multi-Cam Playback

In-car systems haven't changed in decades. Until now. Featuring improved front and rear cameras, Axon Fleet 2 is a breakthrough video system that unlocks the power of Axon's network. Offload video anywhere. Watch up to four videos at once on Evidence.com. Axon Fleet 2 is upgraded continuously behind the scenes, so you'll always have the latest, greatest in-car tech connected to the Axon network of people, devices, and apps.

| FLEET 2 FEATURES AND BENEFITS

LICENSE PLATE READABILITY: Up to 4X digital zoom make license plates readable at up to 30 feet (9.1 meters).

WIRELESS MIC: Capture audio up to 1,000 feet (305 meters) away.

NIGHTTIME VISABILITY: Capture what happens inside the car at night with Axon Fleet 2's infrared capability.

WIRELESS ACTIVATION: Compatible with Axon Signal, which reports events like when you open the car door or activate the light bar, so that your nearby cameras can detect them and start recording.

WIRELESS OFFLOAD: Offload video evidence anywhere using LTE or Wi-Fi.

PRE-EVENT BUFFER: Capture up to two minutes before an event.

MDT APP: Stream, tag and replay any camera's videos, plus write notes and upload footage, right from your MDT with Axon View XL.

MULTI-CAM PLAYBACK: Review up to four videos simultaneously before sharing footage on Evidence.com.

UNPRECEDENTED PRICE: Build an upgrade into your Axon Fleet program to ensure you have the latest tech.

CONTINUOUS UPGRADES: Full-featured solution that receives new capabilities via regular software upgrades.

LTE is a trademark of the European Telecommunications Standards Institute, and Wi-Fi is a trademark of the Wi-Fi Alliance.

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

▲ ▲ AXON, Axon, Axon Fleet 2, Axon Signal, Axon View XL, and Evidence.com are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information, visit www.axon.com/legal. All rights reserved. © 2018 Axon Enterprise, Inc.

REV B





YOUR CAMERA'S FOCUSED RIGHT WHEN YOU ARE

Axon Signal is a technology that enables certain Axon cameras to sense events up to 30 feet away and start recording. Whether you're driving your vehicle, using your TASER CEW, or drawing your sidearm, Signal operates effortlessly, allowing you to focus on what matters most.

AXON SIGNAL PRODUCTS



AXON SIGNAL VEHICLE: Enables events like opening the car door or activating the light bar to alert your cameras to start recording. Ideal for cars, SUVs, and motorcycles.



AXON SIGNAL PERFORMANCE POWER MAGAZINE (SPPM): Capture critical footage when using your TASER X2 or X26P Smart Weapon. The SPPM reports to your camera when your weapon is armed and logs the moment that the trigger is pulled and arc is engaged.

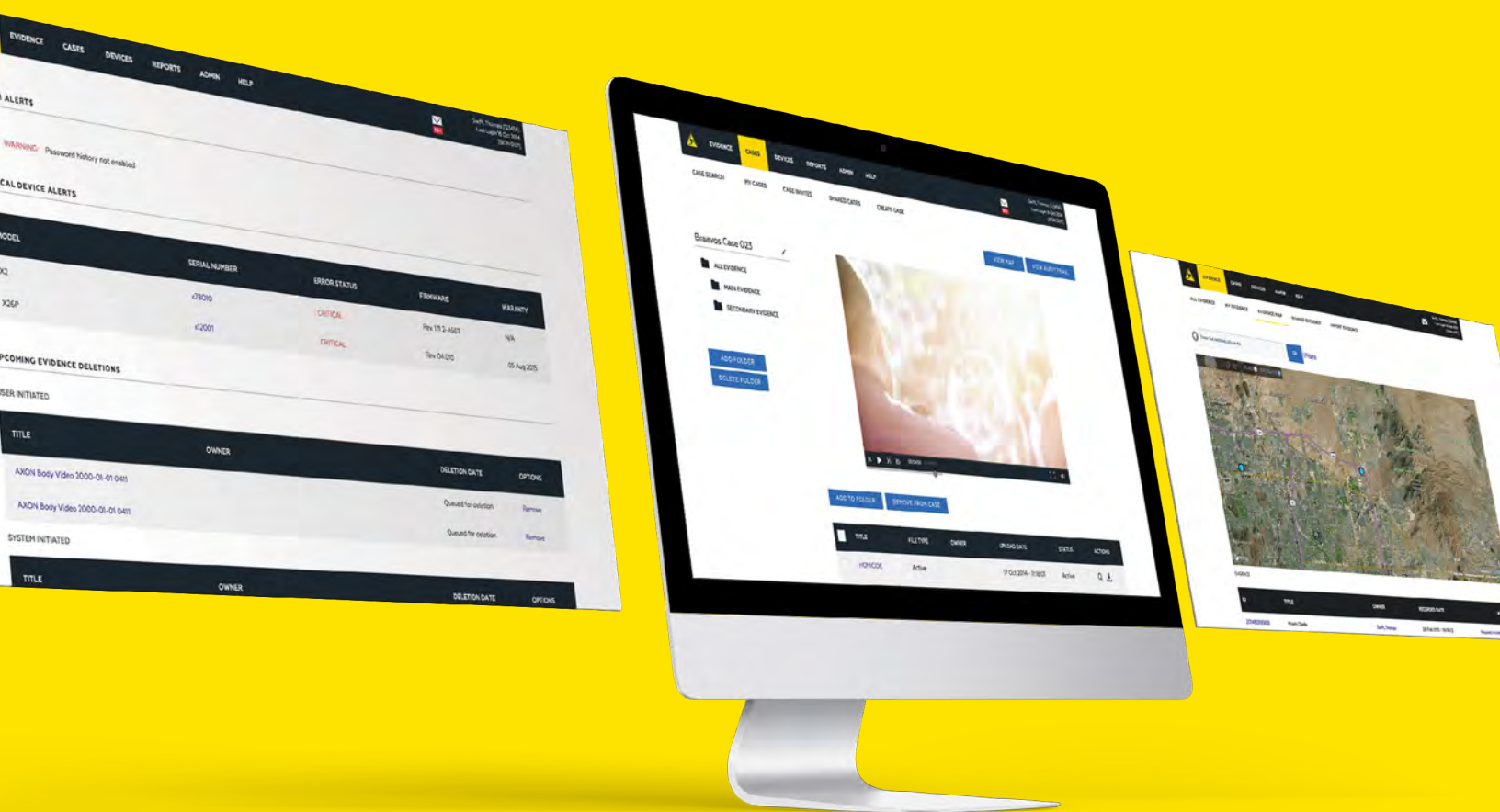


AXON SIGNAL SIDEARM: This easy-to-install smart sensor attaches to the large majority of sidearm holsters. Axon cameras within 30 feet can detect the removal of your sidearm from its holster and start recording via a wireless signal, so you can act with confidence in the field.

Axon Signal Vehicle Unit SKU: 70112

800-978-2737
Get early access at axon.com/signal

AXON, Axon, Axon Signal, X2, X26P, TASER, and  are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information, visit www.axon.com/legal. All rights reserved. © 2017 Axon Enterprise, Inc.



MANAGE ALL OF YOUR DIGITAL EVIDENCE FROM CAPTURE TO COURTROOM

Evidence.com is a scalable, cloud-based system that consolidates all of your digital files, making them easy to manage, access and share while maintaining security and chain of custody.

UNIFY YOUR DIGITAL ASSETS

Eliminate data silos and manage all types of digital media from capture to courtroom, all with one secure system.

FASTER WORKFLOWS

Achieve the fastest speed of evidence processing through automation. Save time and money with industry-leading redaction technologies and secure digital sharing tools.

SCALABLE TECHNOLOGY

Enable deployments of any size with active directory integration, groups, reports, CAD/RMS Integration, automatic retention schedules and more.

THE AXON ADVANTAGE

Start immediately with no hardware to set up. Choose between plans with fixed or unlimited storage, and adjust instantly if needed. Stay up to date with free, automatic updates every month.

800-978-2737 axon.com/evidence

EVIDENCE.COM FEATURES AND BENEFITS

LOWEST TOTAL COST OF OWNERSHIP:

Evidence.com eliminates the cost of an in-house data center and the time associated with manual processes.

AVAILABILITY: Hosted securely in the cloud, Evidence.com can be accessed anytime, anywhere.

ONE-CLICK SEARCH: Search by officer name, incident ID, location and other tags to find files quickly.

CONFIGURABLE RETENTION: Schedule automatic retention periods based on incident type or crime severity.

CASE MANAGEMENT: Quickly view and share all digital files related by case number.

REDACTION SUITE: Save time with automated redaction, bulk redaction, clips, markers, thumbnails and more.

CAD/RMS INTEGRATION: Automate Axon video tagging by pulling in the correct metadata from existing systems.

PROSECUTOR WORKFLOW: Connect digitally with the prosecutor using the most scalable sharing solution available.

MOBILE INTEGRATION: Store and manage files captured with mobile devices in the field.

ANALYTICS AND AUDIT TOOLS: Monitor system usage, from total videos uploaded to who has reviewed, shared and deleted files.

EVIDENCE.COM SECURITY FEATURES

CJIS-COMPLIANCE

Evidence.com is fully CJIS compliant.

AUDIT TRAIL AND CHAIN OF CUSTODY

Data is tamper-proof and all access events are reported in a secure audit trail.

CUSTOMIZABLE USER PERMISSIONS

Administrators can determine what files can be viewed by users and groups of users.

DATA ENCRYPTION

All information is fully encrypted in transit and at rest.

For more information, visit axon.com/security.



A background image showing the back of a person with long, wavy brown hair, wearing a dark pinstriped suit jacket, sitting in a courtroom. Other people are blurred in the background.

EVIDENCE.COM FOR PROSECUTORS

MANAGING EVIDENCE FROM CAPTURE TO COURT

As body camera footage and other forms of digital evidence become more prevalent, law enforcement agencies are faced with an unprecedented amount of data. That's why we offer Evidence.com for Prosecutors, a free evidence management solution that streamlines your workflow, making it manageable to handle agencies' growing amounts of evidence without having to grow your staff.

SHARE EVIDENCE WITH EASE

Evidence.com is easy to use. With a few clicks, you can add evidence to cases and share them with relevant parties, cutting a weeklong sharing process down to just minutes. Evidence.com also requires no ramp-up time to implement, and because of its instantly scalable, cloud-based system, increasing storage capacity is seamless.

KNOW YOUR DATA IS SECURE

We employ industry-leading security practices that have earned us the trust of thousands of agencies on our platform. Data is encrypted, and all actions are recorded in an audit log to ensure chain of custody and authenticity. That way, evidence managed through Evidence.com is still admissible in court.

DON'T BREAK YOUR BUDGET

We understand that attorneys don't always have the budgets that law enforcement agencies may have for new technology. Our standard plan lets you share cases, receive files from multiple agencies, upload digital data, instantly provide e-discovery, and more—for free. Plus, you won't have to hire additional staff to accommodate the influx of evidence. You can also redact footage, eliminating costs for external consultants.

STANDARD FEATURES

- Receive shared cases and share evidence externally for discovery
- Upload any type of digital data
- Add evidence to cases
- Create video clips and markers
- Customize user roles and permissions
- Set automated deletion schedules
- Bulk reassign, edit, and share

WANT TO LEARN MORE?

Contact us to hear about your options and to start your trial.

EVIDENCE.COM PROSECUTOR LICENSES

PLAN	STANDARD	PRO
PRICE PER USER	FREE	\$39/Month
STORAGE OF SHARED EVIDENCE	Unlimited	Unlimited
ADDITIONAL STORAGE PER MONTH	6.25¢/GB/Month	6.25¢/GB/Month
Receive Shared Cases	✓	✓
Share Evidence Externally for Discovery	✓	✓
Upload Any Type of Digital Data	✓	✓
Add Evidence to Cases	✓	✓
Create Video Clips and Markers	✓	✓
Customize User Roles and Permissions	✓	✓
Automated Deletion Schedules	✓	✓
Bulk Reassign, Share, Edit	✓	✓
Redact Videos		✓
Generate Agency Usage Reports		✓
Export Search Results to CSV		✓
Create Organizational Groups		✓
Single Sign-On		✓





EVIDENCE Sync

- ▶ **Desktop Evidence Control** - Allows management of digital evidence and TASER® products from any computer with an internet connection, including an MDT.
- ▶ **Any File, Any Source** - Upload any audio, video, photo or other files currently on CDs, memory cards, servers or a hard drive to EVIDENCE.com.
- ▶ **Handsfree Transfer** - Select the data to upload to EVIDENCE.com, then log out and walk away while the app keeps working.

The newest version of EVIDENCE Sync makes your workflows easier and saves you time. Use Sync to preview, annotate and upload digital evidence from any source to EVIDENCE.com, plus manage your agency's TASER products and update firmware. And as always, your data is secure and easy to access at any point.

EVIDENCE.COM

▶ scan this QR code to learn more





FEATURES & BENEFITS



Upload Any Digital Evidence

Upload any format and size of photo, video or audio recording.



Manage TASER Products

Collect evidence, change settings, assign, and update firmware for your CEWs or AXON® cameras.



Add Metadata

Tag evidence with Title, Event ID, and Category, and assign evidence at upload.



Schedule Uploads

Select a folder or file on your hard drive or network to upload at set times.



Upload from Servers

Upload interview room or dash-cam videos from shared drives.



Upload from Camera, CD, or SD Card

Upload crime scene photos from any source.



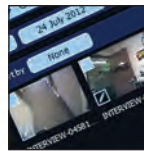
Upload from the Field

Run the app from your MDT and access from the field.



Walk Away During Uploads

Log out while uploads keep going in the background.



View Files in a Gallery

Quickly manage photos and videos using thumbnails.



Search Easily

Find any file and search by title, date, keyword or other fields.

EVIDENCE.COM

► scan this QR code to learn more



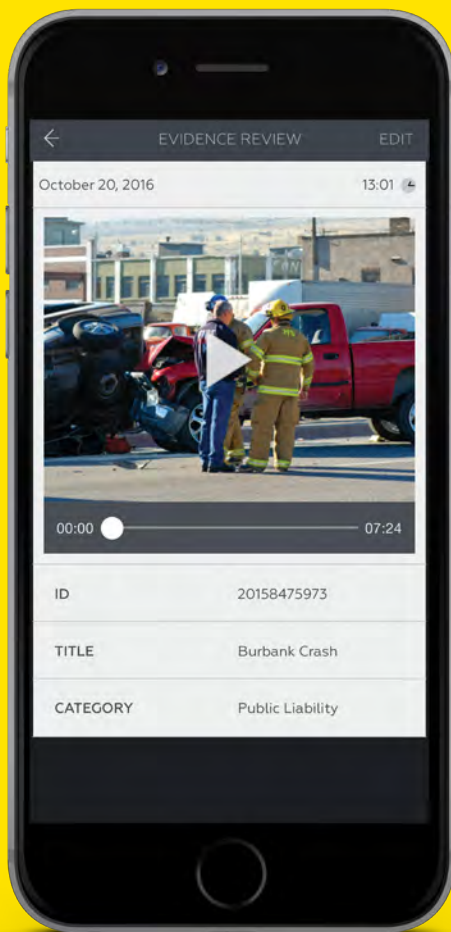
✉ Help@EVIDENCE.com

☎ 1.877.270.0553

📍 Scottsdale, Arizona, U.S.A.



INSTANT VIDEO PLAYBACK IN THE FIELD



AXON VIEW

See what your camera sees

TURN ROUTINE VIDEO INTO VALUABLE EVIDENCE

Live Feed | GPS Tagging | Metadata Input

Axon View is a mobile application that wirelessly connects with your Axon camera to provide instant playback of unfolding events in the field. Axon View automatically maps video with GPS data and allows real-time tagging of metadata, such as Case ID and Category, from your phone. Before you set foot in the station, your video is automatically filed into the correct case report and retention schedule.

800-978-2737 axon.com/view

AXON VIEW FEATURES & BENEFITS

INSTANT REPLAY: Prevent frivolous disputes over recorded events

MOBILE TAGGING: Input data on the scene for easy searching and accurate retention

GPS: Map video evidence automatically

LIVE STREAMING: Achieve optimal camera placement

SECURE STORAGE: Information is viewed but not stored on the mobile device



APP AVAILABLE FOR
APPLE AND ANDROID

AXON VIEW SPECIFICATIONS

IOS:

Compatible with Apple iOS 8.0 and above on iPhone, iPad, and iPod touch

Size: 29.5 MB

Language: English, Spanish, and French

ANDROID:

Compatible with Android Devices Version 4.1 and above

Size: Varies by device

Language: English, Spanish, and French

Android is a trademark of Google, Inc., IOS is a trademark of Cisco Technology, Inc., and Apple, the Apple logo, iPhone, iPad and iPod touch are trademarks of Apple, Inc. The Android robot is reproduced or modified from work created and shared by Google and used according to terms described in the Creative Commons 3.0 Attribution License.

AXON, Axon, and Axon View are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information, visit www.axon.com/legal. All rights reserved. © 2017 Axon Enterprise, Inc.



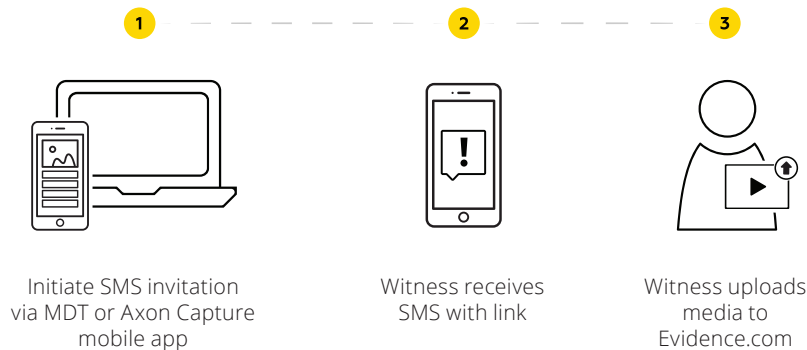
COMMUNITY EVIDENCE, NOW PART OF THE AXON NETWORK

For too long, agencies have struggled to securely receive evidence from the community and determine what content is useful for an investigation. Axon Citizen, makes it easier for community members to submit photos and videos of an incident and for your agency to manage that media in Evidence.com, helping lead to more prosecutions.

HOW IT WORKS

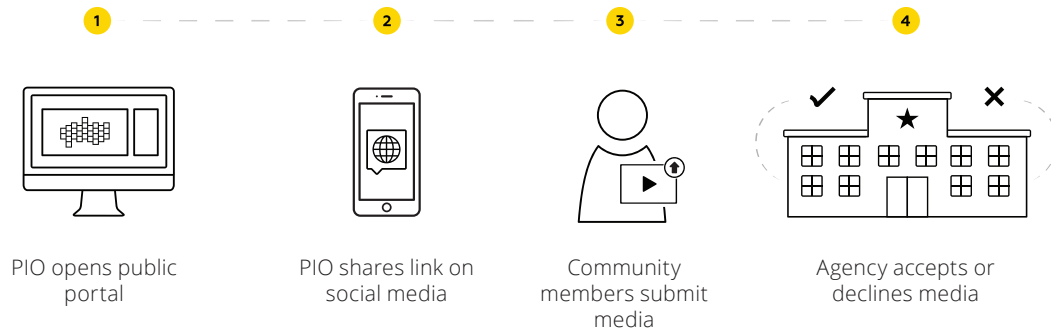
CITIZEN FOR OFFICERS: ONE-ON-ONE EVIDENCE COLLECTION

When you respond to a scene, you should be able to collect photos and videos from witnesses without worrying about the chain of evidence. With Axon Citizen, you can invite witnesses to securely send their media through the Axon Capture mobile application or Evidence.com on your MDT. Once collected, their submissions go straight into Evidence.com and are immediately logged in the audit trail instead of sitting on your camera roll or in your email.



CITIZEN FOR COMMUNITIES: PUBLIC EVIDENCE COLLECTION

You always want help from the community — but you don't want to be overwhelmed. Axon Citizen simplifies the collection process, letting you create public portals where community members can upload photos and videos, which are immediately screened for viruses. Then, your agency can review the media as fast as possible to accept or reject submissions. All submissions are instantly categorized and searchable.



AXON CITIZEN FEATURES & BENEFITS

CENTRALIZES YOUR EVIDENCE: Submissions go straight into Evidence.com with your agency's other files, eliminating any need to download media, print it or transfer it to a USB drive, and submit it to the evidence locker.

PROTECTS THE CHAIN OF CUSTODY: Axon Citizen utilizes Evidence.com's secure audit trail to show which officer initiated the collection, for which incident, at what time and place, and from which community member.

ACCELERATES THE REVIEW PROCESS: Axon Citizen's triage tool allows the officer reviewing submissions to quickly decide which submissions to accept or decline.

STREAMLINES SEARCHING: All submissions will be automatically categorized and searchable within Evidence.com to simplify case building.

OFFERS NETWORK RELIABILITY: Axon Citizen manages all the infrastructure and tools needed to support large volumes of submissions, so your agency can remain confident that the service will work during large-scale events.

AXON CITIZEN SPECIFICATIONS

COMPATIBILITY:

Citizen for Officers: Axon Capture (Android and iOS) or Evidence.com

Citizen for Communities: Evidence.com

Citizen Submission: Any web-enabled smartphone

UPLOAD METHOD

Upload data via any 3G or 4G data connection, or via a Wi-Fi connection

ACCESS

Officers must log in to their active Evidence.com account to use the application

STORAGE

The application will only upload data to Evidence.com secured storage

LANGUAGE

Available in English

Android is a trademark of Google Inc.; Apple, iPhone, and iPod touch are trademarks of Apple Inc.; iOS is a trademark of Cisco, and Wi-Fi is a trademark of the Wi-Fi alliance.

▲, ▲ AXON, Axon and Evidence.com are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information, visit www.axon.com/legal. All rights reserved. © 2017 Axon Enterprise, Inc.



Pennsylvania Chiefs of Police Association



Request For Information Police Body Worn Cameras

(A.K.A. non-vehicle-mounted mobile video recording systems)

January 8, 2019

The Pennsylvania Chiefs of Police Association (PCPA) in cooperation with the Local Technology Workgroup (LTW) of the Pennsylvania Commission on Crime and Delinquency (PCCD) is requesting any information from manufacturers, vendors or resellers that would assist Pennsylvania's police departments in purchasing police officer worn body camera.

BACKGROUND

The Pennsylvania Chiefs of Police Association (PCPA) with the Local Technology Workgroup (LTW) of the Pennsylvania Commission on Crime and Delinquency (PCCD) has been working with several hundred police departments on purchasing and deploying body worn cameras. PCCD has been awarded over a million dollars in federal grant funds to assist the procurement of police worn body cameras. However, Pennsylvania has specific laws and regulations on the use of non-vehicle-mounted mobile video recording systems and the federal grant has more requirements. Therefore, PCPA on behalf of Pennsylvania's police departments is requesting information from anyone in the business of providing equipment and services as defined by Pennsylvania Law and regulations of non-vehicle-mounted mobile video recording systems.

Pennsylvania has over 30,000 sworn officers working in over 1200 police departments. PCPA believes providing this information to us benefits both the police departments and the providers of these body worn cameras and their accompanying services. While some departments will only require a few body worn cameras and simple storage solutions, others will need hundreds and complex storage. Providing this information to PCPA, LTW, PCCD and Pennsylvania's police departments will allow a more complete understanding of the technology, products and the service they can acquire.

The benefit to manufacturers, vendors or resellers is that you get the opportunity to present your technology products and services in a fashion that meets the specific needs of Pennsylvania's police and presents that to a large group leading the state effort.

INFORMATION REQUESTED

The information requested includes the manufacturers, vendors or resellers of specific products and services that meet Pennsylvania Laws, standards and regulations that allow them to develop the necessary policies required. In addition, cost and discounted price are requested. Please provide at least the following information:

- How does your non-vehicle-mounted mobile video recording systems and technology meet Pennsylvania's published requirements?
- Have you submitted your non-vehicle-mounted mobile video recording systems to the Pennsylvania State Police for certification?
- Is your non-vehicle-mounted mobile video recording systems already certified by the Pennsylvania State Police?
- Are you offering a storage solution?
- Will you offer storage solutions bundled (no line item distinction) with the cost of each camera purchased?

- How does your storage solution meet Pennsylvania's published requirements?
- List the products and services that are already available on State Contract or PA CoStars.
- List your costs for products and services you offer.
- Will you offer a discount of those prices if multiple police departments group together to buy your products and services?

PENNSYLVANIA LAWS AND PUBLISHED REQUIREMENTS

To help you provide your information the following laws and published standards and regulations are in the APPENDIX attached to this RFI:

- PA Title 18 CHAPTER 57 WIRETAPPING AND ELECTRONIC SURVEILLANCE
- PA ACT 22, 2017
- PA Bulletin Doc 45 5482, 8/29/15
- PA Bulletin Doc 45 5712, 9/19/15
- PA Bulletin Doc 46 116, 1/2/16
- PA Bulletin Doc 47 7815, 12/31/17
- PCCD Body-Worn Camera (BWC) Policy Recommendations

PROVIDING YOUR INFORMATION

Please send your information to:

Christopher J. Braun M.S. IT
 Technology Coordinator Pennsylvania Chiefs of Police Association
 3905 N. Front Street, Harrisburg, PA 17110
 Email: cjbraun@pachiefs.org

The preferred method is email or in a digital format. However, all information provided will be used. Please include the name of a contact, phone number, email address and website.
 Deadline: Please send your information by 4 PM January 25, 2019.

Request For Information

Police Body Worn Cameras

APPENDIX

PA Title 18 CHAPTER 57 WIRETAPPING AND ELECTRONIC SURVEILLANCE

CHAPTER 57

WIRETAPPING AND ELECTRONIC SURVEILLANCE

Subchapter

- A. General Provisions
- B. Wire, Electronic or Oral Communication
- C. Stored Wire and Electronic Communications and Transactional Records Access
- D. Mobile Tracking Devices
- E. Pen Registers, Trap and Trace Devices and Telecommunication Identification Interception Devices
- F. Miscellaneous

Enactment. Present Chapter 57 was added October 4, 1978, P.L.831, No.164, effective in 60 days.

Prior Provisions. Former Chapter 57, which related to invasion of privacy, was added December 6, 1972, P.L.1482, No.334, and repealed October 4, 1978, P.L.831, No.164, effective in 60 days.

Cross References. Chapter 57 is referred to in section 1522 of Title 4 (Amusements); section 3575 of Title 42 (Judiciary and Judicial Procedure).

SUBCHAPTER A

GENERAL PROVISIONS

Sec.

5701. Short title of chapter.

5702. Definitions.

Subchapter Heading. The heading of Subchapter A was added October 21, 1988, P.L.1000, No.115, effective immediately.

§ 5701. Short title of chapter.

This chapter shall be known and may be cited as the "Wiretapping and Electronic Surveillance Control Act."

§ 5702. Definitions.

As used in this chapter, the following words and phrases shall have the meanings given to them in this section unless the context clearly indicates otherwise:

"Aggrieved person." A person who was a party to any intercepted wire, electronic or oral communication or a person against whom the interception was directed.

"Aural transfer." A transfer containing the human voice at any point between and including the point of origin and the point of reception.

"Communication common carrier." Any person engaged as a common carrier for hire, in intrastate, interstate or foreign communication by wire or radio or in intrastate, interstate or foreign radio transmission of energy; however, a person engaged in radio broadcasting shall not, while so engaged, be deemed a common carrier.

"Communication service." Any service which provides to users the ability to send or receive wire or electronic communications.

"Communication system." Any wire, radio, electromagnetic, photo-optical or photoelectronic facilities for the transmission of communications and any computer facilities or related electronic equipment for the electronic storage of such communications.

"Contents." As used with respect to any wire, electronic or oral communication, is any information concerning the substance, purport, or meaning of that communication.

"Court." The Superior Court. For the purposes of Subchapter C only, the term shall mean the court of common pleas.

"Crime of violence." Any of the following:

(1) Any of the following crimes:

(i) Murder in any degree as defined in section 2502(a), (b) or (c) (relating to murder).

(ii) Voluntary manslaughter as defined in section 2503 (relating to voluntary manslaughter), drug delivery resulting in death as defined in section 2506(a) (relating to drug delivery resulting in death), aggravated assault as defined in section 2702(a)(1) or (2) (relating to aggravated assault), kidnapping as defined in section 2901(a) or (a.1) (relating to kidnapping), rape as defined in section 3121(a), (c) or (d) (relating to rape), involuntary deviate sexual intercourse as defined in section 3123(a), (b) or (c) (relating to involuntary deviate sexual intercourse), sexual assault as defined in section 3124.1 (relating to sexual assault), aggravated indecent assault as defined in section 3125(a) or (b) (relating to aggravated indecent assault), incest as defined in section 4302(a) or (b) (relating to incest), arson as defined in section 3301(a) (relating to arson and related offenses), burglary as defined in section 3502(a)(1) (relating to burglary), robbery as defined in section 3701(a)(1)(i), (ii) or (iii) (relating to robbery) or robbery of a motor vehicle as defined in section 3702(a) (relating to robbery of a motor vehicle).

(iii) Intimidation of witness or victim as defined in section 4952(a) and (b) (relating to intimidation of witnesses or victims).

(iv) Retaliation against witness, victim or party as defined in section 4953(a) and (b) (relating to retaliation against witness, victim or party).

(v) Criminal attempt as defined in section 901(a) (relating to criminal attempt), criminal solicitation as defined in section 902(a) (relating to criminal solicitation) or criminal conspiracy as defined in section 903(a) (relating to criminal conspiracy) to commit any of the offenses specified in this definition.

(2) Any offense equivalent to an offense under paragraph (1) under the laws of this Commonwealth in effect at the time of the commission of that offense or under the laws of another jurisdiction.

"Electronic communication." Any transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo-optical system, except:

(1) (Deleted by amendment).

(2) Any wire or oral communication.

(3) Any communication made through a tone-only paging device.

(4) Any communication from a tracking device (as defined in this section).

"Electronic communication service." (Deleted by amendment).

"Electronic communication system." (Deleted by amendment).

"Electronic, mechanical or other device." Any device or apparatus, including, but not limited to, an induction coil or a telecommunication identification interception device, that can be used to intercept a wire, electronic or oral communication other than:

(1) Any telephone or telegraph instrument, equipment or facility, or any component thereof, furnished to the subscriber or user by a provider of wire or electronic communication service in the ordinary course of its business, or furnished by such subscriber or user for connection to the facilities of such service and used in the ordinary course of its business, or being used by a communication common carrier in the ordinary course of its business, or by an investigative or law enforcement officer in the ordinary course of his duties.

(2) A hearing aid or similar device being used to correct subnormal hearing to not better than normal.

(3) Equipment or devices used to conduct interceptions under section 5704(15) (relating to exceptions to prohibition of interception and disclosure of communications).

"Electronic storage."

(1) Any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof.

(2) Any storage of such a communication by an electronic communication service for purpose of backup protection of the communication.

"Home." The residence of a nonconsenting party to an interception, provided that access to the residence is not generally permitted to members of the public and the party has a reasonable expectation of privacy in the residence under the circumstances.

"In-progress trace." The determination of the origin of a telephonic communication to a known telephone during an interception.

"Intercept." Aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device. The term shall include the point at which the contents of the communication are monitored by investigative or law enforcement officers. The term shall not include the acquisition of the contents of a communication made through any electronic, mechanical or other device or telephone instrument to an investigative or law enforcement officer, or between a person and an investigative or law enforcement officer, where the investigative or law enforcement officer poses as an actual person who is the intended recipient of the communication, provided that the Attorney General, a deputy attorney general designated in writing by the Attorney General, a district attorney or an assistant district attorney designated in writing by a district attorney of the county wherein the investigative or law enforcement officer is to receive or make the communication has reviewed the facts and is satisfied that the communication involves suspected criminal activities and has given prior approval for the communication.

"Investigative or law enforcement officer." Any officer of the United States, of another state or political subdivision thereof or of the Commonwealth or political subdivision thereof, who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter or an equivalent crime in another jurisdiction, and any attorney authorized by law to prosecute or participate in the prosecution of such offense.

"Judge." When referring to a judge authorized to receive applications for, and to enter, orders authorizing interceptions of wire, electronic or oral communications pursuant to Subchapter B (relating to wire, electronic or oral communication), any judge of the Superior Court.

"Mobile communications tracking information." Information generated by a communication common carrier or a communication service which indicates the location of an electronic device supported by the communication common carrier or communication service.

"One call system." A communication system established by users to provide a single telephone number for contractors or designers or any other person to call notifying users of the caller's intent to engage in demolition or excavation work.

"Oral communication." Any oral communication uttered by a person possessing an expectation that such communication is not subject to interception under circumstances justifying such expectation. The term does not include the following:

(1) An electronic communication.

(2) A communication made in the presence of a law enforcement officer on official duty who is in uniform or otherwise clearly identifiable as a law enforcement officer and who is using an electronic, mechanical or other device which has been approved under section 5706(b)(4) (relating to exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices) to intercept the communication in the course of law enforcement duties. As used in this paragraph only, "law enforcement officer" means a member of the Pennsylvania State Police, an individual employed as a police officer who holds a current certificate under 53 Pa.C.S. Ch. 21 Subch. D (relating to municipal police education and training), a sheriff or a deputy sheriff.

"Organized crime."

(1) The unlawful activity of an association trafficking in illegal goods or services, including but not limited to, gambling, prostitution, loan sharking, controlled substances, labor racketeering, or other unlawful activities; or

(2) any continuing criminal conspiracy or other unlawful practice which has as its objective:

- (i) large economic gain through fraudulent or coercive practices; or
- (ii) improper governmental influence.

"Pen register." A device which is used to capture, record or decode electronic or other impulses which identify the numbers dialed or otherwise transmitted, with respect to wire or electronic communications, on the targeted telephone. The term includes a device which is used to record or decode electronic or other impulses which identify the existence of incoming and outgoing wire or electronic communications on the targeted telephone. The term does not include a device used by a provider or customer of a wire or electronic communication service for billing, or recording as an incident to billing, for communication service provided by the provider, or any device used by a provider, or customer of a wire communication service for cost accounting or other like purposes in the ordinary course of business.

"Person." Any employee, or agent of the United States or any state or political subdivision thereof, and any individual, partnership, association, joint stock company, trust or corporation.

"Readily accessible to the general public." As used with respect to a radio communication, that such communication is not:

- (1) scrambled or encrypted;
- (2) transmitted using modulation techniques of which the essential parameters have been withheld from the public with the intention of preserving the privacy of the communication;
- (3) carried on a subscriber or other signal subsidiary to a radio transmission;
- (4) transmitted over a communication system provided by a common carrier, unless the communication is a tone-only paging system communication; or
- (5) transmitted on frequencies allocated under 47 CFR Parts 25, 74D, E, F or 94, unless, in the case of a communication transmitted on a frequency allocated under Part 74 which is not exclusively allocated to broadcast auxiliary services, the communication is a two-way voice communication by radio.

"Remote computing service." The provision to the public of computer storage or processing services by means of an electronic communications system.

"Signed, written record." A memorialization of the contents of any wire, electronic or oral communication intercepted in accordance with this subchapter, including the name of the investigative or law enforcement officer who transcribed the record, kept in electronic, paper or any form. The signature of the transcribing officer shall not be required to be written, but may be electronic.

"State." Any state of the United States, the District of Columbia, the Commonwealth of Puerto Rico and any territory or possession of the United States.

"Suspected criminal activity." A particular offense that has been, is or is about to occur as set forth under section 5709(3)(ii) (relating to application for order), any communications to be intercepted as set forth under section 5709(3)(iii) or any of the criminal activity set forth under section 5709(3)(iv) establishing probable cause for the issuance of an order.

"Telecommunication identification interception device." Any equipment or device capable of intercepting any electronic communication which contains any electronic serial number, mobile

identification number, personal identification number or other identification number assigned by a telecommunication service provider for activation or operation of a telecommunication device.

"Tracking device." An electronic or mechanical device which permits only the tracking of the movement of a person or object.

"Trap and trace device." A device which captures the incoming electronic or other impulses which identify the originating number of an instrument or device from which a wire or communication was transmitted. The term includes caller ID, deluxe caller ID or any other features available to ascertain the telephone number, location or subscriber information of a facility contacting the facility whose communications are to be intercepted.

"User." Any person or entity who:

(1) uses an electronic communication service; and

(2) is duly authorized by the provider of the service to engage in the use.

"Wire communication." Any aural transfer made in whole or in part through the use of facilities for the transmission of communication by wire, cable or other like connection between the point of origin and the point of reception, including the use of such a connection in a switching station, furnished or operated by a telephone, telegraph or radio company for hire as a communication common carrier.

(Dec. 23, 1981, P.L.593, No.175, eff. 60 days; Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.; Dec. 9, 2002, P.L.1350, No.162, eff. 60 days; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days; July 7, 2017, P.L.304, No.22, eff. 60 days)

2017 Amendment. Act 22 amended the def. of "oral communication."

2012 Amendment. Act 202 amended the defs. of "intercept," "trap and trace device" and "wire communication," added the defs. of "communication service," "communication system," "crime of violence," "mobile communications tracking information" and "signed, written record" and deleted the defs. of "electronic communication service" and "electronic communication system."

2002 Amendment. Act 162 added the def. of "suspected criminal activity."

1998 Amendment. Act 19 amended the defs. of "electronic communication," "electronic, mechanical or other device," "intercept," "investigative or law enforcement officer," "judge," "pen register" and "wire communication" and added the defs. of "home," "state" and "telecommunication identification interception device."

Cross References. Section 5702 is referred to in sections 911, 5706, 5903, 6321 of this title; section 901 of Title 34 (Game); section 67A07 of Title 42 (Judiciary and Judicial Procedure); sections 57A12, 57B02 of Title 53 (Municipalities Generally); section 2604.1 of Title 66 (Public Utilities).

SUBCHAPTER B

WIRE, ELECTRONIC OR ORAL COMMUNICATION

Sec.

5703. Interception, disclosure or use of wire, electronic or oral communications.

5704. Exceptions to prohibition of interception and disclosure of communications.

5705. Possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices and telecommunication identification interception devices.

5706. Exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices.

5707. Seizure and forfeiture of electronic, mechanical or other devices.

5708. Order authorizing interception of wire, electronic or oral communications.

5709. Application for order.

5710. Grounds for entry of order.

5711. Privileged communications.

5712. Issuance of order and effect.

5712.1. Target-specific orders.

5713. Emergency situations.

5713.1. Emergency hostage and barricade situations.

5714. Recording of intercepted communications.

5715. Sealing of applications, orders and supporting papers.

5716. Service of inventory and inspection of intercepted communications.

5717. Investigative disclosure or use of contents of wire, electronic or oral communications or derivative evidence.

5718. Interception of communications relating to other offenses.

5719. Unlawful use or disclosure of existence of order concerning intercepted communication.

5720. Service of copy of order and application before disclosure of intercepted communication in trial, hearing or proceeding.

5721. Suppression of contents of intercepted communication or derivative evidence (Repealed).

5721.1. Evidentiary disclosure of contents of intercepted communication or derivative evidence.

5722. Report by issuing or denying judge.

5723. Annual reports and records of Attorney General and district attorneys.

5724. Training.

5725. Civil action for unlawful interception, disclosure or use of wire, electronic or oral communication.

5726. Action for removal from office or employment.

5727. Expiration (Repealed).

5728. Injunction against illegal interception.

Subchapter Heading. The heading of Subchapter B was added October 21, 1988, P.L.1000, No.115, effective immediately.

Cross References. Subchapter B is referred to in section 5702 of this title.

§ 5703. Interception, disclosure or use of wire, electronic or oral communications.

Except as otherwise provided in this chapter, a person is guilty of a felony of the third degree if he:

- (1) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, electronic or oral communication;
- (2) intentionally discloses or endeavors to disclose to any other person the contents of any wire, electronic or oral communication, or evidence derived therefrom, knowing or having reason to know that the information was obtained through the interception of a wire, electronic or oral communication; or
- (3) intentionally uses or endeavors to use the contents of any wire, electronic or oral communication, or evidence derived therefrom, knowing or having reason to know, that the information was obtained through the interception of a wire, electronic or oral communication.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.)

§ 5704. Exceptions to prohibition of interception and disclosure of communications.

It shall not be unlawful and no prior court approval shall be required under this chapter for:

- (1) An operator of a switchboard, or an officer, agent or employee of a provider of wire or electronic communication service, whose facilities are used in the transmission of a wire communication, to intercept, disclose or use that communication in the normal course of his employment while engaged in any activity which is a necessary incident to the rendition of his service or to the protection of the rights or property of the provider of wire or electronic communication service. However, no provider of wire or electronic communication service shall utilize service observing or random monitoring except for mechanical or service quality control checks.
- (2) Any investigative or law enforcement officer or any person acting at the direction or request of an investigative or law enforcement officer to intercept a wire, electronic or oral communication involving suspected criminal activities, including, but not limited to, the crimes enumerated in section 5708 (relating to order authorizing interception of wire, electronic or oral communications), where:
 - (i) (Deleted by amendment).
 - (ii) one of the parties to the communication has given prior consent to such interception. However, no interception under this paragraph shall be made unless the Attorney General or a deputy attorney general designated in writing by the Attorney General, or the district attorney, or an assistant district attorney designated in writing by the district attorney, of the county wherein the interception is to be initiated, has reviewed the facts and is satisfied that the consent is voluntary and has given prior approval for the interception; however, such interception shall be subject to the recording and record keeping requirements of section 5714(a) (relating to recording of intercepted communications) and that the Attorney General, deputy attorney general, district attorney or assistant district attorney authorizing the interception shall be the custodian of recorded evidence obtained therefrom;

(iii) the investigative or law enforcement officer meets in person with a suspected felon and wears a concealed electronic or mechanical device capable of intercepting or recording oral communications. However, no interception under this subparagraph may be used in any criminal prosecution except for a prosecution involving harm done to the investigative or law enforcement officer. This subparagraph shall not be construed to limit the interception and disclosure authority provided for in this subchapter; or

(iv) the requirements of this subparagraph are met. If an oral interception otherwise authorized under this paragraph will take place in the home of a nonconsenting party, then, in addition to the requirements of subparagraph (ii), the interception shall not be conducted until an order is first obtained from the president judge, or his designee who shall also be a judge, of a court of common pleas, authorizing such in-home interception, based upon an affidavit by an investigative or law enforcement officer that establishes probable cause for the issuance of such an order. No such order or affidavit shall be required where probable cause and exigent circumstances exist. For the purposes of this paragraph, an oral interception shall be deemed to take place in the home of a nonconsenting party only if both the consenting and nonconsenting parties are physically present in the home at the time of the interception.

(3) Police and emergency communications systems to record telephone communications coming into and going out of the communications system of the Pennsylvania Emergency Management Agency or a police department, fire department or county emergency center, if:

(i) the telephones thereof are limited to the exclusive use of the communication system for administrative purposes and provided the communication system employs a periodic warning which indicates to the parties to the conversation that the call is being recorded;

(ii) all recordings made pursuant to this clause, all notes made therefrom, and all transcriptions thereof may be destroyed at any time, unless required with regard to a pending matter; and

(iii) at least one nonrecorded telephone line is made available for public use at the Pennsylvania Emergency Management Agency and at each police department, fire department or county emergency center.

(4) A person, to intercept a wire, electronic or oral communication, where all parties to the communication have given prior consent to such interception.

(5) Any investigative or law enforcement officer, or communication common carrier acting at the direction of an investigative or law enforcement officer or in the normal course of its business, to use a pen register, trap and trace device or telecommunication identification interception device as provided in Subchapter E (relating to pen registers, trap and trace devices and telecommunication identification interception devices).

(6) Personnel of any public utility to record telephone conversations with utility customers or the general public relating to receiving and dispatching of emergency and service calls provided there is, during such recording, a periodic warning which indicates to the parties to the conversation that the call is being recorded.

(7) A user, or any officer, employee or agent of such user, to record telephone communications between himself and a contractor or designer, or any officer, employee or agent of such contractor or designer, pertaining to excavation or demolition work or other related matters, if the user or its agent indicates to the parties to the conversation that the call will be or is being recorded. As used in this paragraph, the terms "user," "contractor," "demolition work," "designer" and "excavation work" shall have the meanings given to them in the act of December 10, 1974 (P.L.852, No.287), referred to as

the Underground Utility Line Protection Law; and a one call system shall be considered for this purpose to be an agent of any user which is a member thereof.

(8) A provider of electronic communication service to record the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service toward the completion of the wire or electronic communication, or a user of that service, from fraudulent, unlawful or abusive use of the service.

(9) A person or entity providing electronic communication service to the public to divulge the contents of any such communication:

(i) as otherwise authorized in this section or section 5717 (relating to investigative disclosure or use of contents of wire, electronic or oral communications or derivative evidence);

(ii) with the lawful consent of the originator or any addressee or intended recipient of the communication;

(iii) to a person employed or authorized, or whose facilities are used, to forward the communication to its destination; or

(iv) which were inadvertently obtained by the service provider and which appear to pertain to the commission of a crime, if such divulgence is made to a law enforcement agency.

A person or entity providing electronic communication service to the public shall not intentionally divulge the contents of any communication (other than one directed to the person or entity, or an agent thereof) while in transmission of that service to any person or entity other than an addressee or intended recipient of the communication or an agent of the addressee or intended recipient.

(10) Any person:

(i) to intercept or access an electronic communication made through an electronic communication system configured so that the electronic communication is readily accessible to the general public;

(ii) to intercept any radio communication which is transmitted:

(A) by a station for the use of the general public, or which relates to ships, aircraft, vehicles or persons in distress;

(B) by any governmental, law enforcement, civil defense, private land mobile or public safety communication system, including police and fire systems, readily accessible to the general public;

(C) by a station operating on an authorized frequency within the bands allocated to the amateur, citizens band or general mobile radio services; or

(D) by any marine or aeronautical communication system;

(iii) to engage in any conduct which:

(A) is prohibited by section 633 of the Communications Act of 1934 (48 Stat. 1105, 47 U.S.C. § 553); or

(B) is excepted from the application of section 705(a) of the Communications Act of 1934 (47 U.S.C. § 605(a)) by section 705(b) of that act (47 U.S.C. § 605(b)); or

(iv) to intercept any wire or electronic communication the transmission of which is causing harmful interference to any lawfully operating station, to the extent necessary to identify the source of the interference.

(11) Other users of the same frequency to intercept any radio communication made through a system which utilizes frequencies monitored by individuals engaged in the provisions or use of the system, if the communication is not scrambled or encrypted.

(12) Any investigative or law enforcement officer or any person acting at the direction or request of an investigative or law enforcement officer to intercept a wire or oral communication involving suspected criminal activities where the officer or the person is a party to the communication and there is reasonable cause to believe that:

(i) the other party to the communication is either:

(A) holding a hostage; or

(B) has barricaded himself and taken a position of confinement to avoid apprehension; and

(ii) that party:

(A) may resist with the use of weapons; or

(B) is threatening suicide or harm to himself or others.

(13) An investigative officer, a law enforcement officer or employees of the Department of Corrections for State correctional facilities to intercept, record, monitor or divulge any oral communication, electronic communication or wire communication from or to an inmate in a facility under the following conditions:

(i) The Department of Corrections shall adhere to the following procedures and restrictions when intercepting, recording, monitoring or divulging any oral communication, electronic communication or wire communication from or to an inmate in a State correctional facility as provided for by this paragraph:

(A) Before the implementation of this paragraph, all inmates of the facility shall be notified in writing that, as of the effective date of this paragraph, their oral communication, electronic communication or wire communication may be intercepted, recorded, monitored or divulged.

(B) Unless otherwise provided for in this paragraph, after intercepting or recording an oral communication, electronic communication or wire communication, only the superintendent, warden or a designee of the superintendent or warden or other chief administrative official or his or her designee, or law enforcement officers shall have access to that recording.

(C) The contents of an intercepted and recorded oral communication, electronic communication or wire communication shall be divulged only as is necessary to safeguard the orderly operation of the facility, in response to a court order or in the prosecution or investigation of any crime.

(ii) So as to safeguard the attorney-client privilege, the Department of Corrections shall not intercept, record, monitor or divulge an oral communication, electronic communication or wire communication between an inmate and an attorney.

(iii) Persons who are engaging in an oral communication, electronic communication or wire communication with an inmate shall be notified that the communication may be recorded or monitored. Notice may be provided by any means reasonably designed to inform the noninmate party of the recording or monitoring.

(iv) The Department of Corrections shall promulgate guidelines to implement the provisions of this paragraph for State correctional facilities.

(14) An investigative officer, a law enforcement officer or employees of a county correctional facility to intercept, record, monitor or divulge an oral communication, electronic communication or wire communication from or to an inmate in a facility under the following conditions:

(i) The county correctional facility shall adhere to the following procedures and restrictions when intercepting, recording, monitoring or divulging an oral communication, electronic communication or wire communication from or to an inmate in a county correctional facility as provided for by this paragraph:

(A) Before the implementation of this paragraph, all inmates of the facility shall be notified in writing that, as of the effective date of this paragraph, their oral communications, electronic communications or wire communications may be intercepted, recorded, monitored or divulged.

(B) Unless otherwise provided for in this paragraph, after intercepting or recording an oral communication, electronic communication or wire communication, only the superintendent, warden or a designee of the superintendent or warden or other chief administrative official or his or her designee, or law enforcement officers shall have access to that recording.

(C) The contents of an intercepted and recorded oral communication, electronic communication or wire communication shall be divulged only as is necessary to safeguard the orderly operation of the facility, in response to a court order or in the prosecution or investigation of any crime.

(ii) So as to safeguard the attorney-client privilege, the county correctional facility shall not intercept, record, monitor or divulge an oral communication, electronic communication or wire communication between an inmate and an attorney.

(iii) Persons who are engaging in an oral communication, electronic communication or wire communication with an inmate shall be notified that the communication may be recorded or monitored. Notice may be provided by any means reasonably designed to inform the noninmate party of the recording or monitoring.

(iv) The superintendent, warden or a designee of the superintendent or warden or other chief administrative official of the county correctional system shall promulgate guidelines to implement the provisions of this paragraph for county correctional facilities.

(15) The personnel of a business engaged in telephone marketing or telephone customer service by means of wire, oral or electronic communication to intercept such marketing or customer service communications where such interception is made for the sole purpose of training, quality control or monitoring by the business, provided that one party involved in the communications has consented to such intercept. Any communications recorded pursuant to this paragraph may only be used by the business for the purpose of training or quality control. Unless otherwise required by Federal or State law, communications recorded pursuant to this paragraph shall be destroyed within one year from the date of recording.

(16) (Deleted by amendment).

(17) Any victim, witness or private detective licensed under the act of August 21, 1953 (P.L.1273, No.361), known as The Private Detective Act of 1953, to intercept the contents of any wire, electronic or oral communication, if that person is under a reasonable suspicion that the intercepted party is committing, about to commit or has committed a crime of violence and there is reason to believe that evidence of the crime of violence may be obtained from the interception.

(18) A person to intercept oral communications for disciplinary or security purposes on a school bus or school vehicle, as those terms are defined in 75 Pa.C.S. § 102 (relating to definitions), if all of the following conditions are met:

- (i) The school board has adopted a policy that authorizes audio interception on school buses or school vehicles for disciplinary or security purposes.
- (ii) Each school year, the school board includes the policy in a student handbook and in any other publication of the school entity that sets forth the comprehensive rules, procedures and standards of conduct for the school entity.
- (iii) The school board posts a notice that students may be audiotaped, which notice is clearly visible on each school bus or school vehicle that is furnished with audio-recording equipment.
- (iv) The school entity posts a notice of the policy on the school entity's publicly accessible Internet website.

This paragraph shall not apply when a school bus or school vehicle is used for a purpose that is not school related.

(July 10, 1981, P.L.227, No.72, eff. 60 days; Dec. 23, 1981, P.L.593, No.175, eff. 60 days; Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Sept. 26, 1995, 1st Sp.Sess., P.L.1056, No.20, eff. 60 days; Dec. 19, 1996, P.L.1458, No.186, eff. 60 days; Feb. 18, 1998, P.L.102, No.19, eff. imd.; June 11, 2002, P.L.367, No.52, eff. imd.; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days; Feb. 4, 2014, P.L.21, No.9; June 23, 2016, P.L.392, No.56, eff. 60 days; July 7, 2017, P.L.304, No.22, eff. 60 days)

2017 Amendment. Act 22 amended pars. (13) and (14) and deleted par. (16).

2016 Amendment. Act 56 amended par. (18).

2014 Amendment. Act 9 amended par. (16) and added par. (18), effective in 60 days as to par. (16) and immediately as to the remainder of the section.

2012 Amendment. Act 202 amended pars. (2)(ii), (12)(ii), (13)(i)(B) and (14)(i)(B) and added par. (17).

1998 Amendment. Act 19 amended the intro. par. and pars. (2), (5) and (9) and added par. (15).

1996 Amendment. Act 186 amended par. (2) and added par. (14).

1995 Amendment. Act 20, 1st Sp.Sess., added par. (13).

Cross References. Section 5704 is referred to in sections 5702, 5706, 5717, 5720, 5721.1, 5742, 5747, 5749, 5782 of this title; section 901 of Title 30 (Fish); section 901 of Title 34 (Game).

§ 5705. Possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices and telecommunication identification interception devices.

Except as otherwise specifically provided in section 5706 (relating to exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices), a person is guilty of a felony of the third degree if he does any of the following:

- (1) Intentionally possesses an electronic, mechanical or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of a wire, electronic or oral communication.

(2) Intentionally sells, transfers or distributes an electronic, mechanical or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of a wire, electronic or oral communication.

(3) Intentionally manufactures or assembles an electronic, mechanical or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of a wire, electronic or oral communication.

(4) Intentionally places in any newspaper, magazine, handbill, or other publication any advertisement of an electronic, mechanical or other device, knowing or having reason to know that the design of such device renders it primarily useful for the purpose of the surreptitious interception of a wire, electronic or oral communication or of an electronic, mechanical or other device where such advertisement promotes the use of such device for the purpose of the surreptitious interception of a wire, electronic or oral communication.

(5) Intentionally possesses a telecommunication identification interception device.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days)

2012 Amendment. Act 202 amended the section heading and added par. (5).

§ 5706. Exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices.

(a) Unlawful activities.--It shall not be unlawful under this chapter for:

(1) a provider of wire or electronic communication service or an officer, agent or employee of, or a person under contract with, such a provider, in the normal course of the business of providing the wire or electronic communication service; or

(2) a person under contract with the United States, the Commonwealth or a political subdivision thereof, a state or a political subdivision thereof, or an officer, agent or employee of the United States, the Commonwealth or a political subdivision thereof, or a state or a political subdivision thereof,

to possess, sell, distribute, manufacture, assemble or advertise an electronic, mechanical or other device, while acting in furtherance of the appropriate activities of the United States, the Commonwealth or a political subdivision thereof, a state or a political subdivision thereof or a provider of wire or electronic communication service.

(b) Responsibility.--

(1) Except as provided under paragraph (2), the Attorney General and the district attorney or their designees so designated in writing shall have the sole responsibility to buy, possess and loan any electronic, mechanical or other device which is to be used by investigative or law enforcement officers for purposes of interception as authorized under section 5704(2), (5) and (12) (relating to exceptions to prohibition of interception and disclosure of communications), 5712 (relating to issuance of order and effect), 5713 (relating to emergency situations) or 5713.1 (relating to emergency hostage and barricade situations).

(2) The division or bureau or section of the Pennsylvania State Police responsible for conducting the training in the technical aspects of wiretapping and electronic surveillance as required by section 5724 (relating to training) may buy and possess any electronic, mechanical or other device which is to

be used by investigative or law enforcement officers for purposes of interception as authorized under section 5704(2), (5) and (12), 5712, 5713 or 5713.1 for the purpose of training. However, any electronic, mechanical or other device bought or possessed under this provision may be loaned to or used by investigative or law enforcement officers for purposes of interception as authorized under section 5704(2), (5) and (12), 5712, 5713 or 5713.1 only upon written approval by the Attorney General or a deputy attorney general designated in writing by the Attorney General or the district attorney or an assistant district attorney designated in writing by the district attorney of the county wherein the suspected criminal activity has been, is or is about to occur.

(3) With the permission of the Attorney General or a district attorney who has designated any supervising law enforcement officer for purposes of interceptions as authorized under section 5713.1, the law enforcement agency which employs the supervising law enforcement officer may buy, possess, loan or borrow any electronic, mechanical or other device which is to be used by investigative or law enforcement officers at the direction of the supervising law enforcement officer solely for the purpose of interception as authorized under sections 5704(12) and 5713.1.

(4) The Pennsylvania State Police shall annually establish equipment standards for any electronic, mechanical or other device which is to be used by law enforcement officers for purposes of recording a communication under circumstances within paragraph (2) of the definition of "oral communication" in section 5702 (relating to definitions). The equipment standards shall be published annually in the Pennsylvania Bulletin.

(5) The Pennsylvania State Police shall annually establish and publish standards in the Pennsylvania Bulletin for the secure onsite and off-site storage of an audio recording made in accordance with paragraph (4) or any accompanying video recording. The standards shall comply with the Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy.

(6) A vendor to law enforcement agencies which stores data related to audio recordings and video recordings shall, at a minimum, comply with the standards set forth by the Pennsylvania State Police under paragraphs (4) and (5). Law enforcement agencies under contract with a vendor for the storage of data before the effective date of this paragraph shall comply with paragraphs (4) and (5) and this paragraph upon expiration or renewal of the contract.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.; June 11, 2002, P.L.367, No.52, eff. imd.; Dec. 9, 2002, P.L.1350, No.162, eff. 60 days; July 7, 2017, P.L.304, No.22, eff. 60 days)

2017 Amendment. Act 22 amended subsec. (b).

Cross References. Section 5706 is referred to in sections 5702, 5705 of this title; section 901 of Title 34 (Game); section 67A07 of Title 42 (Judiciary and Judicial Procedure).

§ 5707. Seizure and forfeiture of electronic, mechanical or other devices.

Any electronic, mechanical or other device possessed, used, sent, distributed, manufactured, or assembled in violation of this chapter is hereby declared to be contraband and may be seized and forfeited to the Commonwealth in accordance with 42 Pa.C.S. §§ 5803 (relating to asset forfeiture), 5805 (relating to forfeiture procedure), 5806 (relating to motion for return of property), 5807 (relating to restrictions on use), 5807.1 (relating to prohibition on adoptive seizures) and 5808 (relating to exceptions).

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; June 29, 2017, P.L.247, No.13, eff. July 1, 2017)

Cross References. Section 5707 is referred to in section 5803 of Title 42 (Judiciary and Judicial Procedure).

§ 5708. Order authorizing interception of wire, electronic or oral communications.

The Attorney General, or, during the absence or incapacity of the Attorney General, a deputy attorney general designated in writing by the Attorney General, or the district attorney or, during the absence or incapacity of the district attorney, an assistant district attorney designated in writing by the district attorney of the county wherein the suspected criminal activity has been, is or is about to occur, may make written application to any Superior Court judge for an order authorizing the interception of a wire, electronic or oral communication by the investigative or law enforcement officers or agency having responsibility for an investigation involving suspected criminal activities when such interception may provide evidence of the commission of any of the following offenses, or may provide evidence aiding in the apprehension of the perpetrator or perpetrators of any of the following offenses:

(1) Under this title:

Section 911 (relating to corrupt organizations)

Section 2501 (relating to criminal homicide)

Section 2502 (relating to murder)

Section 2503 (relating to voluntary manslaughter)

Section 2702 (relating to aggravated assault)

Section 2706 (relating to terroristic threats)

Section 2709.1 (relating to stalking)

Section 2716 (relating to weapons of mass destruction)

Section 2901 (relating to kidnapping)

Section 3011 (relating to trafficking in individuals)

Section 3012 (relating to involuntary servitude)

Section 3121 (relating to rape)

Section 3123 (relating to involuntary deviate sexual intercourse)

Section 3124.1 (relating to sexual assault)

Section 3125 (relating to aggravated indecent assault)

Section 3301 (relating to arson and related offenses)

Section 3302 (relating to causing or risking catastrophe)

Section 3502 (relating to burglary)

Section 3701 (relating to robbery)

Section 3921 (relating to theft by unlawful taking or disposition)

Section 3922 (relating to theft by deception)

Section 3923 (relating to theft by extortion)

Section 4701 (relating to bribery in official and political matters)

Section 4702 (relating to threats and other improper influence in official and political matters)

Section 5512 (relating to lotteries, etc.)

Section 5513 (relating to gambling devices, gambling, etc.)

Section 5514 (relating to pool selling and bookmaking)

Section 5516 (relating to facsimile weapons of mass destruction)

Section 6318 (relating to unlawful contact with minor)

(2) Under this title, where such offense is dangerous to life, limb or property and punishable by imprisonment for more than one year:

Section 910 (relating to manufacture, distribution or possession of devices for theft of telecommunications services)

Section 2709(a)(4), (5), (6) or (7) (relating to harassment)

Section 3925 (relating to receiving stolen property)

Section 3926 (relating to theft of services)

Section 3927 (relating to theft by failure to make required disposition of funds received)

Section 3933 (relating to unlawful use of computer)

Section 4108 (relating to commercial bribery and breach of duty to act disinterestedly)

Section 4109 (relating to rigging publicly exhibited contest)

Section 4117 (relating to insurance fraud)

Section 4305 (relating to dealing in infant children)

Section 4902 (relating to perjury)

Section 4909 (relating to witness or informant taking bribe)

Section 4911 (relating to tampering with public records or information)

Section 4952 (relating to intimidation of witnesses or victims)

Section 4953 (relating to retaliation against witness or victim)

Section 5101 (relating to obstructing administration of law or other governmental function)

Section 5111 (relating to dealing in proceeds of unlawful activities)

Section 5121 (relating to escape)

Section 5902 (relating to prostitution and related offenses)

Section 5903 (relating to obscene and other sexual materials and performances)

Section 7313 (relating to buying or exchanging Federal Supplemental Nutrition Assistance Program (SNAP) benefit coupons, stamps, authorization cards or access devices)

(3) Under the act of March 4, 1971 (P.L.6, No.2), known as the Tax Reform Code of 1971, where such offense is dangerous to life, limb or property and punishable by imprisonment for more than one year:

Section 1272 (relating to sales of unstamped cigarettes)

Section 1273 (relating to possession of unstamped cigarettes)

Section 1274 (relating to counterfeiting)

(4) Any offense set forth under section 13(a) of the act of April 14, 1972 (P.L.233, No.64), known as The Controlled Substance, Drug, Device and Cosmetic Act, not including the offense described in clause (31) of section 13(a).

(5) Any offense set forth under the act of November 15, 1972 (P.L.1227, No.272).

(6) Any conspiracy to commit any of the offenses set forth in this section.

(7) Under the act of November 24, 1998 (P.L.874, No.110), known as the Motor Vehicle Chop Shop and Illegally Obtained and Altered Property Act.

(Dec. 2, 1983, P.L.248, No.67, eff. imd.; Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 2, 1990, P.L.4, No.3, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.; Dec. 21, 1998, P.L.1086, No.145, eff. 60 days; June 28, 2002, P.L.481, No.82, eff. 60 days; Nov. 20, 2002, P.L.1104, No.134, eff. 60 days; Dec. 9, 2002, P.L.1350, No.162, eff. 60 days; Dec. 9, 2002, P.L.1759, No.218, eff. 60 days; Nov. 9, 2006, P.L.1340, No.139, eff. 60 days; July 2, 2014, P.L.945, No.105, eff. 60 days; Oct. 24, 2018, P.L.1159, No.160, eff. 60 days)

2018 Amendment. Act 160 amended par. (2).

2014 Amendment. Act 105 amended par. (1).

2002 Amendments. Act 82 amended par. (1), Act 134 amended par. (1), Act 162 amended the entire section and Act 218 amended pars. (1) and (2). Act 162 overlooked the amendment by Act 134 and Act 218 overlooked the amendments by Acts 134 and 162, but the amendments do not conflict in substance and have been given effect in setting forth the text of section 5708.

Effective Date. After January 20, 2003, and before February 7, 2003, section 5708 will reflect only the amendment by Act 134, as follows:

§ 5708. Order authorizing interception of wire, electronic or oral communications.

The Attorney General, or, during the absence or incapacity of the Attorney General, a deputy attorney general designated in writing by the Attorney General, or the district attorney or, during the absence or incapacity of the district attorney, an assistant district attorney designated in writing by the district attorney of the county wherein the interception is to be made, may make written application to any Superior Court judge for an order authorizing the interception of a wire, electronic or oral communication by the investigative or law enforcement officers or agency having responsibility for an investigation involving suspected criminal activities when such interception may provide evidence of the commission of any of the following offenses, or may provide evidence aiding in the apprehension of the perpetrator or perpetrators of any of the following offenses:

(1) Under this title:

Section 911 (relating to corrupt organizations)

Section 2501 (relating to criminal homicide)

Section 2502 (relating to murder)

Section 2503 (relating to voluntary manslaughter)

Section 2702 (relating to aggravated assault)

Section 2706 (relating to terroristic threats)

Section 2709(b) (relating to harassment and stalking)

Section 2716 (relating to weapons of mass destruction)

Section 2901 (relating to kidnapping)

Section 3121 (relating to rape)

Section 3123 (relating to involuntary deviate sexual intercourse)

Section 3124.1 (relating to sexual assault)

Section 3125 (relating to aggravated indecent assault)

Section 3301 (relating to arson and related offenses)

Section 3302 (relating to causing or risking catastrophe)

Section 3502 (relating to burglary)

Section 3701 (relating to robbery)

Section 3921 (relating to theft by unlawful taking or disposition)

Section 3922 (relating to theft by deception)

Section 3923 (relating to theft by extortion)

Section 4701 (relating to bribery in official and political matters)

Section 4702 (relating to threats and other improper influence in official and political matters)

Section 5512 (relating to lotteries, etc.)

Section 5513 (relating to gambling devices, gambling, etc.)

Section 5514 (relating to pool selling and bookmaking)

Section 5516 (relating to facsimile weapons of mass destruction)

Section 6318 (relating to unlawful contact with minor)

(2) Under this title, where such offense is dangerous to life, limb or property and punishable by imprisonment for more than one year:

Section 910 (relating to manufacture, distribution or possession of devices for theft of telecommunications services)

Section 3925 (relating to receiving stolen property)

Section 3926 (relating to theft of services)

Section 3927 (relating to theft by failure to make required disposition of funds received)

Section 3933 (relating to unlawful use of computer)

Section 4108 (relating to commercial bribery and breach of duty to act disinterestedly)

Section 4109 (relating to rigging publicly exhibited contest)

Section 4117 (relating to insurance fraud)

Section 4305 (relating to dealing in infant children)

Section 4902 (relating to perjury)

Section 4909 (relating to witness or informant taking bribe)

Section 4911 (relating to tampering with public records or information)

Section 4952 (relating to intimidation of witnesses or victims)

Section 4953 (relating to retaliation against witness or victim)

Section 5101 (relating to obstructing administration of law or other governmental function)

Section 5111 (relating to dealing in proceeds of unlawful activities)

Section 5121 (relating to escape)

Section 5504 (relating to harassment by communication or address)

Section 5902 (relating to prostitution and related offenses)

Section 5903 (relating to obscene and other sexual materials and performances)

Section 7313 (relating to buying or exchanging Federal food order coupons, stamps, authorization cards or access devices)

(3) Under the act of March 4, 1971 (P.L.6, No.2), known as the Tax Reform Code of 1971, where such offense is dangerous to life, limb or property and punishable by imprisonment for more than one year:

Section 1272 (relating to sales of unstamped cigarettes)

Section 1273 (relating to possession of unstamped cigarettes)

Section 1274 (relating to counterfeiting)

(4) Any offense set forth under section 13(a) of the act of April 14, 1972 (P.L.233, No.64), known as The Controlled Substance, Drug, Device and Cosmetic Act, not including the offense described in clause (31) of section 13(a).

(5) Any offense set forth under the act of November 15, 1972 (P.L.1227, No.272).

(6) Any conspiracy to commit any of the offenses set forth in this section.

(7) Under the act of November 24, 1998 (P.L.874, No.110), known as the Motor Vehicle Chop Shop and Illegally Obtained and Altered Property Act.

References in Text. The act of November 15, 1972 (P.L.1227, No.272), referred to in this section, amended the act of December 8, 1970 (P.L.874, No.276), known as The Pennsylvania Corrupt Organizations Act of 1970, which was repealed by the act of December 6, 1972 (P.L.1482, No.334). The subject matter is now contained in section 911 of Title 18.

Section 3933, referred to in this section, is repealed.

Section 5504, referred to in this section, is repealed.

The act of November 24, 1998 (P.L.874, No.110), known as the Vehicle Chop Shop and Illegally Obtained and Altered Property Act, referred to in paragraph (7), was repealed by the act of October 25, 2012 (P.L.1645, No.203). The subject matter is now contained in Chapter 77 of this title.

Cross References. Section 5708 is referred to in sections 5704, 5710, 5713, 5742 of this title.

§ 5709. Application for order.

Each application for an order of authorization to intercept a wire, electronic or oral communication shall be made in writing upon the personal oath or affirmation of the Attorney General or a district attorney of the county wherein the suspected criminal activity has been, is or is about to occur and shall contain all of the following:

- (1) A statement of the authority of the applicant to make such application.
- (2) A statement of the identity and qualifications of the investigative or law enforcement officers or agency for whom the authority to intercept a wire, electronic or oral communication is sought.
- (3) A sworn statement by the investigative or law enforcement officer who has knowledge of relevant information justifying the application, which shall include:
 - (i) The identity of the particular person, if known, committing the offense and whose communications are to be intercepted.
 - (ii) The details as to the particular offense that has been, is being, or is about to be committed.
 - (iii) The particular type of communication to be intercepted.
 - (iv) A showing that there is probable cause to believe that such communication will be communicated on the wire communication facility involved or at the particular place where the oral communication is to be intercepted.
 - (v) The character and location of the particular wire communication facility involved or the particular place where the oral communication is to be intercepted.
 - (vi) A statement of the period of time for which the interception is required to be maintained, and, if the character of the investigation is such that the authorization for interception should not automatically terminate when the described type of communication has been first obtained, a particular statement of facts establishing probable cause to believe that additional communications of the same type will occur thereafter.
 - (vii) A particular statement of facts showing that other normal investigative procedures with respect to the offense have been tried and have failed, or reasonably appear to be unlikely to succeed if tried or are too dangerous to employ.
- (4) Where the application is for the renewal or extension of an order, a particular statement of facts showing the results thus far obtained from the interception, or a reasonable explanation of the failure to obtain such results.

(5) A complete statement of the facts concerning all previous applications, known to the applicant made to any court for authorization to intercept a wire, electronic or oral communication involving any of the same facilities or places specified in the application or involving any person whose communication is to be intercepted, and the action taken by the court on each such application.

(6) A proposed order of authorization for consideration by the judge.

(7) Such additional testimony or documentary evidence in support of the application as the judge may require.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Dec. 9, 2002, P.L.1350, No.162, eff. 60 days)

Cross References. Section 5709 is referred to in sections 5702, 5712.1, 5713.1 of this title.

§ 5710. Grounds for entry of order.

(a) Application.--Upon consideration of an application, the judge may enter an ex parte order, as requested or as modified, authorizing the interception of wire, electronic or oral communications anywhere within the Commonwealth, if the judge determines on the basis of the facts submitted by the applicant that there is probable cause for belief that all the following conditions exist:

(1) the person whose communications are to be intercepted is committing, has or had committed or is about to commit an offense as provided in section 5708 (relating to order authorizing interception of wire, electronic or oral communications);

(2) particular communications concerning such offense may be obtained through such interception;

(3) normal investigative procedures with respect to such offense have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous to employ;

(4) the facility from which, or the place where, the wire, electronic or oral communications are to be intercepted, is, has been, or is about to be used, in connection with the commission of such offense, or is leased to, listed in the name of, or commonly used by, such person;

(5) the investigative or law enforcement officers or agency to be authorized to intercept the wire, electronic or oral communications are qualified by training and experience to execute the interception sought, and are certified under section 5724 (relating to training); and

(6) in the case of an application, other than a renewal or extension, for an order to intercept a communication of a person or on a facility which was the subject of a previous order authorizing interception, the application is based upon new evidence or information different from and in addition to the evidence or information offered to support the prior order, regardless of whether such evidence was derived from prior interceptions or from other sources.

(b) Corroborative evidence.--As part of the consideration of an application in which there is no corroborative evidence offered, the judge may inquire in camera as to the identity of any informants or any other additional information concerning the basis upon which the investigative or law enforcement officer or agency has applied for the order of authorization which the judge finds relevant in order to determine if there is probable cause pursuant to this section.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.)

Cross References. Section 5710 is referred to in sections 5712, 5721.1 of this title.

§ 5711. Privileged communications.

No otherwise privileged communication intercepted in accordance with, or in violation of, the provisions of this chapter shall lose its privileged character.

§ 5712. Issuance of order and effect.

(a) Authorizing orders.--An order authorizing the interception of any wire, electronic or oral communication shall state the following:

(1) The identity of the investigative or law enforcement officers or agency to whom the authority to intercept wire, electronic or oral communications is given and the name and official identity of the person who made the application.

(2) The identity of, or a particular description of, the person, if known, whose communications are to be intercepted.

(3) The character and location of the particular communication facilities as to which, or the particular place of the communication as to which, authority to intercept is granted.

(4) A particular description of the type of the communication to be intercepted and a statement of the particular offense to which it relates.

(5) The period of time during which such interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

(b) Time limits.--No order entered under this section shall authorize the interception of any wire, electronic or oral communication for a period of time in excess of that necessary under the circumstances. Every order entered under this section shall require that such interception begin and terminate as soon as practicable and be conducted in such a manner as to minimize or eliminate the interception of such communications not otherwise subject to interception under this chapter by making reasonable efforts, whenever possible, to reduce the hours of interception authorized by said order. In the event the intercepted communication is in a code or foreign language and an expert in that code or foreign language is not reasonably available during the interception period, minimization may be accomplished as soon as practicable after such interception. No order entered under this section shall authorize the interception of wire, electronic or oral communications for any period exceeding 30 days. The 30-day period begins on the day on which the investigative or law enforcement officers or agency first begins to conduct an interception under the order, or ten days after the order is entered, whichever is earlier. Extensions or renewals of such an order may be granted for additional periods of not more than 30 days each. No extension or renewal shall be granted unless an application for it is made in accordance with this section, and the judge makes the findings required by section 5710 (relating to grounds for entry of order).

(c) Responsibility.--The order shall require the Attorney General or the district attorney, or their designees, to be responsible for the supervision of the interception.

(d) Progress reports.--Whenever an order authorizing an interception is entered, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. The reports shall be made at such intervals as the judge may require.

(e) Final report.--Whenever an interception is authorized pursuant to this section, a complete written list of names of participants and evidence of offenses discovered, including those not stated in the

application for order, shall be filed with the court as soon as practicable after the authorized interception is terminated.

(f) Assistance.--An order authorizing the interception of a wire, electronic or oral communication shall, upon request of the applicant, direct that a provider of communication service shall furnish the applicant forthwith all information, facilities and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that such service provider is affording the person whose communications are to be intercepted. The obligation of a provider of communication service under such an order may include, but is not limited to, installation of a pen register or of a trap and trace device, providing caller ID, deluxe caller ID or any other features available to ascertain the telephone number, location or subscriber information of a facility contacting the facility whose communications are to be intercepted, disclosure of a record or other information otherwise available under section 5743 (relating to requirements for governmental access), including conducting an in-progress trace during an interception, provided that such obligation of a provider of communications service is technologically feasible. The order shall apply regardless of whether the electronic service provider is headquartered within this Commonwealth, if the interception is otherwise conducted within this Commonwealth as provided under this chapter. The order regarding disclosure of a record or other information otherwise available under section 5743 shall apply to all electronic service providers who service facilities which contact or are contacted by the facility whose communications are to be intercepted, regardless of whether the order specifically names any provider of communication service. The order may specify the period of time an electronic service provider has to furnish to the applicant who requests disclosure of a record or other information otherwise available under section 5743. Any provider of communication service furnishing such facilities or technical assistance shall be compensated therefor by the applicant for reasonable expenses incurred in providing the facilities or assistance. The service provider shall be immune from civil and criminal liability for any assistance rendered to the applicant pursuant to this section.

(g) Entry by law enforcement officers.--An order authorizing the interception of a wire, electronic or oral communication shall, if requested, authorize the entry of premises or facilities specified in subsection (a)(3), or premises necessary to obtain access to the premises or facilities specified in subsection (a)(3), by the law enforcement officers specified in subsection (a)(1), as often as necessary solely for the purposes of installing, maintaining or removing an electronic, mechanical or other device or devices provided that such entry is reasonably necessary to accomplish the purposes of this subchapter and provided that the judge who issues the order shall be notified of the time and method of each such entry prior to entry if practical and, in any case, within 48 hours of entry.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days)

2012 Amendment. Act 202 amended subsecs. (a) intro. par. and (f).

1998 Amendment. Act 19 amended subsecs. (e), (f) and (g).

Cross References. Section 5712 is referred to in sections 5706, 5712.1, 5713.1, 5721.1 of this title.

§ 5712.1. Target-specific orders.

(a) Target-specific wiretaps.--The requirements of sections 5712(a)(3) (relating to issuance of order and effect) and 5709(3)(iv) and (v) (relating to application for order) shall not apply if:

(1) In the case of an application with respect to the interception of an oral communication, all of the following apply:

(i) The application contains a full and complete statement as to why specification is not practical and identifies the person committing the offense and whose communications are to be intercepted.

(ii) The judge finds the specification is not practical.

(2) In the case of an application with respect to a wire or electronic communication, all of the following apply:

(i) The application identifies the person believed to be committing the offense and whose communications are to be intercepted and the applicant makes a showing that there is probable cause to believe that the person's actions could have the effect of thwarting interception by changing facilities or devices.

(ii) The judge finds that the purpose has been adequately shown.

(b) Supplementary orders.--Following the issuance of a target-specific wiretap order, the judge shall sign supplementary orders upon request and in a timely manner, authorizing the investigative or law enforcement officers or agency to intercept additional communications devices or facilities upon a showing of reasonable suspicion that all of the following apply:

(1) The target of the original order has in fact changed communications devices or facilities or is presently using additional communications devices, communications facilities or places.

(2) The target of the original order is likely to use the specified communications device or facility for criminal purposes similar to or related to those specified in the original order.

(c) Application for supplementary orders.--An application for a supplementary order shall contain all of the following:

(1) The identity of the investigative or law enforcement officers or agency to whom the authority to intercept wire, electronic or oral communications is given and the name and official identity of the person who made the application.

(2) The identity of or a particular description of the person, if known, whose communications are to be intercepted.

(3) The period of time during which the interception is authorized, including a statement as to whether or not the interception shall automatically terminate when the described communication has been first obtained.

(4) A showing of reasonable suspicion that the target of the original order has in fact changed communications devices or facilities.

(5) A showing of reasonable suspicion that the target of the original order is likely to use the additional facility or device or place for criminal purposes similar to or related to those specified in the original order.

(d) Time limits.--A supplementary order shall not act as an extension of the time limit identified in section 5712(b).

(e) Responsibility.--The order shall require the Attorney General or the district attorney, or their designees, to be responsible for the supervision of the interception.

(f) Progress reports.--If an order authorizing an interception is entered, the order may require reports to be made to the judge who issued the order showing what progress has been made toward achievement of the authorized objective and the need for continued interception. The reports shall be made at intervals as the judge may require.

(g) Final report.--If an interception is authorized under this section, a complete written list of names of participants and evidence of offenses discovered, including those not stated in the application for order, shall be filed with the court as soon as practical after the authorized interception is terminated.

(h) Assistance.--

(1) An order authorizing the interception of a wire, electronic or oral communication shall, upon request of the applicant, direct that a provider of communication service furnish the applicant with all information, facilities and technical assistance necessary to accomplish the interception unobtrusively and with a minimum of interference with the services that the service provider is affording the person whose communications are to be intercepted.

(2) The obligation of a provider of communication service under an order may include installation of a pen register or trap and trace device and disclosure of a record or other information otherwise available under section 5743 (relating to requirements for governmental access), including conducting an in-progress trace during an interception, if the obligation of a provider of communications service is technologically feasible.

(3) A provider of communication service furnishing facilities or technical assistance shall be compensated by the applicant for reasonable expenses incurred in providing the facilities or assistance.

(4) A service provider shall be immune from civil and criminal liability for any assistance rendered to an applicant under this section.

(i) Entry by law enforcement officers.--An order authorizing the interception of a wire, electronic or oral communication shall, if requested, authorize the entry of premises or facilities specified under subsection (c)(3) or premises necessary to obtain access to the premises or facilities specified under subsection (c)(3) by law enforcement officers specified under subsection (c)(1) as often as necessary solely for the purposes of installing, maintaining or removing an electronic, mechanical or other device, if all of the following apply:

(1) The entry is reasonably necessary to accomplish the purposes of this subchapter.

(2) The judge who issues the order is notified of the time and method of each entry prior to entry within 48 hours of entry.

(Oct. 25, 2012, P.L.1634, No.202, eff. 60 days)

2012 Amendment. Act 202 added section 5712.1.

§ 5713. Emergency situations.

(a) Application.--Whenever, upon informal application by the Attorney General or a designated deputy attorney general authorized in writing by the Attorney General or a district attorney or an assistant district attorney authorized in writing by the district attorney of a county wherein the suspected criminal activity has been, is or is about to occur, a judge determines there are grounds upon which an order could be issued pursuant to this chapter, and that an emergency situation exists

with respect to the investigation of an offense designated in section 5708 (relating to order authorizing interception of wire, electronic or oral communications), and involving conspiratorial activities characteristic of organized crime or a substantial danger to life or limb, dictating authorization for immediate interception of wire, electronic or oral communications before an application for an order could with due diligence be submitted to him and acted upon, the judge may grant oral approval for such interception without an order, conditioned upon the filing with him, within 48 hours thereafter, of an application for an order which, if granted, shall recite the oral approval and be retroactive to the time of such oral approval. Such interception shall immediately terminate when the communication sought is obtained or when the application for an order is denied, whichever is earlier. In the event no application for an order is made, the content of any wire, electronic or oral communication intercepted shall be treated as having been obtained in violation of this subchapter.

(b) Further proceedings.--In the event no application is made or an application made pursuant to this section is denied, the court shall cause an inventory to be served as provided in section 5716 (relating to service of inventory and inspection of intercepted communications) and shall require the tape or other recording of the intercepted communication to be delivered to, and sealed by, the court. Such evidence shall be retained by the court in accordance with section 5714 (relating to recording of intercepted communications) and the same shall not be used or disclosed in any legal proceeding except in a civil action brought by an aggrieved person pursuant to section 5725 (relating to civil action for unlawful interception, disclosure or use of wire, electronic or oral communication) or as otherwise authorized by court order. In addition to other remedies and penalties provided by this chapter, failure to effect delivery of any such tape or other recording shall be punishable as contempt by the court directing such delivery. Evidence of oral authorization to intercept wire, electronic or oral communications shall be a defense to any charge against the investigating or law enforcement officer for engaging in unlawful interception.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.; Dec. 9, 2002, P.L.1350, No.162, eff. 60 days)

2002 Amendment. Act 162 amended subsec. (a).

Cross References. Section 5713 is referred to in sections 5706, 5713.1, 5716, 5721.1, 5747 of this title.

§ 5713.1. Emergency hostage and barricade situations.

(a) Designation.--The Attorney General or a district attorney may designate supervising law enforcement officers for the purpose of authorizing the interception of wire or oral communications as provided in this section.

(b) Procedure.--A supervising law enforcement officer who reasonably determines that an emergency situation exists that requires a wire or oral communication to be intercepted before an order authorizing such interception can, with due diligence, be obtained, and who determines that there are grounds upon which an order could be entered under this chapter to authorize such interception, may intercept such wire or oral communication. An application for an order approving the interception must be made by the supervising law enforcement officer in accordance with section 5709 (relating to application for order) within 48 hours after the interception has occurred or begins to occur. Interceptions pursuant to this section shall be conducted in accordance with the procedures of this subchapter. Upon request of the supervising law enforcement officer who determines to authorize interceptions of wire communications under this section, a provider of electronic

communication service shall provide assistance and be compensated therefor as provided in section 5712(f) (relating to issuance of order and effect). In the absence of an order, such interception shall immediately terminate when the situation giving rise to the hostage or barricade situation ends or when the application for the order is denied, whichever is earlier. In the event such application for approval is denied or in any other case where the interception is terminated without an order having been issued, the contents of any wire or oral communication intercepted shall be treated as having been obtained in violation of this subchapter, and an inventory shall be served as provided in section 5716 (relating to service of inventory and inspection of intercepted communications). Thereafter, the supervising law enforcement officer shall follow the procedures set forth in section 5713(b) (relating to emergency situations).

(c) Defense.--A good faith reliance on the provisions of this section shall be a complete defense to any civil or criminal action brought under this subchapter or any other statute against any law enforcement officer or agency conducting any interceptions pursuant to this section as well as a provider of electronic communication service who is required to provide assistance in conducting such interceptions upon request of a supervising law enforcement officer.

(d) Definitions.--As used in this section, the following words and phrases shall have the meanings given to them in this subsection:

"Emergency situation." Any situation where:

- (1) a person is holding a hostage and is threatening serious physical injury and may resist with the use of weapons; or
- (2) a person has barricaded himself and taken a position of confinement to avoid apprehension and:
 - (i) has the ability to resist with the use of weapons; or
 - (ii) is threatening suicide or harm to himself or others.

"Supervising law enforcement officer."

(1) For designations by a district attorney, any law enforcement officer trained pursuant to section 5724 (relating to training) to carry out interceptions under this section who has attained the rank of lieutenant or higher in a law enforcement agency within the county or who is in charge of a county law enforcement agency.

(2) For designations by the Attorney General, any member of the Pennsylvania State Police trained pursuant to section 5724 to carry out interceptions under this section and designated by the Commissioner of the Pennsylvania State Police who:

- (i) has attained the rank of lieutenant or higher; or
- (ii) is in charge of a Pennsylvania State Police barracks.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days)

2012 Amendment. Act 202 amended subsec. (d).

1998 Amendment. Act 19 amended subsecs. (b) and (c).

1988 Amendment. Act 115 added section 5713.1.

Cross References. Section 5713.1 is referred to in sections 5706, 5716, 5721.1 of this title.

§ 5714. Recording of intercepted communications.

(a) Recording and monitoring.--Any wire, electronic or oral communication intercepted in accordance with this subchapter shall, if practicable, be recorded by tape or other comparable method. The recording shall be done in such a way as will protect it from editing or other alteration. Whenever an interception is being monitored, the monitor shall be an investigative or law enforcement officer certified under section 5724 (relating to training), and where practicable, keep a signed, written record which shall include the following:

- (1) The date and hours of surveillance.
- (2) The time and duration of each intercepted communication.
- (3) The participant, if known, in each intercepted conversation.
- (4) A summary of the content of each intercepted communication.

(b) Sealing of recordings.--Immediately upon the expiration of the order or extensions or renewals thereof, all monitor's records, tapes and other recordings shall be transferred to the judge issuing the order and sealed under his direction. Custody of the tapes, or other recordings shall be maintained wherever the court directs. They shall not be destroyed except upon an order of the court and in any event shall be kept for ten years. Duplicate tapes, or other recordings may be made for disclosure or use pursuant to section 5717 (relating to investigative disclosure or use of contents of wire, electronic or oral communications or derivative evidence). The presence of the seal provided by this section, or a satisfactory explanation for its absence, shall be a prerequisite for the disclosure of the contents of any wire, electronic or oral communication, or evidence derived therefrom, under section 5717(b).

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.)

Cross References. Section 5714 is referred to in sections 5704, 5713, 5749, 5773 of this title.

§ 5715. Sealing of applications, orders and supporting papers.

Applications made, final reports, and orders granted pursuant to this subchapter and supporting papers and monitor's records shall be sealed by the court and shall be held in custody as the court shall direct and shall not be destroyed except on order of the court and in any event shall be kept for ten years. They may be disclosed only upon a showing of good cause before a court of competent jurisdiction except that any investigative or law enforcement officer may disclose such applications, orders and supporting papers and monitor's records to investigative or law enforcement officers of this or another state, any of its political subdivisions, or of the United States to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure. In addition to any remedies and penalties provided by this subchapter, any violation of the provisions of this section may be punished as contempt of the court.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.)

§ 5716. Service of inventory and inspection of intercepted communications.

(a) Service of inventory.--Within a reasonable time but not later than 90 days after the termination of the period of the order or of extensions or renewals thereof, or the date of the denial of an order applied for under section 5713 (relating to emergency situations) or 5713.1 (relating to emergency hostage and barricade situations), the issuing or denying judge shall cause to be served on the

persons named in the order, application, or final report an inventory which shall include the following:

(1) Notice of the entry of the order or the application for an order denied under section 5713 or 5713.1.

(2) The date of the entry of the order or the denial of an order applied for under section 5713 or 5713.1.

(3) The period of authorized or disapproved interception.

(4) The fact that during the period wire or oral communications were or were not intercepted.

(b) Postponement.--On an ex parte showing of good cause to the issuing or denying judge the service of the inventory required by this section may be postponed for a period of 30 days. Additional postponements may be granted for periods of not more than 30 days on an ex parte showing of good cause to the issuing or denying judge.

(c) Inspections.--The court, upon the filing of a motion, shall make available to such persons or their attorneys for inspection, the intercepted communications and monitor's records to which the movant was a participant and the applications and orders.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.)

Cross References. Section 5716 is referred to in sections 5713, 5713.1 of this title.

§ 5717. Investigative disclosure or use of contents of wire, electronic or oral communications or derivative evidence.

(a) Law enforcement personnel.--Any investigative or law enforcement officer who, under subsection (a.1), (b), (b.1) or (c), has obtained knowledge of the contents of any wire, electronic or oral communication, or evidence derived therefrom, may disclose such contents or evidence to another investigative or law enforcement officer to the extent that such disclosure is appropriate to the proper performance of the official duties of the officer making or receiving the disclosure.

(a.1) Use of information.--Any investigative or law enforcement officer who, by any means authorized by this subchapter, has obtained knowledge of the contents of any wire, electronic or oral communication or evidence derived therefrom may use such contents or evidence to the extent such use is appropriate to the proper performance of his official duties.

(b) Evidence.--Any person who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, electronic or oral communication, or evidence derived therefrom, may disclose such contents or evidence to an investigative or law enforcement officer and may disclose such contents or evidence while giving testimony under oath or affirmation in any criminal proceeding in any court of this Commonwealth or of another state or of the United States or before any state or Federal grand jury or investigating grand jury.

(b.1) Criminal cases.--Any person who by means authorized by section 5704(17) (relating to exceptions to prohibition of interception and disclosure of communications) has obtained knowledge of the contents of any wire, electronic or oral communication, or evidence derived therefrom, may in addition to disclosures made under subsection (b) disclose such contents or evidence, on the condition that such disclosure is made for the purpose of providing exculpatory evidence in an open or closed criminal case.

(c) Otherwise authorized personnel.--

(1) Except as provided under paragraph (2), any person who, by any means authorized by the laws of another state or the Federal Government, has obtained knowledge of the contents of any wire, electronic or oral communication, or evidence derived from any wire, electronic or oral communication, may disclose the contents or evidence to an investigative or law enforcement officer and may disclose the contents or evidence where otherwise admissible while giving testimony under oath or affirmation in any proceeding in any court of this Commonwealth.

(2) The contents of a nonconsensual interception authorized by the laws of the Federal Government or another state shall not be admissible unless the interception was authorized by a court upon a finding of probable cause that the target of the surveillance is engaged or will engage in a violation of the criminal laws of the Federal Government or any state.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days)

2012 Amendment. Act 202 amended subsec. (a) and added subsecs. (b.1) and (c).

Cross References. Section 5717 is referred to in sections 5704, 5714, 5718, 5721.1, 5749 of this title.

§ 5718. Interception of communications relating to other offenses.

When an investigative or law enforcement officer, while engaged in court authorized interceptions of wire, electronic or oral communications in the manner authorized herein, intercepts wire, electronic or oral communications relating to offenses other than those specified in the order of authorization, the contents thereof, and evidence derived therefrom, may be disclosed or used as provided in section 5717(a) (relating to investigative disclosure or use of contents of wire, electronic or oral communications or derivative evidence). Such contents and evidence may be disclosed in testimony under oath or affirmation in any criminal proceeding in any court of this Commonwealth or of another state or of the United States or before any state or Federal grand jury when authorized by a judge who finds on subsequent application that the contents were otherwise intercepted in accordance with the provisions of this subchapter. Such application shall be made as soon as practicable.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.)

§ 5719. Unlawful use or disclosure of existence of order concerning intercepted communication.

Except as specifically authorized pursuant to this subchapter any person who willfully uses or discloses the existence of an order authorizing interception of a wire, electronic or oral communication is guilty of a misdemeanor of the second degree.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.)

§ 5720. Service of copy of order and application before disclosure of intercepted communication in trial, hearing or proceeding.

The contents of any wire, electronic or oral communication intercepted in accordance with the provisions of this subchapter, or evidence derived therefrom, shall not be disclosed in any trial, hearing, or other adversary proceeding before any court of the Commonwealth unless, not less than ten days before the trial, hearing or proceeding the parties to the action have been served with a copy of the order, the accompanying application and the final report under which the interception

was authorized or, in the case of an interception under section 5704 (relating to exceptions to prohibition of interception and disclosure of communications), notice of the fact and nature of the interception. The service of inventory, order, application, and final report required by this section may be waived by the court only where it finds that the service is not feasible and that the parties will not be prejudiced by the failure to make the service.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.)

Suspension by Court Rule. Section 5720 was suspended by Pennsylvania Rule of Juvenile Court Procedure No. 800(14), amended February 12, 2010, insofar as it is inconsistent with Rule 340(B)(6) relating to pre-adjudicatory discovery and inspection.

Section 5720 was suspended by Pennsylvania Rule of Criminal Procedure No. 1101(5), adopted March 1, 2000, insofar as it is inconsistent with Rule No. 573 only insofar as section 5720 may delay disclosure to a defendant seeking discovery under Rule No. 573(B)(1)(g).

§ 5721. Suppression of contents of intercepted communication or derivative evidence (Repealed).

1998 Repeal. Section 5721 was repealed February 18, 1998 (P.L.102, No.19), effective immediately.

§ 5721.1. Evidentiary disclosure of contents of intercepted communication or derivative evidence.

(a) Disclosure in evidence generally.--

(1) Except as provided in paragraph (2), no person shall disclose the contents of any wire, electronic or oral communication, or evidence derived therefrom, in any proceeding in any court, board or agency of this Commonwealth.

(2) Any person who has obtained knowledge of the contents of any wire, electronic or oral communication, or evidence derived therefrom, which is properly subject to disclosure under section 5717 (relating to investigative disclosure or use of contents of wire, electronic or oral communications or derivative evidence) may also disclose such contents or evidence in any matter relating to any criminal, quasi-criminal, forfeiture, administrative enforcement or professional disciplinary proceedings in any court, board or agency of this Commonwealth or of another state or of the United States or before any state or Federal grand jury or investigating grand jury. Once such disclosure has been made, then any person may disclose the contents or evidence in any such proceeding.

(3) Notwithstanding the provisions of paragraph (2), no disclosure in any such proceeding shall be made so long as any order excluding such contents or evidence pursuant to the provisions of subsection (b) is in effect.

(b) Motion to exclude.--Any aggrieved person who is a party to any proceeding in any court, board or agency of this Commonwealth may move to exclude the contents of any wire, electronic or oral communication, or evidence derived therefrom, on any of the following grounds:

(1) Unless intercepted pursuant to an exception set forth in section 5704 (relating to exceptions to prohibition of interception and disclosure of communications), the interception was made without prior procurement of an order of authorization under section 5712 (relating to issuance of order and effect) or an order of approval under section 5713(a) (relating to emergency situations) or 5713.1(b) (relating to emergency hostage and barricade situations).

(2) The order of authorization issued under section 5712 or the order of approval issued under section 5713(a) or 5713.1(b) was not supported by probable cause with respect to the matters set forth in section 5710(a)(1) and (2) (relating to grounds for entry of order).

(3) The order of authorization issued under section 5712 is materially insufficient on its face.

(4) The interception materially deviated from the requirements of the order of authorization.

(5) With respect to interceptions pursuant to section 5704(2), the consent to the interception was coerced by the Commonwealth.

(6) Where required pursuant to section 5704(2)(iv), the interception was made without prior procurement of a court order or without probable cause.

(c) Procedure.--

(1) The motion shall be made in accordance with the applicable rules of procedure governing such proceedings. The court, board or agency, upon the filing of such motion, shall make available to the movant or his counsel the intercepted communication and evidence derived therefrom.

(2) In considering a motion to exclude under subsection (b)(2), both the written application under section 5710(a) and all matters that were presented to the judge under section 5710(b) shall be admissible.

(3) The movant shall bear the burden of proving by a preponderance of the evidence the grounds for exclusion asserted under subsection (b)(3) and (4).

(4) With respect to exclusion claims under subsection (b)(1), (2) and (5), the respondent shall bear the burden of proof by a preponderance of the evidence.

(5) With respect to exclusion claims under subsection (b)(6), the movant shall have the initial burden of demonstrating by a preponderance of the evidence that the interception took place in his home. Once he meets this burden, the burden shall shift to the respondent to demonstrate by a preponderance of the evidence that the interception was in accordance with section 5704(2)(iv).

(6) Evidence shall not be deemed to have been derived from communications excludable under subsection (b) if the respondent can demonstrate by a preponderance of the evidence that the Commonwealth or the respondent had a basis independent of the excluded communication for discovering such evidence or that such evidence would have been inevitably discovered by the Commonwealth or the respondent absent the excluded communication.

(d) Appeal.--In addition to any other right of appeal, the Commonwealth shall have the right to appeal from an order granting a motion to exclude if the official to whom the order authorizing the intercept was granted shall certify to the court that the appeal is not taken for purposes of delay. The appeal shall be taken in accordance with the provisions of Title 42 (relating to judiciary and judicial procedure).

(e) Exclusiveness of remedies and sanctions.--The remedies and sanctions described in this subchapter with respect to the interception of wire, electronic or oral communications are the only judicial remedies and sanctions for nonconstitutional violations of this subchapter involving such communications.

(Feb. 18, 1998, P.L.102, No.19, eff. imd.)

1998 Amendment. Act 19 added section 5721.1.

Cross References. Section 5721.1 is referred to in section 5749 of this title.

§ 5722. Report by issuing or denying judge.

Within 30 days after the expiration of an order or an extension or renewal thereof entered under this subchapter or the denial of an order confirming verbal approval of interception, the issuing or denying judge shall make a report to the Administrative Office of Pennsylvania Courts stating the following:

- (1) That an order, extension or renewal was applied for.
- (2) The kind of order applied for.
- (3) That the order was granted as applied for, was modified, or was denied.
- (4) The period of the interceptions authorized by the order, and the number and duration of any extensions or renewals of the order.
- (5) The offense specified in the order, or extension or renewal of an order.
- (6) The name and official identity of the person making the application and of the investigative or law enforcement officer and agency for whom it was made.
- (7) The character of the facilities from which or the place where the communications were to be intercepted.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.)

§ 5723. Annual reports and records of Attorney General and district attorneys.

(a) Judges.--In addition to reports required to be made by applicants pursuant to Title 18 U.S.C. § 2519, all judges who have issued orders pursuant to this title shall make annual reports on the operation of this chapter to the Administrative Office of Pennsylvania Courts. The reports by the judges shall contain the following information:

- (1) The number of applications made.
- (2) The number of orders issued.
- (3) The effective periods of such orders.
- (4) The number and duration of any renewals thereof.
- (5) The crimes in connection with which the orders were sought.
- (6) The names and official identity of the applicants.
- (7) Such other and further particulars as the Administrative Office of Pennsylvania Courts may require.

(b) Attorney General.--In addition to reports required to be made by applicants pursuant to Title 18 U.S.C. § 2519, the Attorney General shall make annual reports on the operation of this chapter to the Administrative Office of Pennsylvania Courts and to the Judiciary Committees of the Senate and House of Representatives. The reports by the Attorney General shall contain the same information which must be reported pursuant to 18 U.S.C. § 2519(2).

(c) District attorneys.--Each district attorney shall annually provide to the Attorney General all of the foregoing information with respect to all applications authorized by that district attorney on forms prescribed by the Attorney General.

(d) Other reports.--The Chief Justice of the Supreme Court and the Attorney General shall annually report to the Governor and the General Assembly on such aspects of the operation of this chapter as they deem appropriate and make any recommendations they feel desirable as to legislative changes or improvements to effectuate the purposes of this chapter and to assure and protect individual rights.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.)

§ 5724. Training.

The Attorney General and the Commissioner of the Pennsylvania State Police shall establish a course of training in the legal and technical aspects of wiretapping and electronic surveillance as allowed or permitted by this subchapter, shall establish such regulations as they find necessary and proper for such training program and shall establish minimum standards for certification and periodic recertification of Commonwealth investigative or law enforcement officers as eligible to conduct wiretapping or electronic surveillance under this chapter. The Pennsylvania State Police shall charge each investigative or law enforcement officer who enrolls in this training program a reasonable enrollment fee to offset the costs of such training.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.)

Cross References. Section 5724 is referred to in sections 5706, 5710, 5713.1, 5714, 5749 of this title.

§ 5725. Civil action for unlawful interception, disclosure or use of wire, electronic or oral communication.

(a) Cause of action.--Any person whose wire, electronic or oral communication is intercepted, disclosed or used in violation of this chapter shall have a civil cause of action against any person who intercepts, discloses or uses or procures any other person to intercept, disclose or use, such communication; and shall be entitled to recover from any such person:

(1) Actual damages, but not less than liquidated damages computed at the rate of \$100 a day for each day of violation, or \$1,000, whichever is higher.

(2) Punitive damages.

(3) A reasonable attorney's fee and other litigation costs reasonably incurred.

(b) Waiver of sovereign immunity.--To the extent that the Commonwealth and any of its officers, officials or employees would be shielded from liability under this section by the doctrine of sovereign immunity, such immunity is hereby waived for the purposes of this section.

(c) Defense.--It is a defense to an action brought pursuant to subsection (a) that the actor acted in good faith reliance on a court order or the provisions of this chapter.

(July 10, 1981, P.L.228, No.73, eff. 60 days; Oct. 21, 1988, P.L.1000, No.115, eff. imd.)

Cross References. Section 5725 is referred to in section 5713 of this title.

§ 5726. Action for removal from office or employment.

(a) Cause of action.--Any aggrieved person shall have the right to bring an action in Commonwealth Court against any investigative or law enforcement officer, public official or public employee seeking the officer's, official's or employee's removal from office or employment on the grounds that the officer, official or employee has intentionally violated the provisions of this chapter. If the court shall conclude that such officer, official or employee has in fact intentionally violated the provisions of this chapter, the court shall order the dismissal or removal from office of said officer, official or employee.

(b) Defense.--It is a defense to an action brought pursuant to subsection (a) that the actor acted in good faith reliance on a court order or the provisions of this chapter.

(July 10, 1981, P.L.228, No.73, eff. 60 days)

§ 5727. Expiration (Repealed).

1988 Repeal. Section 5727 was repealed October 21, 1988 (P.L.1000, No.115), effective immediately.

§ 5728. Injunction against illegal interception.

Whenever it shall appear that any person is engaged or is about to engage in any act which constitutes or will constitute a felony violation of this subchapter, the Attorney General may initiate a civil action in the Commonwealth Court to enjoin the violation. The court shall proceed as soon as practicable to the hearing and determination of the action and may, at any time before final determination, enter a restraining order or prohibition, or take such other action, as is warranted to prevent a continuing and substantial injury to the Commonwealth or to any person or class of persons for whose protection the action is brought. A proceeding under this section is governed by the Pennsylvania Rules of Civil Procedure, except that, if a criminal complaint has been filed against the respondent, discovery is governed by the Pennsylvania Rules of Criminal Procedure.

(Oct. 21, 1988, P.L.1000, No.115, eff. imd.)

1988 Amendment. Act 115 added section 5728.

SUBCHAPTER C

STORED WIRE AND ELECTRONIC COMMUNICATIONS

AND TRANSACTIONAL RECORDS ACCESS

Sec.

5741. Unlawful access to stored communications.

5742. Disclosure of contents and records.

5743. Requirements for governmental access.

5743.1. Administrative subpoena.

5744. Backup preservation.

5745. Delayed notice.

5746. Cost reimbursement.

5747. Civil action.

5748. Exclusivity of remedies.

5749. Retention of certain records.

Enactment. Subchapter C was added October 21, 1988, P.L.1000, No.115, effective immediately.

§ 5741. Unlawful access to stored communications.

(a) Offense.--Except as provided in subsection (c), it is an offense to obtain, alter or prevent authorized access to a wire or electronic communication while it is in electronic storage by intentionally:

(1) accessing without authorization a facility through which an electronic communication service is provided; or

(2) exceeding the scope of one's authorization to access the facility.

(b) Penalty.--

(1) If the offense is committed for the purpose of commercial advantage, malicious destruction or damage, or private commercial gain, the offender shall be subject to:

(i) a fine of not more than \$250,000 or imprisonment for not more than one year, or both, in the case of a first offense; or

(ii) a fine of not more than \$250,000 or imprisonment for not more than two years, or both, for any subsequent offense.

(2) In any other case, the offender shall be subject to a fine of not more than \$5,000 or imprisonment for not more than six months, or both.

(c) Exceptions.--Subsection (a) of this section does not apply with respect to conduct authorized:

(1) by the person or entity providing a wire or electronic communication service;

(2) by a user of that service with respect to a communication of or intended for that user; or

(3) in section 5743 (relating to requirements for governmental access) or 5744 (relating to backup preservation).

§ 5742. Disclosure of contents and records.

(a) Prohibitions.--Except as provided in subsection (b) and (c):

(1) A person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service:

(i) On behalf of, and received by means of electronic transmission from, or created by means of computer processing of communications received by means of electronic transmission from, a subscriber or customer of the service.

(ii) Solely for the purpose of providing storage or computer processing services to the subscriber or customer, if the provider is not authorized to access the contents of any such communication for the purpose of providing any services other than storage or computer processing.

(2) A person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service:

(i) On behalf of, and received by means of electronic transmission from, or created by means of computer processing of communications received by means of electronic transmission from, a subscriber or customer of the service.

(ii) Solely for the purpose of providing storage or computer processing services to the subscriber or customer, if the provider is not authorized to access the contents of any such communication for the purpose of providing any services other than storage or computer processing.

(3) A person or entity providing an electronic communication service or remote computing service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to, or customer of, the service.

(b) Exceptions.--A person or entity may divulge the contents of a communication:

(1) to an addressee or intended recipient of the communication or an agent of the addressee or intended recipient;

(2) as otherwise authorized in section 5704(1) (relating to prohibition of interception and disclosure of communications), 5708 (relating to order authorizing interception of wire, electronic or oral communications) or 5743 (relating to governmental access);

(3) with the lawful consent of the originator or an addressee or intended recipient of the communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward the communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of the service; or

(6) to a law enforcement agency, if the contents:

(i) Were inadvertently obtained by the service provider.

(ii) Appear to pertain to the commission of a crime.

(c) Exceptions for disclosure of records or other information.--A person or entity may divulge a record or other information pertaining to a subscriber to, or customer of, the service if any of the following paragraphs apply:

(1) A record or other information may be divulged incident to any service or other business operation or to the protection of the rights or property of the provider.

(2) A record or other information may be divulged to any of the following:

- (i) An investigative or law enforcement official as authorized in section 5743.
 - (ii) The subscriber or customer upon request.
 - (iii) A third party, upon receipt from the requester of adequate proof of lawful consent from the subscriber to, or customer of, the service to release the information to the third party.
 - (iv) A party to a legal proceeding, upon receipt from the party of a court order entered under subsection (c.1). This subparagraph does not apply to an investigative or law enforcement official authorized under section 5743.
- (3) Notwithstanding paragraph (2), a record or other information may be divulged as authorized by a Commonwealth statute or as authorized by a Commonwealth regulatory agency with oversight over the person or entity.
- (4) Subject to paragraph (2), a record or other information may be divulged as authorized by Federal law or as authorized by a Federal regulatory agency having oversight over the person or entity.
- (c.1) Order for release of records.--
- (1) An order to divulge a record or other information pertaining to a subscriber or customer under subsection (c)(2)(iv) must be approved by a court presiding over the proceeding in which a party seeks the record or other information.
 - (2) The order may be issued only after the subscriber or customer received notice from the party seeking the record or other information and was given an opportunity to be heard.
 - (3) The court may issue a preliminary order directing the provider to furnish the court with the identity of or contact information for the subscriber or customer if the party does not possess this information.
 - (4) An order for disclosure of a record or other information shall be issued only if the party seeking disclosure demonstrates specific and articulable facts to show that there are reasonable grounds to believe that the record or other information sought is relevant and material to the proceeding. In making its determination, the court shall consider the totality of the circumstances, including input of the subscriber or customer, if any, and the likely impact of the provider.
- (Oct. 9, 2008, P.L.1403, No.111, eff. imd.)

2008 Amendment. Act 111 amended the section heading and subsec. (a) intro. par. and added subsecs. (a)(3), (c) and (c.1).

Cross References. Section 5742 is referred to in section 5746 of this title.

§ 5743. Requirements for governmental access.

- (a) Contents of communications in electronic storage.--Investigative or law enforcement officers may require the disclosure by a provider of communication service of the contents of a communication which is in electronic storage in a communication system for:
 - (1) One hundred eighty days or less only pursuant to a warrant issued under the Pennsylvania Rules of Criminal Procedure.
 - (2) More than 180 days by the means available under subsection (b).
- (b) Contents of communications in a remote computing service.--

(1) Investigative or law enforcement officers may require a provider of remote computing service to disclose the contents of any communication to which this paragraph is made applicable by paragraph (2):

(i) without required notice to the subscriber or customer if the investigative or law enforcement officer obtains a warrant issued under the Pennsylvania Rules of Criminal Procedure; or

(ii) with prior notice from the investigative or law enforcement officer to the subscriber or customer if the investigative or law enforcement officer:

(A) uses an administrative subpoena authorized by a statute or a grand jury subpoena; or

(B) obtains a court order for the disclosure under subsection (d);

except that delayed notice may be given pursuant to section 5745 (relating to delayed notice).

(2) Paragraph (1) is applicable with respect to a communication which is held or maintained on that service:

(i) On behalf of and received by means of electronic transmission from, or created by means of computer processing of communications received by means of electronic transmission from, a subscriber or customer of the remote computing service.

(ii) Solely for the purpose of providing storage or computer processing services to the subscriber or customer, if the provider is not authorized to access the contents of any such communication for the purpose of providing any services other than storage or computer processing.

(c) Records concerning electronic communication service or remote computing service.--

(1) (Deleted by amendment).

(2) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of the service, not including the contents of communications covered by subsection (a) or (b), to an investigative or law enforcement officer only when the investigative or law enforcement officer:

(i) uses an administrative subpoena authorized by a statute or a grand jury subpoena;

(ii) obtains a warrant issued under the Pennsylvania Rules of Criminal Procedure;

(iii) obtains a court order for the disclosure under subsection (d); or

(iv) has the consent of the subscriber or customer to the disclosure.

(3) An investigative or law enforcement officer receiving records or information under paragraph (2) is not required to provide notice to the customer or subscriber.

(d) Requirements for court order.--A court order for disclosure under subsection (b) or (c) shall be issued only if the investigative or law enforcement officer shows that there are specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation. A court issuing an order pursuant to this section, on a motion made promptly by the service provider, may quash or modify the order if the information or records requested are unusually voluminous in nature or compliance with the order would otherwise cause an undue burden on the provider.

(e) No cause of action against a provider disclosing information under this subchapter.--No cause of action shall lie against any provider of wire or electronic communication service, its officers, employees, agents or other specified persons for providing information, facilities or assistance in accordance with the terms of a court order, warrant, subpoena or certification under this subchapter.

(Feb. 18, 1998, P.L.102, No.19, eff. imd.; Oct. 9, 2008, P.L.1403, No.111, eff. imd.; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days)

2012 Amendment. Act 202 amended subsecs. (a) and (b).

2008 Amendment. Act 111 deleted subsec. (c)(1).

1998 Amendment. Act 19 amended subsecs. (d) and (e).

Cross References. Section 5743 is referred to in sections 5712, 5712.1, 5741, 5742, 5743.1, 5744, 5745, 5746, 5747 of this title.

§ 5743.1. Administrative subpoena.

(a) Authorization.--

(1) In an ongoing investigation that monitors or utilizes online services or other means of electronic communication to identify individuals engaged in an offense involving the sexual exploitation or abuse of children, the following shall apply:

(i) The following may issue in writing and cause to be served a subpoena requiring the production and testimony under subparagraph (ii):

(A) The Attorney General.

(B) A deputy attorney general designated in writing by the Attorney General.

(C) A district attorney.

(D) An assistant district attorney designated in writing by a district attorney.

(ii) A subpoena issued under subparagraph (i) may be issued to a provider of electronic communication service or remote computing service:

(A) requiring disclosure under section 5743(c)(2) (relating to requirements for governmental access) of a subscriber or customer's name, address, telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address, which may be relevant to an authorized law enforcement inquiry; or

(B) requiring a custodian of the records of the provider to give testimony or affidavit concerning the production and authentication of the records or information.

(2) A subpoena under this section shall describe the information required to be produced and prescribe a return date within a reasonable period of time within which the information can be assembled and made available.

(3) If summoned to appear under paragraph (1)(ii)(B), a custodian of records subpoenaed under this section shall be paid the same fees and mileage that are paid to witnesses in the courts of this Commonwealth.

(4) Prior to the return date specified in the subpoena, the person or entity subpoenaed may, in the court of common pleas of the county in which the person or entity conducts business or resides, petition for an order modifying or setting aside the subpoena or for a prohibition of disclosure ordered by a court under paragraph (7).

(5) The following shall apply:

(i) Except as provided under subparagraph (ii), if no case or proceeding arises from the production of materials under this section within a reasonable time after the materials are produced, the agency to which the materials were delivered shall, upon written demand made by the person producing the materials, return the materials to the person.

(ii) This paragraph shall not apply if the production required was of copies rather than originals.

(6) A subpoena issued under paragraph (1) may require production as soon as possible.

(7) Without court approval, no person or entity may disclose to any other person or entity, other than to an attorney in order to obtain legal advice, the existence of the subpoena for a period of up to 90 days.

(8) A subpoena issued under this section may not require the production of anything that would be protected from production under the standards applicable to a subpoena for the production of documents issued by a court.

(b) Service.--The following shall apply:

(1) A subpoena issued under this section may be served by any person who is at least 18 years of age and is designated in the subpoena to serve it.

(2) Service upon a natural person may be made by personal delivery of the subpoena to the person.

(3) Service may be made upon a domestic or foreign corporation or upon a partnership or other unincorporated association which is subject to suit under a common name by delivering the subpoena to any of the following:

(i) An officer of the entity.

(ii) A managing or general agent of the entity.

(iii) An agent authorized by appointment or by law to receive service of process in this Commonwealth.

(4) The affidavit of the person serving the subpoena entered on a true copy of the subpoena by the person serving it shall be proof of service.

(c) Enforcement.--The following shall apply:

(1) The Attorney General or a district attorney, or a designee may invoke the aid of a court of common pleas within the following jurisdictions to compel compliance with the subpoena:

(i) The jurisdiction in which the investigation is being conducted.

(ii) The jurisdiction in which the subpoenaed person resides, conducts business or may be found.

(2) The court may issue an order requiring the subpoenaed person to appear before the Attorney General or a district attorney, or a designee to produce records or to give testimony concerning the production and authentication of the records. A failure to obey the order of the court may be

punished by the court as contempt of court. All process may be served in a judicial district of the Commonwealth in which the person may be found.

(d) Immunity from civil liability.--Notwithstanding any State or local law, any person receiving a subpoena under this section who complies in good faith with the subpoena and produces the records sought shall not be liable in a court of this Commonwealth to a subscriber, customer or other person for the production or for the nondisclosure of that production to the subscriber, customer or person.

(e) Annual reports and records of Attorney General and district attorneys.--The following shall apply:

(1) On or before April 1 following the effective date of this section and annually thereafter, including the year following the expiration of this section, the Attorney General shall make a report on the operation of this section to the Judiciary Committee of the Senate and the Judiciary Committee of the House of Representatives. The reports by the Attorney General shall contain the following information for the previous calendar year:

(i) The number of administrative subpoenas issued.

(ii) The number of investigations for which an administrative subpoena was issued.

(iii) The number of court orders issued under subsections (a)(4) and (7) and (c)(2).

(iv) The number of arrests made and the type of charge filed in cases in which an administrative subpoena was issued.

(v) The number of cases in which an administrative subpoena was issued and in which no arrests or prosecutions resulted.

(2) On or before March 1 following the effective date of this section and annually thereafter, including the year following the expiration of this section, each district attorney shall provide to the Attorney General all of the information under paragraph (1) with respect to all administrative subpoenas issued by that district attorney on forms prescribed by the Attorney General.

(f) Expiration.--(Deleted by amendment).

(g) Definitions.--As used in this section, the following words and phrases shall have the meanings given to them in this subsection:

"Offense involving the sexual exploitation or abuse of children." An offense, including an attempt, conspiracy or solicitation involving any of the following, in which a victim is an individual who is under the age of 18 years:

(1) Chapter 29 (relating to kidnapping).

(2) Chapter 30 (relating to human trafficking).

(3) Chapter 31 (relating to sexual offenses).

(4) Section 6312 (relating to sexual abuse of children).

(5) Section 6318 (relating to unlawful contact with minor).

(6) Section 6320 (relating to sexual exploitation of children).

(Oct. 22, 2014, P.L.2522, No.151, eff. 60 days; Dec. 22, 2017, P.L.1218, No.67, eff. imd.)

2014 Amendment. Act 151 added section 5743.1.

§ 5744. Backup preservation.

(a) Backup preservation.--

(1) An investigative or law enforcement officer acting under section 5743(b)(2) (relating to requirements for governmental access) may include in its subpoena or court order a requirement that the service provider to whom the request is directed create a backup copy of the contents of the electronic communications sought in order to preserve those communications. Without notifying the subscriber or customer of the subpoena or court order, the service provider shall create the backup copy as soon as practicable, consistent with its regular business practices, and shall confirm to the investigative or law enforcement officer that the backup copy has been made. The backup copy shall be created within two business days after receipt by the service provider of the subpoena or court order.

(2) Notice to the subscriber or customer shall be made by the investigative or law enforcement officer within three days after receipt of confirmation that the backup copy has been made, unless the notice is delayed pursuant to section 5745(a) (relating to delayed notice).

(3) The service provider shall not destroy or permit the destruction of the backup copy until the later of:

(i) the delivery of the information; or

(ii) the resolution of all proceedings, including appeals of any proceeding, concerning the government's subpoena or court order.

(4) The service provider shall release the backup copy to the requesting investigative or law enforcement officer no sooner than 14 days after the officer's notice to the subscriber or customer if the service provider has not:

(i) received notice from the subscriber or customer that the subscriber or customer has challenged the officer's request; and

(ii) initiated proceedings to challenge the request of the officer.

(5) An investigative or law enforcement officer may seek to require the creation of a backup copy under paragraph (1) if in his sole discretion the officer determines that there is reason to believe that notification under section 5743 of the existence of the subpoena or court order may result in destruction of or tampering with evidence. This determination is not subject to challenge by the subscriber, customer or service provider.

(b) Customer challenges.--

(1) Within 14 days after notice by the investigative or law enforcement officer to the subscriber or customer under subsection (a)(2), the subscriber or customer may file a motion to quash the subpoena or vacate the court order, copies to be served upon the officer and written notice of the challenge to be given to the service provider. A motion to vacate a court order shall be filed in the court which issued the order. A motion to quash a subpoena shall be filed in the court which has authority to enforce the subpoena. The motion or application shall contain an affidavit or sworn statement:

(i) stating that the applicant is a customer of or subscriber to the service from which the contents of electronic communications maintained for the applicant have been sought; and

(ii) containing the applicant's reasons for believing that the records sought are not relevant to a legitimate investigative or law enforcement inquiry or that there has not been substantial compliance with the provisions of this subchapter in some other respect.

(2) Service shall be made under this section upon the investigative or law enforcement officer by delivering or mailing by registered or certified mail a copy of the papers to the person, office or department specified in the notice which the customer has received pursuant to this subchapter. For the purposes of this section, the term "delivery" has the meaning given that term in the Pennsylvania Rules of Civil Procedure.

(3) If the court finds that the customer has complied with paragraphs (1) and (2), the court shall order the investigative or law enforcement officer to file a sworn response, which may be filed in camera if the investigative or law enforcement officer includes in its response the reasons which make in camera review appropriate. If the court is unable to determine the motion or application on the basis of the parties' initial allegations and responses, the court may conduct such additional proceedings as it deems appropriate. All such proceedings shall be completed and the motion or application decided as soon as practicable after the filing of the officer's response.

(4) If the court finds that the applicant is not the subscriber or customer for whom the communications sought by the investigative or law enforcement officer are maintained, or that there is reason to believe that the investigative or law enforcement inquiry is legitimate and that the communications sought are relevant to that inquiry, it shall deny the motion or application and order the process enforced. If the court finds that the applicant is the subscriber or customer for whom the communications sought by the governmental entity are maintained, and that there is not reason to believe that the communications sought are relevant to a legitimate investigative or law enforcement inquiry, or that there has not been substantial compliance with the provisions of this subchapter, it shall order the process quashed.

(5) A court order denying a motion or application under this section shall not be deemed a final order, and no interlocutory appeal may be taken therefrom. The Commonwealth or investigative or law enforcement officer shall have the right to appeal from an order granting a motion or application under this section.

(Feb. 18, 1998, P.L.102, No.19, eff. imd.)

1998 Amendment. Act 19 amended subsec. (b).

Cross References. Section 5744 is referred to in sections 5741, 5746 of this title.

§ 5745. Delayed notice.

(a) Delay of notification.--

(1) An investigative or law enforcement officer acting under section 5743(b) (relating to requirements for governmental access) may:

(i) where a court order is sought, include in the application a request for an order delaying the notification required under section 5743(b) for a period not to exceed 90 days, which request the court shall grant if it determines that there is reason to believe that notification of the existence of the court order may have an adverse result described in paragraph (2); or

(ii) where an administrative subpoena authorized by a statute or a grand jury subpoena is obtained, delay the notification required under section 5743(b) for a period not to exceed 90 days upon the

execution of a written certification of a supervisory official that there is reason to believe that notification of the existence of the subpoena may have an adverse result described in paragraph (2).

(2) An adverse result for the purposes of paragraph (1) is:

- (i) endangering the life or physical safety of an individual;
- (ii) flight from prosecution;
- (iii) destruction of or tampering with evidence;
- (iv) intimidation of potential witnesses; or
- (v) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

(3) The investigative or law enforcement officer shall maintain a true copy of a certification under paragraph (1)(ii).

(4) Extensions of the delay of notification provided for in section 5743 of up to 90 days each may be granted by the court upon application or by certification by a supervisory official in the case of an administrative or grand jury subpoena.

(5) Upon expiration of the period of delay of notification under paragraph (1) or (4), the investigative or law enforcement officer shall serve upon, or deliver by registered or first class mail to, the customer or subscriber a copy of the process or request together with notice which:

- (i) states with reasonable specificity the nature of the investigative or law enforcement inquiry; and
- (ii) informs the customer or subscriber:

(A) that information maintained for the customer or subscriber by the service provider named in the process or request was supplied to or requested by the investigative or law enforcement officer and the date on which the supplying or request took place;

(B) that notification of the customer or subscriber was delayed;

(C) the identity of the investigative or law enforcement officer or the court which made the certification or determination pursuant to which that delay was made; and

(D) which provision of this subchapter authorizes the delay.

(6) As used in this subsection, the term "supervisory official" means the investigative agent or assistant investigative agent in charge, or an equivalent, of an investigative or law enforcement agency's headquarters or regional office, or the chief prosecuting attorney or the first assistant prosecuting attorney, or an equivalent, of a prosecuting attorney's headquarters or regional office.

(b) Preclusion of notice to subject of governmental access.--An investigative or law enforcement officer acting under section 5743, when he is not required to notify the subscriber or customer under section 5743(b)(1), or to the extent that it may delay such notice pursuant to subsection (a), may apply to a court for an order commanding a provider of electronic communication service or remote computing service to whom a warrant, subpoena or court order is directed, not to notify any other person of the existence of the warrant, subpoena or court order for such period as the court deems appropriate. The court shall enter such an order if it determines that there is reason to believe that notification of the existence of the warrant, subpoena or court order will result in:

- (1) endangering the life or physical safety of an individual;
- (2) flight from prosecution;

- (3) destruction of or tampering with evidence;
- (4) intimidation of a potential witness; or
- (5) otherwise seriously jeopardizing an investigation or unduly delaying a trial.

Cross References. Section 5745 is referred to in sections 5743, 5744 of this title.

§ 5746. Cost reimbursement.

(a) Payment.--Except as otherwise provided in subsection (c), an investigative or law enforcement officer obtaining the contents of communications, records or other information under section 5742 (relating to disclosure of contents and records), 5743 (relating to requirements for governmental access) or 5744 (relating to backup preservation) shall reimburse the person or entity assembling or providing the information for such costs as are reasonably necessary and which have been directly incurred in searching for, assembling, reproducing and otherwise providing the information. Reimbursable costs shall include any costs due to necessary disruption of normal operations of any electronic communication service or remote computing service in which the information may be stored.

(b) Amount.--The amount of the reimbursement provided for in subsection (a) shall be as mutually agreed upon by the investigative or law enforcement officer and the person or entity providing the information or, in the absence of agreement, shall be as determined by the court which issued the order for production of the information or the court before which a criminal prosecution relating to the information would be brought, if no court order was issued for production of the information.

(c) Applicability.--The requirement of subsection (a) does not apply with respect to records or other information maintained by a communication common carrier which relates to telephone toll records and telephone listings obtained under section 5743. The court may, however, order reimbursement as described in subsection (a) if the court determines the information required is unusually voluminous or otherwise caused an undue burden on the provider.

(d) Regulations.--The Attorney General shall promulgate regulations to implement this section.

(Oct. 9, 2008, P.L.1403, No.111, eff. imd.; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days)

2012 Amendment. Act 202 added subsec. (d).

2008 Amendment. Act 111 amended subsec. (a).

§ 5747. Civil action.

(a) Cause of action.--Except as provided in subsection 5743(e) (relating to requirements for governmental access), any provider of electronic communication service, subscriber or customer aggrieved by any violation of this subchapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity which engaged in the violation such relief as may be appropriate.

(b) Relief.--In a civil action under this section, appropriate relief shall include:

- (1) such preliminary and other equitable or declaratory relief as may be appropriate;
- (2) damages under subsection (c); and

(3) reasonable attorney fees and other litigation costs reasonably incurred.

(c) Damages.--The court may assess as damages in a civil action under this section the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of \$1,000.

(d) Defense.--A good faith reliance on:

(1) a court warrant or order, a grand jury subpoena, a legislative authorization or a statutory authorization;

(2) a request of an investigative or law enforcement officer under section 5713 (relating to emergency situations); or

(3) a good faith determination that section 5704(10) (relating to exceptions to prohibitions of interception and disclosure of communications) permitted the conduct complained of;

is a complete defense to any civil or criminal action brought under this subchapter or any other law.

(e) Limitation.--A civil action under this section may not be commenced later than two years after the date upon which the claimant first discovered or had a reasonable opportunity to discover the violation.

(Feb. 18, 1998, P.L.102, No.19, eff. imd.; Oct. 22, 2014, P.L.2522, No.151, eff. 60 days)

2014 Amendment. Act 151 amended subsec. (b).

1998 Amendment. Act 19 amended subsec. (d).

§ 5748. Exclusivity of remedies.

The remedies and sanctions described in this subchapter are the only judicial remedies and sanctions for nonconstitutional violations of this subchapter.

§ 5749. Retention of certain records.

(a) Retention.--The commander shall maintain all recordings of oral communications intercepted under section 5704(16) (relating to exceptions to prohibition of interception and disclosure of communications) for a minimum of 31 days after the date of the interception. All recordings made under section 5704(16) shall be recorded over or otherwise destroyed no later than 90 days after the date of the recording unless any of the following apply:

(1) The contents of the recording result in the issuance of a citation. Except as otherwise authorized under this subsection, any recording maintained under this paragraph shall be recorded over or destroyed no later than 90 days after the conclusion of the proceedings related to the citation. All recordings under this paragraph shall be maintained in accordance with section 5714(a) (relating to recording of intercepted communications), except that monitors need not be certified under section 5724 (relating to training).

(2) The commander or a law enforcement officer on the recording believes that the contents of the recording or evidence derived from the recording may be necessary in a proceeding for which disclosure is authorized under section 5717 (relating to investigative disclosure or use of contents of wire, electronic or oral communications or derivative evidence) or 5721.1 (relating to evidentiary disclosure of contents of intercepted communication or derivative evidence) or in a civil proceeding.

All recordings under this paragraph shall be maintained in accordance with section 5714(a), except that monitors need not be certified under section 5724.

(3) A criminal defendant who is a participant on the recording reasonably believes that the recording may be useful for its evidentiary value at some later time in a specific criminal proceeding and, no later than 30 days following the filing of criminal charges, provides written notice to the commander indicating a desire that the recording be maintained. The written notice must specify the date, time and location of the recording; the names of the parties involved; and, if known, the case docket number.

(4) An individual who is a participant on the recording intends to pursue a civil action or has already initiated a civil action and, no later than 30 days after the date of the recording, gives written notice to the commander indicating a desire that the recording be maintained. The written notice must specify the date, time and location of the recording; the names of the parties involved; and, if a civil action has been initiated, the case caption and docket number.

(5) The commander intends to use the recording for training purposes.

(b) Disclosure.--In addition to any disclosure authorized under sections 5717 and 5721.1, any recording maintained:

(1) Under subsection (a)(4) shall be disclosed pursuant to an order of court or as required by the Pennsylvania Rules of Civil Procedure or the Pennsylvania Rules of Evidence; and

(2) Under subsection (a)(5) shall be disclosed consistent with written consent obtained from the law enforcement officer and all participants.

(c) Definitions.--As used in this section, the following words and phrases shall have the meanings given to them in this subsection:

"Commander." The:

(1) commissioner or a designee, if the recording at issue was made by a member of the Pennsylvania State Police; or

(2) chief or a designee of the law enforcement agency which made the recording at issue.

"Law enforcement officer." A member of the Pennsylvania State Police or an individual employed as a police officer who is required to be trained under 53 Pa.C.S. Ch. 21 Subch. D (relating to municipal police education and training).

(June 11, 2002, P.L.370, No.53, eff. imd.)

2002 Amendment. Act 53 added section 5749. Section 3 of Act 53 provided that section 5749 shall apply upon the enactment of a statute providing for the intercepting and recording of oral communications under 18 Pa.C.S. § 5704. Act 52 of 2002, effective June 11, 2002, added provisions relating to the intercepting and recording of oral communications under 18 Pa.C.S. § 5704.

References in Text. The reference to "commissioner" in par. (1) of the def. of "commander" in subsec. (c) probably should have been a reference to Commissioner of the Pennsylvania State Police.

Cross References. Section 5749 is referred to in section 5782 of this title.

SUBCHAPTER D

MOBILE TRACKING DEVICES

Sec.

5761. Mobile tracking devices.

Enactment. Subchapter D was added October 21, 1988, P.L.1000, No.115, effective immediately.

§ 5761. Mobile tracking devices.

(a) Authority to issue.--Orders for the installation and use of mobile tracking devices may be issued by a court of common pleas.

(b) Jurisdiction.--Orders permitted by this section may authorize the use of mobile tracking devices if the device is installed and monitored within this Commonwealth. The court issuing the order must have jurisdiction over the offense under investigation.

(c) Standard for issuance of order.--An order authorizing the use of one or more mobile tracking devices may be issued to an investigative or law enforcement officer by the court of common pleas upon written application. Each application shall be by written affidavit, signed and sworn to or affirmed before the court of common pleas. The affidavit shall:

(1) state the name and department, agency or address of the affiant;

(2) identify the vehicles, containers or items to which, in which or on which the mobile tracking device shall be attached or be placed, and the names of the owners or possessors of the vehicles, containers or items;

(3) state the jurisdictional area in which the vehicles, containers or items are expected to be found; and

(4) provide a statement setting forth all facts and circumstances which provide the applicant with probable cause that criminal activity has been, is or will be in progress and that the use of a mobile tracking device will yield information relevant to the investigation of the criminal activity.

(d) Notice.--The court of common pleas shall be notified in writing within 72 hours of the time the mobile tracking device has been activated in place on or within the vehicles, containers or items.

(e) Term of authorization.--Authorization by the court of common pleas for the use of the mobile tracking device may continue for a period of 90 days from the placement of the device. An extension for an additional 90 days may be granted upon good cause shown.

(f) Removal of device.--Wherever practicable, the mobile tracking device shall be removed after the authorization period expires. If removal is not practicable, monitoring of the mobile tracking device shall cease at the expiration of the authorization order.

(g) Movement of device.--Movement of the tracking device within an area protected by a reasonable expectation of privacy shall not be monitored absent exigent circumstances or an order supported by probable cause that criminal activity has been, is or will be in progress in the protected area and that

the use of a mobile tracking device in the protected area will yield information relevant to the investigation of the criminal activity.

(Oct. 9, 2008, P.L.1403, No.111, eff. imd.; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days)

2012 Amendment. Act 202 amended subsecs. (b) and (c)(4).

SUBCHAPTER E

PEN REGISTERS, TRAP AND TRACE DEVICES

AND TELECOMMUNICATION IDENTIFICATION

INTERCEPTION DEVICES

Sec.

5771. General prohibition on use of certain devices and exception.

5772. Application for an order for use of certain devices.

5773. Issuance of an order for use of certain devices.

5774. Assistance in installation and use of certain devices.

5775. Reports concerning certain devices.

Enactment. Subchapter E was added October 21, 1988, P.L.1000, No.115, effective immediately.

Subchapter Heading. The heading of Subchapter E was amended February 18, 1998, P.L.102, No.19, effective immediately.

Cross References. Subchapter E is referred to in section 5704 of this title.

§ 5771. General prohibition on use of certain devices and exception.

(a) General rule.--Except as provided in this section, no person may install or use a pen register or a trap and trace device or a telecommunication identification interception device without first obtaining a court order under section 5773 (relating to issuance of an order for use of certain devices).

(b) Exception.--The prohibition of subsection (a) does not apply with respect to the use of a pen register, a trap and trace device or a telecommunication identification interception device by a provider of electronic or wire communication service:

(1) relating to the operation, maintenance and testing of a wire or electronic communication service or to the protection of the rights or property of the provider, or to the protection of users of the service from abuse of service or unlawful use of service;

(2) to record the fact that a wire or electronic communication was initiated or completed in order to protect the provider, another provider furnishing service toward the completion of the wire communication or a user of the service from fraudulent, unlawful or abusive use of service; or

(3) with the consent of the user of the service.

(b.1) Limitation.--A government agency authorized to install and use a pen register under this chapter shall use technology reasonably available to it that restricts the recording or decoding of electronic or other impulses to the dialing and signaling information utilized in call processing.

(c) Penalty.--Whoever intentionally and knowingly violates subsection (a) is guilty of a misdemeanor of the third degree.

(Feb. 18, 1998, P.L.102, No.19, eff. imd.)

Cross References. Section 5771 is referred to in section 5773 of this title.

§ 5772. Application for an order for use of certain devices.

(a) Application.--The Attorney General or a deputy attorney general designated in writing by the Attorney General or a district attorney or an assistant district attorney designated in writing by the district attorney may make application for an order or an extension of an order under section 5773 (relating to issuance of an order for use of certain devices) authorizing or approving disclosure of mobile communications tracking information or, if necessary, the production and disclosure of mobile communications tracking information, the installation and use of a pen register, a trap and trace device or a telecommunication identification interception device under this subchapter, in writing, under oath or equivalent affirmation, to a court of common pleas having jurisdiction over the offense under investigation or to any Superior Court judge when an application for an order authorizing interception of communications is or has been made for the targeted telephone or another application for interception under this subchapter has been made involving the same investigation.

(b) Contents of application.--An application under subsection (a) shall include:

(1) The identity and authority of the attorney making the application and the identity of the investigative or law enforcement agency conducting the investigation.

(2) A certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.

(3) An affidavit by an investigative or law enforcement officer which establishes probable cause for the issuance of an order or extension of an order under section 5773.

(Feb. 18, 1998, P.L.102, No.19, eff. imd.; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days)

2012 Amendment. Act 202 amended subsec. (a).

1998 Amendment. Act 19 amended the section heading and subsec. (a).

Cross References. Section 5772 is referred to in section 5773 of this title.

§ 5773. Issuance of an order for use of certain devices.

(a) In general.--Upon an application made under section 5772 (relating to application for an order for use of certain devices), the court shall enter an ex parte order authorizing the disclosure of mobile

communications tracking information, the installation and use of a pen register, a trap and trace device or a telecommunication identification interception device within this Commonwealth if the court finds that there is probable cause to believe that information relevant to an ongoing criminal investigation will be obtained by such installation and use on the targeted telephone. If exigent circumstances exist, the court may verbally authorize the disclosure of mobile communications tracking information, the installation and use of a pen register, a trap and trace device or a telecommunication identification interception device. The written order authorizing the disclosure must be entered within 72 hours of the court's verbal authorization.

(b) Contents of order.--An order issued under this section shall:

(1) Specify:

(i) That there is probable cause to believe that information relevant to an ongoing criminal investigation will be obtained from the targeted telephone.

(ii) The identity, if known, of the person to whom is leased or in whose name is listed the targeted telephone, or, in the case of the use of a telecommunication identification interception device, the identity, if known, of the person or persons using the targeted telephone.

(iii) The identity, if known, of the person who is the subject of the criminal investigation.

(iv) In the use of pen registers and trap and trace devices only, the physical location of the targeted telephone.

(v) A statement of the offense to which the information likely to be obtained by the pen register, trap and trace device or the telecommunication identification interception device relates.

(2) Direct, upon the request of the applicant, the furnishing of information, facilities and technical assistance necessary to accomplish the installation of the pen register under section 5771 (relating to general prohibition on use of certain devices and exception).

(3) In the case of a telecommunication identification interception device, direct that all interceptions be recorded and monitored in accordance with section 5714(a)(1) and (2) and (b) (relating to recording of intercepted communications).

(c) Time period and extensions.--

(1) An order issued under this section shall authorize the installation and use of a pen register, trap and trace device or a telecommunication identification interception device for a period not to exceed 60 days.

(2) Extensions of such an order may be granted but only upon an application for an order under section 5772 and upon the judicial finding required by subsection (a). The period of each extension shall be for a period not to exceed 30 days.

(d) Nondisclosure of existence of pen register, trap and trace device or a telecommunication identification interception device.--An order authorizing or approving the installation and use of a pen register, a trap and trace device or a telecommunication identification interception device shall direct that:

(1) The order be sealed until otherwise ordered by the court.

(2) The person owning or leasing the targeted telephone, or who has been ordered by the court to provide assistance to the applicant, not disclose the existence of the pen register, trap and trace

device or telecommunication identification interception device or the existence of the investigation to the listed subscriber, or to any other person, unless or until otherwise ordered by the court.

(Feb. 18, 1998, P.L.102, No.19, eff. imd.; Oct. 25, 2012, P.L.1634, No.202, eff. 60 days)

2012 Amendment. Act 202 amended subsecs. (a) and (c).

Cross References. Section 5773 is referred to in sections 5771, 5772, 5774 of this title.

§ 5774. Assistance in installation and use of certain devices.

(a) Pen register.--Upon the request of an applicant under this subchapter, a provider of wire or electronic communication service, landlord, custodian or other person shall forthwith provide all information, facilities and technical assistance necessary to accomplish the installation of the pen register unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if assistance is directed by a court order as provided in section 5773(b)(2) (relating to issuance of an order for use of certain devices).

(b) Trap and trace device.--Upon the request of an applicant under this subchapter, a provider of a wire or electronic communication service, landlord, custodian or other person shall install the device forthwith on the appropriate line and shall furnish all additional information, facilities and technical assistance, including installation and operation of the device unobtrusively and with a minimum of interference with the services that the person so ordered by the court accords the party with respect to whom the installation and use is to take place, if installation and assistance are directed by a court order as provided in section 5773. Unless otherwise ordered by the court, the results of the trap and trace device shall be furnished to the applicant designated in the court order at reasonable intervals during regular business hours for the duration of the order.

(c) Compensation.--A provider of wire or electronic communication service, landlord, custodian or other person who furnishes facilities or technical assistance pursuant to this section shall be reasonably compensated for reasonable expenses incurred in providing the facilities and assistance.

(d) No cause of action against a provider disclosing information under this subchapter.--No cause of action shall lie in any court against any provider of a wire or electronic communication service, its officers, employees, agents or other specified persons for providing information, facilities or assistance in accordance with the terms of a court order under this subchapter.

(e) Defense.--A good faith reliance on a court order or a statutory authorization is a complete defense against any civil or criminal action brought under this subchapter or any other law.

(Feb. 18, 1998, P.L.102, No.19, eff. imd.)

§ 5775. Reports concerning certain devices.

(a) Attorney General.--The Attorney General shall annually report to the Administrative Office of Pennsylvania Courts on the number of orders for pen registers, trap and trace devices and telecommunication identification interception devices applied for by investigative or law enforcement agencies of the Commonwealth or its political subdivisions.

(b) District attorney.--Each district attorney shall annually provide to the Attorney General information on the number of orders for pen registers, trap and trace devices and telecommunication identification interception devices applied for on forms prescribed by the Attorney General.

(Feb. 18, 1998, P.L.102, No.19, eff. imd.)

SUBCHAPTER F

MISCELLANEOUS

Sec.

5781. Expiration of chapter.

5782. Regulations.

Enactment. Subchapter F was added October 21, 1988, P.L.1000, No.115, effective immediately.

§ 5781. Expiration of chapter.

This chapter expires December 31, 2023, unless extended by statute.

(Dec. 12, 1994, P.L.1248, No.148, eff. imd.; Feb. 18, 1998, P.L.102, No.19, eff. imd.; Nov. 29, 2004, P.L.1349, No.173, eff. imd.; Oct. 9, 2008, P.L.1403, No.111, eff. imd.; Nov. 27, 2013, P.L.1147, No.102, eff. imd.; July 7, 2017, P.L.304, No.22, eff. 60 days)

§ 5782. Regulations.

The commissioner of the Pennsylvania State Police, in consultation with the Attorney General, shall promulgate regulations consistent with sections 5704(16) (relating to exceptions to prohibition of interception and disclosure of communications) and 5749 (relating to retention of certain records) setting forth procedures to be followed by law enforcement officers regarding the interception, maintenance and destruction of recordings made under section 5704(16).

(June 11, 2002, P.L.370, No.53, eff. imd.)

2002 Amendment. Act 53 added section 5782. Section 3 of Act 53 provided that section 5782 shall apply upon the enactment of a statute providing for the intercepting and recording of oral communications under 18 Pa.C.S. § 5704. Act 52 of 2002, effective June 11, 2002, added provisions relating to the intercepting and recording of oral communications under 18 Pa.C.S. § 5704.

PA ACT 22, 2017

CRIMES CODE (18 PA.C.S.) AND JUDICIAL CODE (42 PA.C.S.) - OMBINUS AMENDMENTS

Act of Jul. 7, 2017, P.L. 304, No. 22

Cl. 18

Session of 2017

No. 2017-22

SB 560

AN ACT

Amending Titles 18 (Crimes and Offenses) and 42 (Judiciary and Judicial Procedure) of the Pennsylvania Consolidated Statutes, in wiretapping and electronic surveillance, further providing for definitions, for exceptions to prohibition of interception and disclosure of communications, for exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices and for expiration of chapter; and providing for recordings by law enforcement officers.

The General Assembly of the Commonwealth of Pennsylvania hereby enacts as follows:

Section 1. The definition of "oral communication" in section 5702 of Title 18 of the Pennsylvania Consolidated Statutes is amended to read:

§ 5702. Definitions.

As used in this chapter, the following words and phrases shall have the meanings given to them in this section unless the context clearly indicates otherwise:

* * *

"Oral communication." Any oral communication uttered by a person possessing an expectation that such communication is not subject to interception under circumstances justifying such expectation. The term does not include [any electronic communication.] the following:

(1) An electronic communication.

(2) A communication made in the presence of a law enforcement officer on official duty who is in uniform or otherwise clearly identifiable as a law enforcement officer and who is using an electronic, mechanical or other device which has been approved under section 5706(b)(4) (relating to exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices) to intercept the communication in the course of law enforcement duties. As used in this paragraph only, "law enforcement officer" means a member of the Pennsylvania State Police, an individual employed as a police officer who holds a current certificate under 53 Pa.C.S. Ch. 21 Subch. D (relating to municipal police education and training), a sheriff or a deputy sheriff.

* * *

Section 2. Sections 5704(13), (14) and (16), 5706(b) and 5781 of Title 18 are amended to read:

§ 5704. Exceptions to prohibition of interception and disclosure of communications.

It shall not be unlawful and no prior court approval shall be required under this chapter for:

* * *

(13) An investigative officer, a law enforcement officer or employees of the Department of Corrections for State correctional facilities to intercept, record, monitor or divulge any [telephone calls] oral communication, electronic communication or wire communication from or to an inmate in a facility under the following conditions:

(i) The Department of Corrections shall adhere to the following procedures and restrictions when intercepting, recording, monitoring or divulging any [telephone calls] oral communication, electronic communication or wire communication from or to an inmate in a State correctional facility as provided for by this paragraph:

(A) Before the implementation of this paragraph, all inmates of the facility shall be notified in writing that, as of the effective date of this paragraph, their [telephone conversations] oral communication, electronic communication or wire communication may be intercepted, recorded, monitored or divulged.

(B) Unless otherwise provided for in this paragraph, after intercepting or recording [a telephone conversation] an oral communication, electronic communication or wire communication, only the superintendent, warden or a designee of the superintendent or warden or other chief administrative official or his or her designee, or law enforcement officers shall have access to that recording.

(C) The contents of an intercepted and recorded [telephone conversation] oral communication, electronic communication or wire communication shall be divulged only as is necessary to safeguard the orderly operation of the facility, in response to a court order or in the prosecution or investigation of any crime.

(ii) So as to safeguard the attorney-client privilege, the Department of Corrections shall not intercept, record, monitor or divulge [any conversation] an oral communication, electronic communication or wire communication between an inmate and an attorney.

(iii) [Persons who are calling in to a facility to speak to an inmate shall be notified that the call may be recorded or monitored.] Persons who are engaging in an oral communication, electronic communication or wire communication with an inmate shall be notified that the communication may be recorded or monitored. Notice may be provided by any means reasonably designed to inform the noninmate party of the recording or monitoring.

(iv) The Department of Corrections shall promulgate guidelines to implement the provisions of this paragraph for State correctional facilities.

(14) An investigative officer, a law enforcement officer or employees of a county correctional facility to intercept, record, monitor or divulge [any telephone calls] an oral communication, electronic communication or wire communication from or to an inmate in a facility under the following conditions:

(i) The county correctional facility shall adhere to the following procedures and restrictions when intercepting, recording, monitoring or divulging [any telephone calls] an oral communication, electronic communication or wire communication from or to an inmate in a county correctional facility as provided for by this paragraph:

(A) Before the implementation of this paragraph, all inmates of the facility shall be notified in writing that, as of the effective date of this paragraph, their [telephone conversations] oral communications, electronic communications or wire communications may be intercepted, recorded, monitored or divulged.

(B) Unless otherwise provided for in this paragraph, after intercepting or recording [a telephone conversation] an oral communication, electronic communication or wire communication, only the superintendent, warden or a designee of the superintendent or warden or other chief administrative official or his or her designee, or law enforcement officers shall have access to that recording.

(C) The contents of an intercepted and recorded [telephone conversation] oral communication, electronic communication or wire communication shall be divulged only as is necessary to safeguard the orderly operation of the facility, in response to a court order or in the prosecution or investigation of any crime.

(ii) So as to safeguard the attorney-client privilege, the county correctional facility shall not intercept, record, monitor or divulge [any conversation] an oral communication, electronic communication or wire communication between an inmate and an attorney.

(iii) [Persons who are calling into a facility to speak to an inmate shall be notified that the call may be recorded or monitored.] Persons who are engaging in an oral communication, electronic communication or wire communication with an inmate shall be notified that the communication may be recorded or monitored. Notice may be provided by any means reasonably designed to inform the noninmate party of the recording or monitoring.

(iv) The superintendent, warden or a designee of the superintendent or warden or other chief administrative official of the county correctional system shall promulgate guidelines to implement the provisions of this paragraph for county correctional facilities.

* * *

[(16) A law enforcement officer, whether or not certified under section 5724 (relating to training), acting in the performance of his official duties to intercept and record an oral communication between individuals in accordance with the following:

(i) At the time of the interception, the oral communication does not occur inside the residence of any of the individuals.

(ii) At the time of the interception, the law enforcement officer:

(A) is in uniform or otherwise clearly identifiable as a law enforcement officer;

(B) is in close proximity to the individuals' oral communication;

(C) is using an electronic, mechanical or other device which has been approved under section 5706(b)(4) (relating to exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices) to intercept the oral communication; and

(D) informs, as soon as reasonably practicable, the individuals identifiably present that he has intercepted and recorded the oral communication.

(iii) As used in this paragraph, the term "law enforcement officer" means a member of the Pennsylvania State Police or an individual employed as a police officer who holds a current certificate under 53 Pa.C.S. Ch. 21 Subch. D (relating to municipal police education and training).]

* * *

§ 5706. Exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices.

* * *

(b) Responsibility.--

(1) Except as provided under paragraph (2), the Attorney General and the district attorney or their designees so designated in writing shall have the sole responsibility to buy, possess and loan any electronic, mechanical or other device which is to be used by investigative or law enforcement officers for purposes of interception as authorized under section 5704(2), (5) and (12) (relating to exceptions to prohibition of interception and disclosure of communications), 5712 (relating to issuance of order and effect), 5713 (relating to emergency situations) or 5713.1 (relating to emergency hostage and barricade situations).

(2) The division or bureau or section of the Pennsylvania State Police responsible for conducting the training in the technical aspects of wiretapping and electronic surveillance as required by section 5724 (relating to training) may buy and possess any electronic, mechanical or other device which is to be used by investigative or law enforcement officers for purposes of interception as authorized under section 5704(2), (5) and (12), 5712, 5713 or 5713.1 for the purpose of training. However, any electronic, mechanical or other device bought or possessed under this provision may be loaned to or used by investigative or law enforcement officers for purposes of interception as authorized under section 5704(2), (5) and (12), 5712, 5713 or 5713.1 only upon written approval by the Attorney General or a deputy attorney general designated in writing by the Attorney General or the district attorney or an assistant district attorney designated in writing by the district attorney of the county wherein the suspected criminal activity has been, is or is about to occur.

(3) With the permission of the Attorney General or a district attorney who has designated any supervising law enforcement officer for purposes of interceptions as authorized under section 5713.1, the law enforcement agency which employs the supervising law enforcement officer may buy, possess, loan or borrow any electronic, mechanical or other device which is to be used by investigative or law enforcement officers at the direction of the supervising law enforcement officer solely for the purpose of interception as authorized under sections 5704(12) and 5713.1.

(4) The Pennsylvania State Police shall annually establish equipment standards for any electronic, mechanical or other device which is to be used by law enforcement officers for purposes of [interception as authorized under section 5704(16).] recording a communication under circumstances within paragraph (2) of the definition of "oral communication" in section 5702 (relating to definitions). The equipment standards shall be published annually in the Pennsylvania Bulletin.

(5) The Pennsylvania State Police shall annually establish and publish standards in the Pennsylvania Bulletin for the secure onsite and off-site storage of an audio recording made in accordance with paragraph (4) or any accompanying video recording. The standards shall comply with the Federal Bureau of Investigation's Criminal Justice Information Services (CJIS) Security Policy.

(6) A vendor to law enforcement agencies which stores data related to audio recordings and video recordings shall, at a minimum, comply with the standards set forth by the Pennsylvania State Police under paragraphs (4) and (5). Law enforcement agencies under contract with a vendor for the storage of data before the effective date of this paragraph shall comply with paragraphs (4) and (5) and this paragraph upon expiration or renewal of the contract.

§ 5781. Expiration of chapter.

This chapter expires December 31, [2018] 2023, unless extended by statute.

Section 3. Title 42 is amended by adding a chapter to read:

CHAPTER 67A

RECORDINGS BY LAW ENFORCEMENT OFFICERS

Sec.

67A01. Definitions.

67A02. Scope of chapter.

67A03. Requests for law enforcement audio recordings or video recordings.

67A04. Law enforcement review.

67A05. Procedure.

67A06. Petition for judicial review.

67A07. Audio recording or video recording policies.

67A08. Construction.

67A09. Applicability.

§ 67A01. Definitions.

The following words and phrases when used in this chapter shall have the meanings given to them in this section unless the context clearly indicates otherwise:

"Confidential information." Any of the following:

- (1) The identity of a confidential source.
- (2) The identity of a suspect or witness to whom confidentiality has been assured.
- (3) Information made confidential by law or court order.

"Information pertaining to an investigation." An audio recording or video recording which contains any of the following:

- (1) Complaints or depictions of criminal conduct, including all actions or statements made before or after the criminal conduct that are part of or relate to the same incident or occurrence.
- (2) Upon disclosure, information that would:
 - (i) reveal the institution, progress or result of a criminal investigation;
 - (ii) deprive an individual of the right to a fair trial or an impartial adjudication;
 - (iii) impair the ability of the Attorney General, a district attorney or a law enforcement officer to locate a defendant or codefendant;
 - (iv) hinder the ability of the Attorney General, a district attorney or a law enforcement officer to secure an arrest, prosecution or conviction; or
 - (v) endanger the life or physical safety of an individual.
- (3) Upon disclosure, information that would:
 - (i) Reveal the institution, progress or result of an agency investigation.
 - (ii) Deprive a person of the right to an impartial administrative adjudication.
 - (iii) Constitute an unwarranted invasion of privacy.
 - (iv) Hinder an agency's ability to secure an administrative or civil sanction.
 - (v) Endanger the life or physical safety of an individual.

"Law enforcement agency." The Office of Attorney General, a district attorney's office or an agency that employs a law enforcement officer.

"Law enforcement officer." An officer of the United States, the Commonwealth or a political subdivision thereof, another state or political subdivision thereof or who is empowered by law to conduct investigations of or to make arrests for offenses enumerated in this chapter or an equivalent

crime in another jurisdiction, a sheriff or deputy sheriff and any attorney authorized by law to prosecute or participate in the prosecution of the offense.

"Victim." An individual who was subjected to an act that was committed by another individual, including a juvenile, which constitutes any of the following:

(1) An offense committed under any of the following:

(i) The act of April 14, 1972 (P.L.233, No.64), known as The Controlled Substance, Drug, Device and Cosmetic Act.

(ii) 18 Pa.C.S. (relating to crimes and offenses).

(iii) 30 Pa.C.S. § 5502 (relating to operating watercraft under influence of alcohol or controlled substance).

(iv) 30 Pa.C.S. § 5502.1 (relating to homicide by watercraft while operating under influence).

(v) 75 Pa.C.S. § 3732 (relating to homicide by vehicle).

(vi) 75 Pa.C.S. § 3735 (relating to homicide by vehicle while driving under influence).

(vii) 75 Pa.C.S. § 3735.1 (relating to aggravated assault by vehicle while driving under the influence).

(viii) 75 Pa.C.S. § 3742 (relating to accidents involving death or personal injury).

(ix) 75 Pa.C.S. Ch. 38 (relating to driving after imbibing alcohol or utilizing drugs).

(x) Any other Federal or State law.

(2) An offense similar to an offense listed under paragraph (1) committed outside of this Commonwealth.

(3) An offense which would constitute grounds for the issuance of relief under Chapter 62A (relating to protection of victims of sexual violence or intimidation) or 23 Pa.C.S. Ch. 61 (relating to protection from abuse).

(4) An offense against a resident of this Commonwealth which is an act of international terrorism.

"Victim information." Information that would disclose the identity or jeopardize the safety of a victim.

§ 67A02. Scope of chapter.

(a) Exemption.--The provisions of this chapter, and not the act of February 14, 2008 (P.L.6, No.3), known as the Right-to-Know Law, shall apply to any audio recording or video recording made by a law enforcement agency.

(b) Limitation.--Nothing in this chapter nor the Right-to-Know Law shall establish a right to production of an audio recording or video recording made inside a facility owned or operated by a law enforcement agency or to any communications between or within law enforcement agencies concerning an audio or video recording.

§ 67A03. Requests for law enforcement audio recordings or video recordings.

The following shall apply:

(1) An individual who requests an audio recording or video recording made by a law enforcement agency shall, within 60 days of the date when the audio recording or video recording was made, serve

a written request to the individual who is designated as the open-records officer for the law enforcement agency under section 502 of the act of February 14, 2008 (P.L.6, No.3), known as the Right-to-Know Law. Service is effective upon receipt of the written request by the open-records officer from personal delivery or certified mail with proof of service.

(2) The request under paragraph (1) shall specify with particularity the incident or event that is the subject of the audio recording or video recording, including the date, time and location of the incident or event.

(3) The request shall include a statement describing the requester's relationship to the incident or event that is the subject of the audio or video recording.

(4) If the incident or event that is the subject of the audio recording or video recording occurred inside a residence, the request shall identify each individual who was present at the time of the audio recording or video recording unless not known and not reasonably ascertainable.

§ 67A04. Law enforcement review.

(a) Determination.--Except as provided in this section, if a law enforcement agency determines that an audio recording or video recording contains potential evidence in a criminal matter, information pertaining to an investigation or a matter in which a criminal charge has been filed, confidential information or victim information and the reasonable redaction of the audio or video recording would not safeguard potential evidence, information pertaining to an investigation, confidential information or victim information, the law enforcement agency shall deny the request in writing. The written denial shall state that reasonable redaction of the audio recording or video recording will not safeguard potential evidence, information pertaining to an investigation, confidential information or victim information.

(b) Agreement.--A law enforcement agency may enter into a memorandum of understanding with the Attorney General or the district attorney with jurisdiction to:

(1) ensure consultation regarding the reviewing of audio recordings or video recordings in order to make a determination; or

(2) require the Attorney General or district attorney with jurisdiction to issue a denial permitted under subsection (a).

§ 67A05. Procedure.

(a) Disclosure.--A law enforcement agency that receives a request under section 67A03 (relating to requests for law enforcement audio recordings or video recordings) for an audio recording or video recording shall provide the audio recording or video recording or identify in writing the basis for denying the request within 30 days of receiving the request, unless the requester and law enforcement agency agree to a longer time period. If an agreement under section 67A04(b)(2) (relating to law enforcement review) is in effect between the law enforcement agency and the Attorney General or district attorney with jurisdiction, then an agreement to a longer time period must be between the requester and the Attorney General or district attorney with jurisdiction.

(b) Denials by operation of law.--The request under section 67A03 shall be deemed denied by operation of law if the law enforcement agency does not provide the audio recording or video recording to the requester or explain why the request is denied within the time period specified or agreed to under subsection (a).

(c) Preservation.--A law enforcement agency that has received a request for an audio recording or video recording shall preserve the unaltered audio recording or video recording that has been requested for no less than the time periods provided in this chapter for service of and responses to written requests for the production of the audio recording or video recording and any period within which a petition for judicial review is allowable or pending.

(d) Fees.--A law enforcement agency may establish reasonable fees relating to the costs incurred to disclose audio recordings or video recordings. The fees shall be paid by the requesting party at the time of disclosure of the audio recording or video recording.

(e) Construction.--Nothing in this section shall be construed to prohibit a law enforcement agency from redacting an audio recording or video recording in order to protect potential evidence in a criminal matter, information pertaining to an investigation, confidential information or victim information.

§ 67A06. Petition for judicial review.

(a) Petition.--

(1) If a request under section 67A03 (relating to requests for law enforcement audio recordings or video recordings) is denied, the requester may file a petition for judicial review in the court of common pleas with jurisdiction within 30 days of the date of denial.

(2) The respondent to a petition filed under this section shall be the entity that denied the request for the audio recording or video recording under section 67A05(a) (relating to procedure) unless the request is denied under section 67A05(b), in which case the law enforcement agency that created the audio recording or video recording shall be the respondent.

(b) Duties of petitioner.--A petitioner under this section shall have the following duties:

(1) The petitioner shall pay a filing fee of \$125.

(2) If the incident or event that is the subject of the request occurred inside a residence, the petitioner shall certify that notice of the petition has been served or that service was attempted on each individual who was present at the time of the audio recording or video recording and on the owner and occupant of the residence. Notice shall not be required under this paragraph if the identity of an individual present or the location is unknown and not reasonably ascertainable by the petitioner. Service shall be effective upon receipt from personal delivery or certified mail with proof of service.

(3) The petitioner shall include with the petition a copy of the written request under section 67A03 that was served on the law enforcement agency and any written responses to the request that were received.

(4) The petitioner shall serve the petition on the open-records officer of the respondent within five days of the date that the petitioner files the petition with the court of common pleas with jurisdiction, and service shall be effective upon receipt by the open-records officer for personal delivery or certified mail with proof of service.

(c) Intervention as matter of right.--If not a respondent, a prosecuting attorney with jurisdiction may intervene in the action as a matter of right.

(d) Summary dismissal.--It shall be grounds for summary dismissal of a petition filed under this section if:

(1) the request to the law enforcement agency under section 67A03 or the filing of the petition under subsection (a) is untimely;

(2) the request to the law enforcement agency failed to describe with sufficient particularity the incident or event that is the subject of the audio recording or video recording, including the date, time and location of the incident or event; or

(3) the petitioner has not complied with the requirements of subsection (b)(1), (2), (3) and (4).

(e) Approval.--A court of common pleas with jurisdiction may grant a petition under this section, in whole or in part, and order the disclosure of the audio recording or video recording only if the court determines that the petitioner has established all of the following by a preponderance of the evidence:

(1) The request was not denied under section 67A04 (relating to law enforcement review) or the request was denied under section 67A04 and the court of common pleas with jurisdiction determines that the denial was arbitrary and capricious.

(2) The public interest in disclosure of the audio recording or video recording or the interest of the petitioner outweighs the interests of the Commonwealth, the law enforcement agency or an individual's interest in nondisclosure. In making a determination under this paragraph, the court of common pleas may consider the public's interest in understanding how law enforcement officers interact with the public, the interests of crime victims, law enforcement and others with respect to safety and privacy and the resources available to review and disclose the audio recording or video recording.

§ 67A07. Audio recording or video recording policies.

(a) Policies.--A municipal law enforcement agency or sheriff that makes audio recordings or video recordings of communications under circumstances within paragraph (2) of the definition of "oral communication" in 18 Pa.C.S. § 5702 (relating to definitions) shall comply with the guidelines established under 18 Pa.C.S. § 5706(b)(4), (5) and (6) (relating to exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices) and shall establish written policies, which shall be public, for the following:

(1) The training of law enforcement officers authorized to make audio recordings or video recordings.

(2) The time periods when an electronic, mechanical or other device shall be in operation to make audio recordings or video recordings.

(3) The proper use, maintenance and storage of the electronic, mechanical or other device to make audio recordings or video recordings, including equipment inspections and audits and procedures to address malfunctioning equipment.

(4) The information collected from audio recordings or video recordings, including the information's storage, accessibility and retrieval.

(5) Electronic records retention.

(6) The use of facial recognition software or programs.

(7) A statement that a violation of the agency's policy subjects the violator to the agency's disciplinary policy.

(8) Supervisory responsibilities.

(b) Pennsylvania Commission on Crime and Delinquency.--The Pennsylvania Commission on Crime and Delinquency is authorized to condition funding or a grant related to the implementation, use, maintenance or storage of body-worn cameras or recordings from body-worn cameras on the following:

- (1) Requiring the grantee to have protocols, guidelines or written policies related to the implementation, use, maintenance or storage of body-worn cameras.
- (2) Requiring that such protocols, guidelines or written policies are publicly accessible, including being retrievable on a municipal website.
- (3) Ensuring that the protocols, guidelines or written policies substantially comply with applicable recommendations by the commission.

§ 67A08. Construction.

The following shall apply:

- (1) Nothing in this chapter shall be construed to alter the responsibilities of parties to any criminal or civil litigation to exchange information in accordance with applicable rules of procedure.
- (2) Nothing in this chapter shall be construed to preclude a prosecuting attorney with jurisdiction or a law enforcement agency from disclosing an audio recording or video recording in the absence of a written request or beyond the time periods stated in this chapter.
- (3) The prosecuting attorney with jurisdiction must agree in writing to the disclosure by a law enforcement agency if the prosecuting attorney determines that:
 - (i) the audio recording or video recording contains potential evidence in a criminal matter, information pertaining to an investigation, confidential information or victim information; and
 - (ii) reasonable redaction of the audio recording or video recording will not safeguard the potential evidence, information pertaining to an investigation, confidential information or victim information.

§ 67A09. Applicability.

Nothing in this chapter shall apply to an audio recording or video recording that is otherwise prohibited or protected from disclosure under any other Federal or State law.

Section 4. This act shall take effect in 60 days.

APPROVED--The 7th day of July, A.D. 2017.TOM WOLF

Pennsylvania Bulletins

NOTICES

STATE POLICE

Mobile Video Recording System Equipment Standards and Approved Mobile Video Recording Systems

[Saturday, August 29, 2015]

The State Police, under the authority of 18 Pa.C.S. §§ 5704(16)(ii)(C) and 5706(b)(4) (relating to exceptions to prohibition of interception and disclosure of communications; and exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices), has approved, until the next comprehensive list is published, subject to interim amendment, the following equipment standards for electronic, mechanical or other devices (mobile video recording systems) which may be used by law enforcement officers for the purpose of interception as authorized under 18 Pa.C.S. § 5704(16). Mobile video recording systems must consist of the following components.

Vehicle-Mounted Mobile Video Recording Systems Overview

Vehicle-Mounted Mobile Video Recording Systems shall be defined as those which are permanently mounted in vehicles requiring the operator to possess a Class A, B, C or M Pennsylvania Driver's License, as defined in 75 Pa.C.S. § 1504 (relating to classes of licenses). The design of the vehicle-mounted mobile video recording system must use technology, which includes a camera, monitor, wireless voice transmitter/receiver and a recording device with a secure protective enclosure for the recording device, electronics and receiver components. The vehicle-mounted mobile video recording system must be powered from a standard automotive vehicle operating at 11 to 16.5 volts DC, negative ground. Current drain on the vehicle electrical system must not exceed 3.0 amps. The system must operate over the following temperature range: -4°F to 130°F (-20°C to 55°C).

Camera

The camera component must have the following features:

- A. Auto focus and auto iris.
- B. Flexible mounting bracket to allow manual aiming controls.
- C. Auto zoom (automatic zoom in then back out to normal distance).
- D. Minimum sensitivity rating of 2.0 lux.
- E. Minimum horizontal resolution of 330 TV lines.

Monitor

The monitor component must have the following features:

- A. Controls for picture brightness and contrast.
- B. Capability of being switched off without affecting recording.
- C. A speaker and volume control system.

The monitor must be capable of displaying:

- A. Camera image (live).
- B. Previously recorded information from the recording unit.
- C. Date and time.
- D. Recording index indicator.
- E. In-car/wireless microphone activity indicator.

Wireless Voice Transmitter/Receiver

The wireless voice transmitter/receiver must have the following features:

- A. Battery powered wireless microphone transmitter.
- B. Antenna incorporated into the microphone.
- C. A plug-in connector and a clothing clip on the microphone.
- D. FCC: Type acceptable under 47 CFR Part 74, Subpart H (relating to low power auxiliary stations).
- E. The transmitter must not have recording capabilities.
- F. The wireless audio system must be equipped with either a digital coded squelch or a PL tone squelch circuit to prevent accidental activation of the record mode in stray RF fields.

Recording Device

The recording device must be capable of recording onto tape or other comparable media and have the following features:

- A. Enclosed in a secure housing protected from physical damage and unauthorized access.
- B. Capable of recording audio and video for a minimum of 2 continuous hours.
- C. Record time/date, recording index and remote microphone indicator.
- D. Record over protection.

System Control

The control console must be mounted within easy reach of the operator. The control console must contain the controls to operate the following functions:

- A. Power.
- B. Record.

C. Play.

D. Rewind.

E. Fast forward.

F. Pause.

The State Police, under the authority of 18 Pa.C.S. §§ 5704(16)(ii)(C) and 5706(b)(4), has approved for use, until the next comprehensive list is published, subject to interim amendment, the following list of approved vehicle-mounted mobile video recording systems which meet the minimum equipment standards in this notice.

System 7, Mobile Vision, Boonton, NJ
Eyewitness, Kustom Signals, Lenexa, KS
Patrol Cam, Kustom Signals, Lenexa, KS
Motor Eye, Kustom Signals, Lenexa, KS
Cruise Cam, The Cruisers Division, Mamaroneck, NY
I Track, McCoy's Law Line, Chanute, KS
Docucam, MPH Industries Inc., Owensboro, KY
Digital Mobile Witness, T.A.W. Security Concepts, Wheat Ridge, CO
Car Camera AV360, A.S.S.I.S.T. International, New York, NY
OPV, On Patrol Video, Ontario, OH
Gemini System, Decatur Electronics, Decatur, IL
SVS-500, ID Control Inc., Derry, NH
PAVE System, Video Systems Plus, Bryan, TX
InCharge 5555, Applied Integration, Tucson, AZ
VMDT, Coban Research and Technology, Houston, TX
Mobile Vision 5-C Video Recording System, Mobile Vision, Boonton, NJ
Stalker Vision VHS, Applied Concepts Inc., Plano, TX
Stalker Vision HI8, Applied Concepts Inc., Plano, TX
Digital Eyewitness, Kustom Signals, Lenexa, KS
Eagleye Model 800, Eagleye Technologies, Inc., Rome, GA
Eagleye Model 900, Eagleye Technologies, Inc., Rome, GA
Flashback, Mobile Vision, Inc., Boonton, NJ
Digital Patroller, Integrian, Morrisville, NC
Digital Patroller 2 Mobile Video Recorder, Digital Safety Technologies, Morrisville, NC
Panasonic Arbitrator 360 Mobile Video Recorder, Panasonic Corporation of North America, Secaucus, NJ
WatchGuard DV-1 Mobile Video Recorder, WatchGuard Video, Plano, TX
EDGE Mobile Video Recorder, Coban Technologies, Stafford, TX
DVM-500 Plus and DVM-750 Mobile Video Recorders, Digital Ally, Overland Park, KS
WatchGuard 4RE Mobile Video Recorder, WatchGuard, Plano, TX
DigitalPatroller 3 Mobile Video Recorder, Digital Safety Technologies, Morrisville, NC
X22 Mobile Video Recorder, RDR Mobility, Flemington, NJ
Data 911 Mobile Digital Video System, Data 911 Mobile, Computer Systems, Alameda, CA
DVM-400 Mobile Video Recorder, Digital Ally, Lenexa, KS
DVB-777 Mobile Video Recorder, Digital Ally, Lenexa, KS

MVX1000 Mobile Video Recorder, Motorola Solutions Inc., Schaumburg, IL
DVM800, Digital Ally, Lenexa, KS
DVR-704, PRO-VISION, Byron Center, MI
1200-PA SD2+2, 10-8 Digital Video Evidence Solutions, Fayetteville, TN

Non-Vehicle-Mounted Mobile Video Recording Systems Overview

Non-Vehicle-Mounted Mobile Video Recording Systems shall be defined as those which are not permanently mounted in vehicles requiring the operator to possess a Class A, B, C or M Pennsylvania Driver's License, as defined in 75 Pa.C.S. § 1504. Non-vehicle-mounted mobile video recording systems shall include, but not be limited to, mobile video recorders worn on or about a law enforcement officer's person or affixed to an all-terrain vehicle, bicycle or horse.

The design of the non-vehicle-mounted mobile video recording system must use technology which includes a camera with date/time stamp capability, a microphone and a recording device, enclosed in secure protective enclosure(s). It may also contain controls, a monitor, GPS, wireless transceiver components and other electronic components. The non-vehicle-mounted mobile video recording system must be powered from a battery internal to the protective enclosure and must be weatherproof. The internal battery may be integral to the unit or removable. It is permissible to have an external battery to extend the operating life of the system. The non-vehicle-mounted mobile video recording system must have a minimum record time of 2 continuous hours. The system must operate over the following temperature range: -4°F to 122°F (-20°C to 50°C).

Camera

The camera component must have the following features:

- A. Must be color video.
- B. Minimum of 640 x 480 pixel resolution.
- C. Minimum of 68 degrees field of view.
- D. Minimum of 30 frames per second.
- E. Minimum sensitivity rating of 3.4 lux or lower. Unit may use Infrared LED illumination to obtain lower than 3.4 lux equivalent.
- F. Camera does not have to be in the same enclosure as the recorder. Can be connected to the recorder either by cable or wireless connection.

Recorder

The recorder component must have the following features:

- A. Enclosed in a secure housing protected from physical damage.
- B. Date/time recording index.
- C. Minimum of 4 gigabytes of nonremovable solid state memory, 4 gigabytes

removable media or a combination of both removable and nonremovable memory.

D. Editing and record-over protection.

System Control

The system must:

A. Be capable of recording audio and video simultaneously, but may also provide the user with the option to record video only or audio only.

B. Provide the user with the capability to manually turn the power on and off as necessary.

Wireless Link (optional)

The unit may use a wireless link to connect the camera to the recorder, recorder to another device, combination camera/recorder to another device or be used to download the evidence. The wireless link must have the following features:

A. Use a secure digital connection.

B. Wireless link can be used to play back a locally stored event on the recorder or store the media to a remote location such as secure Cloud storage.

C. FCC Type acceptable under 47 CFR Part 15 (relating to radio frequency devices).

The State Police, under the authority of 18 Pa.C.S. §§ 5704(16)(ii)(C) and 5706(b)(4), has approved for use, until the next comprehensive list is published, subject to interim amendment, the following list of approved non-vehicle-mounted mobile video recording systems which meet the minimum equipment standards in this notice.

AXON Body Mobile Video Recorder, TASER, Scottsdale, AZ

AXON Flex Mobile Video Recorder, TASER, Scottsdale, AZ

FIRST Vu, Digital Ally, Lenexa, KS

FIRST Vu HD, Digital Ally, Lenexa, KS

LE 3 Mobile Video Recorder, VIEVU, Seattle, WA

BODYCAM BC-100, PRO-VISION, Byron Center, MI

Prima Facie, Safety Vision LLC, Houston, TX

Conducted Electrical Weapons with integrated Mobile Video Recording Systems

Notwithstanding any other standards or requirements contained in this notice, conducted electrical weapons equipped with integrated mobile video recording systems are only required to meet the following minimum specifications:

A. Be capable of recording audio and video simultaneously, but may also provide the user with the option to record video only or audio only.

B. Be capable of having the audio video recording extracted from the conducted electrical weapon by means of downloading or by the removal of a media storage device.

Nothing in this notice prohibits the authorized use of a mobile video recording system that is not specifically identified if the mobile video recording system otherwise meets the equipment standards in this notice. Moreover, mobile video recording systems that are not activated to record oral communications or do not have an oral recording capability need not meet the equipment standards in this notice. Manufacturers may submit equipment to be added to the list by contacting the State Police, Bureau of Patrol (Bureau). New units must be in full commercial production. No prototype models will be considered. Proof of current sales and delivery of the specified equipment over the past 6 months must be provided, in writing, referencing current customers with contacts and phone numbers for verification. When requested by the Bureau, the manufacturer/bidder must furnish a complete working system installed in a vehicle for inspection within 30 days.

Comments, suggestions or questions should be directed to the State Police, Bureau of Patrol, Department Headquarters, 1800 Elmerton Avenue, Harrisburg, PA 17110.

COLONEL TYREE C. BLOCKER,
Acting Commissioner

[Pa.B. Doc. No. 15-1613. Filed for public inspection August 28, 2015, 9:00 a.m.]

NOTICES

STATE POLICE

Mobile Video Recording System Equipment Standards and Approved Mobile Video Recording Systems

[45 Pa.B. 5772]
[Saturday, September 19, 2015]

The State Police, under 18 Pa.C.S. §§ 5704(16)(ii)(C) and 5706(b)(4) (relating to exceptions to prohibition of interception and disclosure of communications; and exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices), published at 45 Pa.B. 5482 (August 29, 2015) a notice of Mobile Video Recording System Equipment Standards and Approved Mobile Video Recording Systems for use until the next comprehensive list is published.

As an addendum to the listing of approved mobile video recording systems published at 45 Pa.B. 5482, the State Police, under the authority cited previously, has approved for use, until the next comprehensive list is published, subject to interim amendment, the following additional mobile video recording system, which meets the minimum equipment standards published at 45 Pa.B. 5482:

Non-Vehicle-Mounted Mobile Video Recording System:

VISTA, Watchguard Video, Allen, TX

Comments, suggestions or questions should be directed to the State Police, Bureau of Patrol, Department Headquarters, 1800 Elmerton Avenue, Harrisburg, PA 17110.

COLONEL TYREE C. BLOCKER,
Acting Commissioner

[Pa.B. Doc. No. 15-1718. Filed for public inspection September 18, 2015, 9:00 a.m.]

NOTICES

STATE POLICE

Mobile Video Recording System Equipment Standards and Approved Mobile Video Recording Systems

[46 Pa.B. 116]
[Saturday, January 2, 2016]

The State Police, under 18 Pa.C.S. §§ 5704(16)(ii)(C) and 5706(b)(4) (relating to exceptions to prohibition of interception and disclosure of communications; and exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices), published at 45 Pa.B. 5482 (August 29, 2015) a notice of Mobile Video Recording System Equipment Standards and Approved Mobile Video Recording Systems for use until the next comprehensive list is published.

As an addendum to the listing of approved mobile video recording systems published at 45 Pa.B. 5482, the State Police, under the authority cited previously, has approved for use, until the next comprehensive list is published, subject to interim amendment, the following additional mobile video recording systems, which meet the minimum equipment standards published at 45 Pa.B. 5482:

Non-Vehicle-Mounted Mobile Video Recording Systems:

CopTrax SmartGLASS, CopTrax, Plano, TX

WOLFCOM Vision, WOLFCOM Enterprises, Hollywood, CA

Comments, suggestions or questions should be directed to the State Police, Bureau of Patrol, Department Headquarters, 1800 Elmerton Avenue, Harrisburg, PA 17110.

COLONEL TYREE C. BLOCKER,
Commissioner

NOTICES

STATE POLICE

Law Enforcement Officer Camera System Data Handling Requirements

[47 Pa.B. 7815]
[Saturday, December 23, 2017]

The State Police, under 18 Pa.C.S. § 5706(b)(4) and (5) (relating to exceptions to prohibitions in possession, sale, distribution, manufacture or advertisement of electronic, mechanical or other devices), publishes this notice of the minimum standards to comply with the Federal Bureau of Investigation (FBI), Criminal Justice Information Service (CJIS), Security Policy, Version 5.6 (CJIS Policy) and 18 Pa.C.S. §§ 9101—9183 (relating to Criminal History Record Information Act) (CHRIA).

Camera systems used by criminal justice agencies in accordance with paragraph (2) of the definition of "oral communication" in 18 Pa.C.S. § 5702 (relating to definitions) have a high probability of capturing criminal justice information (CJI) and personally identifiable information. For these reasons, audio or video data, or both, (herein called "data") captured by these camera systems are considered CJI and shall be handled in accordance with the CJIS Policy, CHRIA and Commonwealth Law Enforcement Assistance Network (CLEAN) regulations. *Reference:* CJIS Policy; 18 Pa.C.S. § 9106(b) (3) (relating to information in central repository or automated systems); and the CLEAN regulations, State Police, CLEAN Administrative Section.

Criminal justice agencies shall request approval from the State Police, CLEAN Administrative Section, prior to storing any data onsite or offsite. This approval will ensure compliance with CJIS Policy requirements and CHRIA. In accordance with 18 Pa.C.S. § 5706(b)(5), the following are the minimum requirements that must be met for any storage of an audio recording made in accordance with 18 Pa.C.S. § 5706(b)(4), or any accompanying video recording:

A. Camera system

1. While worn by the officer, a camera system shall be considered a physically secure location.
2. Upon removal from the officer's body, the camera system shall be maintained in a physically secure location in accordance with CJIS Policy standards.

3. If a camera system is located in a criminal justice conveyance, it shall be considered located in a physically secure location. If the camera or hard drive is removed from the criminal justice conveyance, it shall conform with the CJIS Policy. A criminal justice conveyance is any enclosed mobile vehicle used for the purposes of criminal justice activities with the capability to comply, during operational periods. A physically secure location, as stated in section 5.9.1 of the CJIS Policy (relating to physically secure location) is as follows:

A physically secure location is a facility, a criminal justice conveyance, or an area, room or a group of rooms within a facility, with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control, State Identification Bureau control, FBI CJIS security addendum, or a combination thereof, and shall consist of the following:

- a. Security perimeter—area that is posted, separated and secured.
- b. Physical access authorizations—list of authorized personnel.
- c. Physical access control—control all physical access points (AP).
- d. Access control for transmission medium—control physical access to information systems, distribution and lines.
- e. Access control for display medium—not visible to unauthorized personnel.
- f. Monitoring physical access—monitor and respond to security incidents.
- g. Visitor control—authenticate and escort visitors.
- h. The agency shall authorize and control information system-related items entering and exiting the physically secure location (delivery and removal).

B. Data transfer or downloading the data

1. If accomplished through a wireless connection, agencies shall meet the CJIS Policy requirements, as stated in section 5.13.1.1 (relating to 802.11 wireless protocols).

Note: Wired Equivalent Privacy and Wi-Fi Protected Access cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for Federal Information Processing Standard (FIPS) 140-2 and may not be used.

2. Agencies shall implement the following controls for all agency-managed wireless APs with access to an agency's network that processes unencrypted CJI:

- a. Perform validation testing to ensure rogue APs do not exist in the 802.11 wireless local area network and to fully understand the wireless network security posture.
- b. Maintain a complete inventory of all APs and 802.11 wireless devices.

- c. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
- d. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.
- e. Enable user authentication and encryption mechanisms for the management interface of the AP.
- f. Ensure that all APs have strong administrative passwords and ensure all passwords are changed in accordance with section 5.6.2.1 of the CJIS Policy (relating to standard authenticators), as follows:
 - (1) Be a minimum length of eight characters on all systems.
 - (2) Not be a dictionary word or proper name.
 - (3) Not be the same as the user ID.
 - (4) Expire within a maximum of 90 calendar days.
 - (5) Not be identical to the previous ten passwords.
 - (6) Not be transmitted in the clear, outside the secure location.
 - (7) Not be displayed when entered.
- g. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.
- h. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, and the like) or services.
- i. Enable all security features of the wireless product, including the cryptographic authentication, firewall and other available privacy features.
- j. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
- k. Ensure that the ad-hoc mode has been disabled.
- l. Disable all nonessential management protocols on the APs.
- m. Ensure all management access and authentication occurs through FIPS-compliant secure protocols (for example, SFTP, HTTPS, SNMP over TLS, and the like). Disable non-FIPS-compliant secure access to the management interface.

n. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum, logs shall be reviewed monthly.

o. Insulate, virtually (for example, virtual local area network and access control lists) or physically (for example, firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.

p. When disposing of APs that will no longer be used by the agency, clear AP configuration to prevent disclosure of network configuration, keys, passwords, and the like.

3. If the data is manually downloaded by an individual or retained outside of a physically secure location, it will need to be encrypted at rest and in transit, per sections 5.10.1.2.1 and 5.10.1.2.2 of the CJIS Policy (relating to encryption for CJI in transit; and encryption for CJI at rest).

C. Storage of the data

Storage of data on location, if considered a physically secure location, shall be treated the same as all CJI at the location. Storage offsite, or in the cloud, shall meet all the requirements of the CJIS Policy for encryption while in transit and at rest, if applicable. If encryption is not used at rest, any person with access to the data or systems storing the data shall be properly vetted with a fingerprint-based background check and Security Awareness Training, and required agreements shall be maintained.

1. As stated in section 5.10.1.2.1 of the CJIS Policy:

When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit strength to protect CJI.

2. As stated in section 5.10.1.2.2 of the CJIS Policy:

When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption. When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.

D. Reviewing and release of data

1. Data from the camera system shall only be reviewed by authorized personnel; that is, personnel that have been cleared through a fingerprint-based background check, have received Security Awareness Training and have signed the appropriate agreements, if applicable. If required, the Management Control Agreement for local government IT, or The Security Addendum for private contractors, shall be completed and on file.

2. Prior to the release of data from the camera system, the data shall be reviewed and any areas containing CJI shall be removed or rendered unintelligible. Any data received from CLEAN or the National Crime Information Center in either video or audio format, or both, shall be removed or rendered unintelligible prior to release to any unauthorized or unintended personnel.

E. Retention of data

Data shall be stored for 60 days unless needed for prosecution, courts, litigation, appeals or other operational needs.

F. Destruction of data

The data, or the data storage devices that are to be destroyed, shall be destroyed in compliance with the CJIS Policy, and a written destruction procedure that complies with the CJIS Policy shall be maintained at the agency. As stated in section 5.8.3 of the CJIS Policy (relating to digital media sanitization and disposal):

The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

COLONEL TYREE C. BLOCKER,
Commissioner

[Pa.B. Doc. No. 17-2155. Filed for public inspection December 22, 2017, 9:00 a.m.]

PCCD Policy

These policy recommendations have been adopted by the Pennsylvania Commission on Crime and Delinquency (PCCD) in accordance with §67A07 of the Act 22 of 2017, which requires PCCD to condition grant funding related to body worn cameras (BWCs) on the following:

(b) The Pennsylvania Commission on Crime and Delinquency is authorized to condition funding or a grant related to the implementation, use, maintenance or storage of body worn cameras or recordings from body worn cameras on the following:

(b)(1) Requiring the grantee to have a protocol, guidelines or written policies related to the implementation, use, maintenance or storage of body worn cameras.

(b)(2) Requiring that such a protocol, guidelines or written policies are publicly accessible, including being retrievable on a municipal website.

(b)(3) Ensuring that the protocol, guidelines, or written policies substantially comply with applicable recommendations by the Commission.

According to these provisions, in order to be eligible for BWC related grant funding, agencies must issue a written, publicly accessible policy prior to implementing a BWC program that meets or exceeds these policy recommendations. Each of these agencies shall make a reasonable effort to comply with these recommendations. In some cases, agencies are at liberty to meet the policy recommendations in a manner that best suits their unique local needs and organizational structure.

PCCD strongly encourages agencies to develop their BWC policies and protocols in accordance with best practices with input from their Criminal Justice Advisory Board (CJAB) and community stakeholders, such as local victim service providers, community police review boards, and other interested parties.

The Body-Worn Camera Policy and Implementation Program (BWC PIP) aims to support the implementation of body-worn camera programs in law enforcement agencies across the country. The BWC PIP addresses the development and implementation of policies and practices for effective program adoption, and includes factors such as the purchase, deployment, and maintenance of camera systems and equipment; data storage and access; and privacy considerations. While BWC equipment may be purchased, award recipients must first demonstrate a commitment and adherence to a strong BWC policy framework, including comprehensive policy adoption and requisite training.

As a guideline, in months one through six of the grant, agencies will be expected to review and develop policies and training programs. As every agency faces different challenges and applicable laws, BJA will not set standards for policies and procedures. Policies must conform to applicable federal, state, local, and tribal laws. The Training and Technical Assistance (TTA) provider will work with the agency to document and validate the policy development process. The TTA provider must make recommendations to BJA that an agency has met the policy development requirements before BJA releases any award funds to the agency prior to implementation. During months seven through twenty-four, the grantees will be expected to deploy BWCs, continue their training efforts, and collect outcome measures to assess their BWC implementation.

Agencies are required to work with the BJA-funded BWC training and technical assistance (TTA) provider as part of the policy development process prior to the release of funds for implementation. Agencies must demonstrate appropriate policy development and internal law enforcement adoption prior to full funding being released by BJA for BWC procurement and implementation. Please note that PCCD funding is reimbursable (funds must be obligated or expended prior to PCCD's release of funds). Please use the following link for more information on TTA: <http://www.bwcetta.com/training-and-technical-assistance>

Responses to PCPA's RFI on Police Body Worn Cameras

On January 8, 2019, PCPA issued a Request for Information about police body worn cameras, also known as non-vehicle-mounted mobile video recording systems according to Pennsylvania's regulations.

Vendors were asked to provide at least the following information:

- How does your non-vehicle-mounted mobile video recording systems and technology meet Pennsylvania's published requirements?
- Have you submitted your non-vehicle-mounted mobile video recording systems to the Pennsylvania State Police for certification?
- Is your non-vehicle-mounted mobile video recording systems already certified by the Pennsylvania State Police?
- Are you offering a storage solution?
- Will you offer storage solutions bundled (no line item distinction) with the cost of each camera purchased?
- How does your storage solution meet Pennsylvania's published requirements?
- List the products and services that are already available on State Contract or PA CoStars.
- List your costs for products and services you offer.
- Will you offer a discount of those prices if multiple police departments group together to buy your products and services?

As of February 18, 2019, the Following vendors responded:

- Axon Enterprise, Inc. (Axon)
- Digital Ally, Inc
- Kustom Signals, Inc
- Municipal Emergency Services, Inc.
- WatchGuard, Inc.

Here is How they each answered those questions.

How does your non-vehicle-mounted mobile video recording systems and technology meet Pennsylvania's published requirements?

Vendor	Response
Axon Enterprise, Inc.	List all the specifications that meet or exceed Pa's requirements
Digital Ally, Inc	Digital Ally's FirstVu HD Body Camera is in full compliance with the State of Pennsylvania's published requirements
Kustom Signals, Inc	Kustom Signals' Eyewitness Vantage meets the following published requirements.
Municipal Emergency Services, Inc	In all cases our products meet and exceed current requirements
WatchGuard, Inc	Lists all the specifications that meet or exceed Pa's requirements.

Have you submitted your non-vehicle-mounted mobile video recording systems to the Pennsylvania State Police for certification?

Vendor	Response
Axon Enterprise, Inc.	Yes, the Axon Body 2 and the Axon Flex 2 cameras are in the list of PA State List of certified body-worn cameras
Digital Ally, Inc	Yes, Digital Ally submitted our FirstVu HD Body Camera system to the Pennsylvania State Police, and it was certified on the Pennsylvania State Bulletin.
Kustom Signals, Inc	Kustom Signals has not yet submitted the Eyewitness Vantage for certification but would be very interested in doing so.
Municipal Emergency Services, Inc	Not yet, however we would appreciate the opportunity, and are confident that with our technology, we be certified.
WatchGuard, Inc	Yes

Is your non-vehicle-mounted mobile video recording systems already certified by the Pennsylvania State Police?

Vendor	Response
Axon Enterprise, Inc.	Yes, Axon Body 2 and Axon Flex 2 cameras are certified by the Pennsylvania State Police.
Digital Ally, Inc	Yes, Digital Ally submitted our FirstVu HD Body Camera system to the Pennsylvania State Police, and it was certified on the Pennsylvania State Bulletin.
Kustom Signals, Inc	Kustom Signals Eyewitness Vantage is not already certified by the Pennsylvania State Police
Municipal Emergency Services, Inc	Not yet, however we would appreciate the opportunity, and are confident that with our technology, we be certified.
WatchGuard, Inc	Yes, we are currently under contract with the Pennsylvania State Police

Are you offering a storage solution?

Vendor	Response
Axon Enterprise, Inc.	Yes, Axon's Body-worn cameras are paired with Axon Evidence (Evidence.com), a robust end-to-end solution that not only allows agencies to store data, it also enables new workflows for managing and sharing that data securely from anywhere
Digital Ally, Inc	Yes, Digital Ally is offering both a cloud storage solution and a local on-premise (on-site server-based) storage solution.
Kustom Signals, Inc	The Eyewitness Data Vault (EDV) file management system allows agencies to easily transfer, store and manage video files recorded by Kustom Signals' in-car video and/or body-worn video systems. EDV provides quick and easy file searching, easy playback and file duplication. Storage can be expanded locally. EDV is also compatible with Active Directory and LDAP to allow established log in credentials to be used. Kustom Signals does not currently offer a cloud-based solution.
Municipal Emergency Services, Inc	Yes, we offer multiple storage solutions as our Hydra Digital Evidence Management Software is storage agnostic. We have NAS storage which is outlined in our pricing scenario, however we would welcome the opportunity to deploy our software with your existing IT Storage infrastructure if there is potential cost savings. We offer Wasabi CJIS Certified Hot Cloud
WatchGuard, Inc	Yes. We are offering three different storage solutions, On-Premise, Hybrid, and Cloud, which are all outlined within our provided solution.

Will you offer storage solutions bundled (no line item distinction) with the cost of each camera purchased?

Vendor	Response
Axon Enterprise, Inc.	Evidence.com is licensed on a per user basis; a license is required for each camera. As a hosted application, there is no limit to the number of users your agency can add, should administrators or staff without body cameras need access to the system.
Digital Ally, Inc	Yes, Digital Ally is offering bundled storage solutions. We offer three different VuVault.com unlimited cloud storage solution bundles: the Ultimate Plan with 1-year of data retention, the Pro Plan with 180-day data retention, and the Basic Plan with 90-day data retention. Bundled discounts for the FirstVu HD Body Camera and cloud storage are listed in the Unit Price table
Kustom Signals, Inc	Kustom Signals can bundle the cost of the storage unit into the cost of each camera purchased if more than 30 cameras are purchased together
Municipal Emergency Services, Inc	Yes, we offer bundled storage solutions tied to camera cost if it is required. Many vendors have done this, and the pricing scheme ends up as misleading and many times more expensive than unbundled. We will offer both as required by specific RFP's
WatchGuard, Inc	This option is negotiable, if desired

How does your storage solution meet Pennsylvania's published requirements?

Vendor	Response
Axon Enterprise, Inc.	Evidence.com is a robust end-to-end solution that not only allows agencies to store data, it also enables new workflows for managing and sharing that data securely – from anywhere
Digital Ally, Inc	Digital Ally's VuVault.com cloud storage solution and VuVault Software storage solution are both compliant with Pennsylvania's published requirements.
Kustom Signals, Inc	Kustom Signals storage solution supports agency compliance with 18 Pa.C.S. § 5706(b)(5), the following minimum requirements that must be met for any storage of an audio recording made in accordance with 18 Pa.C.S. § 5706(b)(4), or any accompanying video recording
Municipal Emergency Services, Inc	Yes, please see below, we offer Wasabi CJIS Certified Hot Cloud Storage
WatchGuard, Inc	Each of the offered storage solutions has been designed to meet CJIS standards

Will you offer a discount of those prices if multiple police departments group together to buy your products and services?

Vendor	Response
Axon Enterprise, Inc.	Axon may consider a discount from our standard prices. Discounts will be negotiated at the individual agency level.
Digital Ally, Inc	Yes, Digital Ally will offer volume discount pricing on the Retail Unit Price List above for any State of Pennsylvania Police Department and Law Enforcement agency. Our PA COSTARS Contract and State of Pennsylvania Contract both offer our best pricing and already include a State-wide anticipated volume discount. Police Departments and Law Enforcement agencies may contact Digital Ally at any time for a quote.
Kustom Signals, Inc	Yes, Kustom Signals offers discounts on quantity purchases with the following breakdown of 6-14 units and 15+ and will honor these price breakdowns if multiple departments would like to make group purchases.
Municipal Emergency Services, Inc	Yes, we would be happy to offer discounts for multiple agencies are for larger quantities.
WatchGuard, Inc	We are open to negotiations.

List the products and services that are already available on State Contract or PA CoStars

Vendor	Response (see proposal for details)
Axon Enterprise, Inc.	Yes
Digital Ally, Inc	Yes
Kustom Signals, Inc	Yes
Municipal Emergency Services, Inc	No
WatchGuard, Inc	Yes

List your costs for products and services you offer.

Please see the individual responses by each vendor.

January 25, 2019

Pennsylvania Chiefs of Police Association
3905 N. Front Street
Harrisburg, PA 17110
Police Body Worn Cameras RFI

Digital Ally, Inc. is pleased to participate in the Pennsylvania Chiefs of Police Association's Request for Information for **Police Body Worn Cameras**. We believe Digital Ally, Inc. has the experience to successfully furnish State of Pennsylvania Police Departments with a high quality Body Camera system and Digital Evidence Management System.

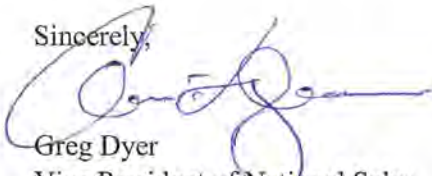
With patented automatic activation (Patents 9253452; 8781292), and an ever improving video storage model, the State of Pennsylvania Police Departments will be a step ahead in the future of policing with the assistance of our Body Camera and Digital Evidence Management solution. We believe automatic activation will prove to be an increasingly important feature to consider with the current climate of policing. With automatic activation, an officer need not worry about activating a body camera during a high-stress incident. It can instead automatically be done for him or her.

Digital Ally has been successfully involved in the implementation of a wide variety of digital In-Car Camera and Body Camera Solutions from the State Police level to the National Law Enforcement Agency level, as well as county and municipal agencies throughout the United States. Digital Ally's products are proudly represented in all 50 states and over 90 countries. We have over 50,000 camera units deployed throughout the world, while working with over 6,000 Law Enforcement agencies. Our sole business is dedicated to designing, manufacturing, and selling quality, leading edge digital video systems and related products. We understand the work, dedication, and commitments involved, and stand ready to perform all the tasks required within the scheduled time period.

With our current and future technology, no-nonsense Advanced Exchange Warranty program, and unparalleled customer service, Digital Ally will prove to be an invaluable team member with the Pennsylvania Chiefs of Police Association's Police Body Worn Cameras project.

Thank you for the opportunity to submit our information. If any of the State of Pennsylvania Police Departments would like to evaluate our systems or would like a detailed in-person presentation, we would be pleased to provide it at their convenience. Choosing a vendor for a Body Camera program is a big decision. Digital Ally stands ready to assist the State of Pennsylvania Police Departments in making this project an unparalleled success.

Sincerely,



Greg Dyer
Vice President of National Sales
Digital Ally, Inc.
9705 Loiret Blvd.
Lenexa, KS 66219
800-440-4947 (Toll-Free)

Table of Contents

Information Requested for Police Body Worn Cameras.....	3
PA COSTARS Contract Number 012-042 Price List.....	4
State of Pennsylvania Contract Number 4400014648 Price List.....	5
Digital Ally’s Retail Unit Price List.....	6
Contact Information for Digital Ally, Inc.	11
Product Information Packet for FirstVu HD Body Camera and Services	12
Product Information Packet for VuSchools Body Camera System for School Resource Officers.....	28

Information Requested

- **How does your non-vehicle-mounted mobile video recording systems and technology meet Pennsylvania's published requirements?**

Digital Ally's FirstVu HD Body Camera (non-vehicle-mounted mobile video recording system and technology) is in full compliance with the State of Pennsylvania's published requirements. Our FirstVu HD Body Camera has been approved on the Pennsylvania State Bulletin and has been tested by the Pennsylvania State Police.

- **Have you submitted your non-vehicle-mounted mobile video recording systems to the Pennsylvania State Police for certification?**

Yes, Digital Ally submitted our FirstVu HD Body Camera system (non-vehicle-mounted mobile video recording system) to the Pennsylvania State Police and it was certified on the Pennsylvania State Bulletin.

- **Is your non-vehicle-mounted mobile video recording systems already certified by the Pennsylvania State Police?**

Yes, Digital Ally's FirstVu HD Body Camera system (non-vehicle-mounted mobile video recording system) is already certified on the Pennsylvania State Bulletin by the Pennsylvania State Police.

- **Are you offering a storage solution?**

Yes, Digital Ally is offering both a cloud storage solution and a local on-premise (on-site server-based) storage solution.

- **Will you offer storage solutions bundled (no line item distinction) with the cost of each camera purchased?**

Yes, Digital Ally is offering bundled storage solutions. We offer three different VuVault.com unlimited cloud storage solution bundles: the Ultimate Plan with 1-year of data retention, the Pro Plan with 180-day data retention, and the Basic Plan with 90-day data retention. Bundled discounts for the FirstVu HD Body Camera and cloud storage are listed in the Unit Price table below.

The following bundled pricing discounts are available with our cloud storage solution bundles:

- 1) VuVault.com Ultimate Plan and FirstVu HD Body Camera Solution
 - 3-year or 5-year contract includes the FirstVu HD Body Camera at no cost
 - 1-year contract includes 50% discount on FirstVu HD Body Camera
- 2) VuVault.com Pro Plan and FirstVu HD Body Camera Solution
 - 5-year contract includes 83% discount on FirstVu HD Body Camera
 - 3-year contract includes 66% discount on FirstVu HD Body Camera
 - 1-year contract includes 39% discount on FirstVu HD Body Camera
- 3) VuVault.com Basic Plan and FirstVu HD Body Camera Solution
 - 5-year contract includes 83% discount on FirstVu HD Body Camera
 - 3-year contract includes 66% discount on FirstVu HD Body Camera
 - 1-year contract includes 33% discount on FirstVu HD Body Camera

We also offer hardware bundled pricing when our FirstVu HD Body Camera is purchased in conjunction with our In-Car Camera System, VuLink automatic activation device, and local on-premise VuVault Software solution. Our patented VuLink provides hands-free automatic activation for both the FirstVu HD Body Camera and our In-Car Camera Systems.

Volume discount pricing is also available when the hardware is purchased in large volume in conjunction with our local on-premise VuVault Software solution.

- **How does your storage solution meet Pennsylvania's published requirements?**

Digital Ally's VuVault.com cloud storage solution and VuVault Software storage solution are both compliant with Pennsylvania's published requirements.

- **List the products and services that are already available on State Contract or PA CoStars.**

Digital Ally products and services that are available on the PA COSTARS Contract Number 012-042:

<i>Product Description</i>	<i>PA COSTARS Contract Price</i>
<i>HARDWARE:</i>	
FirstVu HD Body Camera	\$505.75
Docking Station for Body Cameras	\$2,545.75
VuLink Automatic Recording Activation	\$420.75
<i>SOFTWARE AND CLOUD STORAGE OPTIONS:</i>	
VuVault Standalone Software	\$505.75
VuVault Server Software	\$1,295.00
VuVault Enterprise Software	\$1,525.75
VuVault.com Ultimate Plan	\$708 per user, per year
VuVault.com Pro Plan	\$348 per user, per year
VuVault.com Basic Plan	\$192 per user, per year
<i>EXTENDED WARRANTY:</i>	
Extended Warranty for FirstVu HD Body Camera	\$199 per device, per year
Extended Warranty for the Docking Station	\$495 per device, per year
Additional Warranty for VuLink (One Year only)	\$99 per device
<i>SERVICES AND INSTALLATION:</i>	
VuLink Installation (when installed with DVM system)	\$50 per vehicle
VuLink Installation (when installed standalone or as an add-on to existing system)	\$150 per vehicle
Professional Services Turn-Key Setup: includes onsite training, travel costs, configuration, deployment, implementation, body camera and 12-bay docking station installation	\$2,700.00

Digital Ally products and services that are available on the State of Pennsylvania Contract Number 4400014648:

<i>Product Description</i>	<i>State of Pennsylvania Contract Price</i>
<i>HARDWARE:</i>	
FirstVu HD Body Camera	\$505.75
Docking Station for Body Cameras	\$2,545.75
VuLink Automatic Recording Activation	\$420.75
<i>SOFTWARE AND CLOUD STORAGE OPTIONS:</i>	
VuVault Standalone Software	\$505.75
VuVault Server Software	\$1,295.00
VuVault Enterprise Software	\$1,525.75
VuVault.com Ultimate Plan	\$708 per user, per year
VuVault.com Pro Plan	\$348 per user, per year
VuVault.com Basic Plan	\$192 per user, per year
Administrator License for VuVault.com	\$99 per admin, per year
Share Portal for VuVault Software solution	\$399 per user, per year
Cloud Drive: Includes Block of 100GB of storage (per year)	\$63 per year
<i>EXTENDED WARRANTY:</i>	
Extended Warranty for FirstVu HD Body Camera	\$129 per device, per year
Extended Warranty for the Docking Station	\$495 per device, per year
Additional Warranty for VuLink (One Year only)	\$99 per device
<i>SERVICES AND INSTALLATION:</i>	
VuLink Installation (when installed with DVM system)	\$50 per vehicle
VuLink Installation (when installed standalone or as an add-on to existing system)	\$150 per vehicle
Professional Services Turn-Key Setup: includes onsite training, travel costs, configuration, deployment, implementation, body camera and 12-bay docking station installation	\$2,700.00
<i>BODY CAMERAS AND CLOUD STORAGE FOR SCHOOL RESOURCE OFFICERS AND SCHOOLS:</i>	
VuSchools Body Camera Kit with FirstVu HD Body Camera, Mini-Dock, choice of mounts, and cloud storage: 1 to 500 units (per Account, per Month)	\$65.80 per account, per month
VuSchools Body Camera Kit with FirstVu HD Body Camera, Mini-Dock, choice of mounts, and cloud storage: 501 to 1,000 units (per Account, per Month)	\$59.22 per account, per month
VuSchools Body Camera Kit with FirstVu HD Body Camera, Mini-Dock, choice of mounts, and cloud storage: 1,001 to 2,000 units (per Account, per Month)	\$55.31 per account, per month

- **List your costs for products and services you offer.**

Digital Ally's Retail Unit Price List for our products and services begins on the following page:

Digital Ally, Inc. FirstVu HD Body Camera System Unit Price List

To:

Pennsylvania Chiefs of Police Association
3905 N. Front Street
Harrisburg, PA 17110
Police Body Worn Cameras RFI

Date	Sales Representative	Payment Terms
1/25/2019	John Saunders Direct: 913.232.5348 Main Phone: 800-440-4947 Email: John.Saunders@digitalallyinc.com	Net30

Qty	Description	Unit Price
Body Camera System Hardware:		
1	FirstVu HD Body Camera Kit when VuVault.com Ultimate Plan 3-year or 5-year contract is purchased: includes Advanced Exchange Warranty for full term of contract (with 3-year or 5-year cloud contract)	Included at no cost
1	FirstVu HD Body Camera Kit when VuVault.com Ultimate Plan 1-year contract is purchased: includes Advanced Exchange Warranty for full term of contract (with 1-year cloud contract)	\$299.00
1	FirstVu HD Body Camera Kit when VuVault.com Pro Plan 5-year contract is purchased: includes Advanced Exchange Warranty for full term of contract (with 5-year cloud contract)	\$99.00
1	FirstVu HD Body Camera Kit when VuVault.com Pro Plan 3-year contract is purchased: includes Advanced Exchange Warranty for full term of contract (with 3-year cloud contract)	\$199.00

1	FirstVu HD Body Camera Kit when VuVault.com Pro Plan 1-year contract is purchased: includes Advanced Exchange Warranty for full term of contract (with 1-year cloud contract)	\$359.00
1	FirstVu HD Body Camera Kit when VuVault.com Basic Plan 5-year contract is purchased: includes Advanced Exchange Warranty for full term of contract (with 5-year cloud contract)	\$99.00
1	FirstVu HD Body Camera Kit when VuVault.com Basic Plan 3-year contract is purchased: includes Advanced Exchange Warranty for full term of contract (with 3-year cloud contract)	\$199.00
1	FirstVu HD Body Camera Kit when VuVault.com Basic Plan 1-year contract is purchased: includes Advanced Exchange Warranty for full term of contract (with 1-year cloud contract)	\$399.00
1	FirstVu HD Body Camera Kit includes 1-year Advanced Exchange Warranty (when purchased separately)	\$595.00
1	12-bay Docking Station for the FirstVu HD Body Camera includes 1-year Advanced Exchange Warranty	\$2,995.00

Qty	Description	Unit Price
Cloud Storage Option:		
1	VuVault.com Cloud Ultimate Plan for the FirstVu HD: with Unlimited Storage and 1-year data retention at \$59/user/month with 1-year, 3-year, or 5-year contract Includes: Unlimited Data Storage for 1 Year Advanced Exchange Warranty on hardware for full term of contract Full Software Access & Redaction Share Portal & Case Management	\$708.00 per user per year
1	VuVault.com Cloud Pro Plan for the FirstVu HD: with Unlimited Storage and 180-day data retention at \$29/user/month with 1-year, 3-year, or 5-year contract Includes: Unlimited Data Storage for 180 days Advanced Exchange Warranty on hardware for full term of Contract Full Software Access & Redaction Share Portal & Case Management	\$348.00 per user per year
1	VuVault.com Cloud Basic Plan for the FirstVu HD: with Unlimited Storage and 90-day data retention at \$16/user/month with 1-year, 3-year, or 5-year contract Includes: Unlimited Data Storage for 90 days Advanced Exchange Warranty on hardware for full term of Contract Full Software Access & Redaction Share Portal & Case Management	\$192.00 per user per year
1	VuVault.com Administrator License	\$99 per Admin per year

Qty	Description	Unit Price
Software with On-Premise Storage Option:		
1	VuVault Standalone Software	\$695.00
1	VuVault Server Software	\$1,695.00
1	VuVault Enterprise Server Software	\$1,895.00
Qty	Description	Unit Price
Services:		
1	Activation Fee	\$30.00 per device
1	Professional Services Turn-Key Setup <ul style="list-style-type: none"> • Onsite Product Setup & Configuration • Dedicated Project Manager • Weekly Project Planning Meetings • Best Practices & Implementation Planning Session • Statement of Work • System Administrator & Troubleshooting Training Session • Digital Ally Instructor Training • Implementation Document Packet • Go Live - End User Training • Go Live - Follow-up Review Session 	\$2,000.00 per location
Qty	Description	Unit Price
Optional Products and Services:		
1	VuLink: Patented body camera and in-car camera Automatic Activation Device includes 1-year Advanced Exchange Warranty	\$395.00 per vehicle
1	VuLink and Sync Cable: Patented body camera and in-car camera Automatic Activation Device includes 1-year Advanced Exchange Warranty	\$495.00 per vehicle
1	Installation of VuLink with a DVM system	\$50.00 per vehicle

1	Installation of VuLink as a standalone system or as an add-on to an existing system	\$150.00 per vehicle
1	Cloud Drive 100GB Block of Cloud Storage (for Cloud Solution only)	\$63.00 per year
1	Additional 1-year Advanced Exchange Warranty for FirstVu HD (for Local On-Premise Option only)	\$129.00 per camera per year
1	Dell Customized Server (for Local On-Premise Option only)	Customized Quote available upon request
1	Cloud Share License (Administrator only) Share Portal, Redaction, Case Management (for Local On-Premise Option only)	\$399.00 per license

- **Will you offer a discount of those prices if multiple police departments group together to buy your products and services?**

Yes, Digital Ally will offer volume discount pricing on the Retail Unit Price List above for any State of Pennsylvania Police Department and Law Enforcement agency. Our PA COSTARS Contract and State of Pennsylvania Contract both offer our best pricing and already include a State-wide anticipated volume discount. Police Departments and Law Enforcement agencies may contact Digital Ally at any time for a quote.

Contact information for a price quote:

Pennsylvania Sales Manager

John Saunders

Phone: 913.232.5348

Headquarters: 800-440-4947

Email: John.Saunders@digitalallyinc.com

Contact information for questions about Digital Ally's RFI proposal:

Bid Specialist

Nicole Leiker

Phone: 913.814.7774

Headquarters: 800-440-4947

Email: bids@digitalallyinc.com



FirstVu HD Body Camera



9705 Loiret Blvd. | Lenexa, KS 66219
800.440.4947 | 913.814.7774 | digitalallyinc.com

Table of Contents

Digital Ally, Inc. Company Information.....	3
Corporate Headquarters Location	3
Corporation Information.....	3
Contact Information	3
Company Qualifications	4
Introducing the FirstVu HD Body Camera	5
Mounting Locations	5
Included with Purchase.....	6
Upload Methods and Docking Stations	7
Specifications for Body Camera Solution.....	8
Docking Station Specifications:.....	9
Automatic Activation.....	10
VuLink Specifications	10
Available Video Management Options.....	11
VuVault.com Cloud	11
VuVault.com Unlimited Storage Cloud Plans.....	13
VuVault Local Software.....	14
Specifications for VuVault.com and VuVault.....	15
Product Support Information	16
Training	16
Warranty	16

Digital Ally, Inc. | Company Information

Corporate Headquarters Location

Digital Ally, Inc.

9705 Loiret Boulevard

Lenexa, KS 66219

w: www.digitalallyinc.com

p: 913.814.7774

toll free: 800.440.4947

f: 913.814.7775

Corporation Information

Digital Ally is a publicly held corporation traded under the symbol “DGLY”. We were incorporated in the State of Nevada on December 13, 2000. Digital Ally is overseen by a board of directors and Stanton E. Ross currently sits as the Chairman and CEO. Our company manufactures reliable, rugged, easy-to-use Body and In-Car Camera Systems for law enforcement agencies, security agencies, EMS, commercial fleets, and educational institutions.

Contact Information

Pennsylvania Sales Manager

John Saunders

p: 913.232.5348

e: John.Saunders@digitalallyinc.com

Regional Sales Director

Jeff Milligan

p: 913.814.7774

e: Jeff.Milligan@digitalallyinc.com

Bid Proposal Contact

Nicole Leiker, Bid Specialist

p: 913.814.7774

e: bids@digitalallyinc.com



Company Qualifications

Digital Ally, Inc. is committed to providing law enforcement, security agencies, EMS, commercial fleets, and educational institutions with the highest quality technology to assist in capturing digital evidence. As an industry-leader, Digital Ally designs feature-rich products that are rugged, durable and reliable. Agencies from all 50 States and more than 90 other countries rely on our products every day.

Digital Ally was established in 2004 and revolutionized mobile video by introducing a complete In-Car Camera System integrated into a rear-view mirror. This design provides a more efficient use of space in vehicles, as well as providing a user-friendly system that can be positioned so it is not distracting to users. Our In-Car Camera Systems have high quality video ranging from Enhanced D1 Resolution to full 1080p HD Resolution.

Since the introduction of our series of In-Car Camera Systems, we have expanded our product offering to include the FirstVu HD line of Body Cameras and the patented VuLink automatic activation unit. VuLink enables the automatic activation of your In-Car Camera, wireless Microphone, and Body Camera. The FirstVu HD brings all the advantages of an In-Car Camera system to the shirt pocket of every officer. It is small and lightweight, easy to operate, and allows officers to record high quality video in full 720P HD.

Digital Ally, Inc. has also developed both a dynamic, comprehensible cloud –based solution and a back office software solution for easy management, review, and archiving of recorded evidence. New products are always in the pipeline to enable our customers to stay up to date with the latest in technology.

Digital Ally's sole business is dedicated to designing, manufacturing, and selling quality leading-edge digital video systems and related products. We understand the work, dedication, and commitment it takes to provide agencies of all sizes with Digital In-Car and Body Camera solutions.

All of the video systems designed by Digital Ally, Inc. offer many important benefits such as:

- Being fully-automatic
- Simple to operate
- Enhancing officer safety
- Reducing liability
- Capturing irrefutable evidence
- A total design and support solution

Headquartered in Lenexa, Kansas, Digital Ally, Inc. is publicly traded on the NASDAQ Capital Market under symbol DGLY. We have been awarded several cooperative and statewide contracts that include GSA, NPPGov, HGACBuy, TX-DIR, MiDEAL, PA COSTARS, Purchasing Cooperative of America, and more.

With new, innovative products being designed constantly, Digital Ally, Inc. strives to offer customers the solutions they need to capture the truth in situations where it matters the most.

Introducing the FirstVu HD Body Camera



FirstVu HD

TWO-PIECE SOLUTION

FirstVu HD



The FirstVu HD two-piece model can be mounted on a variety of locations on the officer via the Klick-Fast mounting system, small or large clips, buttons, magnets, Velcro, rail and options for the lapel and tactical helmet.

Mounting Locations:

Chest



Shoulder



Lapel



Helmet



HIGH DEFINITION VIDEO & AUDIO

720p Resolution with 130° field of view

The camera captures exactly what the officer sees during the incident. HD Audio recording built into the camera.



Included with Purchase

- FirstVu HD DVR
Standard Battery Version or Extended Battery Version
- FirstVu HD Camera
11 inch cable or 48 inch cable
- Camera Cable Clamp
- Standard Battery or Extended Battery
- Battery Charger
- AC Outlet Adapter for Battery Charger
- DC Car Adapter for Battery Charger
- Charge/Data Cable
- Standard Fabric Clip Mount
- Velcro Mount
- Button Mount
- Wedge Mount Kit
- Reference User Guide



Item	Qty	Description
1	1	FirstVu HD Camera
2	1	FirstVu HD DVR
3	2	Cable, USB 2.0 Type A to Mini-B
4	1	Velcro Mount
5	1	Fabric Clip
6	1	Quick Reference Guide
7	1	Button Mount
8	1	Home Charger
9	1	Car Charger
10	2	FirstVu HD Battery
11	1	Battery Charger
12	1	Wedge Kit

Optional Accessories:

- Adjustable Mount Kit
- Spring Visor Clip
- Magnet Mount
- Motorcycle Mount Kit
- Car Mount Kit
- Head Mount Kit
- KlickFast Mount Adapter Kit
- Belt Mount Kit
- Belt Loop Holster
- Nylon Pouch
- VuLink Wireless Body Camera and In-Car Camera Link (Automatic Activation)
- FirstVu HD Docking Station

Upload Methods and Docking Stations

Docking Stations

Body Camera footage can be uploaded via USB or by using one of our Docking Stations. Choose from our 12-unit “Smart Dock” or our one-unit Mini-Dock.



12-Unit Dock
(Station Headquarters)



Mini-Dock
(Office/Desk/Home-Use/Cloud Only)



INDUSTRY’S ONLY “SMART DOCK”

Secure Timely Transfer | “Plug & Play”

Our 12-Unit Smart Docking Station has a 500GB Local Memory hard drive that allows for a faster transfer of data to local or cloud software storage. This unit also can simultaneously upload 4 hours per 12 FirstVu HD cameras within a 15-minute shift change. All of this while charging units and making updates to any configuration needed for your devices.

Dock Uploads

Upload methods include a Mini-Dock and 12-bay Docking Station for either the standard battery or extended battery

- Extended Battery Dock:
Charge the extended battery and offload video by dropping the DVR into the Docking Station
- Standard Battery Dock:
Charge both the standard batteries and offload video by dropping the DVR into the Docking Station
- Mini-Dock:
Provides all the benefits of the docking station, in a compact, single user design

Manual Uploads (with VuVault Software only)

- USB port to a computer station
 - FirstVu HD can be placed in secure mode so that it only uploads to certain IP addresses
 - Secure mode restricts access to metadata and recorded video files

Specifications for Body Camera Solution

FirstVu HD Specifications:

Video Resolution	720p (1280x720) or VGA (640x480)
Field of view	Horizontal: 95°, Vertical: 80°, Diagonal: 130°
Low Light Sensitivity	0.08 Lux (minimum); Fixed focus lens
Pre-Event Buffer	60 seconds video & audio; adjustable in one second increments
Internal Memory	32 GB secure internal memory
Encryption	H.264 codec with configurable quality settings
Secure Media Access	May be configured so only designated computers can access recordings
Covert Mode	Deactivates LEDs (vibrating confirmations and LEDs remain off)
Connection	Mini-USB for uploading recordings and charging (Docking Station optional)
Weather Rating	general water rating that is IP56 equivalent
Humidity	10 -90% RH, non-condensing. IP56 water resistant camera head
Operating Temperature	-20° to +70° C
Storage Temperature	-40° to +80° C
Weight	Camera and Cable = 0.8 oz
	Body (DVR) = 3.1 oz
Dimensions	2 5/8"(w) x 4"(h) x 5/8"(d) (Main Recorder)
	1 1/8"(w) x 1 1/2"(h) x 1.0"(d) (Camera Module)
Battery	3.7vDC 2,200mAh, Rechargeable Lithium Ion Polymer Battery, field replaceable
Quality Settings	Eight different HD or SD Quality and Frames per Second configurations
Record Time	16 hours in HD (High Quality Setting)
	54 hours in SD (Lowest Quality Setting)
Videos	Records non-proprietary AVI Videos
Metadata	Saves Date, Time Stamp, and Marks
Extended Battery	up to 16 hours Standby (or up to 96 hours with no activity)
	up to 9 hours continuous record time with pre-event enabled
Standard Battery (2 included with each FirstVu HD purchase)	up to 12 hours Standby each (or up to 48 hours each with no activity)
	up to 9 hours with both batteries (4.5 hours each) continuous record with pre-event enabled
Microphone	Internal (max. input SPL 110dB, sensitivity -42dBV)
Audio	Mono, may be muted by user Multiple configuration options
GPS	Tag GPS location during playback through VuVault GO
Made Where	Assembled in USA. Internals built in Kansas
Cloud Warranty	Advanced Exchange Warranty on hardware for full term of contract
Local Warranty	1-year Advanced Exchange included at no cost

Docking Station Specifications:

Power	
OPERATING VOLTAGE	12 VDC, $\pm 10\%$
POWER CONSUMPTION	9.6W – 24.96W
POWER ADAPTER 1	AC to DC, 12VDC / 5 A
POWER ADAPTER 2	AC to DC, 12VDC / 7.5 A
MINIMUM POWER INPUT	12 VDC, 4 A
Environmental/Mechanical	
OPERATING TEMPERATURE	-20° to +60° C
STORAGE TEMPERATURE	-40° to +85° C
RELATIVE HUMIDITY	95% @ 40° C (non-condensing)UL, CCC, BSMI
SAFETY CERTIFICATIONS	UL, CCC, BSMI
DIMENSIONS	34.6cm (13.5in.) (L) x 36.5cm (14.3in.) (W) x 15.8cm (6.3in.) (H)
WEIGHT	6.12kg (13.5 lbs)
Network	
NETWORK INTERFACE	6.12kg (13.5 lbs)
DATA TRANSFER RATE	Average >8MB/s per device upload to docking station. Up to 1GB/s from docking station to server.



Automatic Activation

VuLink: Patented Automatic Activation

Digital Ally's VuLink was the first product on the market to fully integrate in-car cameras and body worn video. The patented technology behind VuLink enables wireless automatic activation of your In-Car Camera, Wireless Microphone, and Body Camera.

VuLink Technology Features:

- View all related video feeds at the same time: Video from both your In-Car and Body Camera will sync
- Hands Free: Automatically activates Body Camera and In-Car Camera Systems
- Eliminates Distractions: Reduce incidents of user-error and the need to continuously record

Most Common VuLink Triggers:

- Emergency Lights
- G-Force or Impact Events
- Vehicle Speed
- In-Car Camera System
- Gun Lock
- Seat Belt
- Emergency Radio Switch
- Motorcycle Kickstand
- Motorcycle Handle Bar Switch
- Trunk Latch
- Fire Suppression Systems
- Doors
- GPS Zones (with In-Car Camera System)
- 12 Volt Relay



VuLink Specifications

OPERATING VOLTAGE	8-30VDC
CURRENT DRAW	250mA Maximum
MAX TRANSMIT POWER	10dBm
TRANSMIT RANGE	50ft typical
WEIGHT	55.4g (0.12 lbs.)
OPERATING TEMPERATURE	-30° to +60° C
STORAGE TEMPERATURE	-40° to +80° C
DIMENSIONS	23mm (0.9in.)(D) x 91mm (3.6in.)(W) x 61mm (2.4in.)(H)

Available Video Management Options



VuVault.com | Cloud

We at Digital Ally know how important security and flexibility are to our customers. Through proprietary hash algorithms, geographically redundant servers, and Amazon's high security standards, Digital Ally has created an evidence management and video storage solution that is extremely secure and follows CJIS standards. Our solution, VuVault.com is not only secure, it is also completely scalable so that you can adjust to incoming and outgoing officers as needed.

Overview

VuVault.com is built on the Amazon Web Services (AWS) Region application platform with a "security first" approach. The main components of the application are isolated and accessible only from the approved IP address of our portal server. User authentication and access to user data and digital media is granted solely through the portal server. Utilizing strong SSL, all web requests to the portal server and returned content are encrypted. Session-based, always changing encryption is in place for all HTML transactions and application content further obscuring any data patterns. All user and digital media activity is logged and scrutinized for malicious intent and a series of checks and balances is used to prevent unwanted activity within an account.

Customer data is isolated within our application database with steps taken at each page request to guarantee customers gain access only to their data.

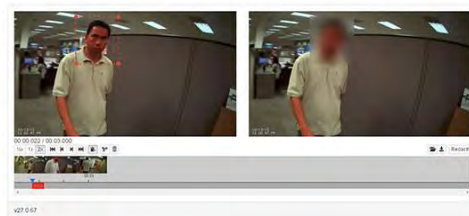


Manage Video and Cases

VuVault.com eases the burden of managing videos. There are several standard search criteria already implemented into the system, along with customizable search criteria to make finding recordings fast and easy. With case management implemented into the standard operating system, putting together case files has never been easier. Case management allows you to link all associated videos, documents, and files from your FirstVu HD and alternate outside sources into one complete case file within VuVault.com.

Redaction

Utilize our integrated redaction technology to quickly and easily redact videos. The system has intuitive automatic face suggestions as well as manual redaction capabilities. Faces, signs, license plates, shirts and other objects can all be redacted quickly and easily. Once complete the redacted video can be downloaded or shared with other users.



API Support

Digital Ally has an Application Program Interface (API) that can be utilized to connect to other vendor software. We would have to create a service contract and determine the development time needed to integrate our system with the existing systems. Digital Ally will work with the Department to determine exactly which features and information need to integrate with our systems.

Cloud Share

VuVault.com includes an extensive, secure and flexible share portal to facilitate convenient sharing of video evidence and case files with designated and credentialed third parties. This functionality can be used on a one-off basis by the issuance of one time credentials, or can be configured to allow regular and continued access by known and trusted third parties (i.e. the prosecutor and staff). These third parties will have the option, if given privileges per share, to review and/or download files in native format to solid state memory. A proprietary player is not needed to review video after it is downloaded.

Environmental Security Features

Amazon Web Services (AWS) data centers utilize innovative architectural and engineering approaches. Each data center is equipped with fire detection and suppression, power failure back-ups climate and temperature controls, and electrical and mechanical management. When a storage device reaches its end of life security measures are taken by Amazon to ensure that data is not exposed to unauthorized individuals. Amazon security platforms also host around the clock surveillance to ensure data locations are secure.

In case of failure, automated processes move data traffic away from the affected area to an alternate secure location. AWS is designed to tolerate system or hardware failures with minimal to no impact to users.

Disaster Recovery

Ensuring your data will always be protected and accessible is our number one priority; that is why we have built VuVault.com on the most trusted web service around. Amazon Web Services supplies three locations separated on the east and west coasts where all of your data will be copied and 100% secured. If one of the locations is wiped out by a natural disaster, your information will still be secured in two alternate locations states away. Any and all of the information that was flowing to that particular location will be directed to substitute locations.

VuVault.com Unlimited Storage Cloud Plans

Digital Ally has the following unlimited storage cloud plans to choose from for the FirstVu HD Body Camera:

1) VuVault.com Ultimate Plan and Body Camera Solution

Includes:

- 1-Year Unlimited Data Storage
- 1-year, 3-year, and 5-year contract plans available
 - 3 or 5-year contract includes body camera at no cost
 - 1-year contract includes 50% discount on FirstVu HD Body Camera
- Full Software Access, Redaction, Case Management, Share Portal
- Advanced Exchange Warranty on hardware for full term of contract

2) VuVault.com Pro Plan and Body Camera Solution

Includes:

- 180-day Unlimited Data Storage
- 1-year, 3-year, and 5-year contract plans available
 - 5-year contract includes 83% discount on FirstVu HD Body Camera
 - 3-year contract includes 66% discount on FirstVu HD Body Camera
 - 1-year contract includes 39% discount on FirstVu HD Body Camera
- Full Software Access, Redaction, Case Management, Share Portal
- Advanced Exchange Warranty on hardware for full term of contract

3) VuVault.com Basic Plan and Body Camera Solution

Includes:

- 90-day Unlimited Data Storage
- 1-year, 3-year, and 5-year contract plans available
 - 5-year contract includes 83% discount on FirstVu HD Body Camera
 - 3-year contract includes 66% discount on FirstVu HD Body Camera
 - 1-year contract includes 33% discount on FirstVu HD Body Camera
- Full Software Access, Redaction, Case Management, Share Portal
- Advanced Exchange Warranty on hardware for full term of contract

Cloud Drive

After the retention period expires, evidence can be transferred to the Cloud Drive for long-term storage. Cloud Drive is available in blocks of 100GB. An unlimited amount of 100GB blocks of Cloud Drive can be purchased at any time. Video that is placed in the Cloud Drive still retains the full cloud functionality available from VuVault.com. This includes redaction and the availability of all metadata.



Digital Ally recordings can be easily archived to DVD, Hard Drive, Tapes, Etc. through the user friendly VuVault Software console. The VuVault™ back office software suite enables law enforcement agencies to quickly and easily manage their digital video evidence across all of Digital Ally's products. VuVault™ is utilized for playing back, downloading, archiving, reviewing, unit configuration and management, running customizable reports and chain of custody logs as well as exporting/burning videos to DVD's for court.



With VuVault, you can also purchase the level of software that will best suit your agency. VuVault comes in Standalone, Server, and Enterprise level software options. VuVault Server and VuVault Enterprise level software come with unlimited workstation licenses.

Device and User Management

Manage all of your Digital Ally™ devices and groups through once simple back office software. VuVault administrators can configure and assign devices, set retention policies and control user and group permissions all through VuVault™

Video Evidence Reporting

Creates reports on just about anything. At the touch of a button will allow you to instantly know which officers have or haven't uploaded videos recently, identify high crime areas, and generate chain of custody reports for court. VuVault gives you the flexibility and functionality you need in a video management system.

Chain of Custody Reporting

Ensures that the exact video that was uploaded into the system is the video that is being shown to the attorneys and used in court. The original video file remains unaltered despite any notes, marks or segmentation that an officer might make to the video.

Active Directory Login

VuVault leverages Microsoft Active Directory for managing system security access and authentication. With Active Directory integration enabled, users will not need to login to VuVault once their username has been associated with an active directory group. All associated permissions for the group will be assigned automatically when logging in making VuVault incredibly easy to deploy across an agency utilizing a Microsoft server environment

Cloud Share (Optional)

Cloud Share Licenses for VuVault are available for purchase and include redaction, a portal to share video, and case management. The Share Portal is an extensive, secure and flexible portal to facilitate convenient sharing of video evidence and case files with designated and credentialed third parties. This functionality can be used on a one-off basis by the issuance of one time credentials, or can be configured to allow regular and continued access by known and trusted third parties (i.e. the prosecutor and staff). These third parties will have the option, if given privileges per share, to review and/or download files in native format to solid state memory. A proprietary player is not needed to review video after it is downloaded.

Specifications for VuVault.com and VuVault

VuVault.com Cloud Specifications

- VuVault.com cloud runs on a Virtual Machine (VM) environment and does not use a traditional SQL database.
- Local server is not required. All data will be stored in the cloud at Amazon Web Services
- Can be accessed on any computer with a modern Internet browser and a VuVault.com account.
- Amazon Web Services has a system uptime of 99.95%.

VuVault Software Specifications

- Server license
- Client license
- SQL
- Full version of VuVault required for more than 200 systems (SQL custom quote available upon request)
- Client unlimited license

VuVault Minimum Specifications

Processor	Intel® Dual Core Processor (2.00 GHz or better)
Operating System	Windows 7 or newer
Memory	4 GB
OS Hard Drive	40GB Free Space
Optical Drive	DVD+/-RW or Blu-ray Writer
Video Card	Intel® HD4000 chipset or comparable
Network Card	100 Mb Ethernet
Card Reader	USB 2.0 Card Reader

VuVault Recommended Specifications

Processor	Intel® Quad Core Processor (3.0GHz or better)
Operating System	Windows 7 or newer
Memory	8 GB or Greater (Note: >4GB of RAM will require a 64-bit OS)
OS Hard Drive	40GB Free Space
Optical Drive	DVD+/-RW or Blu-ray Writer
Video Card	Nvidia® GeForce 710M or comparable
Network Card	Gigabit Ethernet
Card Reader	USB 3.0 Card Reader

Product Support Information

Digital Ally has full-time Product Support Specialists at our corporate office in Lenexa, Kansas. Each Product Support Specialist is factory-trained on all aspects of Digital Ally's products. Our specialists also do the final testing of all software upgrades, write and upgrade manuals, etc. so they are always up to date on our latest releases.

We have Product Support Specialists on staff via telephone and email and will provide on-site assistance if necessary (additional fees may apply). At this time, our office hours are 8:00 to 5:00 Monday through Friday, Central Time Zone. Our approach to user support is simply this; do whatever is necessary to fix the problem and make the customer satisfied as quickly and efficiently as possible.

Training

Our approach to training is that it is vital to ensure that the customer understands the operation of our system and is able to fully utilize all the features available. We have also found that well trained users have much fewer problems than users who have not been trained properly. We are prepared to take whatever steps necessary to train every user, both at the time of delivery and as needed in the future.

Training will include hands-on training, quick reference guides, instructional videos available for replay, and detailed operating guides. Training will cover hardware, video management application, and software or cloud storage.

Training will be divided between end users and supervisors/administrators. Multiple sessions can be scheduled to accommodate group size and various shifts. End user training will be in a train-the-trainer format for Department personnel that will be responsible for training others and those managing/administrating the program. Supervisor/Administrator training will be for those responsible for maintaining the devices and VuVault or VuVault.com.

Warranty

An Advanced Exchange Warranty is included with VuVault.com cloud for the full term of contract. Digital Ally provides a 1-year Advanced Exchange Warranty on the FirstVu HD system with the local VuVault Software solution. The Advanced Exchange Warranty includes any defects in materials or workmanship on all system components, as well as all software upgrades not requiring hardware revisions. Additional 1-year Advanced Exchange Warranties are available for purchase with the local VuVault Software solution. The Warranty period will begin from the date of invoice.

Digital Ally's "Advanced Exchange Program" is the most revolutionary Service Policy in the industry. During our Standard Warranty Period, if the hardware has a service issue, our Technical Support Department will diagnose the problem. If we determine the problem to be a hardware issue, Digital Ally will send you a replacement module to fix the problem. Shipments reach most within 2 business days to keep down time to a minimum.

VuSchools Body Camera System

For School Resource Officers and Educators



Digital-Ally™

9705 Loiret Blvd. | Lenexa, KS 66219
800.440.4947 | 913.814.7774 | digitalallyinc.com

Table of Contents

Digital Ally, Inc. | Company Information3

 Corporate Headquarters Location.....3

 Corporation Information3

 Contact Information.....3

Introducing the VuSchools Wall-Mount/Body Camera Solution.....4

 Included with the VuSchools Body Camera System4

 FirstVu HD Body Camera Specifications.....5

 FirstVu HD Controls6

Cloud Software Solution7

 About Amazon Web Services8

Product Support.....9

Training.....9

Warranty and Maintenance9

Digital Ally, Inc. | Company Information

Corporate Headquarters Location

Digital Ally, Inc.

9705 Loiret Boulevard

Lenexa, KS 66219

w: www.digitalallyinc.com

p: 913.814.7774

toll free: 800.440.4947

f: 913.814.7775

Corporation Information

Digital Ally is a publicly held corporation traded under the symbol “DGLY”. We were incorporated in the State of Nevada on December 13, 2000. Digital Ally is overseen by a board of directors and Stanton E. Ross currently sits as the Chairman and CEO. Our company manufactures reliable, rugged, easy to use body worn and in-car video recording systems for law enforcement agencies.

Contact Information

VuSchools Regional Sales Manager

Kevin Richard

p: 913.274.2501

e: Kevin.Richard@digitalallyinc.com

Bid Specialist

Nicole Leiker

p: 913.814.7774

e: bids@digitalallyinc.com

Introducing the VuSchools Wall-Mount/Body Camera Solution

VuSchools is a secure cloud-based video management system paired with Digital Ally's simple to operate, reliable, high definition body cameras. The FirstVu HD Wall-Mount/Body Camera Solution for School Resource Officers and educators is based on our successful FirstVu HD Body Camera for Law Enforcement. The versatile design of the camera module allows it to adapt to a solution specifically for School Resource Officers and educators.



Two-Piece Model with Mini-Dock

Digital Ally understands that an unobtrusive solution, both in physical appearance and work load is a huge concern. The FirstVu HD is impact and weather resistant and utilizes secure, internal solid state memory. It includes multiple mounting locations with options for a lanyard, belt mount, and classroom wall mount for a wide view of the whole classroom. The unit is small and lightweight, weighing less than 4 ounces. The system is always on, allowing the educator or School Resource Office to perform their job, and not have the focus on the camera. The Docking Station is fully automatic, charging the battery, and uploading data to the VuSchools Cloud Portal.

Stable and tough, the solid state secure memory in the FirstVu HD is unaffected by violent motion. The simplistic design of the FirstVu HD solution puts cameras in the classroom in a safe and uncomplicated way.

Included with the VuSchools Body Camera System

- VuSchools FirstVu HD Body Camera Kit
 - Choice between one-piece lanyard style model or two-piece model
 - 720x480 pixels video resolution
 - Audio
 - Robust form factor
 - 8 hours record time
 - Start/Stop Record Button
 - Charges overnight while offloading video
- Mini-Dock charging and downloading dock
 - View Video Feed
 - Add Notes
 - Playback recorded video
 - View storage and battery life
 - Securely Offloads Videos
 - Charges FirstVu HD camera
 - Secure Encrypted Connection



One-Piece Model



Mini-Dock

- Easy Setup
- One FirstVu HD per Mini Dock
 - Operations:
 - Apply A.C. Power
 - Connect Ethernet cable to network
 - Offload and charges FirstVu HD overnight – typically 8 hours max
- Belt Clip Mount, Lanyard Kit, Pouch, and/or Wall Mount Kit
 - The FirstVu HD one-piece model includes a lanyard style mount, magnet mount, or belt clip mount.
 - The FirstVu HD two-piece model includes a belt clip mount, lanyard style mount, or magnet mount.
 - Both the one-piece and two-piece model can be mounted on a wall with the included Wall Mount Kit
 - Both the one-piece and two-piece model can be stored in the included pouch
- VuSchools Website Service & Cloud Storage License
- VuSchools Program Turnkey Solution & Professional Services-Configuration, Set-Up, and Training
- VuSchools Program Hardware & Software Maintenance Agreement



FirstVu HD Body Camera Specifications

Camera Module	1 1/8" (w) x 1 1/2" (h) x 1.0" (d)
Main Recorder	2 5/8" (w) x 4" (h) x 5/8" (d)
Weight	3.9 oz.
Battery	Rechargeable, lithium polymer battery
Resolution	720p HD Video: 1280 x 720 .08 Lux low light/no light recording
Battery Life	8 hours consistent record time
Memory	32GB of secure, internal, solid state memory
Field of View	H = 95° V = 80° D = 130°
Encryption	H.264 Codec & Configurable Quality Settings
Rating	IPX5
Connection	Mini-USB for uploading recordings and charging
Metadata	Saves Date/Time Stamp & Marks
Pre-Records	30-sec. pre-event recording

FirstVu HD Controls

The FirstVu HD System is simple to operate. Once the DVR is turned on, the unit automatically starts pre-event recording, always capturing the last 30 seconds prior to the record button being pressed. It will only stop recording when the record button is pressed and held for approximately three seconds. Audio is always captured during pre-event and the recording. At the end of the day the FirstVu HD is docked in the included Mini-Dock, where it will automatically offload data, and charge the battery.

System Administrators can request video events from the VuSchools.com cloud portal. Each video event sends and catalogs metadata to the VuSchools.com cloud portal. Video can be reviewed and requested to be sent from the Mini-Dock to the VuSchools cloud portal on demand. If a video is not requested, it is kept for seven days. If a video is requested and uploaded to the VuSchools cloud portal, it will be kept for 30 days for review.





Cloud Software Solution

The VuSchools Cloud Portal enables educators and School Resource Officers to quickly and easily manage their digital video events. VuSchools.com is utilized for playing back video, downloading, reviewing, unit configuration and management, running customizable reports and chain of custody logs, as well as sharing portal to securely share videos with third parties.

With VuSchools.com, all cameras can simply and securely be managed. VuSchools.com includes the ability to manage video events and access the system district-wide with ease. VuSchools is built on the same Amazon Web Services platform Digital Ally uses for our Law Enforcement and Commercial customers.



Features

- Manage - View, share, and manage your digital content from any internet browser.
- Secure - All video evidence is backed up and stored securely on the cloud (Amazon Web Services).
- Easy - Automatically upload your videos straight to the cloud via the Mini-Dock.
- Accessible - Review video from anywhere you are connected to the internet.
- Smart Storyboard - Find your videos more easily from the search results.
- Universal Tagging System
- Basic Incident Management - Import documents, PDFs, and other video media into VuSchools.com
- Video Sharing - Securely share videos with third parties by way of email while maintaining chain of custody

Device & User Management

Each issued device will be connected to your VuSchools account. Simple setup by an Administrator allows for a highly capable rollout of the FirstVu HD System. Each FirstVu HD Body Camera and Mini-Dock will be assigned to an educator and/or School Resource Office to allow for easy backend management of all devices.

Chain of Custody Reporting

The exact video that is upload into the VuSchools.com cloud portal will be the same video that is viewed by an Administrator. The original video file will remain unaltered despite any notes, segmentation, or redaction that might take place. Full activity is tracked with chain of custody reporting.

Incident Management

Incident Management allows the importing of any other electronic document pertinent to the video event. This includes PDFs, Word, Pictures, etc.

About Amazon Web Services

VuSchools, is built on Amazon Web Services (AWS) Region application platform with a security first approach. The main components of the application are isolated and accessible only from the approved IP address of our portal server. User authentication and access to user data and digital media is granted solely through the portal server. Utilizing strong SSL, all web requests to the portal server and returned content are encrypted. Session-based and always changing encryption is in place for all HTML transactions and application content, further obscuring any data patterns. All user and digital media activity is logged and scrutinized for malicious intent, and a series of checks and balances is used to prevent unwanted activity within an account.

Customer data is isolated within our application database with steps taken at each page request to guarantee customers gain access only to their data.

Manage Video

VuSchools.com eases the burden of managing videos. There are several standard search criteria implemented into the system, along with customizable search criteria to make finding recordings fast and easy.

Redaction

VuSchools.com features a nearly automated redaction feature. This feature allows an Administrator to redact faces and facial features so that the video can be released as needed by the Administration. VuSchools.com also features an intuitive manual redaction tool, which allows for the redaction of audio, t-shirts, and other items as needed.

Upload Process

Uploading recordings into VuSchools.com is an easy process. Connect the FirstVu HD to the Mini-Dock with the supplied USB cable. The recorded videos will automatically upload to the Mini-Dock and will remain on the Mini-Dock until requested. All metadata will immediately upload to VuSchools.com for reporting and chain of custody purposes. Video can be reviewed and requested to be sent from the Mini-Dock to the VuSchools cloud portal on demand. If a video is not requested, it is kept for seven days. If a video is requested and uploaded to VuSchools.com, it is kept for 30 days for review. This method allows for a highly scalable solution and keeps network bandwidth to a minimum.

Environmental Security Features

Amazon Web Services (AWS) data centers utilize innovative architectural and engineering approaches. Each data center is equipped with fire detection and suppression, power failure back-ups, climate and temperature controls, and electrical and mechanical management. When a storage device reaches its end-of-life, security measures are taken by AWS to ensure that data is not exposed to unauthorized individuals. AWS security platforms also host around-the-clock surveillance to ensure data locations are secure.

In case of failure, automated processes move data traffic away from the affected area to an alternate secure location. AWS is designed to tolerate system or hardware failures with minimal to no impact to users.

Disaster Recovery

Ensuring your data will always be protected and accessible is our number one priority. This is why we have built VuSchools.com on the most trusted web service around. Amazon Web Services supplies three locations separated on the east and west coasts where all of your data will be copied and 100% secured. If one of the locations is wiped out by a natural disaster, your information will still be secured in two alternate locations states away. Any and all of the information that was streaming to that particular location will be directed to substitute locations.

Product Support

Product Support Information

Digital Ally has full-time Product Support Specialists at our corporate office in Lenexa, Kansas. Each Product Support Specialist is factory-trained on all aspects of Digital Ally's products. Our specialists also do the final testing of all software upgrades, write and upgrade manuals, etc. so they are always up to date on our latest releases.

We have Product Support Specialists on staff via telephone and email and will provide on-site assistance if necessary (additional fees may apply). At this time, our office hours are 8:00 to 5:00 Monday through Friday, Central Time Zone. Our approach to user support is simply this; do whatever is necessary to fix the problem and make the customer satisfied as quickly and efficiently as possible.

Training

Our approach to training is that it is vital to ensure that the customer understands the operation of our system and is able to fully utilize all the features available. We have also found that well trained users have much fewer problems than users who have not been trained properly. We are prepared to take whatever steps necessary to train every user, both at the time of delivery and as needed in the future.

Training will include hands-on training, quick reference guides, instructional videos available for replay, and detailed operating guides. Training will cover hardware, the video management application, and software or cloud storage.

Training will be divided between end users and supervisors/administrators. Multiple sessions can be scheduled to accommodate group size and various shifts. End user training will include train-the-trainer format for personnel that will be responsible for training others and those managing/administrating the program.

Supervisor/Administrator training will be for those responsible for maintaining the devices and VuSchools.com.

Warranty and Maintenance

Digital Ally provides a full warranty on the FirstVu HD hardware throughout the term of the contract. The warranty includes any defects in materials or workmanship on all system components as well as all software upgrades not requiring hardware revisions. The FirstVu HD System is a completely solid state device that does not require any scheduled maintenance. The warranty period will begin from the date of shipment.



Proposal for Police Body Worn Cameras

Pennsylvania Chiefs of Police Association



Pennsylvania
Chiefs of Police Association

Submitted by
WatchGuard, Inc.





25th of January 2019

Christopher J. Braun M.S. IT
Technology Coordinator Pennsylvania Chiefs of Police Association
3905 N. Front Street
Harrisburg, PA 17110

Reference: RFI: Police Body Worn Cameras

WatchGuard has designed and engineered a complete video solution from the ground up that completely integrates the VISTA wearable camera with the Evidence Library software. This development effort was focused on addressing and correcting a lot of issues typically associated with wearable camera deployments as well as adding innovated features and capabilities to improve quality and user experience.

VISTA sets new standards in ruggedness, overall performance, and ease of use. Unlike nearly every competing system, VISTA is constructed with industrial grade components and is manufactured in the U.S.A. It is capable of recording both High Definition and Standard Definition video, and is able to record up to 12 hours of continuous HD video.

EvidenceLibrary.com is a fully cloud hosted back office solution allowing an agency to have the application and all video storage in the cloud. EvidenceLibrary.com utilizes Microsoft Azure Government, which is an isolated version of Azure that is exclusively used by US Government Agencies and qualified vendors.

Evidence Library 4 (EL4) is an enterprise class server application supporting client connections and video sharing and a host of other features. EL4 sets a new standard for back-end capability and ease of use.

Respectfully Submitted,

Troy Montgomery
Vice President of Sales



Contact Information:

Point of Contact

Kyrié Endres, Proposal Manager

(214) 785-2608 - Direct

bids@watchguardvideo.com - Email

Company

WatchGuard, Inc.

415 E. Exchange Parkway

Allen, TX 75002-2616

(800) 605-6734 – Toll Free

(972) 423-9777 – Main

(214) 383-9661 – Fax



Table of Contents

Company Profile_____	1
Response_____	5
Body Worn Camera Solution_____	7
Pricing_____	35

COMPANY PROFILE

WatchGuard's mission is to produce the industry's best video evidence solutions for law enforcement agencies worldwide. We strive to achieve our goal and drive ROI for our customer's investment thru innovative product designs and by using the highest quality materials. We insist on excellence in all we do, leading to superior performance in our products and services.

-Steve Coffman, President

INTRODUCTION

WatchGuard was founded in 2002 and began full production of its mobile video products in September of 2005, with initial shipments beginning in October 2005. All product manufacturing is done domestically in the company's 144,000 square foot facility in Allen, Texas. The North Texas facility features an engineering laboratory, customer service installation bay, pristine production space, and a state-of-the-art training room. All engineering, assembly, and factory service is conducted in this facility.



Company Background

WatchGuard is the world's largest manufacturer of video systems for law enforcement, providing systems to over one third of all U.S. and Canadian law enforcement agencies. In the most recent industry survey by IHS, WatchGuard was again recognized by this independent research organization as the worldwide market share leader in mobile video surveillance systems.

We currently have approximately 6,500 law enforcement agencies as customers and over 77,000 of our mobile DVR systems in the field. WatchGuard has moved solidly into the number one market share position for US sales of digital police in-car video systems.

WatchGuard's commitment to innovation can be seen in the large investments we make in the Research and Development of new products. We have the largest engineering team in the industry, and have invested over \$66 million into the development of digital video systems for law enforcement. We feel that innovation of quality and technically advanced products is essential to maintaining our position in this fast paced and rapidly evolving industry.

WatchGuard produces the most advanced systems, has the most extensive track record of successful deployments, has earned a reputation for extraordinary customer support, is financially sound, and is the best positioned company to service your video needs today and for many years into the future.

The Industry's Most Significant Products

WatchGuard has been pioneering technological innovations since its inception in 2002. Over its history, WatchGuard has been first to market with many technology breakthroughs including (1) the industry's first and only completely integrated and synchronized in-car and body worn system, (2) the industry's first HD in-car video system, (3) Record-After-the-Fact functionality, (4) multiple resolution recording and (5) the industry's first direct-to-DVD in-car video system.

WatchGuard's product strategy revolves around providing premium hardware with functionality that can only be performed in hardware (versus software solutions) and video management solutions that achieve automation through integration. Our hardware roadmap includes further reduction in the size and weight of our body worn camera, continued improvement in the audio and video quality of our already industry leading cameras and microphones, increasing product longevity through improved materials and construction thereby reducing total cost of ownership for our partner agencies, tight integration with most CAD/RMS vendors, further integration, feature improvements and ease of use for our redaction software, and development of next-gen platforms for our body worn, in-car offerings and video management software that take advantage of emerging AI technologies, speech recognition abilities and facial recognition technologies.

WatchGuard continues to invest heavily in projects that bring immediate value to our partner agencies. We have one of the largest and most prolific engineering groups in the industry, and are now investing in a new corporate headquarters facility that will bring additional engineering and production capacity to the company.



Advanced Engineering

Over the past decade, WatchGuard has become the most successful company in law enforcement video. By 2010, the company grew large enough to earn the #1 market share position. Since 2010, the company has continued to grow (80% growth just in the last 36 months) and is now approximately twice the size of the second largest manufacturer.

One of the primary reasons WatchGuard has become the dominant manufacturer of law enforcement video is because of our substantial investment in research and development.

WatchGuard employs the industry's largest engineering team and has invested over \$66Re million specifically into the development of video systems for law enforcement. Our major engineering investments have resulted in numerous technological breakthroughs and patents (14 issued, 19 pending) that have enabled us to demonstrate clear technological leadership and advance the state-of-the-art.

Our current 80+ person (and growing), senior level engineering team is comprised of a wide range of expertise and experience that includes:

- System architecture
- High reliability systems design
- Image processing
- Video encoding/decoding
- Audio encode/decode
- MPEG2/MPEG4/H.264
- High speed data processing
- High speed communication
- Digital signal processing
- FPGA/CPLD designs
- User interface design
- Kernel/driver development

- File system design
- Board design and layout
- Mechanical and industrial design
- Thermal analysis
- Rigorous system validation and testing.

This incredible amount of development horsepower is focused exclusively on the capture, management and integration of law enforcement video.

As a result, WatchGuard is uniquely positioned to offer Department a combination of hardware, evidence management software, and custom development capability that is far beyond any other manufacturer.

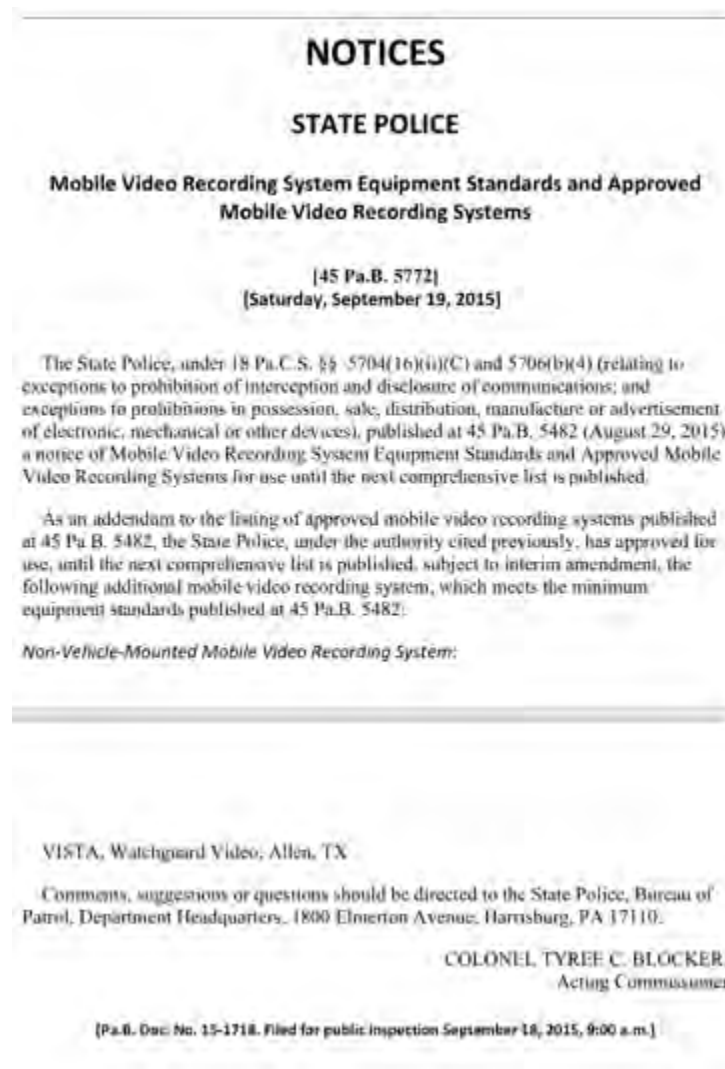
Manufactured in the U.S.A.

The company manufactures its products in its 144,000 square foot, state-of-the-art facility located in North Texas. This two story facility houses all departments including Engineering, Manufacturing, Sales, and Customer Service and it includes an impressive training room, customer installation bay, and pristine production space.

RESPONSE

How does your non-vehicle-mounted mobile video recording system and technology meet Pennsylvania's published requirements?

Our systems have been reviewed for compliance and meet the published requirements as stated below.



Have you submitted your non-vehicle-mounted mobile video recording systems to the Pennsylvania State Police for certification?

Yes.

Is your non-vehicle-mounted mobile video recording systems already certified by the Pennsylvania State Police?

Yes, we are currently under contract with the Pennsylvania State Police.

Are you offering a storage solution?

Yes. We are offering three different storage solutions, On-Premise, Hybrid, and Cloud, which are all outlined within our provided solution.

Will you offer storage solutions bundled (no line item distinction) with the cost of each camera purchased?

This option is negotiable, if desired.

How does your storage solution meet Pennsylvania's published requirements?

Each of the offered storage solutions has been designed to meet CJIS standards.

List the products or services that are already available on State Contract or PA CoStars.

Please see the attachments for our PA CoStars pricing and product listing.

Will you offer a discount of those prices if multiple police departments group together to buy your products and services?

We are open to negotiations.

SOLUTION DESCRIPTION

VISTA SOLUTION DESCRIPTION

Introduction

Over the past decade, WatchGuard Video has become the most successful company in law enforcement video. By 2010, the company grew large enough to earn the #1 market share position. Since 2010, the company has continued to grow (80% growth just in the last 36 months) and is now approximately twice the size of the second largest manufacturer.

One of the primary reasons WatchGuard Video has become the dominant manufacturer of law enforcement video is because we have invested substantially more money in research and development than any other company serving this industry. Our major engineering investments have resulted in numerous technological breakthroughs and patents (14 issued, 19 pending) that have enabled us to demonstrate clear technological leadership and advance the state-of-the-art.

Our current 80+ person, senior level engineering team is comprised electrical engineers, mechanical engineers, FPGA designers, embedded software developers, Windows software programmers, and test engineers. In addition, many of our engineers have Master level degrees or degrees in multiple disciplines (i.e. Electrical Engineering plus Computer Science).

This incredible amount of development horsepower is focused exclusively on the capture, management and integration of law enforcement video.

WatchGuard is uniquely positioned to offer Department a combination of hardware, evidence management software, and custom development capability that is far beyond any other manufacturer.

Because of the unique advantages offered by our In-Car Video products and some deficiencies in the wearable camera market, WatchGuard has spent the last three years developing the VISTA wearable camera. The goal was to incorporate some of the compelling advantages of our In-Car Video products while doing a ground up development of a wearable camera. The result is an ultra-rugged wearable camera with many first-of-a-kind features.

Since the camera itself is only part of the solution, WatchGuard did not stop there. The back-office software application is the piece that makes the cameras and the administration of the cameras and their respective video manageable. WatchGuard Video has designed and engineered a complete video server solution from the ground up that completely integrates the VISTA wearable camera with the 4RE In-Car cameras. The development effort was focused on addressing and correcting a



lot of issues typically associated with wearable camera deployments as well as adding innovative features and capabilities to improve the overall quality and user experience.

MULTIPLE CAMERA OPTIONS

The VISTA HD Wearable Camera is the system being proposed. WatchGuard engineered the VISTA solution and manufactures the product in the North Texas headquarters. VISTA is designed with complete industrial grade components and constructed with cast magnesium, polyurethane rubber and a military grade Polyetherimide resin. The camera is ultra-rugged, weatherproof, and has an operating temperature range of -40° F to +185° F. VISTA is designed to withstand years of real world use in the law enforcement environment.

WatchGuard has developed several camera options to support various department preferences and deployment scenarios. The options that are currently available are detailed below.

VISTA Extended

VISTA Extended is our original body worn camera design that was released in early 2015. It features:

- **Video Clarity and Quality** – VISTA records at 30 frames per second, and has six selectable video recording resolutions, including:
 - 720p (1280x720) – High, Medium and Low
 - 480p (864x480) – High, Medium and Low

VISTA Video Quality and File Sizes			
Setting	Resolution (pixels)	Sample Rate (megabits/second)	Average File Size Per Hour (gigabytes)
HQ-High	1280x720	5	2.32
HQ-Medium	1280x720	4	1.89
HQ-Low	1280x720	3	1.46
SQ-High	864x480	2	1.09
SQ-Medium	864x480	1.5	0.88
SQ-Low	864x480	1	0.66

WatchGuard chose 720p, not because it's the highest possible setting, but because we believe that it is the *right* setting. 720p strikes a great balance between quality and file size. To move to 1080p would significantly increase the file size of every video that is recorded as well as impact battery life by requiring more from the camera's processor.

VISTA uses H.264 High Profile (HP). The H.264 HP technology creates files that are up to 40% smaller than video captured at equivalent qualities using simpler forms of H.264.

VISTA has a 130° Horizontal field of view, and a 90° vertical field of view. The camera lens is capable of being rotated 28 degrees vertically. These angles allow the camera to have a picture covering 8.5 feet wide by 3 feet high, from 24 inches away. An example of the resulting image is below.



- **Ultra-Wide Dynamic Range** – To provide the best video in all lighting conditions, VISTA uses Ultra-Wide Dynamic Range technology. Essentially, the camera records two exposures of each frame of video at the same time: one optimized for light and one optimized for dark. The images are instantly overlaid, resulting in video that accurately represents what the human eye naturally sees. The following picture compares standard camera technology with WatchGuard's Ultra-Wide Dynamic Range camera technology. The child on the bicycle is almost invisible in the picture on the left, but can be clearly seen in the image on the right.



Video Uploading – Video can be uploaded through an individual USB transfer / charging base, or through the 8-Bay Ethernet Transfer Station. One of the weakest parts of a wearable camera is often the cable used to connect it to a PC. Cables and connectors can be prone to breaking or wearing out over the life of a camera as they are subjected to many uses and insertions. WatchGuard has designed a very rugged USB base that is used for transferring video and thus eliminated what is often the weakest piece in a wearable camera solution.



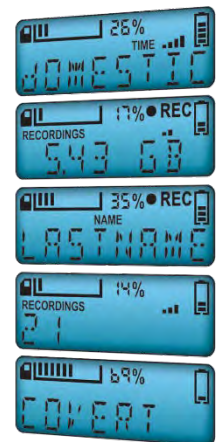
Through the individual USB base, VISTA can transfer video at a speed of 90 seconds per 1GB of data. The USB base also supports Dock and Go functionality allowing an officer to simply dock the camera and walk away. Even if the camera is off or the battery is completely drained, the USB base will power it on and initiate the file transfer.

Additionally, WatchGuard has designed an 8-Bay Transfer Station equipped with a Gigabit Ethernet port to dock and charge VISTA. This has the option of being rack mounted to allow for multiple Transfer Stations to easily be setup at a given location making it a highly scalable solution for any size agency. The Transfer Station can transfer video from 8 cameras simultaneously at up to 300Mbps.



- **Ease of Use** – VISTA was designed to be intuitive and simple to use while providing clear information as to camera status and operating condition. VISTA includes an easy one-touch operation. Simply press the button on the front of the camera to begin recording. Press the button again to end a recording.

Most other cameras use a single blinking LED light to communicate the status of storage, battery life, and recording state. The information available from this is minimal and often confusing. VISTA incorporates an LCD screen on the top of the camera to show exactly how much memory is still available, the exact battery life, how many recordings have been captured, and of course the recording state. The screen is also used to easily categorize recordings once they are stopped.



- **Record-After-The-Fact** – VISTA is designed with 32GB of storage that can be configured to constantly buffer video, even if the system is not actively recording. Depending on the video quality setting, VISTA provides the capability to go back in time from 12 hours up to 45 hours to capture critical information when it's needed. When VISTA is docked, the recorded events automatically upload to Evidence Library and the continuous video buffer stays on the device to be recorded over once it's full. If video is needed from the continuous buffer, this can easily be captured by creating a Record-After-The-Fact (RATF) event in Evidence Library while VISTA is docked. VISTA is the only wearable



camera providing the ability to go back in time and capture critical video that would not otherwise be recorded.

- **Battery Life** – VISTA includes a Lithium Polymer battery that has a stand-by life of 19 hours without pre-event or Record-After-the-Fact enabled. The approximate battery life of a single charge for our Extended Capacity VISTA allows for continuous recording of:
 - 9 Hours of recording at 720p resolution
 - 10 Hours of recording at 480p resolution

Additionally, VISTA includes intelligent standby timers to help further the actual battery life. VISTA has the ability to be configured to enter standby mode after a determined time has elapsed based on two independent options: No Movement – determined by internal accelerometers; or No Button Presses.

An upcoming item we will have available is a magnetic car charging cable that will allow officers in a car to snap the charger to the bottom of the VISTA adapter, and charge the camera while it is still operational and being worn. The cable will break away if ever forgotten to unhook when leaving the vehicle.

- **Mounting Options** – VISTA is available with a unique Chest Mount that overcomes the challenges of other mounting solutions. The Chest Mount system is designed to securely hold the camera to the uniform while keeping it very stable. It mounts the camera just below the shoulder of the Officer, rather than center mass, so that the lens is not obstructed by the user's arms when they are outstretched in front of the body.



Other mounting options include:

- Rotatable Shirt Clip
- Duty Belt Clip
- Molle Loop Mount

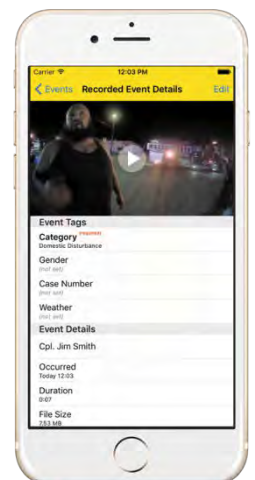
- Velcro® Plate Mount
- Klick Fast® Mount
- Tripod Mount
- RAM® Mount

VISTA WiFi

VISTA WiFi includes the same features of VISTA Extended, but adds additional functionality, including an integrated Wi-Fi radio and GPS capabilities.

VISTA WiFi is designed to add a new level of integration and functionality to 4RE, the industry's leading in-car video system, by maintaining an intelligent link to 4RE with almost no impact to VISTA's battery life. The integrated GPS receiver ensures perfect time synchronization between 4RE and VISTA.

- **Distributed Multi-Peer Recording** – This technology distributes decision-making to each camera in a multi-peer relationship. Imagine a network of cameras continually sensing the recording status of each other, acting in a peer-to-peer relationship.
 - Any camera (4RE or VISTA WiFi) can initiate a recording, and the other cameras, sensing a change in recording status, will begin recording
 - No one camera acts as a single, central controller, thus removing the single point of failure
 - A camera that initiated the group recording can move out of connectivity range without stopping the group recording in progress
 - A VISTA WiFi that's currently recording can "walk into" a group network on which it was previously associated, and the other cameras, sensing the recording status of that VISTA WiFi, will begin recording.
 - A VISTA WiFi not currently recording can "walk into" a group network on which it was previously associated, and sensing the other cameras recording, will begin recording.
- **Stand-Alone Vehicle Trigger Kit** – An upcoming release will include a Vehicle Trigger Kit that will allow VISTA to accept automatic triggers using inputs such as the emergency lights or vehicle siren, without the use of a 4RE in-car video system.
- **In-Field Viewing** – VISTA WiFi uses with SmartConnect, an optional smart phone application that will provide the officer with immediate in-field access to VISTA. Smart Connect includes the ability to:
 - Automatically and securely pairs with VISTA



- Categorize recordings
- Enter incident IDs, case number and more
- Play back recordings in HD at full frame rates
- The live viewfinder lets you see what the camera sees
- Control the VISTA camera remotely
- Change officer alert types, volume and brightness
- Toggle VISTA in or out of Covert Mode

Video from VISTA can also be reviewed with the Evidence Library Viewer application on a laptop or MDT in the police vehicle. The Evidence Library Viewer is designed to allow an officer to review video in the field while also uploading it from the VISTA camera later to the main Evidence Library database.

VISTA XLT

VISTA XLT includes the same features and functionality as VISTA Extended and VISTA WiFi, but offers additional mounting options and an extended battery life. VISTA XLT is WatchGuard's latest offering in body worn cameras.

VISTA XLT is a two-piece body-worn camera system with amazingly small, lightweight, interchangeable head and body-mounted HD cameras that allow officers to adapt to changing assignments and uniform types. Amazingly small, lightweight HD body-mounted camera is extremely comfortable to wear and easy to attach to any uniform, vest, or jacket.

Interchangeable head and body-mounted HD cameras allow officers the ability to record events from the optimal perspective using a single body camera system.

- **12+ Hour Battery Life** – VISTA XLT includes beyond full shift battery life. 12 hours of continuous HD recording allows officers to work beyond scheduled shifts without worrying about the battery keeping up. The two-piece design allows for a larger battery capacity in the DVR, extending the continuous recording life versus VISTA WiFi.

- **Head or Body Camera Options** – VISTA XLT provides a head-mounted or body-mounted HD camera. Each camera records audio and video and is connected to the DVR via a cable, which is often worn under the officer's shirt, vest or jacket. Both cameras, as well as the DVR, have a record button used to start and stop recordings.

The glasses mount snaps in to place around the forward part of the barrel on the head-mounted camera.



The magnetic mount is similar in concept to the clocking chest mount used for VISTA and VISTA WiFi, using under- and outer-shirt plates. The camera is seated in a base and held in place with two quick-release sliders. This forms the outer shirt plate. The under-shirt plate is placed under the officer's shirt.



- **Charging and Event Offloading** – VISTA XLT can charge and offload events using the VISTA USB dock or the 8 Bay Ethernet Transfer Station.

Camera Specification Comparison Table

	VISTA Extended	VISTA WiFi	VISTA XLT
Built-in Wi-Fi and GPS	No	Yes	Yes
Continuous HD Recording	11 Hours	9 Hours	12 Hours
Continuous SD Recording	12 Hours	10 Hours	13 Hours
DVR Size	3"H x 1.9"W x 1.3"D	3"H x 1.9"W x 1.3"D	3.3"H x 1.9"W x 1.3"D
DVR Weight	5.3 Ounces	5.3 Ounces	6.3 Ounces
Storage Capacity	32GB	32GB	32GB
Field of View	130°	130°	130°
Selectable Resolution	720p / 480p	720p / 480p	720p / 480p
Body-Mounted Camera Size	-	-	1.1"H x .84"W x .93"D
Head-Mounted Camera Size	-	-	.84"H x .84"W x 1.84"L
Body-Mounted Camera Weight	-	-	.5 Ounces
Head-Mounted Camera Weight	-	-	.4 Ounces

INTRODUCTION

Since the 4RE HD Digital In-Car Video System was released in 2010, it has continually been improved upon through firmware updates that have added additional features and enhanced the user experience. The latest addition to 4RE is the support for VISTA WiFi, a fully integrated body worn camera.

WatchGuard Video is pleased to present VISTA WiFi/4RE In-Car Camera System. VISTA WiFi is designed to add a new level of integration and functionality to 4RE, the industry's leading in-car video system, by maintaining an intelligent link to 4RE with almost no impact to VISTA's battery life. The integrated GPS receiver ensures perfect time synchronization between 4RE and VISTA.



Integrated in-car/body-worn offers in the market today are limited in two respects. First, many are simply one-directional, single-device recording triggers. At the most basic level, either a device outside the car (i.e. external microphone) signals the in-car video camera to begin recording, or an event in the car (i.e. light bar activation) signals a body-worn camera to begin recording. This operation is similar to using a remote control to start a recording on the DVR in your home entertainment system. It's a one-directional triggered event of a single recording device.

Secondly, even the more advanced offerings that allow connection to multiple devices (cameras) rely on a central controller to provide instruction. This would be equivalent to using a master DVR in your home entertainment system to tell other DVRs throughout your house to begin recording. It's a one-directional, one-to-many recording trigger. Building the architecture around a central controller introduces a single point of failure, should the controller lose connectivity

WatchGuard's Distributed Multi-Peer Recording technology distributes decision-making to each camera in a multi-peer relationship. Imagine a network of cameras continually sensing the recording status of each other, acting in a peer-to-peer relationship.

- Any camera (4RE or VISTA WiFi) can initiate a recording, and the other cameras, sensing a change in recording status, will begin recording
- No one camera acts as a single, central controller, thus removing the single point of failure
- A camera that initiated the group recording can move out of connectivity range without stopping the group recording in progress
- A VISTA WiFi that's currently recording can "walk into" a group network on which it was previously associated, and the other cameras, sensing the recording status of that VISTA WiFi, will begin recording.
- A VISTA WiFi not currently recording can "walk into" a group network on which it was previously associated, and sensing the other cameras recording, will begin recording.



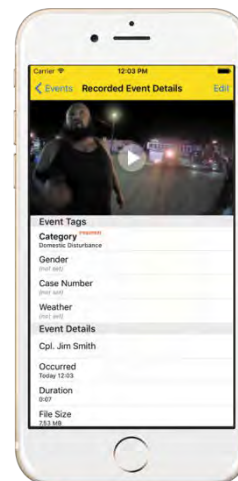
VISTA WiFi removes the need for the 4RE Wireless Microphone by providing the audio for 4RE and it is automatically activated by 4RE and can remotely activate 4RE to record. VISTA WiFi also becomes an additional camera view for 4RE and inherits the event properties of the 4RE recording such as officer name, event category, case number and more.

4RE and VISTA are the components Officers will interface with every day. 4RE is built small, lightweight, rugged, user-friendly, and requires minimal Officer interaction. The system has automotive grade components that feature a sturdy over-molded construction, which increases durability as well as occupant safety. Further adding to the robustness of the system, all vital connections are locking connectors that have been thoroughly tested in this environment.

VISTA is designed with industrial grade components, and constructed of cast magnesium, an ultra-hard military-grade resin and polyurethane rubber. Together the components and construction provide an extremely wide operating range of -40°F - +185°F in an ultra-rugged design to meet the demands of law enforcement.

In addition to working with 4RE, VISTA WiFi will also work with SmartConnect, an optional smart phone application that will provide the officer with immediate in-field access to VISTA.

- Automatically and securely pairs with VISTA
- Categorize recordings
- Enter incident IDs, case number and more
- Play back recordings in HD at full frame rates
- The live viewfinder lets you see what the camera sees
- Control the VISTA camera remotely
- Change officer alert types, volume and brightness
- Toggle VISTA in or out of Covert Mode



EVIDENCE LIBRARY 4 EVIDENCE MANAGEMENT SOFTWARE

The Department's current solution, Evidence Library 4 Web (EL4), utilizes Microsoft SQL Server databases, and can be hosted on premise on agency servers, or deployed as a hybrid solution.

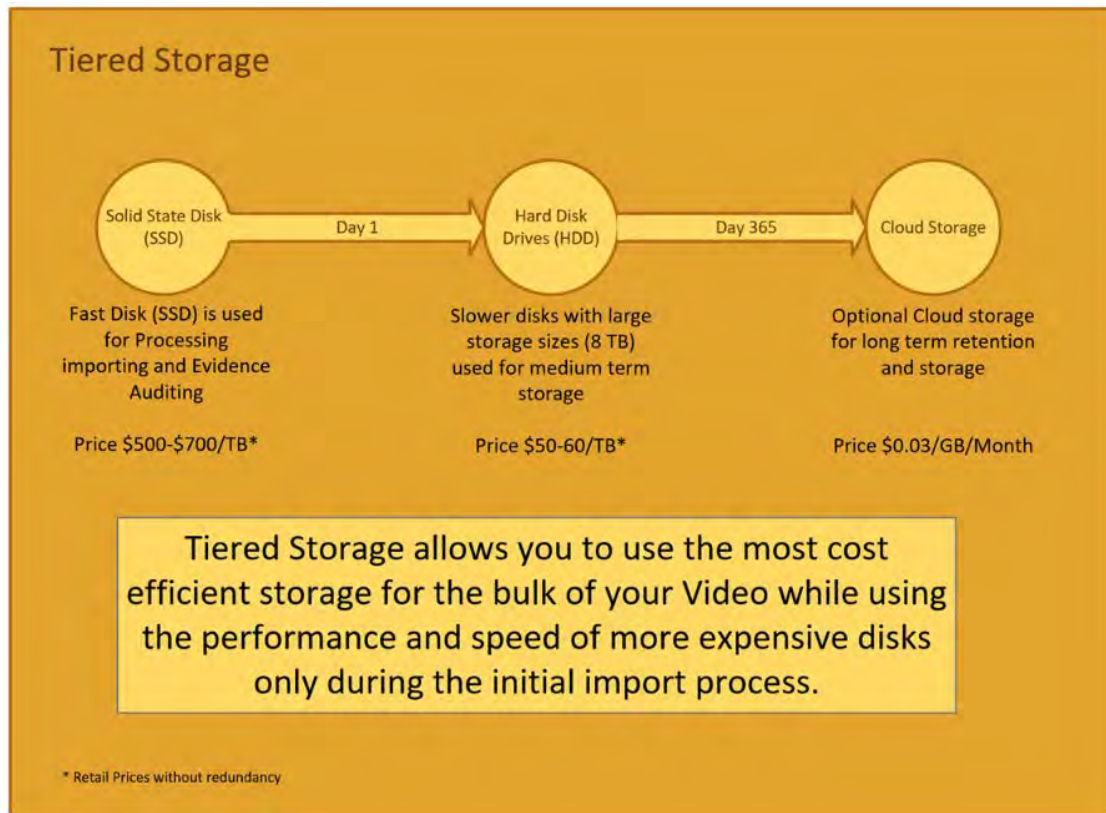
EL4 provides advanced file management, a graphical search engine, the ability to share important evidence, and a feature-rich media player, which is all accessible from a convenient Web Client. WatchGuard engineers designed this software from the ground up to have all of the functionality, features, and the customization options necessary to ensure that law enforcement agencies have a tool they can use to protect, search, copy, share, and create reports for their video evidence.

Evidence Library is primarily based on the Microsoft technology. Using the building blocks of Microsoft Windows Server, Microsoft SQL Server and Active Directory provide for seamless integration in to your existing infrastructure. The primary interface is a modern web browser making deployments fast and easy.

We propose the department utilize the servers already in use for either On-Premise storage or Hybrid. The storage solution that was purchased in 2016 and 2017 includes a large amount of storage and is also expandable at a fraction of the cost of cloud storage.

Storage options include:

- **On Premise Storage** – An on-site storage solution allows video to move rapidly from the cameras to the storage device. The movement of large amounts of video from hundreds of cameras can be complete in minutes instead of hours. This frees up cameras to be used for multiple shifts, which means the Department could purchase fewer cameras, docking stations and transfer bays.
- **Hybrid Storage** – The EL4 hybrid model offers a combination of both on premise storage and cloud storage. This will allow the agency to store video on premise for a defined period of time and then have video moved to the Cloud for long-term storage. This provides the cost efficiency of on premise storage during the time when most access to video is needed while also providing the benefits of CLOUD-SHARE and Cloud storage for long-term retention and archiving.



Hybrid Solution

A hybrid On Site / Cloud storage solution offers a best of both worlds deployment scenario. A hybrid solution provides the Department with the same benefits of an on-site solution, which includes:

- 1) Fastest possible video offload speeds
- 2) Quickest access to video

It also allows the Department to have video stored on premise during the time period when quick access to video is needed (generally right after an important incident has occurred), and then it automatically moves video to a secure CJIS compliant Cloud where it can live out its long-term storage requirements. A hybrid solution also requires considerably less hardware to be purchased and maintained locally than an on-site solution.

This solution works well for an agency that is comfortable with Cloud storage. It can be setup to use an existing Cloud storage agreement, or with a new agreement.

Cloud storage support is currently limited to two types, Microsoft Azure Public and Microsoft Azure Government.

Microsoft Azure Government is an isolated version of Azure that is exclusively used by US Government Agencies and qualified vendors. Microsoft has signed CJIS agreements with multiple states and has committed to maintain strict standards of compliance.

WatchGuard Video is a Microsoft Managed Service Provider for Azure Government and can sell services to our customers if they do not already have Azure Government contracts.

When available, WatchGuard Video will recommend the use of Microsoft Azure for cloud storage. The cloud platform is designed to meet US government demands, including:

- Physical and logical network-isolated instance of Azure
- Dedicated to US government with all data, applications, and hardware residing in the continental United States
- Broad range of compliance certifications critical to US government
- US datacenters located more than 500 miles apart, providing true geographic redundancy
- Support for hybrid scenarios, as well as a vast array of services, programming languages, and tools

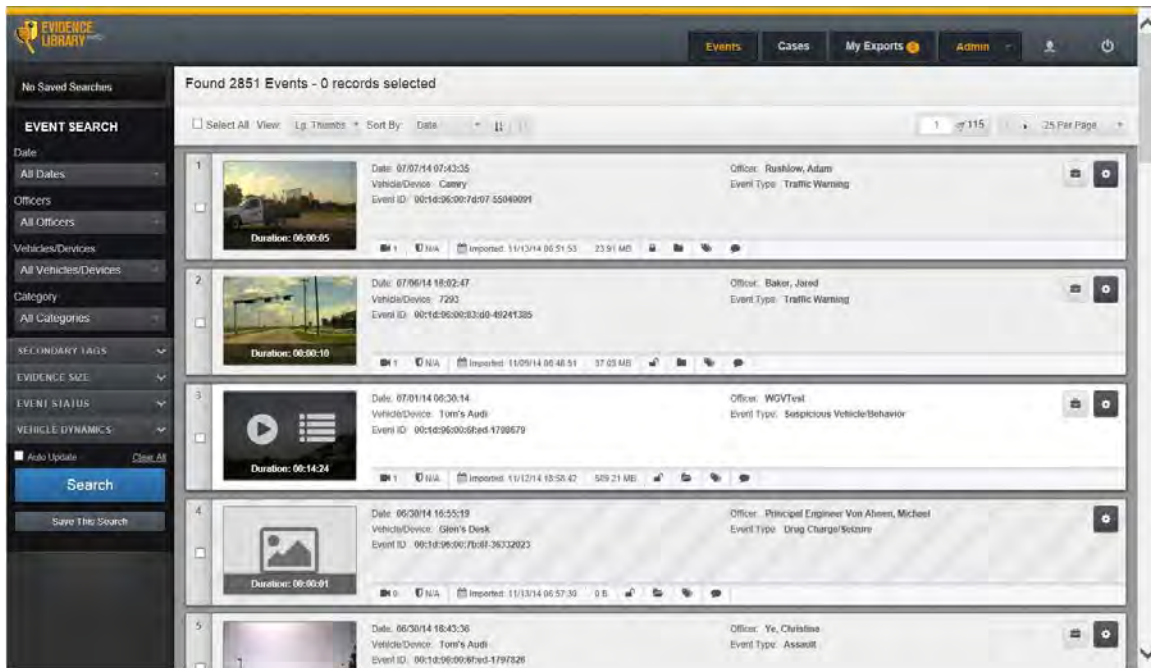
Data centers are located in Iowa and Virginia with redundant data stored at both locations. All servers hosted in the Azure datacenter will be setup so that their disks are globally redundant (exist in both datacenters). In the event of a disaster, the VMs can be recovered in a 24-hour period. All video storage in Azure blobs is also globally redundant with three copies kept in each datacenter. In the event a datacenter is unavailable, all naming references will transition to the redundant datacenter.

Azure Express Route is a private link to either Azure service that increases bandwidth and reduces network latency. It is not required for either solution but is recommended when large volumes of data are going to be sent to Azure.

FEATURES AND FUNCTIONALITY

The Interface

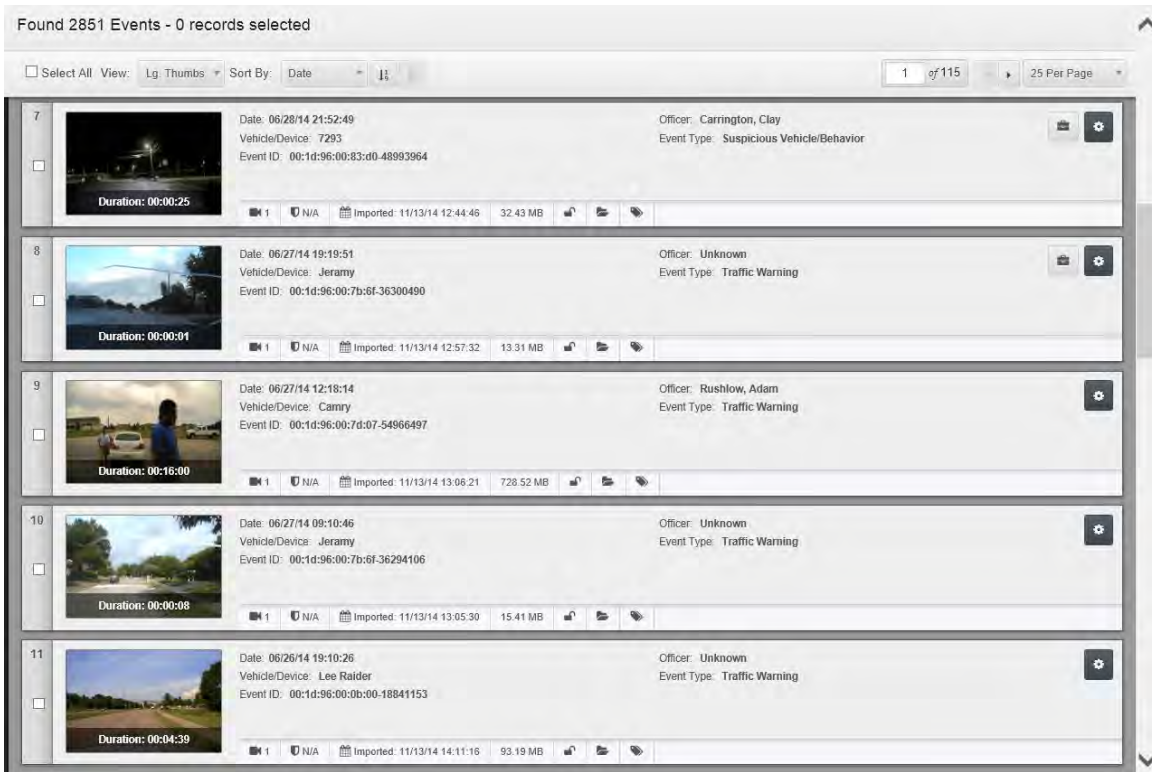
Evidence Library uses a very intuitive graphical and tabbed interface. This interface allows the user to easily toggle between the available functions of EL4, including Events, Cases, Exports, and Admin functions.



Events Tab

The Events tab provides a view of the Recorded Events in EL4 from both VISTA and 4RE. When an officer uses both VISTA and 4RE on the same incident, EL4 automatically links the recordings together based on 4RE and VISTA recordings that have the same officer name and a date and time overlap. With the introduction of VISTA WiFi, the recordings will be linked together through the synchronization in the vehicle as VISTA becomes part of the 4RE system. As a further level of integration, EL4 will also support simultaneous playback allowing for multiple camera streams to be played back in synchronization so the user can watch both the 4RE video and VISTA video at the same time.

From the Events Tab, important information from each event is displayed on this screen including, a thumbnail image from the event, Date/Time, Vehicle/Device, Event ID, Officer Name, and Event Type. Additionally, the user can see other key pieces of information at a glance such as the date the event was imported, the number of camera views, the size of the event, secondary Event Tags like Case Number, and notes. From here, events can easily be played, exported or added to a case.



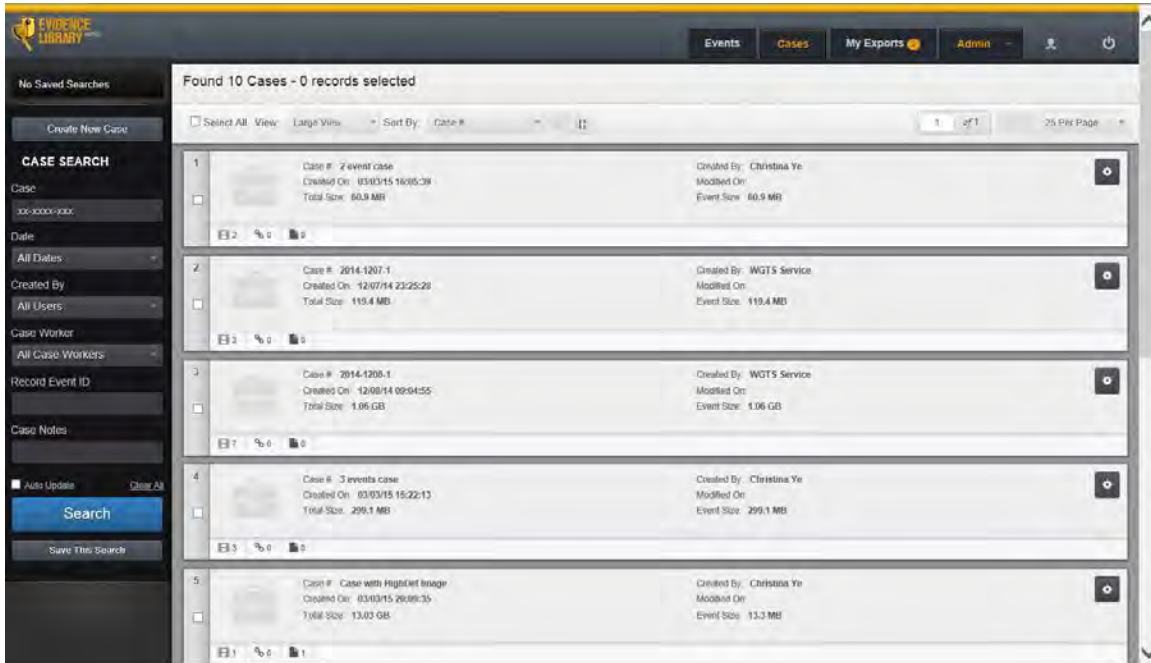
Found 2851 Events - 0 records selected

Select All View: Lg Thumbs Sort By: Date 1 of 115 25 Per Page

Event ID	Date	Vehicle/Device	Officer	Event Type	Duration	Imported	Size
00:1d:96:00:83:d0-48993964	06/28/14 21:52:49	7293	Carrington, Clay	Suspicious Vehicle/Behavior	00:00:25	11/13/14 12:44:46	32.43 MB
00:1d:96:00:7b:6f-36300490	06/27/14 19:19:51	Jeramy	Unknown	Traffic Warning	00:00:01	11/13/14 12:57:32	13.31 MB
00:1d:96:00:7d:07-54966497	06/27/14 12:18:14	Camry	Rushlow, Adam	Traffic Warning	00:16:00	11/13/14 13:06:21	728.52 MB
00:1d:96:00:7b:6f-36294106	06/27/14 09:10:46	Jeramy	Unknown	Traffic Warning	00:00:08	11/13/14 13:05:30	15.41 MB
00:1d:96:00:0b:00-18841153	06/26/14 19:10:26	Lee Raider	Unknown	Traffic Warning	00:04:39	11/13/14 14:11:16	93.19 MB

Cases Tab

EL4 includes the ability to perform Case Management, which allows the ability for case “container” creation and content management. With this feature, users may associate one or more VISTA or 4RE recordings with a case, as well as other general user files such as: PDFs, spreadsheets, reports, videos from 3rd party systems, audio recordings, still pictures, drawings, etc. Cases can be further managed by adding users as Case Workers with specific sets of permissions for that case.

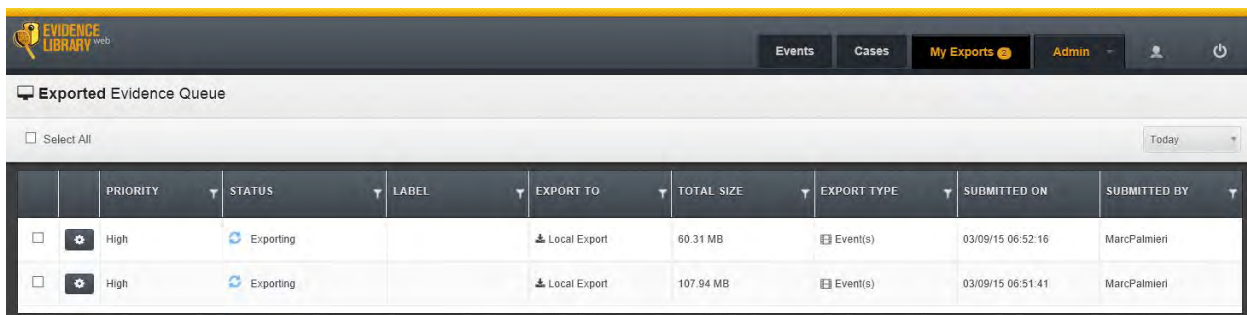


The screenshot shows the 'Cases' tab in the Evidence Library web interface. The top navigation bar includes 'Events', 'Cases', 'My Exports', and 'Admin'. The left sidebar contains search filters for Case, Date, Created By, Case Worker, Record Event ID, and Case Notes. The main area displays a list of 10 cases, with 0 records selected. The cases are sorted by Case # and include details such as Case #, Created On, Total Size, Created By, Modified On, and Event Size.

Case #	Created On	Total Size	Created By	Modified On	Event Size
Case # 2 event case	03/03/15 16:05:39	60.9 MB	Christina Ye		60.9 MB
Case # 2014-1207-1	12/07/14 23:25:29	119.4 MB	WGT'S Service		119.4 MB
Case # 2014-1208-1	12/08/14 09:04:55	1.06 GB	WGT'S Service		1.06 GB
Case # 3 events case	03/03/15 16:22:13	299.1 MB	Christina Ye		299.1 MB
Case # Case with Highlight Image	03/03/15 16:06:35	13.03 GB	Christina Ye		13.3 MB

My Exports Tab

“My Exports” allows a user to see and manage their exports and since EL4 includes a Web Client, this can be done from any computer on the network that the user has access to. The “My Exports” view can easily be sorted and filtered so it can be easily managed.



The screenshot shows the 'My Exports' tab in the Evidence Library web interface. The top navigation bar includes 'Events', 'Cases', 'My Exports', and 'Admin'. The left sidebar contains search filters for Case, Date, Created By, Case Worker, Record Event ID, and Case Notes. The main area displays a table of exported evidence items, sorted by Priority, Status, Label, Export To, Total Size, Export Type, Submitted On, and Submitted By.

PRIORITY	STATUS	LABEL	EXPORT TO	TOTAL SIZE	EXPORT TYPE	SUBMITTED ON	SUBMITTED BY
High	Exporting		Local Export	60.31 MB	Event(s)	03/09/15 06:52:16	Marc Palmieri
High	Exporting		Local Export	107.94 MB	Event(s)	03/09/15 06:51:41	Marc Palmieri

Kiosk Mode

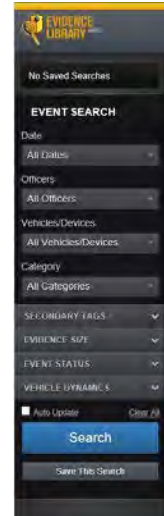
Kiosk mode allows for VISTAs to easily be used in a pooled camera environment where an officer is allowed to use any available camera rather than having a camera assigned to them. For Little Rock Police Department, this means, not as many body worn cameras would need to be purchased.

From the Kiosk (this is a feature of EL4 that is designed to run in a web browser on a network PC), the officer simply selects their name from a dropdown list and then chooses VISTA Checkout. The Kiosk will then determine the best VISTA for the officer based on the following criteria: fully charged battery and all events transferred. The Kiosk then displays the location of the assigned VISTA (Transfer Station and Slot number) and that VISTA will begin to beep and the LCD screen will illuminate and display the officer's name making it easy to identify.



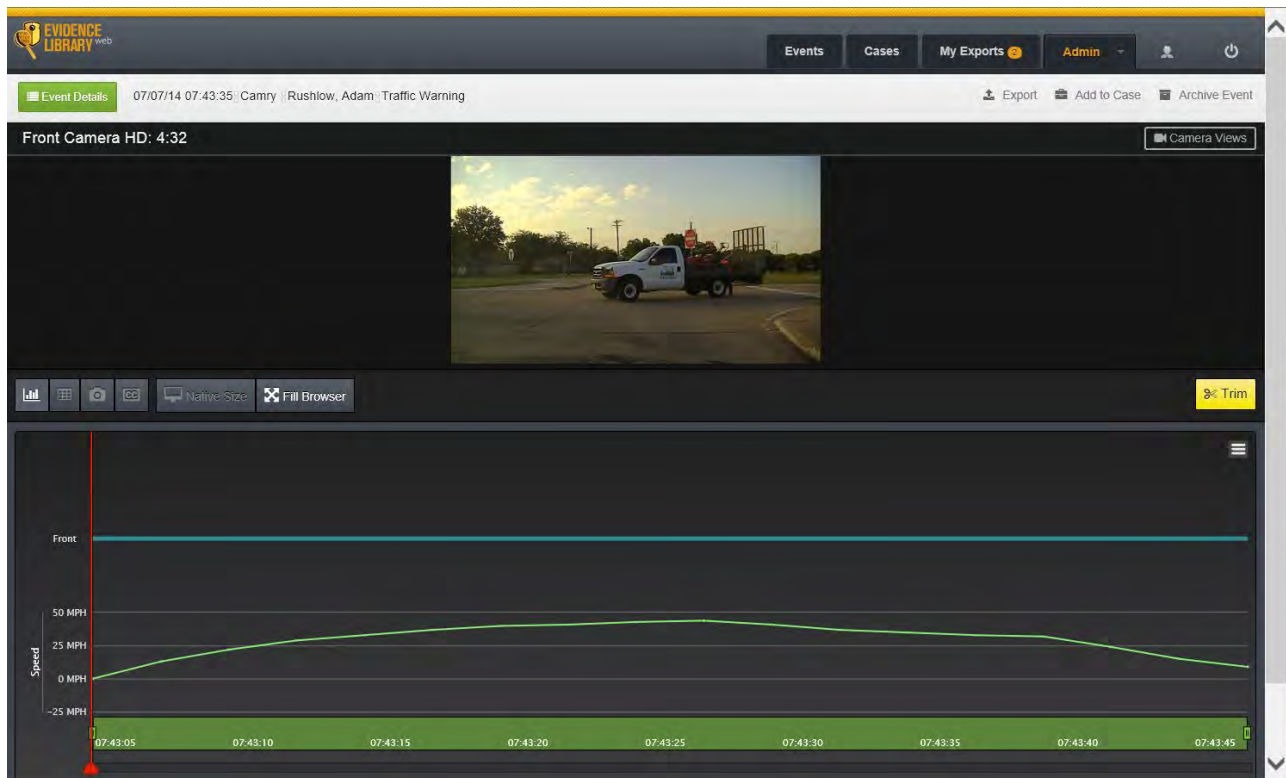
Graphical Search Engine

Searches are performed live on the Search bar, which can be simple or complex in nature, allowing all types of searches to be performed from the same area without leaving the main Records Events screen. The ability to perform complex searches on the Search bar allows for building and saving complex searches using multiple fields, with both specific values or across ranges in a graphical environment. For example, a search could easily be created to find any recordings in the last 60 days tagged as “Traffic” or “Other”, with a radar target speed of 55 MPH or higher, that occurred within 1.25 miles of a specific GPS location.



Media Player with Timeline Graphing

The built-in media player includes a graphical display of the dynamic metadata. Users can visually spot when lights, siren, or brakes were activated during the event timeline or view the patrol speed graph to quickly find moments of interest. Snapshot and copy/export functions are built into the player, including the ability to burn DVDs or convert file formats along with the ability to trim video.



Convenient Export Video Player

Evidence Library makes it easy to share video with attorneys and prepare videos for court. An embedded player can be included during file export, which enables any PC to play the video files without the need to install software prior to playing the video.

CLOUD-SHARE

In addition to the traditional method of exporting video to a disk or other device to then be shared, EL4 includes the ability to share Events and Cases by publishing the information to the Cloud in a Microsoft Azure CJIS certified data center through CLOUD-SHARE. A link with permissions and expiration dates can then be shared with the appropriate individuals. Links can be sent with one of the following permissions:

- Access allowed to anyone with the link.
- Access allowed with a secure access code
- Access only allowed to a registered user

The ability to use CLOUD-SHARE is a permission that must be assigned to EL4 users and parameters, such as how long the information can be made available for and e-mail addresses and domains allowed for sharing, are administratively controlled. After information has been shared, sharing permission can later be revoked if necessary.

With EL4, WatchGuard has developed a locally hosted solution with the ability to share via a secure hosted cloud solution. This offers the benefits of an on premise deployment while providing cloud based sharing for your critical video without the need to store everything in the cloud. This solution avoids the high reoccurring costs of storing everything in the cloud when only a small percentage of video is needed for easy sharing and distribution. On average we find that agencies typically share 5% or less of the total amount of video they accumulate.

Admin Tab

The Admin Tab provides access to Administrator function such as, Fleet Management, Security Management and Evidence Management with Email Notification for Storage Alerts.

Fleet Management – This section of the client is where all of the VISTA Cameras and 4RE DVRs are provisioned and settings are applied. Evidence Library supports a very capable Fleet Management section that includes group level configurations, automatic configuration updates to VISTA Cameras when docked and 4RE DVRs wirelessly or manually by USB, and firmware upgrades that are automatically sent to the VISTA Cameras when docked and the 4RE DVRs wirelessly or manually by USB. Fleet Management is also where all the various policy and system settings for VISTA and 4RE are configured including Event Categorization. Fleet Management consists of four major parts:

- Department Information
 - These settings include Department Name, Units of Measure, The IP address of the Application Server, and the Admin Password that is used in 4RE.

➤ All Devices

- This is the section that will hold all of the device information for the Department's VISTA and 4RE systems. After a device is created, it may then be assigned to a configuration, which is a set of unique settings that will be applied to all the devices assigned to the configuration.
- Once a device is in your Fleet, upon its first upload it will then begin to track its current firmware version and current configuration status. Any out-of-date devices or devices that are not assigned to any configurations will be noted on the list of devices.

➤ All Officers

- The All Officers section will show a global list of all the users who have either the "VISTA/4RE Officer" or "VISTA/4RE Officer and Supervisor" claims. It will also show what Configurations the Officers are assigned to. Essentially, any configuration that an Officer is assigned to means that this Officer's name will appear in the list of Officer Names when checking out a VISTA Camera or logging into the 4RE DVR. From this screen, multiple Officers may be selected and quickly assigned to an existing configuration.

➤ Configurations

- A configuration is a set of VISTA and 4RE policies and settings.
- A configuration contains a unique set of devices assigned to it.
- Multiple configurations may be created.
- Within a configuration lies 4 different sections:
 1. Assigned Devices
 2. Assigned Officers
 3. Recording Properties - All of the Recording settings for VISTA and 4RE are configured in this area. Recording properties affect camera resolution, Pre-Event time, Recording Reminder Alerts, Record-After-The-Fact, and additional criteria.
 4. Device Behavior - The final area of the configuration is Device Behavior. This is where most policy and power settings are made such as Sleep timers and Automatic Off timers.

➤ Event Tag Configuration

- Here the Department may designate which Event Categories should be prompted on VISTA after the Officer stops the recording. Event Category options are often times things like, Warning, Citation, DUI, Arrest, or whatever else may be applicable to the department. In addition to helping

with searching video, Evidence Retention policies can also be tied to Event Category.

- Additional Event Tags may be created for the sole purpose of back office use, and therefore not applied on the VISTA camera. The information for these tags can be entered in EL4 after video has uploaded. Creating and editing the Event Tags is done globally using either a wizard or by manually creating them. Event tags may be any of the following formats:
 1. List of answers
 2. Alphanumeric input
 3. Numeric input
- There is no limit as to how many tags may be created.

Security Management – The Security Management module of EL4 houses all of the user information, permissions and group level security settings. Users of the system must include any person who will be logging into the Web Client or operating a VISTA or 4RE system. After the users are entered into the system (Active Directory integration available) User Groups are created that give a specific set of permissions, or claims. Users are then added into User Groups based on the level of access to the system needed. Based upon the Department's desire for certain users to perform certain tasks, groups may be dynamically created for nearly any circumstance the Department envisions.

Claim Name	What Action The Claim Allows																			
	Login	Search for Unrestricted Record Events	Review and Play Unrestricted Record Events	Mark a Record Event as Restricted	Search for Restricted Record Events	Review and Play Restricted Record Events	Un-Restrict a Record Event	Edit Record Event Properties	Import Record Events via US Transfer	Export Record Events	Setup Users, Groups and Permission Levels	Restore Record Event Data	Evidence Management Access	Audit Log Review	Ability to Archive to Online Storage	Granted In-Car Supervisor Permissions	Create and Manage Case Artifacts	Allows the Viewing of Case Artifacts	Grants Access to Watch Commander	
User	Yes	My	My																	
Enhanced Search		All																		
Enhanced Search and Review		All	All																	
Enable Restricted Access				Yes*																
Search and Review Restricted Events				Yes*	Yes	Yes	Yes													
Edit Record Event Properties								Yes*												
Import									Yes											
Export										Yes*	Yes*									
User Security Management											Yes									
Fleet Management												Yes								
Archive Restore													Yes							
Evidence Management														Yes						
Review Detailed Audit															Yes					
In-Car Officer																Yes				
In-Car Officer and Supervisor																Yes	Yes			
Case Management																	Yes	Yes		
Case Worker																	My	My		
Enhanced Case Worker																		Yes		
Live Video Streaming																			Yes	
Administrator	Yes	All	All	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	

* = Assumes other claims have allowed you access to the given event.

Evidence Management – Rules are created in this section of EL4 that determine how long video is kept before it is either deleted or archived. This section leverages the Event Category that was selected at the time of the recording or later identified in the client. For each Event Category listed, the Department is allowed to specify an action that is performed and at what interval it is performed. Both the retention period and the action performed on the event are choices left up to the Department.

The next configuration related to Data Cleanup is how the Department wants the Data Cleanup procedure to run. It may be set to run on a schedule automatically or manually at times initiated by a user with Evidence Management permissions. Regardless of when and how it runs, Data Cleanup will run through the entire list of retention rules and perform the actions necessary across the entire solution.

System Specifications for Evidence Library	
System	Minimum Requirement
Application / Database	64-bit Hardware Windows Server 2008 R2 64-bit, Windows Server 2012 R2 Microsoft SQL Server 2008 R2 Standard, 2012 Standard, 2014 Std. Virtual Server Support VMware vSphere Hypervisor (ESXi) Microsoft Hyper-V
Client Operating System	Windows 7 64-bit Windows 8.1 Windows 10 Windows Editions: Professional, Ultimate Member of Active Directory Domain
Client Hardware	1.7GHz Dual Core comparable or faster processor 4GB RAM or more 160MB of available hard-disk space DVD-RW drive One available USB 2.0 port Super VGA (1,024x768) or higher-resolution video adapter
Wireless Network	802.11n Compatible 5.2GHz (Recommended) or 2.4GHz band Available 40MHz channel WPA2-AES Encryption (128 bits) using PSK
Network	100Mb/1Gb Ethernet Available RFC 1918 (private) address space Sufficient bandwidth to transport data from Upload Server (if used)
Database Server Storage (Separate from Application Server)	Operating System – Mirrored 2x500GB SATA 7,200 RPM drives SQL Storage – Raid 5 3x500GB SATA 7,200 RPM drives Global Spare – 500GB SATA 7,200 RPM drive
Application Server Storage	Operating System – Mirrored 2x128GB SSD drives SQL Storage on Application Server – RAID 5 3x480GB SSD Drives Video Storage – Raid 5 3x (or more*) 4TB SATA 7,200 RPM drives Global Spare – 4TB SATA 7,200 RPM drive

EvidenceLibrary.com

EvidenceLibrary.com is a fully cloud hosted back office solution allowing an agency to have the application and all video storage in the cloud. EvidenceLibrary.com is a future release, that we expect to be available for deployment mid Q4, 2018.

EvidenceLibrary.com utilizes Microsoft Azure Government, which is an isolated version of Azure that is exclusively used by US Government Agencies and qualified vendors. Microsoft has signed CJIS agreements with multiple states and has committed to maintain strict standards of compliance.

WatchGuard is a Microsoft Managed Service Provider for Azure Government and can sell services to our customers if they do not already have Azure Government contracts. The cloud platform is designed to meet US government demands, including:

- Physical and logical network-isolated instance of Azure
- Dedicated to US government with all data, applications, and hardware residing in the continental United States
- Broad range of compliance certifications critical to US government
- US datacenters located more than 500 miles apart, providing true geographic redundancy
- Support for hybrid scenarios, as well as a vast array of services, programming languages, and tools

Data centers are located in Iowa and Virginia with redundant data stored at both locations. All servers hosted in the Azure datacenter will be setup so that their disks are globally redundant (exist in both datacenters). In the event of a disaster, the VMs can be recovered in a 24-hour period. All video storage in Azure blobs is also globally redundant with three copies kept in each datacenter. In the event a datacenter is unavailable, all naming references will transition to the redundant datacenter.

EvidenceLibrary.com offers two separate storage plans:

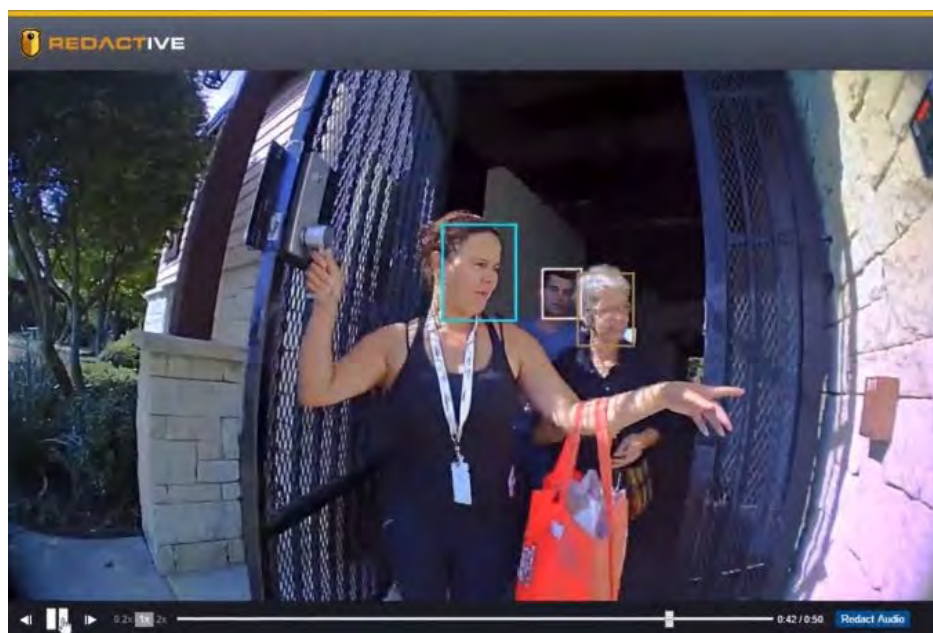
- **Better than Unlimited Plan** – Store an unlimited amount of HD and SD video recordings. The agency will receive unlimited storage for the published price if the data retention policy does not exceed one year for non-evidentiary recordings or 10 years for evidentiary recordings (evidentiary recordings are defined as recordings associated with a case).
 - Includes Unlimited Users – Everyone in the agency can access video evidence. No per user fees. EvidenceLibrary.com is not charged by the number of user accessing the system. It's charged by the number of devices. So, an agency may set up an unlimited number of users (i.e. administrators, supervisors, evidence technicians, officers, etc.) without incurring additional cost.

- Unlimited Sharing – Share video evidence with anyone who has an email address. No user account or fee required. EvidenceLibrary.com users will make use of CLOUD-SHARE to share evidence without service level or number of shares limitations.
 - Credit or Cash Rebate – Receive cash back or credit for using storage management best practices. When the actual data usage across all devices averaged over the year is less than 700GB per device, the agency will receive a rebate at the end of each contract year equal to 36¢ per GB for the year for each GB under 700GBs per device that is actually used. The agency gets to decide if the rebate is in the form of cash or credit.
- **Actual Usage Plan** – As inferred in the name, customers pay for total storage used per month. This plan does include unlimited users.

REDACTIVE Redaction Software

Redaction capabilities are provided by REDACTIVE, the solution currently being utilized by LRPD. Video files are imported in to REDACTIVE and then modified versions are saved. The original file will remain unaltered. REDACTIVE includes:

- Automated Face Detection
 - REDACTIVE quickly scans the entire video clip first, automatically detecting faces, so the user spends much less time manually performing the task
- Forward and Backward Object Scanning
 - Select any object at any point in the video clip and REDACTIVE will automatically scan forward and backward to find it, allowing the user to redact the object before or after the selection point – or throughout the entire clip.
- Simple, Selective Audio Muting
 - Select, preview and redact any portion of the audio track simply by highlighting the area with a click and drag of a mouse.





COSTARS - 12 PRICE LIST - WatchGuard Video

4RE In-Car Video System		MSRP	Contract
4RE-200-GPS-ZSL	4RE In-Car Camera System. Includes GPS, High definition Zero Sightline (720P) forward facing camera, Infrared color cabin camera, DVR, integrated 200GB automotive grade hard drive, 16GB USB removable thumb drive, cabin microphone, 900 MHz Hi Fidelity wireless microphone, hardware & cabling, 1 yr. warranty. Includes Evidence Library Express software.	5,990.00	4,783.00
4RE-64S-GPS-MTR	4RE Motorcycle Camera System. Includes GPS, Waterproof Display, Waterproof standard definition camera, DVR, integrated 64GB solid state hard drive, 16GB USB removable thumb drive, 900MHz Hi Fidelity wireless microphone, Wireless Microphone Lapel Microphone, hardware & cabling and One (1) Year Factory Warranty. Includes Evidence Library Express software.	6,270.00	5,295.00
4RE-200-VIS-INT	4RE High Definition In-Car Video System with Integrated VISTA Wi-Fi Includes: Zero Sightline HD Front Camera, Separate Back Seat Camera, VISTA HD Wi-Fi Integrated Wearable Camera, VISTA HD Wi-Fi Charging / Transfer Base, 4RE, VISTA, Smart PoE Switch (Connects the 4RE In-Car Video System to the VISTA HD Wi-Fi Wearable Camera in the vehicle) Integrated GPS, Crash detection, DVR with integrated 200GB, automotive grade hard drive, 16GB USB drive, 4.3" touch screen remote display control panel, Cabin microphone, All mounting hardware and cabling, One (1) Year Factory Warranty. Includes Evidence Library Express software.	6,995.00	5,495.00
4RE-200-INT-001	4RE Interview Room Solution, One Camera Package - Choice of: traditional dome security camera with integrated microphone, covert motion sensor hidden camera, and covert pinhole camera, DVR with integrated 200GB hard drive, 16GB removable USB flash drive, mounting hardware and cabling, Easy-On wall switch, and Watch Commander Live Video Streaming software.	5,990.00	4,995.00
4RE-200-INT-002	4RE Interview Room Solution, Two Camera Package - Choice of two cameras: traditional dome security camera with integrated microphone, covert motion sensor hidden camera, and covert pinhole camera, DVR with integrated 200GB hard drive, 16GB removable USB flash drive, mounting hardware and cabling, Easy-On wall switch, and Watch Commander Live Video Streaming software.	6,230.00	5,195.00
4RE-WRL-KIT-05G	Upgrade 4RE to wireless upload capability 802.11n 5GHz. Requires Evidence Library 3 software or higher	250.00	199.00
4RE ELITE	Upgrade 4RE DVR to Elite version supporting up to 6 cameras	345.00	275.00
4RE ZOOM UPGRADE	Upgrade front camera to HD zoom camera	250.00	199.00
4RE PANORAMIC UPGRADE	Upgrade front camera to the Panoramic camera	250.00	199.00
DUAL MIC UPGRADE	Upgrade to dual Hi-Fi wireless microphones	985.00	785.00
In-Car Hardware Warranty		MSRP	Contract
WAR-4RE-CAR-2ND	Warranty, 4RE, In-Car, 2nd Year (Months 13-24)	125.00	100.00
WAR-4RE-CAR-3RD	Warranty, 4RE, In-Car, 3rd Year (Months 25-36)	250.00	200.00
WAR-4RE-CAR-4TH	Warranty, 4RE, In-Car, 4th Year (Months 37-48)	410.00	325.00
WAR-4RE-CAR-5TH	Warranty, 4RE, In-Car, 5th Year (Months 49-60)	565.00	450.00
Evidence Library 4 Software		MSRP	Contract
SFW-ELX-KIT-100	Evidence Library Express Software	-	-
KEY-EL4-SRV-001	Evidence Library 4 Web Server Site License	1,250.00	1,000.00
KEY-EL4-DEV-001	Evidence Library 4 Web 4RE In-Car Device License	190.00	150.00
KEY-EL4-DEV-002	Evidence Library 4 Web VISTA Device License	190.00	150.00
KEY-EL4-DEV-003	Evidence Library 4 Web 4RE Combo-Discount Device License Key	95.00	75.00
KEY-EL4-DEV-004	Evidence Library 4 Web VISTA Combo-Discount Device License Key	95.00	75.00
SFW-EL4-CLD-BAS	Evidence Library 4 Web CLOUD-SHARE - Basic Includes 24 shares per device. Included with Evidence Library Software Maintenance.	-	-
SFW-EL4-CLD-FUL	Evidence Library 4 Web CLOUD-SHARE - Full Included 48 shares per device. Optional upgrade.	55.00	45.00
SFW-EL4-CLD-EXT	Evidence Library 4 Web CLOUD SHARE - Extended Includes 72 shares per device. Optional upgrade.	125.00	100.00
SFW-MOB-APP-001	VISTA Mobile Companion (ELX/EL4 No Maintenance Plan)	95.00	75.00
SFW-WCM-LIC-FEE	Watch Commander License Fee (per car)	275.00	250.00



COSTARS - 12 PRICE LIST - WatchGuard Video

SFW-WCM-KIT-100	Watch Commander Live Video Streaming Application	2,900.00	2,500.00
SFW-SQL-SRV-012	Software, SQL Server 2012, w/5 CAL	520.00	415.00
SFW-WIN-SRV-012	Software, Windows Server 2012, w/5C CAL	965.00	770.00
SFW-SQL-CAL-R21	Software CAL, SQL Server 2008, R2, 1 CAL	115.00	90.00
SFW-SQL-CAL-R25	Software CAL, SQL Server 2008, R2, 5 CALs	515.00	410.00
Evidence Library Software Warranty		MSRP	Contract
SFW-MNT-EL4-001	Software Maintenance, Evidence Library, 1st Yr (Months 1-12)	190.00	150.00
SFW-MNT-EL4-002	Software Maintenance, Evidence Library, 2nd Yr (Months 13-24)	190.00	150.00
SFW-MNT-EL4-003	Software Maintenance, Evidence Library, 3rd Yr (Months 25-36)	190.00	150.00
SFW-MNT-EL4-004	Software Maintenance, Evidence Library, 4th Yr (Months 37-48)	190.00	150.00
SFW-MNT-EL4-005	Software Maintenance, Evidence Library, 5th Yr (Months 49-60)	190.00	150.00
Additional Options		MSRP	Contract
USB-DRV-101-16G	4RE, USB 2.0 Thumb Drive, Rubberized, 16GB	50.00	39.00
USB--DRV-100-32G	4RE, USB 2.0 Thumb Drive, Rubberized, 32GB	90.00	70.00
CAM-AUX-SNY-SPR	Camera Assy, Auxiliary, Gimble Bracket Assy, 4RE	245.00	195.00
KEY-4RE-MBL-001	4RE, Mobile App License Key	65.00	50.00
HDW-ETH-SWT-001	4RE, Power Over Ethernet / Gigabit 4-port Switch (required when including both WiFi and Mobile App)	190.00	150.00
MIC-WRL-DTC-400	Hi-Fi Microphone Desktop Charger Kit 1 (Cradle, and AC Charger)	125.00	99.00
SVC-4RE-ONS-300	4RE, On-Site Service, Access Point Installation	1,250.00	1,000.00
SVC-4RE-ONS-400	4RE System Setup, Configuration, Testing and Training (per site)	3,125.00	2,500.00
SVC-4RE-INS-100	4RE System Installation, In-Car (Per Unit Charge)	QUOTED	QUOTED
SVC-VID-REM-100	Video System Removal (Per Unit Charge)	QUOTED	QUOTED
SVC-SIT-SUR-001	Site Survey, 4RE Wireless Discovery and Examination	4,375.00	3,500.00
MIC-WRL-TRN-400	Transmitter, Hi-Fi Microphone (additional)	435.00	345.00



COSTARS - 12 PRICE LIST - WatchGuard Video

Cables		MSRP	Contract
MIC-CBN-100-07F	Cabin Microphone - 7'	35.00	25.00
MIC-CBN-EXT-12F	Cabin Microphone Extension Cable - 12'	15.00	10.00
CAB-ETH-STR-10F	Cable Assembly, Straight Ethernet, CAT5e, 10'	15.00	10.00
CAB-ETH-STR-25F	Cable Assembly, Straight Ethernet, CAT5e, 25'	15.00	10.00
CAB-HDM-4RE-15F	4RE, Cable, HDMI/Mini, Display ONLY, Straight, 15'	25.00	19.00
CAB-HDM-4RE-15F	4RE, Cable, HDMI/Mini, Display ONLY, Straight, 15'	25.00	19.00
CAB-FWD-STR-15F	4RE, Cable, HDMI, Front Cam, Straight, 15'	25.00	19.00
CAB-ZSL-STR-15F	4RE, Cable, HDMI, ZSL, Straight, 15'	35.00	25.00
CAB-BST-STR-16F	4RE, Cable, HDMI, Port 2, Backseat Camera, 2-Pin Connect, Straight, 16'	40.00	30.00
CAB-EXT-MMB-15F	Cable Assy, 4RE, Extension, 15', male Molex/BNC, WardMay/Aux Camera	25.00	19.00
CAB-AUX-STR-03F	4RE, Cable, HDMI, Port 2, Dual, Auxiliary Camera, Straight, 3'	35.00	25.00
CAB-AUX-2PN-18I	Cable Assy, Auxiliary Camera (JCC), 4RE Short 18" (2 pin Molex Male)	35.00	25.00
CAB-MHD-STR-15F	CABLE, 4RE, M-HDMI STR to HDMI STR, 15' (HD Mini Zoom)	35.00	25.00
CAB-RIA-100-SRY	Radar Interface Cable for Stalker, Y-Cable, 10'	95.00	75.00
CAB-RIA-101-DG1	Radar Interface Cable for Decatur Genesis I, 12'	95.00	75.00
CAB-RIA-102-KSE	Radar Interface Cable for Kustom Eagle, 12'	95.00	75.00
CAB-RIA-102-KSR	Radar Interface Cable for Kustom Raptor RP-1, 12'	95.00	75.00
CAB-RIA-103-MPH	Radar Interface Cable, MPH Bee 3, Decatur Genesis II, 9 Pin D-Sub, 12'	95.00	75.00
CAB-RIA-104-DG2	Radar Interface Cable for Decatur Genesis II, 7mm LEMO, 12'	95.00	75.00
Brackets		MSRP	Contract
BRK-4RE-FPK-02I	Bracket Kit, 4RE, DVR, Console Faceplate, 2"	45.00	35.00
BRK-4RE-DVR-100	Bracket Kit, 4RE, DVR, Universal	95.00	75.00
BRK-MRU-200-099	Bracket, 4RE DVR, Mounting Shelf Kit, Ford Crown Victoria 1999-2009	95.00	75.00
BRK-4RE-OHD-101	Bracket Kit, 4RE, Display, Chevy Tahoe, 2007+	95.00	75.00
BRK-4RE-OHD-100	Bracket Kit, 4RE, Display, Ford Crown Vic, 2005(b)+	95.00	75.00
BRK-4RE-OHD-103	Bracket Kit, 4RE, Display, Dodge Charger, 2006-2010	95.00	75.00
BRK-4RE-OHD-104	Bracket Kit, 4RE, Display, Universal Visor Post	95.00	75.00
BRK-4RE-OHM-100	Bracket Kit, 4RE, Overhead Multi, Crown Vic (All), Expedition 03-06	95.00	75.00
BRK-4RE-OHM-101	Bracket Kit, 4RE, Overhead Multi, Headliner Clip, Expedition 07-11+	95.00	75.00
BRK-ANT-NMO-001	4RE, WiFi Vehicle Antenna Mount, NMO, Drill 3/4" Hole, 17' long	95.00	75.00
Servers and Storage Hard Drives		MSRP	Contract
HDW-4RE-SRV-001	Tower Server, Intel i7 3.40 GHz, 8GB RAM, 4x2TB SATA 7,200 RPM drives, 5.5TB usable video storage, Windows 7 Pro 64-bit, SQL Server 2008 R2 (1CAL), 3-Year full service (on-site or reimbursed) warranty.	4,360.00	3,481.00
HDW-4RE-SRV-002	Tower Server, Intel i7 3.40 GHz, 8GB RAM, 4x3TB SATA 7,200 RPM drives, 7.8TB usable video storage, Windows 7 Pro 64-bit, SQL Server 2008 R2 (1CAL), 3-Year full service (on-site or reimbursed) warranty.	4,800.00	3,832.00
HDW-4RE-SRV-102	Server, 4RE, 16 HDD, 3U, 6-15 Concurrent Cars, 5CAL, Gen 3 (3U rack mount, 16 SATA hard drive bays, plus 2 X 128GB SSD 6Gbps drives for the OS Partition, SAS backplane, dual 1200W power supplies, Intel XEON E5-1620 V3 3.5 Ghz 4 Core 8 Thread, 8GB (2x4GB), 1.2 V, DDR4 2133 ECC, LSI 9361-4I 12GB RAID SAS, PCIE 3.0, Microsoft Windows Server 2012 R2 64-Bit, Microsoft SQL Server 2012 Standard (5 CALs), 3 Year full service (on-site or reimbursed) warranty.	9,690.00	7,750.00
HDW-4RE-SRV-201	Server, 4RE, 3U, 16-35 Concurrent Cars, 5CAL (3U rack mount, 16 SATA hard drive bays, plus 2 X 128GB SSD 6Gbps drives for the OS Partition, SAS backplane, dual 1200W power supplies, SM X10SRI-F, Intel C612 Chipset, up to 1TB ECC 3DS RAM, PCI-E 3.0, Intel XEON E5-2620 V3 2.4 Ghz 6 Core 12 Thread, 32GB (4x8GB), 1.2 V, DDR4 PC4-1700, LSI 9361-4I 12GB RAID SAS, PCIE 3.0, Microsoft Windows Server 2012 R2 64-Bit, Microsoft SQL Server 2012 Standard (5 CALs), 3 Year full service (on-site or reimbursed) warranty.	11,065.00	8,850.00
HDW-4RE-HDD-4TB	Hard Drive, Server, 4TB, 7,200, 64MB cache 4RE	400.00	300.00
HDW-4RE-HDD-6TB	Hard Drive, Server, 6TB, 7200RPM, 4RE Enterprise Class	550.00	425.00
HDW-4RE-JBD-012	Storage, JBOD Enclosure, 12-bay, 2U, includes SAS Cable	3,220.00	2,575.00
HDW-4RE-JBD-016	Storage, JBOD Enclosure, 16-bay, 3U, includes SAS Cable	3,655.00	2,925.00
HDW-4RE-JBD-024	Storage, JBOD Enclosure, 24-bay, 4U, includes SAS Cable	4,190.00	3,350.00



COSTARS - 12 PRICE LIST - WatchGuard Video

HDW-4RE-JBD-044	Storage, JBOD Enclosure, 4RE, 44-bay 4U, Included SAS Cable	6,220.00	4,975.00
HDW-4RE-RBT-DVD	Primera Bravo 4101 DVD±/CD-R	3,745.00	2,990.00
HDW-4RE-RBT-BLU	Primera Bravo 4101-Blu DVD±/CD-R/BD-R	4,990.00	3,984.00
WAR-SRV-RCK-5YR	Warranty, Rack Server, Full Service On Site, 5-Year (Months 37-60)	1,470.00	1,175.00
Access Point		MSRP	Contract
WAP-BLD-05G-001	4RE, WiFi Access Point, 802.11n, 5GHz, Sector (includes PoE)	315.00	233.00



COSTARS - 12 PRICE LIST - WatchGuard Video

DV-1 In-Car Video System		MSRP	Contract
DV1-EOH-GPS	DV-1, Overhead System. Includes: Overhead Recorder Unit, Combination Front/Cabin Camera, Cabin Microphone, Hardware & Cabling, Lifetime Firmware Upgrades, One (1) Year Factory Warranty, Wireless Microphone Kit, Leather Holster, 10 Pack DVD+RW Evidence Discs, Fleet Manager Utility, DVD Manager Utility	6,240.00	4,920.00
DV1-EMD-GPS	DV-1, Modular System. Includes: Modular Recording Unit, Remote Display Control Panel, Combination Front/Cabin Camera, Cabin Microphone, Hardware & Cabling, Lifetime Firmware Upgrades, One (1) Year Factory Warranty, Wireless Microphone Kit, Leather Holster, 10 Pack DVD+RW Evidence Discs, Fleet Manager Utility, DVD Manager Utility	6,685.00	5,264.00
In-Car Hardware Warranty		MSRP	Contract
WAR-EXT-PUR-2YR	2 Year Extended Factory Warranty (Months 13 to 24)	315.00	250.00
WAR-EXT-PUR-3YR	3 Year Extended Factory Warranty (Months 13 to 36)	700.00	560.00
WAR-EXT-PUR-4YR	4 Year Extended Factory Warranty (Months 13 to 48)	1,185.00	945.00
WAR-EXT-PUR-5YR	5 Year Extended Factory Warranty, DV-1 (Months 13 to 60)	1,790.00	1,430.00
Additional Options		MSRP	Contract
CAM-AUX-SNY-SPR	Camera Assy, Auxiliary, Gimble Bracket Assy, 4RE	245.00	195.00
HDW-SYS-DCS-100	WatchGuard DVD Copy Station PC with preloaded software	2,370.00	1,892.00
PWR-UPS-INT-200	DV-1, iUPS (Intelligent Uninterruptible Power Supply)	190.00	150.00
DVD-EVI-MED-021	DV-1, Disc, Non-Labeled DVD+RW Blank Media	5.00	0.77
DVD-EVI-MED-011	DV-1, Non-Serialized DVD+RW Red Evidence Label Media	5.00	0.99
DVD-EVI-MED-001	DV-1, Serialized DVD+RW Red Evidence Label Disc Media	5.00	1.25
SVC-DV1-INS-100	DV-1 System Installation (Per Unit Charge)	440.00	350.00
MIC-WRL-TRN-400	Transmitter, Hi-Fi Microphone VERSION 2	435.00	345.00
MIC-WRL-DTC-400	Hi-Fi Microphone Desktop Charger Kit 1 (Cradle, and AC Charger)	125.00	99.00
Brackets		MSRP	Contract
BRK-CRC-103-008	Bracket, Installation Kit, Ford Interceptor SUV (Explorer), 2012	190.00	150.00
BRK-CRC-103-009	Bracket, Installation Kit, Ford Sedan (Taurus), 2012+ Interceptor	190.00	150.00
BRK-CRC-111-009	Bracket, Mounting Kit, DV-1 OH, Ford F-150, 2009+	120.00	95.00
BRK-CRC-109-013	Bracket, Mounting Kit, DV-1 OH, Dodge 1500, 2013	120.00	95.00
BRK-CRC-100-012	Bracket, Mounting Kit, DV-1 OH, Chevy Caprice 2014+	160.00	125.00
BRK-CRH-101-006	Bracket, Ceiling Mount Kit, Chevy Impala 2006-2012 (Remove Headliner)	120.00	95.00
BRK-VPM-101-006	Chevy Impala 2006-2009 (with Console)	60.00	45.00
BRK-CRC-103-008	Chevy Tahoe (2015+), Silverado, 2500, Suburban, Sierra (2014+)	220.00	175.00
BRK-VAC-107-004	Chevy Tahoe (with AC Controls) 2004-2006	160.00	124.00
BRK-CRC-107-007	Bracket, Ceiling Mount Kit, Chevy Tahoe PPV 2007-2013 (Remove Console) Ticket Light Included	220.00	175.00
BRK-VPM-107-099	Visor Post Bracket, Chevy Tahoe/Silverado/2500 Truck 1999-2006	60.00	45.00
BRK-VPM-116-006	Chevy Trail Blazer 2006-07	60.00	45.00
BRK-CRC-106-006	Bracket, Ceiling Mount Kit, Dodge Charger 2006-2010	100.00	75.00
BRK-VPM-105-005	Visor Post Bracket, Dodge Durango 2005-2008	60.00	45.00
BRK-VPM-102-003	Dodge Intrepid 2003	60.00	45.00
BRK-VPM-109-006	Dodge Ram 1500 Pickup 2006	120.00	95.00
BRK-VRC-109-000	Dodge Ram 1500 Pickup 2006 (Remove Console)	120.00	95.00
BRK-VRC-109-013	Dodge Ram 1500 Pickup 2009+ (Remove Console)	160.00	125.00
BRK-VPM-100-099	Visor Post Bracket, Ford Crown Victoria 1999-2005(A)	60.00	45.00
BRK-VPM-100-005	Visor Post Bracket, Ford Crown Victoria 2005(B)-2011	60.00	45.00
BRK-VPM-103-001	Ford Expedition 2001-2002	60.00	45.00
BRK-VPM-103-003	Visor Post Bracket, Ford Expedition 2003-2007	60.00	45.00
BRK-VWC-103-000	Visor Post Bracket, Ford Expedition 2006-2007 (with Console)	60.00	45.00
BRK-CRC-103-007	Bracket, Ceiling Mount Kit, Ford Expedition 2007-2012 (Remove Console) Ticket Light Included	220.00	175.00
BRK-VPM-104-000	Ford Explorer 2000	120.00	95.00
BRK-VPM-104-001	Ford Explorer 2001-2002	120.00	95.00
BRK-VPM-104-003	Ford Explorer 2003-2004	120.00	95.00



COSTARS - 12 PRICE LIST - WatchGuard Video

BRK-VPM-104-005	Visor Post Bracket, Ford Explorer 2005-2007	120.00	95.00
BRK-VPM-104-008	Visor Post Bracket, Ford Explorer 2008-2009, (Remove Console) Ticket Light Included	260.00	205.00
BRK-VPM-111-001	Visor Post Bracket, Ford F-150 Pickup 2001	60.00	45.00
BRK-VPM-111-006	Visor Post Bracket, Ford F-150 Pickup 2006	60.00	45.00
BRK-CRC-111-007	Ford F-150 SuperCrew Pickup 2007-08 (Remove Console)	160.00	125.00
BRK-CRC-111-009	Ford F-150 Pickup 2009-2014 (Remove Console)	160.00	125.00
BRK-VPM-112-006	Ford F-250 Pickup 2006-2009	120.00	95.00
BRK-VPM-114-006	Ford Van E150/E350 2006	60.00	45.00
BRK-RDM-100-06I	Bracket, Modular Remote Display Mount, Rigid - 6"	50.00	39.00
BRK-RDM-100-09I	Modular Remote Display Mount, Rigid - 9"	60.00	45.00
BRK-RDM-100-12I	Modular Remote Display Mount, Rigid - 12"	60.00	45.00
BRK-RDM-200-10I	Modular Remote Display Mount, Flex - 10"	60.00	45.00
BRK-RDM-200-12I	Modular Remote Display Mount, Flex - 12"	60.00	45.00
BRK-RDM-200-14I	Modular Remote Display Mount, Flex - 14"	60.00	45.00
BRK-RDM-RAM-100	Modular Remote Display Mount, Headliner (RAM Mount)	160.00	125.00
BRK-VFS-100-005	Modular Remote Display Visor Post Kit, Ford Crown Victoria 2005-2009 (with Fire Suppression System)	200.00	159.00
BRK-MRU-100-000	Bracket, Modular Recording Unit Base Mounting Plate	35.00	25.00
BRK-MRU-200-099	Bracket, 4RE DVR, Mounting Shelf Kit, Ford Crown Victoria 1999-2009	100.00	79.00



COSTARS - 12 PRICE LIST - WatchGuard Video

VISTA Wearable Camera System		MSRP	Contract
VIS-STD-KIT-001	VISTA Standard Capacity Wearable Camera System. Capable of High Definition (720P) video recording for 6 continuous hours (standard definition recording also available). Includes a transfer/charging base, mounting hardware, One (1) Year Factory Warranty, and Evidence Library Express software.	995.00	795.00
VIS-EXT-KIT-001	VISTA Extended Capacity Wearable Camera System. Capable of High Definition (720P) video recording for 9 continuous hours (standard definition recording also available). Includes a transfer/charging base, mounting hardware, One (1) Year Factory Warranty, and Evidence Library Express software.	1,120.00	895.00
VIS-EXT-WIF-001	VISTA HD, WiFi Extended Wearable Camera (Camera Only)	1,250.00	995.00
VIS-CHG-WIF-BSE	VISTA HD, WiFi Charging Radio Base Station	250.00	200.00
HDW-ETH-SWT-005	4RE, VISTA HD WiFi, Smart PoE Switch	245.00	195.00
SFW-MOB-APP-001	VISTA Mobile Companion (ELX/EL4 No Maintenance)	95.00	75.00
SFW-MOB-APP-002	VISTA Mobile Companion (EL4 w/Maintenance)	Included	Included
VIS-CHG-DTC-001	VISTA USB Charge and Upload Docking Base	120.00	95.00
VIS-MNT-KIT-002	VISTA HD Locking Chest Mount without Straps	80.00	60.00
VIS-BLT-CLP-001	VISTA HD Duty Belt Clip	25.00	20.00
VIS-BLT-CLP-100	VISTA HD Shirt Clip with Slider	40.00	30.00
VIS-MNT-MOL-001	VISTA HD, Molle Vest Adapter Clip	\$25.00	\$20.00
VIS-MNT-TRI-001	VISTA HD, Tripod Mount Base Adapter	\$45.00	\$35.00
VIS-MNT-VEL-001	VISTA HD, Velcro Backing Plate (with Hook/Loop Velcro Set uninstalled)	\$25.00	\$20.00
VIS-MNT-KLK-001	VISTA HD, "Klick Fast" Mount Adapter	\$45.00	\$35.00
VIS-MNT-RAM-001	VISTA HD, Ram Mount Kit	\$45.00	\$35.00
VIS-MNT-RAM-002	VISTA HD, Suction Cup RAM Mount Kit, 6" Arm	\$155.00	\$125.00
VIS-USB-HUB-001	VISTA HD 7 Port USB Hub	40.00	30.00
VIS-VTS-DTC-001	VISTA HD 8 Bay Ethernet Transfer Station	1,870.00	1,495.00
VIS-WRL-BAT-100	VISTA HD Extended Battery, LI-ION, 3.6V 4050mAH	55.00	40.00
VIS-WRL-BAT-001	VISTA HD Standard Batter, LI-ION, 3.6V 2700mAH	40.00	30.00
WAR-VIS-CAM-1ST	VISTA HD Warranty, Standard 1st Year	-	-
WAR-VIS-CAM-NOF	VISTA HD No Fault Warranty, Years 1-3	475.00	380.00

BID ITEM WORKBOOK**COSTARS-12 Emergency Responder Loose Supplies****BID ITEM SHEET****BIDDERS/CONTRACTORS LEGAL NAME**Enforcement Video, LLC**PRICING**

The Bidder may offer any type of discount, mark-up, or other pricing structure such as multiple discounts for different lines of products, or different price lists, or different classes of Purchasers, or different prices for different quantities of products. Please reference Subsection 6.b. of the Special Terms and Conditions for further guidance.

After Contract award, a Contractor may offer, either on its own initiative or at a Purchaser's request, additional discounts, reduced mark-ups, customized lists, or discounted prices for any purchase within the scope of the Contract, even if such discounts, mark-ups, or discounted prices were not included in the bid prices.

The Bid Item Workbook should contain a separate Bid Item Sheet for each manufacturer's price list or cost sheet.

MANUFACTURER:Enforcement Video, LLC**PRICING STANDARD:** (Check that which is applicable.)

☐ Catalog or Manufacturer's/Distributor's Most Recently Published Price List Less % of Discount
☐ Suppliers Cost Plus % of Mark-up
☒ Custom List including Net Prices

PRICE LIST IDENTIFICATION:CATALOG OR PRICE LIST NAME: COSTARS - 12 Price List

IDENTIFICATION NO. (IF APPLICABLE): _____

EFFECTIVE DATE: 27-Sep-13CLASS OF PURCHASER: All Purchasers

(i.e. All Purchasers or separate lines for specific classes, such as Educational Purchasers and Non-educational Purchasers.)

WatchGuard Video		
Law Enforcement / Public Safety Equipment and Supplies		
Part Number	Description	Net Price
DV1-EOH	DV-1 5TH Generation Overhead In-Car Video System	4,895.00
DV1-EMD	DV-1 5TH Generation Modular In-Car Video System	5,250.00
4RE-STD-GPS	4RE HD In-Car Video System	4,790.00
4RE-64S-GPS-MTR	4RE HD Motorcycle Video System	5,295.00
4RE-200-VIS-INT	4RE HD In-Car Video System w/Integrated VISTA WiFi	5,495.00
4RE-200-INT-001	4RE Interview Room Solution, One Camera Package	4,995.00
4RE-200-INT-002	4RE Interview Room Solution, Two Camera Package	5,195.00
KEY-EL4-SRV-001	Evidence Library 4 Web Server Site License	1,000.00
KEY-EL4-DEV-001	Evidence Library 4 Web 4RE In-Car Device License	150.00
KEY-EL4-DEV-002	Evidence Library 4 Web VISTA Device License	150.00
KEY-EL4-DEV-003	Evidence Library 4 Web 4RE Combo-Discount Device License Key	75.00
KEY-EL4-DEV-004	Evidence Library 4 Web VISTA Combo-Discount Device License Key	75.00
SFW-WCM-LIC-FEE	Watch Commander License Fee (per car)	250.00
SFW-WCM-KIT-100	Watch Commander Software Installation Disc w/ Case and Document	2,500.00
VST-STD-KIT-001	VISTA HD Standard Capacity Wearable Camera	795.00
VST-EXT-KIT-001	VISTA HD Extended Capacity Wearable Camera	895.00
VIS-EXT-WIF-001	VISTA HD, WiFi Extended Wearable Camera (Camera Only)	995.00
KEY-WGV-RED-001	Software, REDACTIVE(sm), Single Seat License	3,995.00
WAR-WGR-MNT-001	Software Maintenance, REDACTIVE(sm), 1st Year (Months 1-12)	785.00
WAR-WGR-MNT-002	Software Maintenance, REDACTIVE(sm), 2nd Year (Months 13-24)	785.00
WAR-WGR-MNT-003	Software Maintenance, REDACTIVE(sm), 3rd Year (Months 25-36)	785.00
WAR-WGR-MNT-3YR	Software Maintenance, REDACTIVE(sm), 3-Year Bundle (Months 1-36)	2,250.00
WAR-WGR-MNT-ADD	Software Maintenance, REDACTIVE(sm) +1 Extended Addiitonal Year	785.00



9652 Loiret Blvd.
Lenexa, KS 66219
800.458.7866

Contact: David Nicholl and Rod Smith

Due: Friday, January 25, 2019 at 4:00PM

Request for Information Police Body Worn Cameras





9652 Loiret Blvd TEL: 800.458.7866
Lenexa, KS 66219-2406 913.492.1400
www.KustomSignals.com FAX: 913.492.1703

January 24, 2019

Christopher J. Braun M.S. IT
Technology Coordinator Pennsylvania Chiefs of Police Association
3905 N. Front Street
Harrisburg, PA 17110

SUBJECT: Request for Information Police Body Worn Cameras
DUE DATE: Friday, January 25, 2019 at 4:00PM

Dear Mr. Braun:

Kustom Signals, Inc. has been serving the needs of law enforcement agencies for more than 50 years. We appreciate the opportunity and look forward to working with the Pennsylvania Chiefs of Police Association (PCPA) in cooperation with the Local Technology Workgroup (LTW) of the Pennsylvania Commission on Crime and Delinquency (PCCD). Kustom Signals is offering our state-of-the-art Eyewitness Vantage which will add significant value to your law enforcement program and enhance traffic safety, officer safety, and public safety.

We strive to be the worldwide leader in speed enforcement, the most trusted provider of video evidence solutions and the recognized leader in customer satisfaction. Our history of innovation, commitment to quality, customer loyalty, and focus on service has forged Kustom Signals' identity, and as a direct result we are serving our third generation of officers. We are dedicated to working hard for our customers and are positioned to meet the requirements in the enclosed proposal. Supporting a spirit of cooperation to guarantee your needs are met earns not only your business, but more importantly, your trust.

Our highly qualified team, consisting of Video Product Manager David Nicholl and Domestic Sales Manager Rod Smith, is available to answer questions. Please feel free to contact David at 800-458-7866 extension 3008 and/or Rod at 1-800-458-7866 extension 913-302-8487.

Kustom Signals is well known as an established leader in the law enforcement community and we look forward to sharing our industry experience and robust product offerings with the PCPA.

Sincerely,

A handwritten signature in blue ink that reads 'Chris N. Abel'.

Chris Abel, President

cc: David Nicholl, Video Product Manager
Rod Smith, Domestic Sales Manager

Your Trusted Partner in Law Enforcement

Information Requested

How does your non-vehicle-mounted mobile video recording systems and technology meet Pennsylvania's published requirements?

Kustom Signals' Eyewitness Vantage meets the following published requirements:

The design of the non-vehicle-mounted mobile video recording system must use technology which includes a camera with date/time stamp capability, a microphone and a recording device, enclosed in secure protective enclosure(s). It may also contain controls, a monitor, GPS, wireless transceiver components and other electronic components. The non-vehicle-mounted mobile video recording system must be powered from a battery internal to the protective enclosure and must be weatherproof. The internal battery may be integral to the unit or removable. It is permissible to have an external battery to extend the operating life of the system. The non-vehicle-mounted mobile video recording system must have a minimum record time of 2 continuous hours. The system must operate over the following temperature range: -4°F to 122°F (-20°C to 50°C).

Camera

The camera component must have the following features:

- A. Must be color video.
- B. Minimum of 640 x 480 pixel resolution.
- C. Minimum of 68 degrees field of view.
- D. Minimum of 30 frames per second.
- E. Minimum sensitivity rating of 3.4 lux or lower. Unit may use Infrared LED illumination to obtain lower than 3.4 lux equivalent.
- F. Camera does not have to be in the same enclosure as the recorder. Can be connected to the recorder either by cable or wireless connection.

Recorder

The recorder component must have the following features:

- A. Enclosed in a secure housing protected from physical damage.
- B. Date/time recording index.
- C. Minimum of 4 gigabytes of nonremovable solid state memory, 4 gigabytes removable media or a combination of both removable and nonremovable memory.
- D. Editing and record-over protection.

System Control

The system must:

- A. Be capable of recording audio and video simultaneously, but may also provide the user with the option to record video only or audio only.
- B. Provide the user with the capability to manually turn the power on and off as necessary.

Wireless Link (optional)

The unit may use a wireless link to connect the camera to the recorder, recorder to another device, combination camera/recorder to another device or be used to download the evidence.

The wireless link must have the following features:

- A. Use a secure digital connection.
- B. Wireless link can be used to play back a locally stored event on the recorder or store the media to a remote location such as secure Cloud storage.
- C. FCC Type acceptable under 47 CFR Part 15 (relating to radio frequency devices).

Eyewitness Vantage is a one-piece body-worn camera that provides one-handed, glove-friendly start and stop record functionality. The large start/stop slider is centrally located and is spring loaded to provide tactile feedback so the officer has confidence the camera is in or out of record mode.

Notification LED's provide battery status, record status and file transfer activity. These LED's can be blacked out for officer safety.

Vantage includes the following features:

- Configurable high and standard definition resolution at 1080p at 30 fps; 720p at 60 fps; 720p at 30 fps; and D1 (480p) at 30 fps all using MPEG4 h.264 file format
- 120 degree wide-angle lens without the peripheral distortion found on other body-worn cameras
- Non-removable 32GB compact flash storage
- Configurable pre-event recording (up to 30 seconds for all resolution options)
- Battery life – Standard battery provides 48 hours of operation in Power Save mode - up to 4 hours continuous use in Standby mode. Extended provides 96 hours of operation in Power Save mode - up to 8 hours continuous use in Standby mode.
- Storage capacity (on internal 32GB solid state storage) – up to 6 hours 1080p/30, up to 6 hours 720/60, up to 14 hours 720p/30, up to 17 hours 480p
- Configurable audio mute button
- Configurable bookmark button
- GPS location tagging with incident/bookmarking button (track officer location and incidents during playback in back office software)
- Configurable day/night mode for even better low-light performance
- Configurable infrared illuminators (optional) to see in the dark
- Configurable “beep” and/or “buzz” record status notification
- LEDs provide status of battery capacity, internal media capacity, file transfers, low media, record, and audio mute

The Vantage ships with a rugged spring clip designed to withstand rigorous law enforcement work environments. The clip rotates 360 degrees allowing for flexible uniform mounting locations. An optional magnetic mount is available that allows the camera to be mounted anywhere on the uniform shirt. No modifications will be needed to the current uniform. Should additional mounting options be desired, an interface to Peter Jones' Klickfast mounts is also under development. Please refer to this link for more information: <http://www.peterjonesilg.co.uk/equipment-cameras/index.html>.

Each Vantage comes standard with a docking station for charging and downloading files to the file management system. Multi-docks are available to facilitate larger installations – multiple cameras can be simultaneously transferring files and recharging their internal batteries.

Please refer to the attached product specification sheet at the end of this document for additional product information.

Have you submitted your non-vehicle-mounted mobile video recording systems to the Pennsylvania State Police for certification?

Kustom Signals has not yet submitted the Eyewitness Vantage for certification, but would be very interested in doing so.

Is your non-vehicle-mounted mobile video recording system already certified by the Pennsylvania State Police?

Kustom Signals Eyewitness Vantage is not already certified by the Pennsylvania State Police.

Are you offering a storage solution?

The Eyewitness Data Vault (EDV) file management system allows agencies to easily transfer, store and manage video files recorded by Kustom Signals' in-car video and/or body-worn video systems. EDV provides quick and easy file searching, easy playback and file duplication. Storage can be expanded locally. EDV is also compatible with Active Directory and LDAP to allow established log in credentials to be used. Kustom Signals does not currently offer a cloud-based solution.

When comparing local storage to cloud storage for the video files, Kustom Signals believes you will find pros and cons to each option. Cloud storage takes the responsibility of maintaining the storage off the agency, but it also comes at a cost that can be significantly higher than purchasing and maintaining storage on-site. Further, to end a cloud storage agreement, there can be fees to retrieve video back from the provider, and files retrieved may not include any of the history of what happened with that file. A local storage option is something that the agency owns and has full control over. In the event the agency moved to another body camera provider after several years, the critical evidence and all its history would still be contained on the database maintained and located on hardware owned by the agency. For these reasons, we believe local storage from the on-set is currently the most cost effective solution.

Please refer to the attached product specification sheet for Eyewitness Data Vault Back Office Software at the end of this document for additional product information.

Will you offer storage solutions bundled (no line item distinction) with the cost of each camera purchased?

Kustom Signals can bundle the cost of the storage unit into the cost of the each camera purchased if more than 30 cameras are purchased together.

How does your storage solution meet Pennsylvania's published requirements?

Kustom Signals storage solution supports agency compliance with 18 Pa.C.S. § 5706(b)(5), the following minimum requirements that must be met for any storage of an audio recording made in accordance with 18 Pa.C.S. § 5706(b)(4), or any accompanying video recording:

A. Camera system

1. While worn by the officer, a camera system shall be considered a physically secure location.
2. Upon removal from the officer's body, the camera system shall be maintained in a physically secure location in accordance with CJIS Policy standards.
3. If a camera system is located in a criminal justice conveyance, it shall be considered located in a physically secure location. If the camera or hard drive is removed from the criminal justice conveyance, it shall conform with the CJIS Policy. A criminal justice conveyance is any enclosed mobile vehicle used for the purposes of criminal justice activities with the capability to comply, during operational periods. A physically secure location, as stated in section 5.9.1 of the CJIS Policy (relating to physically secure location) is as follows:

A physically secure location is a facility, a criminal justice conveyance, or an area, room or a group of rooms within a facility, with both the physical and personnel security controls sufficient to protect CJI and associated information systems. The physically secure location is subject to criminal justice agency management control, State Identification Bureau control, FBI CJIS security addendum, or a combination thereof, and shall consist of the following:

- a. Security perimeter—area that is posted, separated and secured.
- b. Physical access authorizations—list of authorized personnel.
- c. Physical access control—control all physical access points (AP).
- d. Access control for transmission medium—control physical access to information systems, distribution and lines.
- e. Access control for display medium—not visible to unauthorized personnel.
- f. Monitoring physical access—monitor and respond to security incidents.
- g. Visitor control—authenticate and escort visitors.
- h. The agency shall authorize and control information system-related items entering and exiting the physically secure location (delivery and removal).

B. Data transfer or downloading the data

1. If accomplished through a wireless connection, agencies shall meet the CJIS Policy requirements, as stated in section 5.13.1.1 (relating to 802.11 wireless protocols).
Note: Wired Equivalent Privacy and Wi-Fi Protected Access cryptographic algorithms, used by all pre-802.11i protocols, do not meet the requirements for Federal Information Processing Standard (FIPS) 140-2 and may not be used.
2. Agencies shall implement the following controls for all agency-managed wireless APs with access to an agency's network that processes unencrypted CJI:
 - a. Perform validation testing to ensure rogue APs do not exist in the 802.11 wireless local area network and to fully understand the wireless network security posture.
 - b. Maintain a complete inventory of all APs and 802.11 wireless devices.

- c. Place APs in secured areas to prevent unauthorized physical access and user manipulation.
 - d. Test AP range boundaries to determine the precise extent of the wireless coverage and design the AP wireless coverage to limit the coverage area to only what is needed for operational purposes.
 - e. Enable user authentication and encryption mechanisms for the management interface of the AP.
 - f. f. Ensure that all APs have strong administrative passwords and ensure all passwords are changed in accordance with section 5.6.2.1 of the CJIS Policy (relating to standard authenticators), as follows:
 - (1) Be a minimum length of eight characters on all systems.
 - (2) Not be a dictionary word or proper name.
 - (3) Not be the same as the user ID.
 - (4) Expire within a maximum of 90 calendar days.
 - (5) Not be identical to the previous ten passwords.
 - (6) Not be transmitted in the clear, outside the secure location.
 - (7) Not be displayed when entered.
 - g. Ensure the reset function on APs is used only when needed and is only invoked by authorized personnel. Restore the APs to the latest security settings, when the reset functions are used, to ensure the factory default settings are not utilized.
 - h. Change the default service set identifier (SSID) in the APs. Disable the broadcast SSID feature so that the client SSID must match that of the AP. Validate that the SSID character string does not contain any agency identifiable information (division, department, street, and the like) or services.
 - i. Enable all security features of the wireless product, including the cryptographic authentication, firewall and other available privacy features.
 - j. Ensure that encryption key sizes are at least 128-bits and the default shared keys are replaced by unique keys.
 - k. Ensure that the ad-hoc mode has been disabled.
 - l. Disable all nonessential management protocols on the APs.
 - m. Ensure all management access and authentication occurs through FIPS-compliant secure protocols (for example, SFTP, HTTPS, SNMP over TLS, and the like). Disable non-FIPS-compliant secure access to the management interface.
 - n. Enable logging (if supported) and review the logs on a recurring basis per local policy. At a minimum, logs shall be reviewed monthly.
 - o. Insulate, virtually (for example, virtual local area network and access control lists) or physically (for example, firewalls), the wireless network from the operational wired infrastructure. Limit access between wireless networks and the wired network to only operational needs.
 - p. When disposing of APs that will no longer be used by the agency, clear AP configuration to prevent disclosure of network configuration, keys, passwords, and the like.
3. 3. If the data is manually downloaded by an individual or retained outside of a physically secure location, it will need to be encrypted at rest and in transit, per sections 5.10.1.2.1 and 5.10.1.2.2 of the CJIS Policy (relating to encryption for CJI in transit; and encryption for CJI at rest).

C. Storage of the data

Storage of data on location, if considered a physically secure location, shall be treated the same as all CJI at the location. Storage offsite, or in the cloud, shall meet all the requirements of the CJIS Policy for encryption while in transit and at rest, if applicable. If encryption is not used at rest, any person with access to the data or systems storing the data shall be properly vetted with a fingerprint-based background check and Security Awareness Training, and required agreements shall be maintained.

1. As stated in section 5.10.1.2.1 of the CJIS Policy: When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via encryption. When encryption is employed, the cryptographic module used shall be FIPS 140-2 certified and use a symmetric cipher key strength of at least 128 bit strength to protect CJI.
2. As stated in section 5.10.1.2.2 of the CJIS Policy: When CJI is at rest (i.e. stored digitally) outside the boundary of the physically secure location, the data shall be protected via encryption. When encryption is employed, agencies shall either encrypt CJI in accordance with the standard in Section 5.10.1.2.1 above, or use a symmetric cipher that is FIPS 197 certified (AES) and at least 256 bit strength.

D. Reviewing and release of data

1. Data from the camera system shall only be reviewed by authorized personnel; that is, personnel that have been cleared through a fingerprint-based background check, have received Security Awareness Training and have signed the appropriate agreements, if applicable. If required, the Management Control Agreement for local government IT, or The Security Addendum for private contractors, shall be completed and on file.
2. Prior to the release of data from the camera system, the data shall be reviewed and any areas containing CJI shall be removed or rendered unintelligible. Any data received from CLEAN or the National Crime Information Center in either video or audio format, or both, shall be removed or rendered unintelligible prior to release to any unauthorized or unintended personnel.

E. Retention of data

Data shall be stored for 60 days unless needed for prosecution, courts, litigation, appeals or other operational needs.

F. Destruction of data

The data, or the data storage devices that are to be destroyed, shall be destroyed in compliance with the CJIS Policy, and a written destruction procedure that complies with the CJIS Policy shall be maintained at the agency. As stated in section 5.8.3 of the CJIS Policy (relating to digital media sanitization and disposal): The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

The agency shall sanitize, that is, overwrite at least three times or degauss digital media prior to disposal or release for reuse by unauthorized individuals. Inoperable digital media shall be destroyed (cut up, shredded, etc.). The agency shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel.

List the products and services that are already available on State Contract or PA CoStars.

Kustom Signals has a contract in place with PA CoStars that includes the following equipment:

- Eyewitness HD In-Car Video System Basic Package w/tablet controller
- Eyewitness HD In-Car Video System Basic Package with MDC interface
- Eyewitness HD In-Car Video System Bundled w/tablet controller
- Eyewitness HD In-Car Video System Bundled with MDC interface
- Vantage Body Worn Video Camera with Standard Battery
- Vantage Body Worn Video Camera with Extended Battery
- Eyewitness Data Vault LITE Back Office Video File Management Software License (CRS 4299)
- Eyewitness Data Vault HQ Video File Management Software License (CRS 4324)
- Eyewitness Data Vault (EDV) Precinct Video File Management Software License (CRS 4325)
- EDV 12000 - includes a workstation with 12TB storage (CRS 4300)
- EDV 24000 - includes a workstation and server w/24TB integrated RAID storage (CRS 4301)
- EDV 32000 includes a workstation and server w/32TB integrated RAID storage (CRS 4302)
- EDV 40000 includes a workstation and server w/40TB integrated RAID storage (CRS 4303)
- EDV 72000 includes a workstation and server w/72TB integrated RAID storage (CRS 4304)
- EDV 96000 includes a workstation and server w/96TB integrated RAID storage (CRS 4305)
- EDV 120000 includes a workstation and server w/120TB integrated RAID storage (CRS 4306)
- EDV Viewing Workstation (CRS 4308)
- EDV Extended Software Support Per Year (CRS 4326)
- Wireless Access Point Kit - Ubiquiti
- Wireless Access Point Accessory Kit (1 kit per site supports up to 6 A/Ps)
- Field Application Engineer (FAE) Time:
 - Includes one day of on-site installation services for service, installation, testing and training
- SMART 650 Speed Awareness Trailer
- SMART 650+ Speed Awareness Trailer
- SMART 800 Speed Awareness Trailer
- SMART 800+ Speed Awareness Trailer
- SMART 850 Speed Awareness Trailer
- SMART 850+ Speed Awareness Trailer
- SMART VMS Model I Speed Awareness Trailer
- SMART VMS Model II Speed Awareness Trailer
- SMART VMS Model III Speed Awareness Trailer
- SMART VMS HT Speed Awareness Trailer
- SMART 275 Pole-Mounted Speed Awareness Display
- SMART 350 Pole-Mounted Speed Awareness Display
- SMART 375 Pole-Mounted Speed Awareness Display
- SMART 400 Pole-Mounted Speed Awareness Display
- SMART 450 Pole-Mounted Speed Awareness Display
- SMART 475 Pole-Mounted Speed Awareness Display
- Tracker

Falcon HR Hand-Held Stationary Radar with Fastest and Carrying Case
 Falcon HR Hand-Held Moving/Stationary Radar with Fastest, 7" Dash Mount & Bracket, and Carrying Case
 Falcon HR Hand-Held Moving/Stationary Radar with Fastest, Same Direction Mode, 7" Dash Mount & Bracket
 and Carrying Case
 Golden Eagle II Dash-mounted Dual KA Band Radar
 Directional Golden Eagle II Dash-mounted Dual KA Band Radar
 Raptor Dash-mounted Single K Band Radar
 Raptor Dash-mounted Dual K Band Radar
 Raptor Dash-mounted Single KA Band Radar
 Raptor Dash-mounted Dual KA Band Radar
 Eagle 3 Dash-mounted Single Ka-band antenna
 Eagle 3 Dash-mounted Dual Ka-band antenna

Will you offer a discount of those prices if multiple police departments group together to buy your products and services?

Yes, Kustom Signals offers discounts on quantity purchases with the following breakdown of 6-14 units and 15+ and will honor these price breakdowns if multiple departments would like to make group purchases.

Our standard price breakdown follows:

Internal Part Number	Description	List Price	1-5 Selling Price	6-14 Selling Price	15+ Selling Price
8000	Vantage, Standard Battery, 32GB	\$ 844	\$ 675	\$ 635	\$ 595
8001	Vantage, Extended Battery, 32GB	\$ 931	\$ 745	\$ 700	\$ 655

Other Relevant Information

History of Kustom Signals

Kustom Signals, Inc. has been dedicated to serving the public safety equipment needs of law enforcement for more than 50 years. We strive to be the **worldwide leader in speed enforcement, the most trusted provider of video evidence solutions and the recognized leader in customer satisfaction**. Our vast array of durable and reliable products positions us to be the Village of Schaumburg's (Village) complete traffic safety equipment source.

Kustom Signals' innovative accomplishments have been marked by the following industry firsts:

- 1970-First Digital Readout Radar (TR6)
- 1972-First Moving Radar (MR7)
- 1975-First Handheld K-band Radar (HR-8)
- 1975-First Two-window Microprocessor Based Radar (KR-11)
- 1976-First Statistical Package (STATPACK for KR-11)
- 1978-First Moving K-band Handheld Radar (HR-12)
- 1979-First Instant-On Function (KR-10)
- 1985-First All-Direction Mode Radar with Stopwatch Mode (H.A.W.K.)
- 1988-First Speed Monitoring Awareness Radar Trailer (SMART)
- 1988-First Patrol Car Video System with Temperature-Controlled Vault (Eyewitness)
- 1990-First LIDAR with Heads-Up-Display (ProLaser)
- 1990-First LIDAR with Continuous Tracking History (ProLaser)
- 1990-First LIDAR with Settable Range (ProLaser)
- 1992-First In-Car Video System with Auto Zoom (Eyewitness)
- 1992-First In-Car Video System with Wireless Microphone Record Activation (Eyewitness)
- 1994-First Three-Window Time/Distance/Speed Computer (Tracker)
- 1994-First Digital Signal Processing based Radar with Fastest Vehicle Mode (EAGLE)
- 1994-First Digital Signal Processing based Radar with Multi-band Antennas (EAGLE)
- 1994-First Digital Signal Processing based Radar with Wireless Remote Control (EAGLE)
- 1996-First Speed Monitoring Trailer with Free-Flow Statistics Method (SMART)
- 1996-First Speed Monitoring Trailer with Violator Alert (SMART)
- 1998-First Digital Signal Processing based Radar with TruTrak Speedometer Input (EAGLE)
- 1998-First Covert, Pole-Mounted Traffic Statistics Gathering Device (StealthStat)
- 1999-First LIDAR with Selectable Environmental Mode (ProLaser III)
- 2002-First Digital In-Car Video Offering Multiple Recording Media Options (Digital Eyewitness)
- 2004-First Digital In-Car Video that Offered Multiple Compression Options and Multiple File Transfer Options (Eyewitness NXT)
- 2004-First In-Car Video Offering Dual Control for MDC and Dedicated Controller (Eyewitness NXT)

- 2006-First Binocular Style Speed Enforcement Laser (Pro-Lite+)
- 2006-First Traffic Lidar to be Powered with AA Batteries
- 2007-First Handheld K-band Planar Array Antenna (Falcon HR)
- 2007-First Traffic Safety Video Lidar with Moving Operation (LASERwitness)
- 2008-First Two-Piece Radar with a Graphical Display (Raptor)
- 2008-First Radar with Target Tracking Bar - DuraTrak™ (Raptor)
- 2006-First two-piece radar with K-band Planar Array Antenna (Raptor)
- 2010-First Four Camera Simultaneous Recording Video, Offering 30 fps and 720x480 Resolution on all Four Channels (G3 Vision)
- 2010-First Digital In-car Video System Utilizing Windows Internet Explorer as MDC User Interface – No Client Application Installed on MDC (G3 Vision)
- 2010-First to Offer a Look-back Buffer on Two Channels (G3 Vision)
- 2011-First Traffic Lidar with Recalled Events Database (ProLaser 4)
- 2011-First Traffic Lidar to be Powered by AA, USB, or 12 VDC Power (ProLaser 4)
- 2013-First Video Laser with AutoTrak™ Automatic Zoom (LaserCam 4)
- 2015-First In-Car Video with Tablet-like User Interface (Eyewitness HD)
- 2015-First In-Car Video with Dedicated Controller Using (essentially) the Same GUI as the MDC Interface (Eyewitness HD)
- 2016-First Body Worn Camera to Offer Pre-Event, GPS, Audio Mute, Bookmarking, Day/Night Mode, and IR LEDs All In One Package (Eyewitness Vantage)

Financial Stability

Founded in 1965 in rural southeastern Kansas, Kustom Signals has grown into a global enterprise. Our history, integrity, collaboration and dedication have enabled Kustom Signals to prosper and the associates, leaders and owners are committed to the company's ongoing business expansion.

Kustom Signals is a wholly owned subsidiary of MPD, Inc. and proudly participates in an Employee Stock Ownership Plan. Earnings from the business continue to be reinvested in product development, operational improvements, productivity tools and key staff additions. We anticipate solid earnings and growth for the foreseeable future.

We have the productive capacity as well as the financial strength and management expertise to successfully deliver what you need. Additionally, we are aligned with strong and successful suppliers who are not only key to our success in product development and manufacturing, but have sufficient capacity to grow with us. Kustom Signals is here to stay.

Customer Service Support

One number...a bundle of services. Kustom Signals' Factory Service Center, which is located in Chanute, Kansas, repairs every product manufactured by Kustom Signals. Additionally, we make it our goal to provide superior support to each and every one of our customers.

After initial implementation is complete, product support (in warranty as well as out of warranty) is structured so the Village receives the necessary assistance from our Factory Service Manager and Kustom Signals' Factory Service Center. In addition to our Factory Service Center support, Regional Sales Manager Jeff Williams and Account Manager Sonya Schoneman are also available to provide assistance as needed.

Kustom Signals' commitment continues long after the sale. Through our extensive service offerings, we link you directly with dedicated and experienced technicians who perform comprehensive diagnostics and resolution for your vehicle and traffic safety equipment needs. Technical support specialists are accessible at our factory through our toll-free telephone number, (800) 835-0156, between 7:00 a.m. and 6:00 p.m. Central Time, Monday through Friday. The type of support needed may vary, as will the person that should be contacted. The sales team will always help connect you to the right support specialist, or you can also visit our website at www.kustomsignals.com, go to the Service & Support drop-down menu, and select Customer Service Contacts. This provides a list of contact information for various parts of our service business. Each support specialist has a minimum of two years of experience as a production technician or service technician, providing a high level of product expertise.

Commitment to Providing Quality Products

The Village can be assured that Kustom Signals' executive-level management will be made aware of potential problems and involved in the resolution. Our commitment to providing top-of-the-line products enhances serviceability. In the event a problem is encountered, the strategy for the resolution begins at the top of our organization. Each week a teleconference is held to review weekly reports received from District Managers and Account Managers.

The purpose of this meeting is to prepare operations for upcoming orders and to discuss potential as well as existing customer concerns. To be proactive in handling potential issues as well as addressing any outstanding issues, action plans are formulated before the meeting is adjourned. Through these meetings and timely follow-up, our top executives are kept informed of concerns directly affecting agencies and can implement the necessary corrective and preventive measures.

By preventing and/or correcting issues related to quality, service, cost and delivery schedules, in a timely manner, Kustom Signals' customers can expect to purchase higher quality products at lower prices. Customer service is a key element of our success. The organization, infrastructure, and supporting processes are focused on ensuring exceptional customer satisfaction for every customer. Kustom Signals spares no effort to ensure a customer's satisfaction is fully met regarding product and service quality, because you are our #1 priority.

Trust Kustom Signals

- **History and Tradition:** Kustom Signals has been serving the public safety equipment needs of law enforcement agencies for more than 50 years. We are proud that three generations of officers have had access to our products. With the most experience in the industry, our solutions meet the needs of more than 17,000 customers across the United States and in 60 foreign countries. Each day Kustom Signals strives for excellence in everything we do.
- **Consistency:** The heritage and reputation of Kustom Signals have been built on a solid Midwestern work ethic. Law enforcement is our only business. We design, assemble, and support our products with Kustom Signals employees, not contractors. In this way, we maintain the quality that our customers have come to expect.

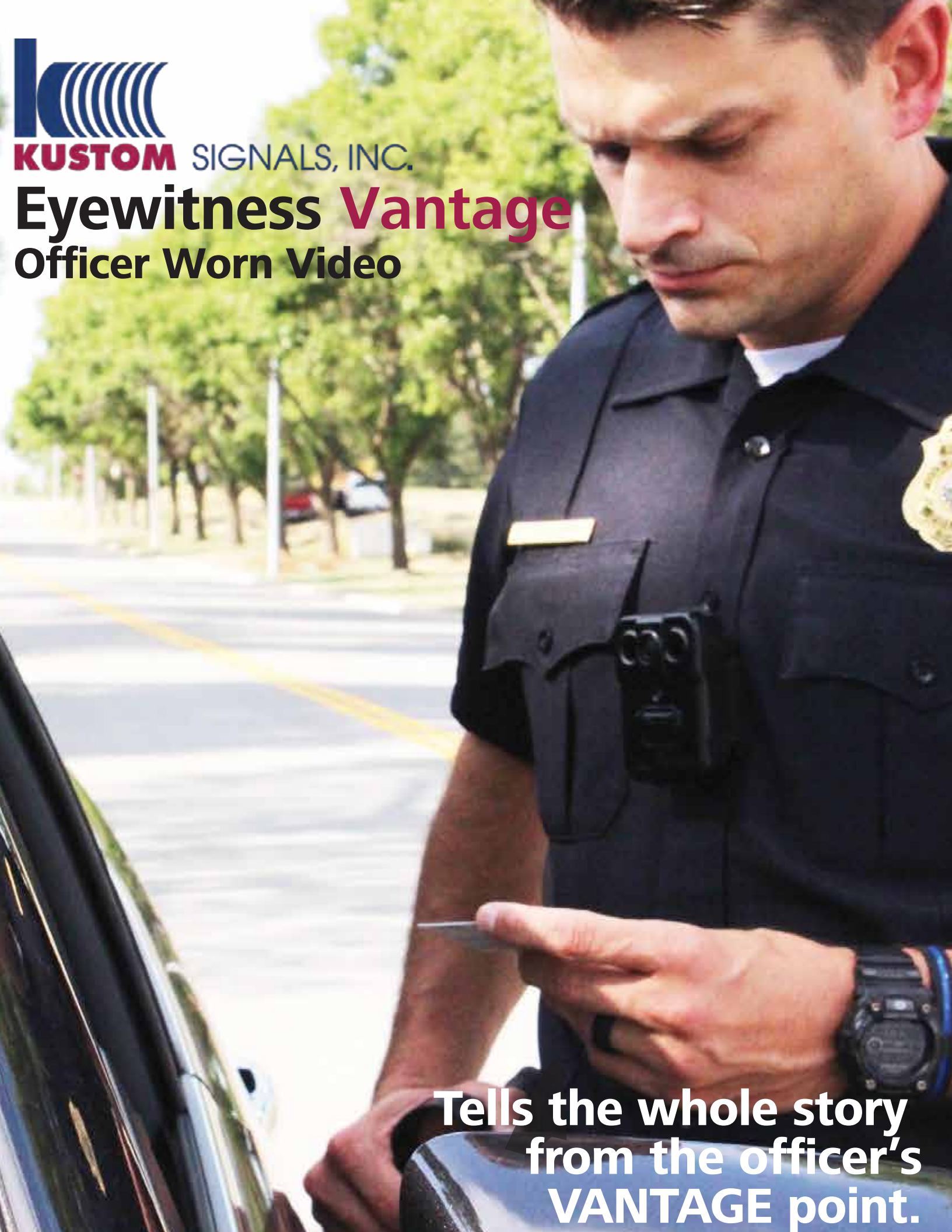
- **Versatility:** Designing and marketing traffic speed radar, lidar, in-car video systems and mobile roadside speed monitoring trailers/displays positions Kustom Signals to be a one-stop-shop for agencies. Our products have been specifically designed for the law enforcement industry, taking into consideration the harsh environment they will encounter. You can feel confident in our products – our team would not sell a product that each of us would not use ourselves.
- **Financial Stability and Support:** Kustom Signals is financially sound and continues to be a strong and growing company. Our long-standing history proves our stability, followed by the fact that officers trust our systems.
- **Customer Focus:** As a full-service solutions provider, Kustom Signals provides product breadth, advanced technology and personalized service support. Our success in the law enforcement industry is because we focus on quality awareness and customer satisfaction.
- **Robust Solutions:** Kustom Signals takes pride in knowing that our solutions are customizable and will help enhance officer safety, ensure accountability and reduce liability.

Kustom Signals is proud to be your trusted partner in delivering critical law enforcement solutions.

Attachments

Please refer to the following product information sheets for:

- Eyewitness Vantage
- Eyewitness Data Vault



KUSTOM SIGNALS, INC.

Eyewitness **Vantage** Officer Worn Video

Tells the whole story
from the officer's
VANTAGE point.

Eyewitness Vantage

Officer Worn Video



Vantage offers true HD video, excellent quality low light recording and wireless file transfer to Kustom's new Eyewitness HD in-car system*.

Available with extended battery for up to 9 hours of record time.

Overview

- Excellent low light performance:
 - Matches what the officer sees
 - Configure with day/night mode for even better low light performance
 - Optional IR LEDs for capturing video in total darkness (Agency configurable)
- Select the resolution/storage combination that is best for your agency: 1080p/30 fps, 720p/60 fps, 720p/30 fps, D1 (480p/30 fps)
- Simple, glove friendly operation allows officers to focus on important tasks
- Wide-angle done right: 120° - capture details others may miss with minimal distortion
- Docking station for convenient dock-and-go file transfers and battery charging



Preferred Features Made Standard

- Pre-event recording (configurable up to 30 seconds)
- GPS - store coordinates with bookmark, support for geo-searches and synchronized clocks
- Configurable audio mute button if needed to comply with privacy laws
- Bookmark button identifies important events saving time during review

File Security/Authentication

- Recording media is non-removable
- File access requires a secure FTP Ethernet connection between the Vantage docking station and EDV/EDV Lite
- MD5 hash is calculated for each file on the camera before transfer
- MD5 is calculated again after transfer and compared against the original MD5 value. Only if there is a match is the file allowed to be ingested into the database and purged from the camera
- Each file's original MD5 value stays with the file for its life on the database. All subsequent MD5 calculations are compared against the original value calculated by the camera to confirm authenticity



Simple operation



HD 1080p
HD 720p
SD 480p



4.5 hours (standard)
9 hours (extended)



Highly configurable



32GB secure storage



Yardarm Holster Aware™



Field of view



Rugged



GPS



Pre-event recording



Bookmarking



Audio mute



WiFi

Multiple recording resolutions

Excellent low-light capability

Superior file integrity

Specifications

Resolution:	Selectable - 1080p/30 fps, 720p/60 fps, 720p/30 fps, D1 (480p/30 fps)
Battery Life:	
Standard:	Up to 4.5 hours SD video, up to 4 hours HD video 720p;
Extended:	Up to 9 hours SD video, up to 8 hours HD video 720p
Power Save Mode:	Standard: 48 hours; Extended: 96 hours
Internal Storage:	32GB
Record Capacity:	Up to 6 hours 1080p/30 fps, up to 6 hours 720p/60, up to 14 hours 720p/30, up to 17 hours 480p
Weight:	4.4 oz (125 g), standard battery; 6 oz (169 g) extended battery excludes clip: 0.5 oz (17 g)
IP64 compatible:	Protection from dust and water
Drop Test:	Complies with MIL STD 810G
Indicators:	Battery level, file transfer status, record status, audio mute, low media
Warranty:	One year



Excellent depth-of-field - objects near and far are crisp and clear

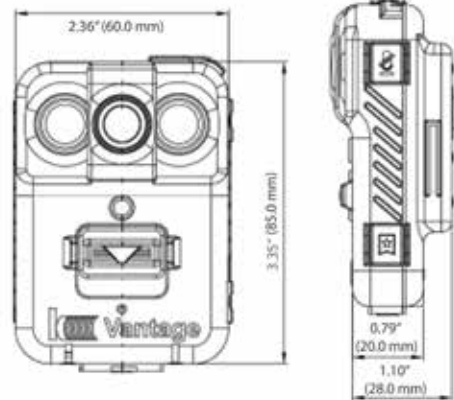


Redacted for privacy*

*Future Enhancement Options

- Redaction and cloud storage through Eyewitness Data Vault back-office software
- Wireless file transfer to Eyewitness HD in-car video system means officers don't have to turn camera in at end of shift
- Vantage files inherit the associated ICV file's stop and hold classifications = no more classifying files back at the station
- Automatic file association between Vantage and Eyewitness HD for easier/time-saving search and simultaneous playback
- Bi-directional record triggering. EyewitnessHD record activations will trigger Vantage recordings (and vice versa)
- Peer to peer record triggering – our design limits record activations to paired cameras only. This avoids the unwanted triggering of other cameras that can happen with systems that broadcast a record trigger to any camera within range
- Interface with Yardarm Holster Aware sensor - unholstering a weapon will automatically start a recording.

Dimensions



Standard: 0.79"
 (20.0mm) deep
 Extended Battery 1.10"
 (28.0mm) deep

Options

- Up to 9 hours record time with extended battery
- Mag-mount (used in lieu of supplied spring-clip)
- Multi-dock (supports six cameras - multiple multi-docks can be connected together to support larger fleets)
- File Management Software - see Eyewitness Data Vault and Eyewitness Data Vault Lite
- Extended warranty
- In car charging kit
- Play Vantage files in the car
- Wired transfer to Eyewitness HD

Yardarm Holster Aware*

- Unholstering a weapon automatically starts a recording
- No officer interaction needed to capture critical events
- Officer attention remains on the event, not the camera
- Attain multiple angles of the situation when configured with two-camera triggering



Vantage File Transfer Options

Stand-Alone

Wired docking station in office for downloading and charging. This can also function as an in-car charger/download station.



- OR -



Eyewitness Data Vault (EDV) or Eyewitness Data Vault Lite

Multi-Dock:
Insert up to 6 cameras for charging and downloading. Connect additional multi-docks together for larger fleets.

With Eyewitness HD*



In-car docking station for syncing, wired downloading to Eyewitness HD and charging.



Eyewitness HD DVR



- or -



Optional wireless* transfer allows camera to stay on officer.



Transfer all files to EDV or EDV Lite. EDV supports manual, wired or wireless transfer from Eyewitness HD. EDV Lite supports only manual transfers.

Eyewitness Data Vault *Lite*

- Ideal file management solution for smaller installations of Kustom video systems that utilize manual file transfer
- Offers the same intuitive look and feel as Eyewitness Data Vault, and retains an impressive list of features: ingest, search, play, burn and file export
- Comprehensive Admin option includes items such as User Management to control which features are accessible to each user
- Economical, customer-installable on your PC
- Included with your Vantage purchase (1 per agency)



EDV Features

EDV *Lite*

EDV

• Customer installable	●	
• Intuitive user interface	●	●
• Simple and advance searches	●	●
• Easy DVD burning	●	●
• Comprehensive audit reports	●	●
• Multiple file retention times		●
• Supports multiple sites (networked clients)		●
• Supports multiple asset types		●
• Supports wired/wireless file transfer		●
• Supports MS Active Directory		●
• Web interface for remote viewing		●
• Fleet Management		●

Intuitive, secure file management

Eyewitness Data Vault is a powerful digital video management solution that automatically and securely manages digital assets locally or across a network. It is configurable and scalable to fit virtually any environment.

Configurable

- Highly scalable - supports small & large installations - expand storage locally
- Flexible storage policy based on officer name, car number, file classification, etc. - Improves file management and resource efficiency
- Highly configurable user and user group management - determine which features within the program and the web interface are accessible to users/groups



Convenient

- Intuitive, user friendly interface simplifies learning and enables efficient use
- Compatible with Active Directory and LDAP - easily integrates with established login credentials
- Quick export from Results screen saves time
- Ingest groups of files (i.e. photos) together and link to a case number
- Easily burn multiple copies of a file
- Include reports and associated files with burned copies

- Manage evidence from all Kustom Signals' digital in-car, motorcycle and body worn video, as well as digital evidence from non-proprietary sources



- Playback timeline - easily cue video to any event (trigger, bookmark)

Secure

- Highly configurable rights management - determine who sees what
- Automatic file integrity checks (MD5) ensures authenticity
- Comprehensive audit reports track and validate chain of custody

Additional Features

- Easy DVD/Blu-Ray burning (Include video file(s), audit report, associated files)
- Powerful search features improve the efficiency and accuracy of searches
- Dashboard application for convenient monitoring of system services/storage
- Web Interface - allows authorized officers to search and play files from web browser

Highly scalable

Easy to use

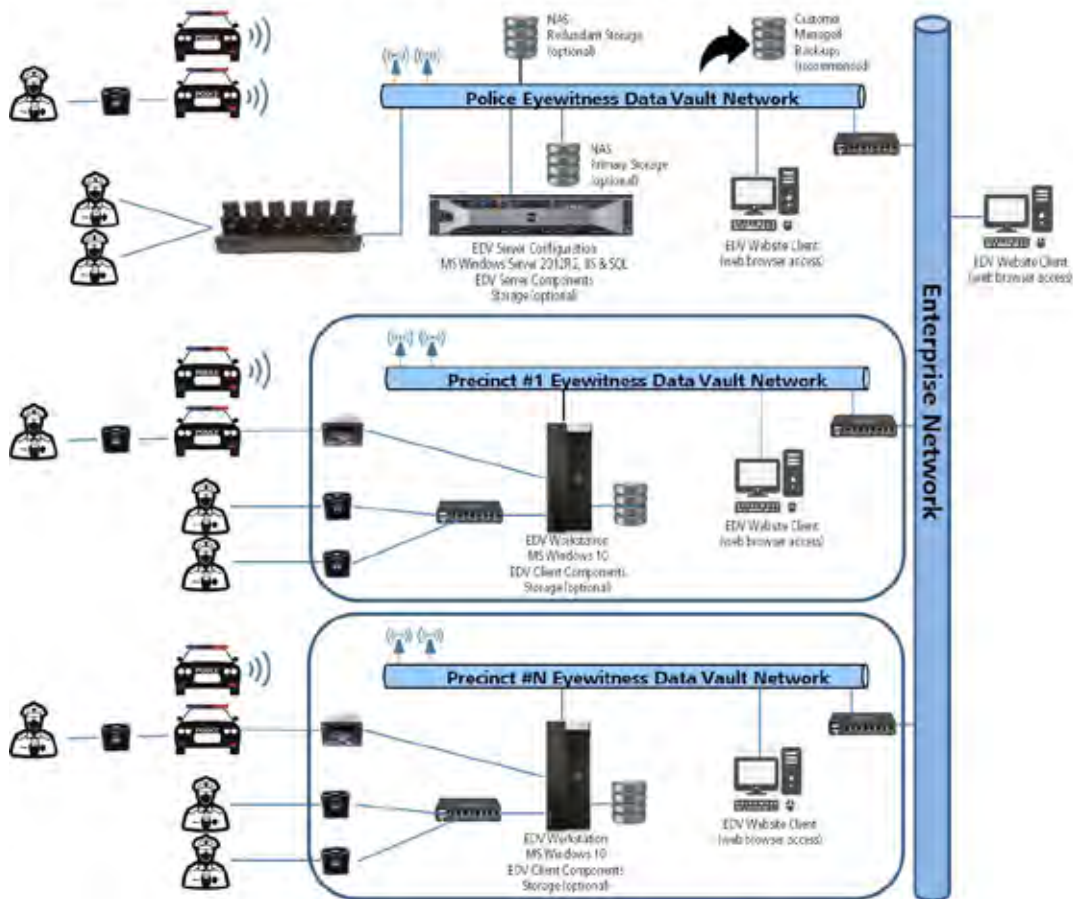
Secure user management

Eyewitness Data Vault

Digital Asset Management System



Eyewitness Data Vault Network Diagram Example



Future Enhancements

- Cloud Storage option
- A/V redaction tool
- Multi-camera synchronized playback



Eyewitness Vault - Data Sheet - USA Eng - Print - 09/2018

Eyewitness Data Vault *Lite*

- Ideal file management solution for smaller installations of Kustom video systems that utilize manual file transfer
- Offers the same intuitive look and feel as Eyewitness Data Vault, and retains an impressive list of features: ingest, search, play, burn and file export
- Comprehensive Admin option includes items such as User Management to control which features are accessible to each user
- Economical, customer-installable on your PC

EDV Features

	EDV <i>Lite</i>	EDV	EDV 3.0
• Customer installable	●		
• Intuitive user interface	●	●	●
• Simple and advance searches	●	●	●
• Easy DVD burning	●	●	●
• Comprehensive audit reports	●	●	●
• Multiple file retention times		●	●
• Supports multiple sites (networked clients)		●	●
• Supports multiple asset types		●	●
• Supports wired/wireless file transfer		●	●
• Supports MS Active Directory		●	●
• Web interface for remote viewing		●	●
• Fleet Management		●	●
• Cloud storage			●
• A/V redaction tool			●
• Multi-camera synchronized playback			●

Municipal Emergency Services, Inc.
Response for:

Request For Information Police
Body Worn Cameras
Pennsylvania Chiefs of Police
Association

25 January 2019

Municipal Emergency Services & Lawmen Supply
Contact: Mark Windover VP/General Manager
203-304-4121
7 Poverty Rd.
Southbury, CT 06488
Fax:203-264-3325
mwindover@mesfire.com

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

Mr. Christopher J. Braun M.S. IT
Technology Coordinator
Pennsylvania Chiefs of Police Association
3905 N. Front Street
Harrisburg, PA 17110

25 January 2019

Re: Request For Information Police Body Worn Cameras

Dear Mr. Braun;

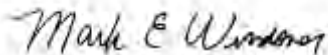
This is to respectfully submit our proposal for the Request For Information Police Body Worn Cameras on behalf of Municipal Emergency Services, Inc. (MES). Our team looks forward to working with you on this exciting project.

The following pages will respond to your statement of work requirements and will provide further background on our company, our project approach, our technology and our ability to satisfactorily meet the needs of Pennsylvania Chiefs of Police Association for your Body Worn Camera program. Most Body camera programs consist of 3 key elements Hardware, Storage and Software. We will offer an extremely unique approach to all aspects of the mission:

- 1) We will provide a robust Body Worn Camera with a full 2-year warranty on all hardware.
- 2) **Unlike most in the industry, MES does not build the mission around making money on storage whether in the cloud or on-premise.** For this program, we are offering Wasabi storage, however the SW is very flexible and can quickly adapt to whatever storage strategy you prefer.
- 3) Our team will provide world class service, with local training and program support, technical support that is led by the developers that wrote every line of the Software code, and a corporate commitment from MES that is unparalleled.

I am the authorized signatory of all technology programs for MES.

All the best,



Mark E Windover
VP/General Manager
Municipal Emergency Services, Inc.

Mark Windover
VP/GM
7 Poverty Rd. Suite 85H
Southbury, CT 06488
203-560-6010
mwindover@mesfire.com

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

Executive Summary

The following response is presented by Municipal Emergency Services (MES) in conjunction with its subsidiary Lawmen Supply, Inc (LSC) and VisioLogix (formerly HD Protech). Our team has the combination of experience in the Public Safety marketplace with best in class solutions that meet and exceed the requirements listed in the Pennsylvania Chiefs of Police Association Request For Information Police Body Worn Cameras. We anticipate that our solution will provide an excellent value for easy to deploy and manage Body Worn Cameras, in an unmatched operational environment.



MES and LSC have 45 years of combined experience in Public Safety. MES is a leading supplier to the Public Safety trades while LSC is a leading Police Safety Products Supplier with 375 Public Safety professionals across the country with an average of 25+ years of experience in the trades.

We are also proud to have as our partners, Transcend, based in Columbia, MD providing world class BWC hardware and VisioLogix, as a key technology provider for the Hydra Mission and Video Management software tool. VisioLogix is an MBE, WBE, and HUB company, from Houston, TX representing over 50% of the goods and services outlined in this proposal.

If you prefer cloud storage, we are offering a safe, CJIS Certified, economical and flexible Cloud Storage option via Wasabi Cloud Storage. Wasabi was started by the founders of Carbonite and has quickly become an outstanding source for secure and fair cloud storage.



The Municipal Emergency Services team has thoughtfully reviewed your requirements and have architected a hardware, software, and services solution that is effective, scalable, easy to administer, and will provide outstanding short and long term value for the Pennsylvania Chiefs of Police Association.

Current State of the BWC Industry



- Agencies have been pressured into costly long-term cloud contracts with ***NO WAY OUT.***
- Microsoft or Amazon Cloud solutions are generally 2X the cost of using your own IT infrastructure or Wasabi Cloud Storage.
- Opportunity to save thousands of dollars by using your current IT infrastructure or via Wasabi Cloud Storage, with **COMPLETE FLEXIBILITY ON THE BACK END SHOULD YOU DECIDE TO MOVE YOUR DATA.**
- MES/Lawmen will help you design the ideal BWC storage solution that will save you money today and over the long term either in your own environment or with Wasabi.
- **We are so committed to your success that we will help you design your own on-premise solution with your own infrastructure, we will sell you on-premise storage, or we will provide Wasabi Storage.**

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

Questions Related to RFI

- 1) *How does your non-vehicle-mounted mobile video recording systems and technology meet Pennsylvania's published requirements?***

In all cases our products meet and exceed current requirements. Please see the response below to the specific requirements.

- 2) *Have you submitted your non-vehicle-mounted mobile video recording systems to the Pennsylvania State Police for certification?***

We have not yet, but would appreciate the opportunity, we are confident that with our technology, we will have a meaningful addition to the certified companies and products with new and exciting technology.

- 3) *Is your non-vehicle-mounted mobile video recording systems already certified by the Pennsylvania State Police?***

Not yet, however we would appreciate the opportunity, and are confident that with our technology, we be certified.

- 4) *Are you offering a storage solution?***

Yes, we offer multiple storage solutions as our Hydra Digital Evidence Management Software is storage agnostic. We have NAS storage which is outlined in our pricing scenario, however we would welcome the opportunity to deploy our software with your existing IT Storage infrastructure if there is potential cost savings. We offer Wasabi CJIS Certified Hot Cloud Storage at simple pricing of \$5.99/TB per month, no long term commitment required.

- 5) *Will you offer storage solutions bundled (no line item distinction) with the cost of each camera purchased?***

Yes, we offer bundled storage solutions tied to camera cost if it is required. Many vendors have done this and the pricing scheme ends up as misleading and many times more expensive than unbundled. We will offer both as required by specific RFP's.

- 6) *How does your storage solution meet Pennsylvania's published requirements?***

Yes, please see below, we offer Wasabi CJIS Certified Hot Cloud Storage.

- 7) *List the products and services that are already available on State Contract or PA CoStars.***

Our Company is a CoStar vendor but the proscribed BWC items are not yet on CoStars. We are however an NPPGov GPO National Purchasing contract and our prices reflect these discounts.

Request For Information Police Body Worn Cameras Pennsylvania Chiefs of Police Association

8) *List your costs for products and services you offer.*

Product	Contract Category	Description	Model #	Net Price
Body Worn Camera	Category 1 Public Safety Video Cameras	64GB Internal memory DrivePro Body 30 Body Camera with a 2 year Warranty.	TS64GDPB30A	\$299.00
Body Worn Camera	Category 1 Public Safety Video Cameras	Docking Station for DrivePro Body cameras (30) with a 2 year Warranty.	TS-DPD6N	\$599.00
Body Worn Camera	Category 1 Public Safety Video Cameras	Description: 16TB, Network attached storage (NAS), DPB Control center with a 2 year Warranty.	TS-DBN1-16T	\$1,299.00
Body Worn Camera	Category 1 Public Safety Video Cameras	The Visiologix CITE A1 is a multi-functional, multi-purpose Law Enforcement tool that has a wide array of uses. The unit can be used as a standalone video recorder. An officer can use the CITE A1 to record 1080p quality video, photograph crime scenes, and record audio statements. CITE A1 records up to 7 hours of video at 1080P (over 13 hours at D1), over 250 hours of audio, and over 10,000 photos based on the internal 32GB storage card. Standard contents include: The Kit includes: Visiologix CITE A1 Camera, Standard Clip, Docking Base, USB Cable and CITE Configuration Tool for downloading videos and making configuration changes. Camera Dimension: 120x73x25mm (4.72"x2.87"x0.98"). Weight: 274g (8.8 oz). Includes 1 Year Warranty	007-1000	\$599.00
Body Worn Camera	Category 1 Public Safety Video Cameras	The Visiologix Z2 is a multi-functional, multi-purpose Law Enforcement tool that has a wide array of uses. The unit can be used as a standalone video recorder. An officer can use the CITE Z2 to record 1080p quality video, photograph crime scenes, and record audio statements. CITE Z2 records up to 8 hours of video at 1080P (approximately 16 hours at D1) based on the internal 32GB storage card. Standard contents include: The Kit includes: Visiologix CITE Z2 Camera, Standard Clip, Docking Base, DSM1 Mount, USB Cable and CITE Configuration Tool for downloading videos and making configuration changes. Camera Dimension: 85x55x23mm (3.35"x2.2"x0.9"). Weight: 140g (4.5 oz). Includes 1 Year Warranty	008-1000	\$349.00
Body Worn Camera	Category 1 Public Safety Video Cameras	CITE Camera M1G3 Intelligent Docking Station for use with EMS Standard/Enterprise Software. The docking station provides eight-port USB transfer and charging capability allowing for up to 4 hours to charge the camera. Web Interface provide easy configuration. Standard 1 Year Warranty. This model only requires a Gigabit network and 110/220V Power source.	518-1000	\$1,499.00
Body Worn Camera	Category 1 Public Safety Video Cameras	Body Worn Video Camera – includes 1080p Video, Still camera, voice recorder with automatic and program infrared to work in complete darkness. Includes a GPS transponder for location services, and a 32GB storage card which can capture up to 14 hours of video, 500 hours of audio, or over 20,000 photos. Package includes Long and Short Clip, Power Charger, DC Cable, USB Cable, and a camera software utility tool for downloading videos and making configuration changes.	004-1000	\$399.05
Body Worn Camera Video Management Software Annual Fee	Category 2 Data Management Software	Body Worn Video Camera software tool for managing the video output, the chain of video evidence, with the ability to attach records to each video file, which can be virtually any file type including audio, video, pdf, xls, doc, ppt etc. Key tool for managing the BWC asset at the agency level and managing security and full WAN/LAN capability.	SAS-1002	\$249.00
004-1000 Annual Support and Maintenance	Category 6 Services	Year 2 and beyond Product support for the Body Camera 004-1000 priced per body camera	004-1001	\$97.16
BWC Specialized NAS Server	Category 3 Data Storage and Upload Services	4 Bay NAS Server Capable of deploying up to 16TB of raw storage via 4 drives with 4TB Each	BWC NAS-16	\$2,226.00
Professional Installation Support	Category 6 Services	Day rate for Engineering support for remote install	151201-1000	\$2,499.00
Specialized Phone Support (Per Incident)	Category 6 Services	Dedicated phone support for remote access into agency PC or server priced per incident	151201-1008	\$345.45

9) *Will you offer a discount of those prices if multiple police departments group together to buy your products and services?*

Yes, we would be happy to offer discounts for multiple agencies are for larger quantities.

7 Poverty Road, 85H Bennett Square, Southbury, CT 06488 Phone: 203-304-4121

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

Response to Requirements

The following will respond to the requirements set forth in the RFI. While MES sells many different Body Worn Cameras that meet and exceed the requirements listed, we are focusing our remarks on our leading product today the Transcend DPB30 IP67 64GB Body Worn Camera.

Date/time stamp capability

The DPB30 has a date/time and GPS stamp capability that provides embedded stamping on every frame of video or still photo captured by the device. The image delivered looks like this and is an immutable element of the file once produced.



Microphone and a recording device, enclosed in secure protective enclosure(s).

The DPB30 has an IP67 enclosure that has been drop tested following the MIL-STD-810G 516.6-Transit Drop Testing protocols.

It may also contain controls, a monitor, GPS, wireless transceiver components and other electronic components.

The DPB30 has a free smartphone application that allows the user to control, monitor, provide GPS connectivity, as well as a secure wifi streaming (BWC to phone) capability.



**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

The non-vehicle-mounted mobile video recording system must be powered from a battery internal to the protective enclosure and must be weatherproof. The internal battery may be integral to the unit or removable. It is permissible to have an external battery to extend the operating life of the system.

The non-vehicle-mounted mobile video recording system must have a minimum record time of 2 continuous hours.

The DPB30 has a 3120mAh non-removable battery in an IP67 enclosure. The battery provides for up to 12 hours of continuous video. A USB cable is included with each camera which provides for recharging either from a DC source or external USB driven battery.

The system must operate over the following temperature range: -4°F to 122°F (-20°C to 50°C).

The DPB30 has an operating temperature range of -20°C (-4°F) ~ 65°C (149°F).

Camera

The camera component must have the following features:

- A. Must be color video.*
- B. Minimum of 640 x 480 pixel resolution.*
- C. Minimum of 68 degrees field of view.*
- D. Minimum of 30 frames per second.*
- E. Minimum sensitivity rating of 3.4 lux or lower. Unit may use Infrared LED illumination to obtain lower than 3.4 lux equivalent.*
- F. Camera does not have to be in the same enclosure as the recorder. Can be connected to the recorder either by cable or wireless connection.*

The DPB30 provides the following:

- A) Full color video in standard operation
- B) Delivers 480P, 720P, up to 1080P resolution
- C) Operates has a 130° Field of View
- D) 30 Frames per second delivered at all resolutions
- E) Operates down to <1 Lux and has an Infrared illumination tool for less light.
- F) The DPB30 has the camera and recorder in the same enclosure, however we have a unit that has an external camera.

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

Recorder

The recorder component must have the following features:

- A. Enclosed in a secure housing protected from physical damage.*
- B. Date/time recording index.*
- C. Minimum of 4 gigabytes of nonremovable solid state memory, 4 gigabytes removable media or a combination of both removable and nonremovable memory.*
- D. Editing and record-over protection.*

The DPB30 provides the following:

- A) IP 67 Mil Spec enclosure.
- B) Date and Time stamp embedded in each frame of the video and still photos.
- C) 64GB of non-removable memory
- D) All cameras are password protected to prevent editing and record-over protection.

System Control

The system must:

- A. Be capable of recording audio and video simultaneously, but may also provide the user with the option to record video only or audio only.*
- B. Provide the user with the capability to manually turn the power on and off as necessary.*

The DPB30 provides the following:

- A) Simultaneous and synchronized audio and visual recording with the option to mute audio with a touch of a button and can toggle back on from a muted state.
- B) Camera turns off/on with the touch of a single button.



**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

Wireless Link (optional)

The unit may use a wireless link to connect the camera to the recorder, recorder to another device, combination camera/recorder to another device or be used to download the evidence. The wireless link must have the following features:

- A. Use a secure digital connection.*
- B. Wireless link can be used to play back a locally stored event on the recorder or store the media to a remote location such as secure Cloud storage.*
- C. FCC Type acceptable under 47 CFR Part 15 (relating to radio frequency devices).*

The DPB30 has a free smartphone application that allows the user to control, monitor, provide GPS connectivity, as well as a secure wifi streaming (BWC to phone) capability. It is recommended that the unit be charged with data uploaded via the 6 port docking station outlined below. All DPB30 cameras and accessories are certified by; CE, FCC, BSMI, NCC, and MIC.

Law Enforcement Officer Camera System Data Handling Requirements

A. Camera system

- 1. While worn by the officer, a camera system shall be considered a physically secure location.*

The DPB30 has multiple secure mounting options to secure the device to the operator. A recent Police Magazine article indicated that 58% of officers surveyed indicated that their BWC unit had fallen off. MES and Transcend have taken great care in created a sturdy and stable environment to properly secure the devices to the officers. The DPB30 has multiple mounting options with its secure heavy-duty clip solution. There are also magnetic, molle, and Velcro mounting solutions as well.



**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

2. Upon removal from the officer's body, the camera system shall be maintained in a physically secure location in accordance with CJIS Policy standards.

Per the description above, we highly recommend the use of the proscribed docking station in a secure agency location to ensure proper CJIS security protocols. All data is moved through the system via the Hydra Digital Evidence Management software (DEMS) via encrypted protocols. Please see schematic in our Technology Summary.

6 Port Docking Station



B. Data transfer or downloading the data

The DPB30 has non-removable media storage which allows only the secure offloading of data. Also, the memory card is 64GB eMMC (embedded multimedia card) which is soldered on the board, therefore there is no memory card you can simply pop out and plug in to another device. In the event the camera is stolen or gets in the wrong hands, you cannot access the data without a password. All data transfers are done via secure communication using HTTPS and all data transferred are secured using 256-bit encrypted communication with 2048-bit root keys.

C. Storage of the data

Storage of data on location, if considered a physically secure location, shall be treated the same as all CJI at the location.

The MES BWC solution with the Hydra DEMS is storage agnostic. Many agencies have chosen to deploy via a cloud environment which in our case is CJIS secured via Wasabi Hot Cloud Storage (Please see attached schematic). Many BWC companies will force agencies into 3-5 year inflexible cloud contracts to lock up their business. We would much rather earn the business every year with great service and let the agency decide for themselves. 90% of the time agencies have the on-premise storage resources already in place which is where the mission should begin. If over time substantial infrastructure investment is required then consider making the call between insourced (on-premise) or outsourced (cloud) storage solutions.

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

D. Reviewing and release of data

1. Data from the camera system shall only be reviewed by authorized personnel; that is, personnel that have been cleared through a fingerprint-based background check, have received Security Awareness Training and have signed the appropriate agreements, if applicable. If required, the Management Control Agreement for local government IT, or The Security Addendum for private contractors, shall be completed and on file.

The MES BWC solution with the Hydra DEMS provides for RBAC (Role Based Access Controls) which provide a full spectrum of personnel access authorization protocols. Please see our technology description for further details.

2. Prior to the release of data from the camera system, the data shall be reviewed and any areas containing CJI shall be removed or rendered unintelligible. Any data received from CLEAN or the National Crime Information Center in either video or audio format, or both, shall be removed or rendered unintelligible prior to release to any unauthorized or unintended personnel.

The MES BWC solution with the Hydra DEMS provides for a deletion mechanism that is complete and tracked via an extensive logging system throughout the process. Please see our technology description for further details.

E. Retention of data

Data shall be stored for 60 days unless needed for prosecution, courts, litigation, appeals or other operational needs.

The MES BWC solution with the Hydra DEMS provides for an unlimited number of retention schedules so a 60 day retention is standard. Please see our technology description for further details.

F. Destruction of data

The MES BWC solution with the Hydra DEMS provides for a deletion mechanism that is complete and tracked via an extensive logging system throughout the process. Please see our technology description for further details.

Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association

Technology Description

BWC – Digital Evidence Management and Storage Solution

The Body Worn Camera mission is centered around 4 key components; 1) Hardware, 2) Software, 3) Application Assurance, and 4) Storage. Our software is the foundational element of the entire ecosystem as it allows many different types of BWC hardware, while accommodating on-premise, Cloud, or Hybrid storage.

1) Hardware

We are delivering best in class IP-67 SHD hardware that has been tested in the toughest of environments and real field punishment. Our goal is to make the camera itself incidental to the mission with a care free ownership experience with an extremely quick training requirement.

2) Software

Our globally deployed C-3 Sentinel client software has been adapted onto a Web version called Hydra. As before, the interface is elegant with simple to follow steps for a secure and efficient operational and administrative experience. This software is not only hardware agnostic, it can be used in virtually any storage environment. Hydra makes CJIS compliance a breeze with its RBAC administrative control protocols.







3) Application Assurance

Hydra Application infrastructure is deployed via Microsoft Azure Government Cloud Services. This provides the highest level of security for the application which includes all of the file metadata and supporting infrastructure for the object storage in Wasabi. This secures all of the web hosting aspects of the Hydra software suite as well.

4) Storage

Our docking station and DrivePro™ Body Control Center provides 16TB of data storage per 2 6-bay docks at the local center level which provides additional speedy back up for immediate review and an excellent redundancy for your on-premise storage. Our Hydra Software is completely storage agnostic so you are able to continue to deploy whatever storage array you prefer and move data at any time to either additional on-premise resources, cloud storage options, or a hybrid, 100% your call.

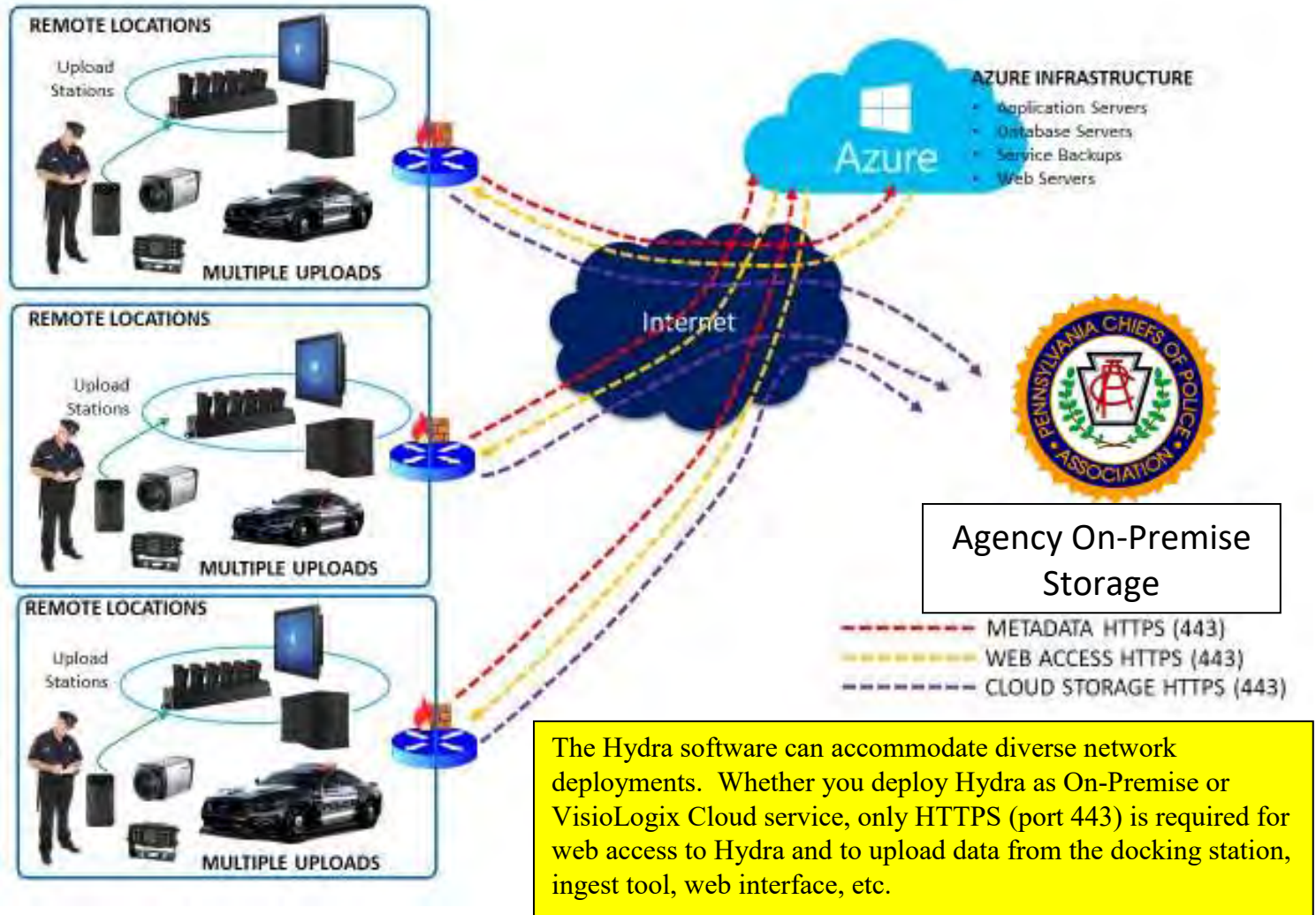
Our all-star line-up:

Software	Application	Hardware	Storage
			
			On-Premise provisioned at the docking station level or on the Cloud VisioLogix Hydra Software is agnostic to storage preference.

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

On Premise Storage Schema for Pennsylvania Chiefs of Police Association

Data is uploaded from the camera to the local redundant DrivePro™ Body Control Center at the docking center level, data is then sent to the Hydra DEMS application is delivered and managed via the Microsoft Azure application layer. All Data is then uploaded from remote locations via the internet to your secure on-premise storage.



**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

DEMS Mission Schema for Pennsylvania Chiefs of Police Association

The VisioLogix BWC program is an easy to deploy and efficient way to manage this critical mission. It starts with the camera being taken from the intelligent docking station. No sign out is required unless the assets are shared. The easy to use DPB30 Camera gets deployed to the field and captures video, pictures, etc. While in the field, the operator is able to review the captured case data on an MDT.

Outlined in Step #3 is our EMS Mobile Client Software which (if authorized by the administrator) allows the operator to review and annotate captured files via the light weight client software that can be installed on the MDT. The operator is able to add key metadata elements including case #, the address, the event classification, along with any video clips that the operator would like to make to help support the case.

All of this data is saved to the camera for each file and is then uploaded at the docking station at the end of shift or whenever the operator chooses to upload their data. The data is then immediately uploaded to the Hydra Database in the Wasabi hot storage cloud.



**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

Solution Overview

The MES/Lawmen Body Worn Camera solution provides a comprehensive solution that will provide best in class BWC hardware, and managed data storage, along with an industry leading Mission Management software solution.



The primary camera proposed is an IP-67 waterproof heavy duty camera that is a full featured camera that offers a WiFi and Bluetooth connection and a free App which allows the officer to review videos prior to downloading to the system. The camera the unit delivers a 130° field of view with a 3120 mA battery delivering up to 12 hours of video at standard definition with 24+ hours of standby.

An important element of our proposed solution is a GPS module. The Transcend DPB30 camera has a GPS module that delivers location to all video files captured. When combined with the vehicle MDT GPS, provides an added dimension to the data delivered. There is also low light capability which allows the camera to operate down to less than 1 Lux and has an infrared capability that captures up to 10ft at low or no light situations.

Triggering the Drive ProBody Body Team Sync for Mutual Aid

When a team is created and Bluetooth is turned on, when Camera #1 is activated, all surrounding connected team member Cameras are triggered and activated to support Camera #1.

Team Sync



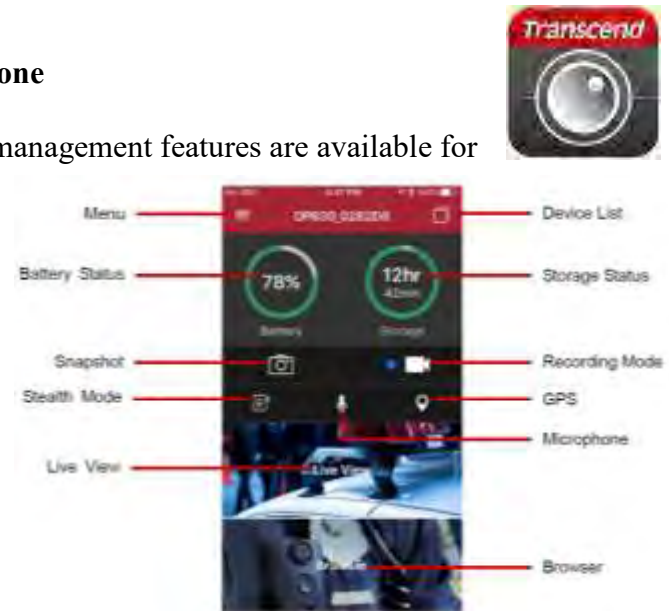
**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

DrivePro Body App for any Android or IOS Smartphone

Simply download the free app for your phone and many management features are available for your mission.

Once the camera is paired, you are able to see exactly how much battery and storage remain and are able to live view via BlueTooth and WiFi.

Operators are able to see live view from the video camera from up to 25ft. Browsing and reviewing files is also possible via the app.



Docking Station

The Docking Station allows you to securely ingest camera data from multiple locations. With the capability to throttle bandwidth, the docking station will never saturate a slow Internet connection. This solution provides a cost and time effective answer for ingesting camera data and returning cameras to the field faster.



DrivePro™ Body Control Center

Transcend's DrivePro Body Control Center is a digital evidence management system designed specifically to work with the TS-DPD6N networked docking station. With up to 16TB storage capacity, this secure, centralized server can store more than 4,000 hours of 1080P video recordings. All data transfers are done via secure communication using HTTPS and all data transferred are secured using 256-bit encrypted communication with 2048-bit root keys. We have estimated the following for potential storage requirements.



While the hardware is critical, we firmly believe that it is our software that sets us apart

Request For Information Police Body Worn Cameras Pennsylvania Chiefs of Police Association

Software Solution

We at MES/Lawmen firmly believe that the software component of a body worn camera is the most critical from managing evidentiary files, to managing user access, and file management issues, the software is what an agency lives with every day. The hardware on the road becomes incidental to the mission, it's the software that will enable PCPA to operate efficiently and effectively.

Video Evidence Management Software – The Hydra Mission Management and Video software tool is a highly intuitive software package that allows administrators to provide for solid management of the Dash Camera and Body Worn Camera assets, while providing the necessary tools to regulate and assign access to files and functions. The system was designed with the end game of providing solid legal ground for the control and management of the video, photo, and audio files captured by your cameras.

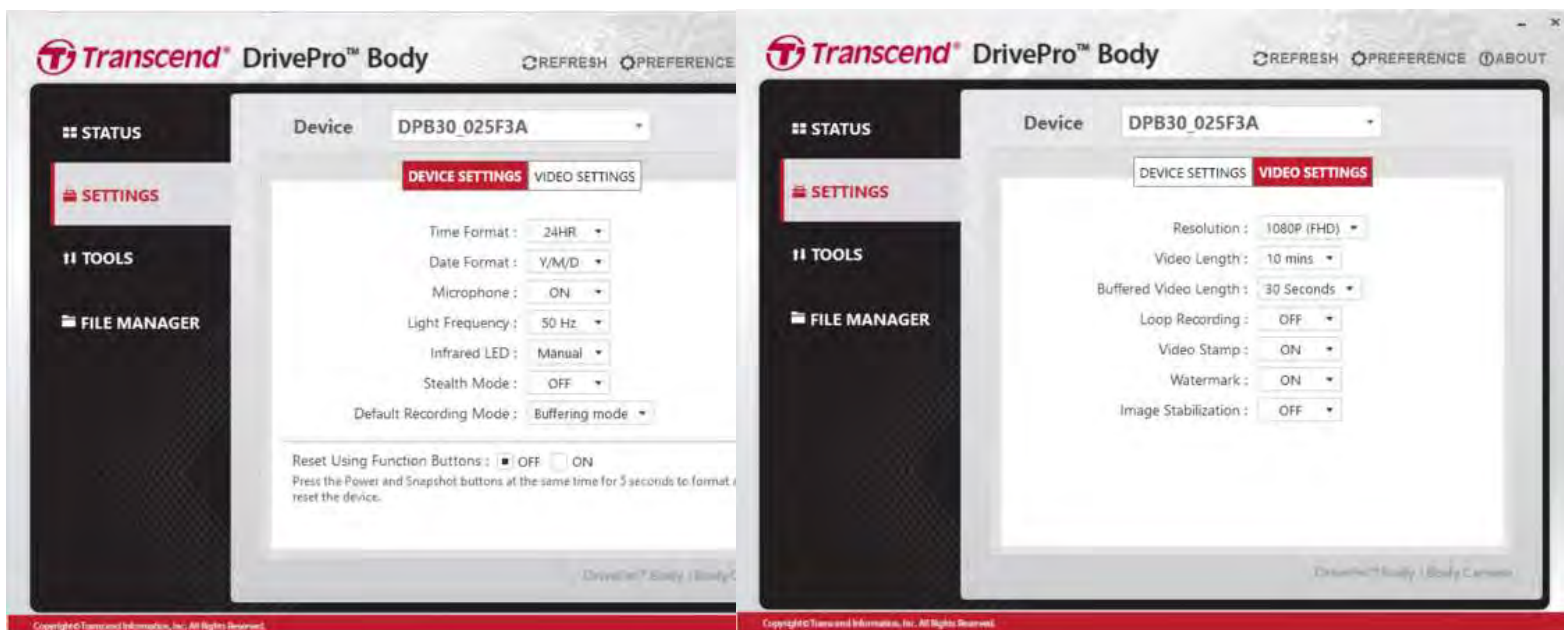
It is understood that policies surrounding the Body Worn Camera mission will continue to evolve over time. The Lawmen/VisioLogix mission management and video software solution provides for complete flexibility as it relates to many key policy issues including; retention, file access, chain of evidence and many other issues.

To further explain the capabilities of the software, we have divided the Body Worn Camera mission into 8 steps from assigning the camera to the eventual transfer of evidentiary files.

Step #1 Managing the Camera asset

A critical task of any large-scale Body Worn Camera as proposed for RPD is the management of the camera asset. We offer a very convenient tool that allows administrators to perform a wide variety of tasks while maintaining a well-managed inventory of cameras and users.

The Drive Pro Tool Box allows administrators to easily assign an identical camera profile to all of the cameras in the mission. The Admin is able to set all camera settings and to assign cameras to an individual officer. Agency Administrators truly appreciate the convenience and elegance of this tool.



Request For Information Police Body Worn Cameras Pennsylvania Chiefs of Police Association

#2 Deploy in Field

When an officer commences video capture, they simply push the record button to capture video of an event, at which time a programmable audible/haptic response of a beep or a buzz emitted from the device. To complete the recording, the officer then pushes the record button and then 2 beeps or buzzes will be emitted from the device indicating that the video was completed. While the officer is recording the event, a red light indicates that the event is being recorded, if desired. An officer may review the video via the smartphone app, but will not be able to remove or alter any of the captured video data.



#3 Classify Critical Evidence

One of the keys to efficient management of the body camera video file assets is to create and execute an effective retention policy and methodology. The C3 Sentinel software provides a tool for agencies to effectively and efficiently remove unnecessary files in a consistent and fair way. The software has a classification system that will automatically assign times and dates for unnecessary files to be purged from the video file storage system in order to properly manage volume and the inherit costs and complexity associated with managing large volumes of data.

The classification of a video file can be made at the mission software level and is able to be assigned to the video files at the camera level following a recorded event. This will streamline the check in administrative process. These classifications not only allow for retention length, they can assign specific users levels that can review these events, and important can route events to different storage locations if desired.

Settings

Classifications

Classification	Code	Primary	Mobile	RBAC	Retention Policy
Arson	AR-0912	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	30 Day
Assault-NoWeapon	ANW-101	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	6 Month
Assault-Weapon	AW-123	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	6 Month
Auto Accident	AA-200	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	60 Day
Auto Arson	AA-100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	60 Day
Auto Theft	AT-1231	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	60 Day
Bank Fraud	BF-882	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Sergeant Role	1 Year
Burglary	BR-1221	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	90 Day
Domestic Violence	DV-100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	No Security	90 Day
DWI	DWI-010	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	90 Day
Felony 1	DM-090	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Officer Role	30 Day
Homicide	HC-919	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Detective Role	1 Year
Parking Violation	PVX-100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	90 Day
Robbery	RB-1921	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	6 Month
Runaway	RXX-100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	6 Month
Stolen Property	SPX-100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	90 Day
Suicide	SSX-100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	1 Year
Traffic Violation	TR-100	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Officer Role	6 Month

☒ Primary Classification
☒ Mobile Classification
Classification Name
Assault-NoWeapon
Classification Code
ANW-101
RBAC, Security
Officer Role
☒ Enable Retention Policy
6 Month
☐ Enable Aging Policy
Storage Device

Save
Reset
Delete

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

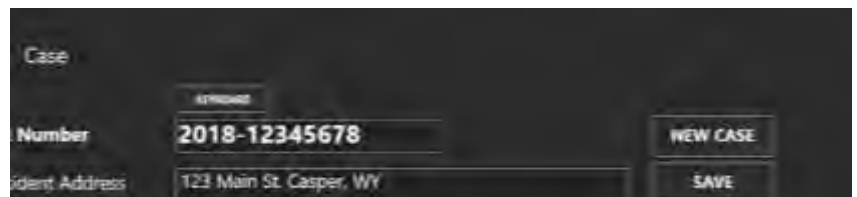
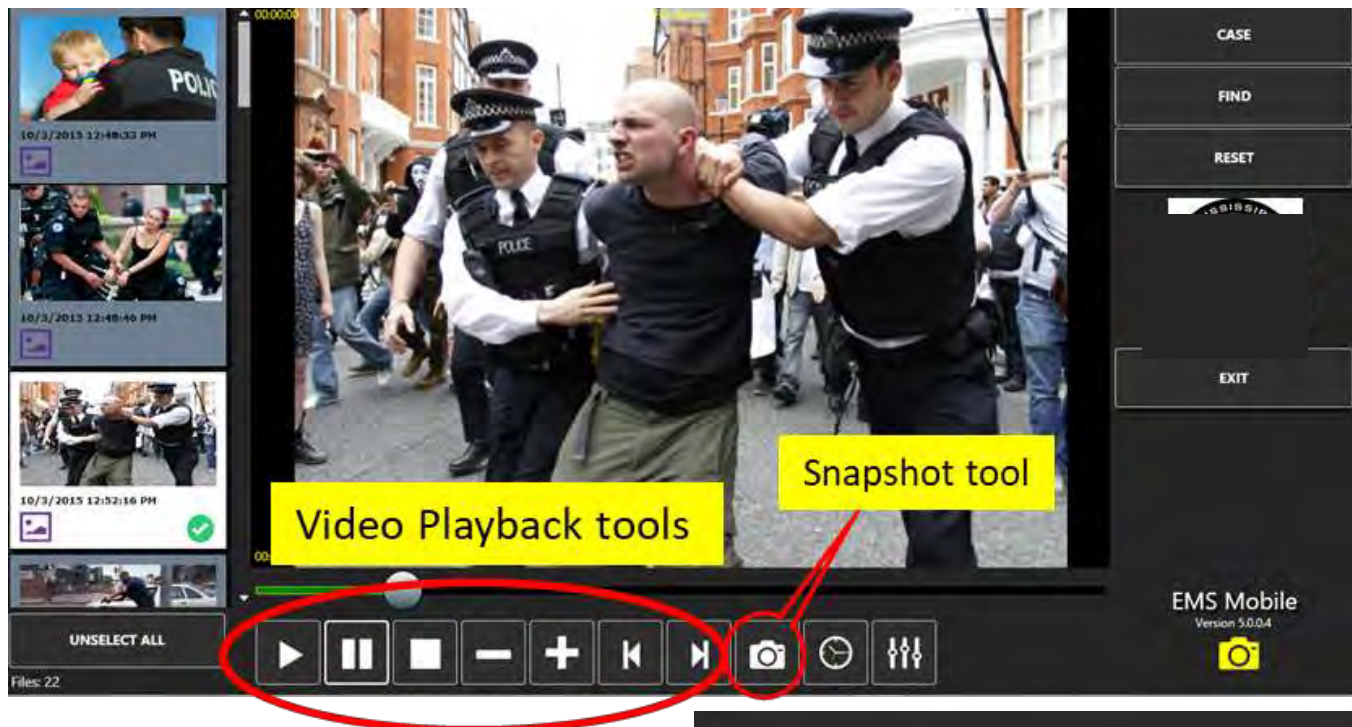
#4 Review and Annotate Files in the field via the MDT

EMS Mobile Client software can be installed on the MDT allowing officers to securely review BWC files (without downloading), and add notes and metadata which can include case#, ticket#, and critical event classification information that are attached automatically to the files to be downloaded from the cameras.

This tool allows the officer the opportunity to review video, tag pertinent sections, attach additional reports of virtually every file type, and to take snapshots of elements of the video for evidentiary management.

The field review of files allows the operators to make the best possible notes while the event is still fresh in their mind to “do once at once”. All of the notes and metadata are added to the file and stored in the camera until the operator comes to the shop to securely download. If the file has been properly coded, there is little that the officer must do once the camera is docked.

The Mobile Client on the MDT is extremely convenient and easy to use.



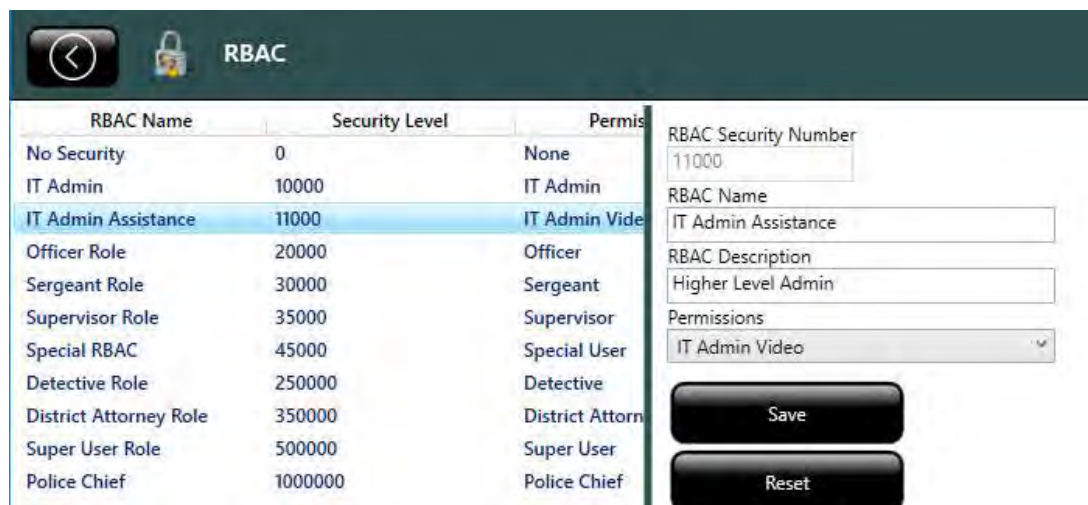
- Deploys RBAC permission standards
- Unlimited number of Permission Groups.
- 33 Key System Activities as permissions.
- Completely controls access to the system.

Request For Information Police Body Worn Cameras Pennsylvania Chiefs of Police Association

RBAC System access protocols

The Hydra system was pressure tested with the British Home Office with some of the strictest of RBACs (Rules Based Access Controls) in the world. Our system was designed with this in mind so we are able to manage roles in a wide range of ways.

The first level of group permissions is at the full RBAC level which assigns an infinite number of permissions level for your agency. In this case, the chief is at the highest level of 10000000, the next highest level is at 500000 at the Super User level. This allows the agency to classify the most sensitive of files at whichever level is most convenient and to allow the most defensible allocation of access to those who need it.



RBAC Name	Security Level	Permissions
No Security	0	None
IT Admin	10000	IT Admin
IT Admin Assistance	11000	IT Admin Video
Officer Role	20000	Officer
Sergeant Role	30000	Sergeant
Supervisor Role	35000	Supervisor
Special RBAC	45000	Special User
Detective Role	250000	Detective
District Attorney Role	350000	District Attorney
Super User Role	500000	Super User
Police Chief	1000000	Police Chief

RBAC Security Number: 11000

RBAC Name: IT Admin Assistance

RBAC Description: Higher Level Admin

Permissions: IT Admin Video

Save

Reset

RBAC at the rank level is also critical. This provides an efficient and consistent application of the access control discipline in a hierarchical and chain of command manner. In your case, the Commander would get a higher permissions level than the officer. This is all definable at the agency level.



RBAC Name	Security Level	Permissions	Accounts
No Security	0	None	0
IT Admin	10000	IT Admin	0
IT Admin Assistance	11000	IT Admin Video	0
Officer Role	20000	Officer	1
Sergeant Role	30000	Sergeant	1
Supervisor Role	35000	Supervisor	1
Special RBAC	45000	Special User	0
Detective Role	250000	Detective	0
District Attorney Role	350000	District Attorney	0
Super User Role	500000	Super User	4
Police Chief	1000000	Police Chief	0
TEST PROFILE	5000000	Test	0

RBAC Security Number: 500000

RBAC Name: Patrol Commander

Description: Super Supervisor

Permissions: Super User

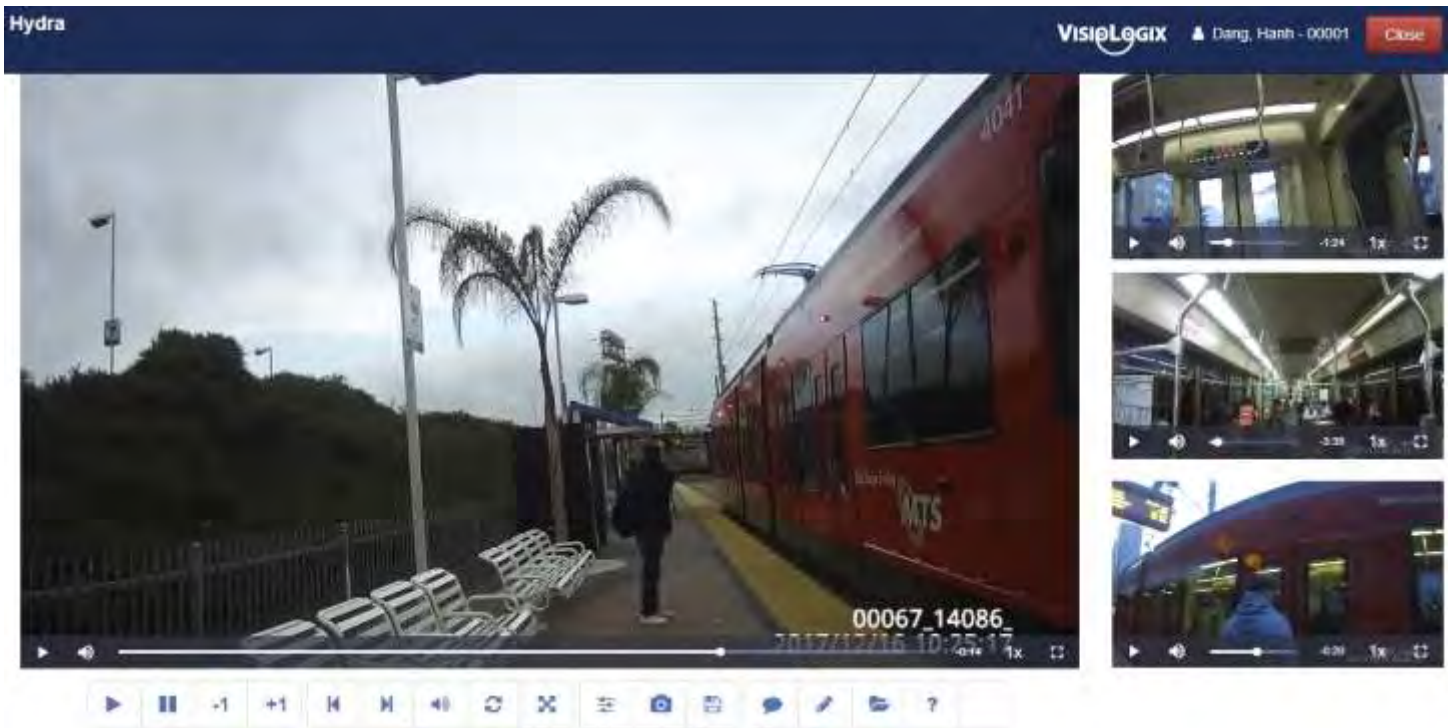
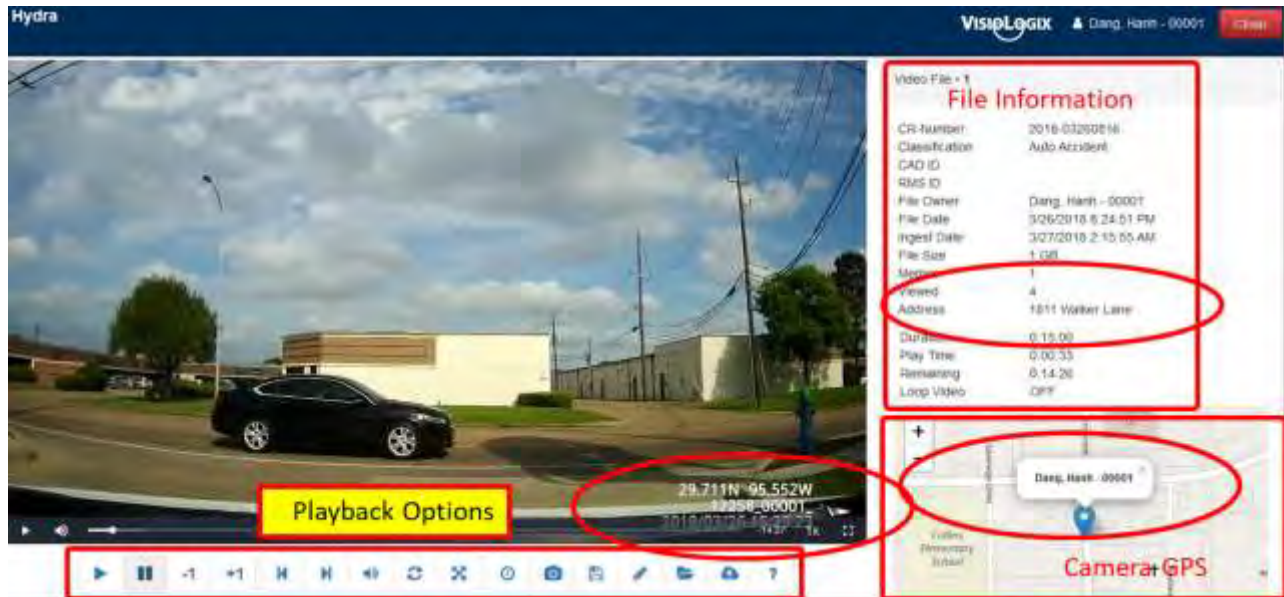
Save

Reset

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

#7 Review and Manage Files

The VisioLogix VEMS has a thoughtful and easy to use file review system with easy search with Boolean operators as well as an array of tools for viewing, classifying, annotating and redacting files. The interface is simple.



Request For Information Police Body Worn Cameras Pennsylvania Chiefs of Police Association

#8 Data Security

All files ingested in to the system are assigned a SHA2 hash code unique to the file. The hash code for each file is stored with the file metadata in the database. The system will automatically alert if the file has been tampered with. The figure to the right is an example of how the hashing files look as well as the structure of the metadata.

File Owner	Windover, Mark - 902
Original Name	ICV_20180509114520.mpg
File Name	83ee2ed7-2d62-4ac1-8ce0-c0f55ada0d84.MP4
File Time	5/9/2018 1:02:35 PM
Ingest Time	5/9/2018 2:02:35 PM
Last View	5/9/2018 2:03:10 PM
View Count	1
Duration	00:00:07
File Size	1.3 MB
Camera ID	107.77.223.139

In compliance with the IACP recommendation, all video captured has a digital signature applied via the camera check out process. When an officer checks out their camera and inputs their PIN, all files that are captured on the camera, will have the officers badge number (or other designation as determined by the agency) embedded directly to the files.

There are a number of critical safeguards in our solution that prevent deletion of files; 1) Camera memory is embedded and not removable, 2) Video, Audio, and Photo files can be reviewed at the camera level with no opportunity to delete or change files in any way, 3) Once the files have been downloaded into the system, the Mission Management Video system assigns file management access at the administrator level, 4) Only personnel assigned by the administrator (we recommend only 1 or 2) are able to manually delete files.

The C3 Sentinel Software suite has an easy to use administrative function (see Step #6 above) that assigns user access by individual or group. The system has the ability to use Microsoft Active Directory as a means to allow for authentication at the user level. Password strength is completely programmable at the administrator level with 8 system parameters.

Hydra | Dashboard | Settings | Reports | Alerts | Accounts | Help

SYSTEM SETTINGS

Category	Description	Value
ENV - CUSTOMER	Customer Account Name	VisionLogix Corporation
ENV - CUSTOMER	Account Logo URL Reference	http://visionlogix.com/content/uploads/2018/02/VisionLogix_Logo.png
ENV - CUSTOMER	Logo Image Height	50
ENV - CUSTOMER	Logo Image Width	100
ENV - ADDRESS	Default Account Address	6100 Corporate Drive, Suite 234
ENV - ADDRESS	Default Agency Address City	Houston
ENV - ADDRESS	Default Address State	Texas
ENV - ADDRESS	Default Postal Code	77039
ENV - MISC	Port Display for Case Number	Case Number
ENV - RETAIN	Retention service enabled	True
ENV - RETAIN	Run Retention Check	True
ENV - RETAIN	Time of day to run retention agent (HH:MM)	01:30
ENV - RETAIN	Erasure status unlocks after n days	True
ENV - RETAIN	Min days to delete unerase files	120
ENV - RETAIN	Frequency - day of the week (S-D)	1
ENV - RETAIN	Retention - File Purge Check Period Days	30
ENV - PWD	Enable Password Restrictions	True
ENV - PWD	Minimum pass length	8
ENV - PWD	Requires uppercase letter	True
ENV - PWD	Requires a number	True
ENV - PWD	Not be same as user Login ID	True
ENV - PWD	Password must contain special characters (REGEX)	False
ENV - SECURITY	Enable 2 Factor Authentication	True
ENV - SECURITY	Allow User Access to Reset PWD	True

Description:

Value:

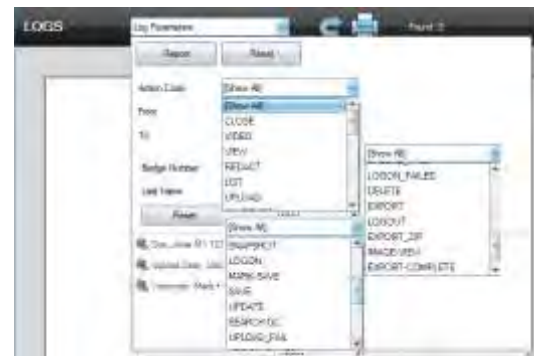
Units Type: INT

Request For Information Police Body Worn Cameras Pennsylvania Chiefs of Police Association

Logging and Control Capabilities

The Hydra software has a thorough logging methodology that allows administrators and supervisors to have complete transparency into all aspects of the DEMS operation. The report logs 20 different account activities as it relates to system access. There is also an extensive SQL reporting feature that provides a complete look at all account, camera, evidence and file activities.

The Hydra software suite also has complete logging at the user, PC, and camera level. Every call on the system is completely tracked to manage user activity on the system. This is a critical element of maintenance of evidentiary integrity. Since the software supports SQL Reports, anyone with SQL Reports knowledge will be able to produce additional reports as needed. For example, PCPA can set up an SQL Report server to centralize all reports created by the IT Department.



ACCOUNT ACTIVITY

0000 Admin, IT
11/29/2014 2:37:04 PM / 7/7/2015 11:25:39 AM

0. 6/8/2015 7:32:36 PM Action Code: LOGON
Domain: ME SFIRE Machine: ME S-LPT-21426S Machine account: mwindover
IP: 10.100.10.187 Machine ID: 3691-1B0D-B7BD-570B-4570-B7B4-12DE-02AA
Admin, IT [0000]/ admin

1. 6/8/2015 7:42:09 PM Action Code: LIST
Domain: ME SFIRE Machine: ME S-LPT-21426S
IP: 10.100.10.187 Machine ID: 3691-1B0D-B7BD-570B-4570-B7B4-12DE-02AA
List Accounts

2. 6/8/2015 7:45:44 PM Action Code: LOG
Domain: ME SFIRE Machine: ME S-LPT-21426S
IP: 10.100.10.187 Machine ID: 3691-1B0D-B7BD-570B-4570-B7B4-12DE-02AA
Admin, IT [0000]

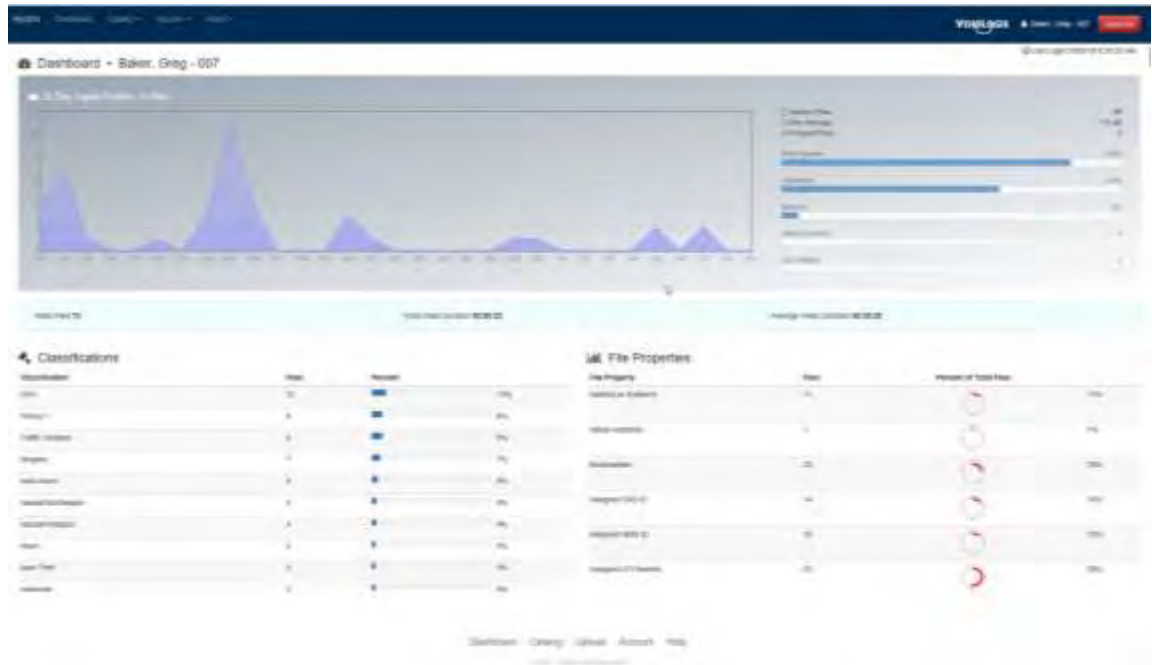


Request For Information Police Body Worn Cameras Pennsylvania Chiefs of Police Association

Reporting Capabilities

The C-3 Hydra DEMS has extensive reporting capabilities that provide users and administrators important metrics on the BWC mission. Below is an example of the customizable dashboard that users can see when entering the system.

Dashboard



Highly Customizable Reporting Structure

The reporting structure form includes the following fields and options:

- Global Search:** A search bar for finding specific records.
- Classification:** A dropdown menu with options like "Auto", "Auto Accident", "Auto Theft", etc.
- Address:** A text field for the location of the incident.
- CAD ID:** A text field for the CAD system ID.
- RBAC Security:** A dropdown menu for role-based access control.
- From Date:** A date picker for the start of the report period.
- To Date:** A date picker for the end of the report period.
- By File Date:** A checkbox to filter by file date.
- City:** A text field for the city of the incident.
- State/Province:** A text field for the state or province.
- Postal Code:** A text field for the postal code.
- RMS ID:** A text field for the RMS system ID.
- Classification:** A dropdown menu with options like "Auto", "Auto Accident", "Auto Theft", etc.
- By File Date:** A checkbox to filter by file date.
- By File Date:** A checkbox to filter by file date.
- By File Date:** A checkbox to filter by file date.

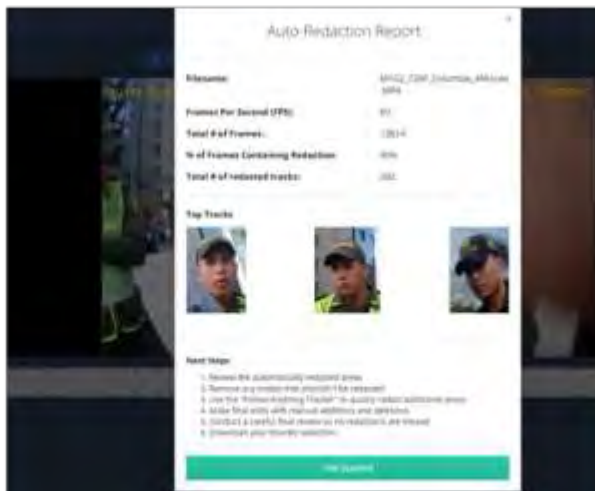
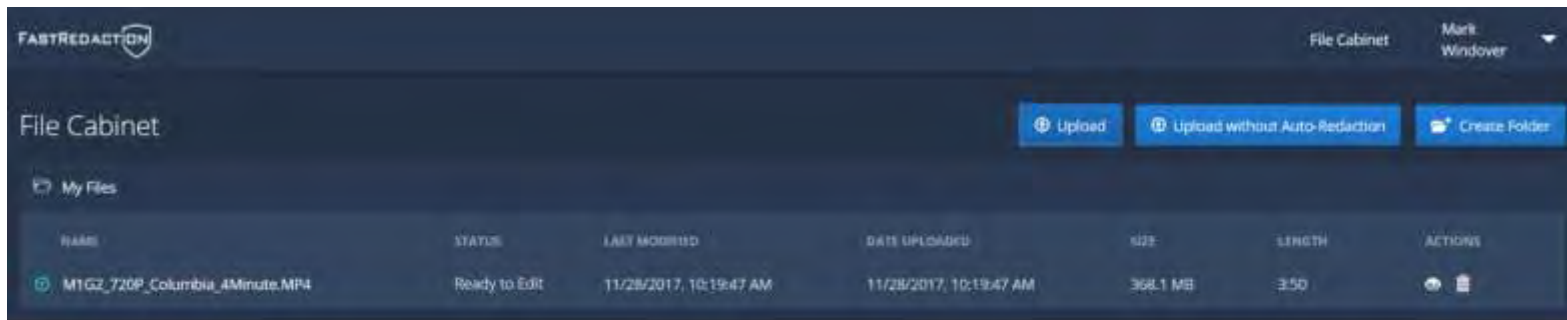
Request For Information Police Body Worn Cameras Pennsylvania Chiefs of Police Association

Redaction Capabilities

We are recommending obtaining a seat license for Fast Redaction, which is a robust and easy to use Web based redaction tool. It is extremely easy to deploy this software in any number of locations via the web. Every file is placed in a secure cloud based CJIS secure environment.

Fast Redaction has industry leading algorithms that have been used in major agencies like Cleveland, OH PD and New Haven PD and is quickly being adapted by agencies all over the country. The VisioLogix DEMS solution will provide a simple web interface for working within Fast Redaction's CJIS compliant cloud environment. The figure below outlines the end product which easily and automatically blurs face and other key identifying features like license plates without human intervention.

Here is the web interface for use with any video sources of data.



**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

Wasabi Cloud Storage

Wasabi features a highly parallelized system architecture that delivers breakthrough performance. A fully compliant Amazon S3 API protects and extends previous investments and gives customers a choice in storage management applications and backup tool



Strong Security Systems and Practices Safeguard Customer Data

Wasabi hot cloud storage is engineered for extreme data durability, integrity and security. The service is built and managed according to security best practices and standards, and is designed to comply with a range of industry and government regulations including HIPAA, HITECH, FINRA, MiFID, CJIS and FERPA.

Wasabi takes a “defense-in-depth” approach to security to protect against the widest range of threats. We ensure the physical security of our data centers; employ strong authentication and authorization controls for all cloud compute, storage and networking infrastructure; and encrypt data at rest and in transit to safeguard confidential data.



Physical Security

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

Secure Network Architecture

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

Immediate Access to Data

Wasabi doesn't play games with Hot or Cold archived data. With Wasabi all stored data is Hot and always immediately accessible at the highest speeds in the industry.

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

Data Privacy and Security

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

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

Data Durability, Protection, and Redundancy

Wasabi hot cloud storage is engineered for extreme data durability and integrity. Wasabi provides eleven 9s (99.999999999%) object durability, protecting data against hardware failures and media errors. In addition, Wasabi supports an optional data immutability capability that protects data against administrative mishaps or malicious attacks.

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

All data has $2N + 1$ redundancy, which means there are two parallel arrays with the same exact architecture and the two arrays are integrated together and communicating which workloads are where for protection purposes. If something happens to one array, you have another adjacent array in constant communication which can pick up right where the other one may have failed.

Wasabi 2N+1 Redundancy



Absolute Flexibility

Unlike all other Public Cloud Providers, Wasabi allows you complete access to all of your data with the ability to migrate any or all of your data to another source whether it be local or another cloud provider. After all...your data is always your data.



Summary

Wasabi is engineered to meet stringent data security and privacy requirements. The service is built and managed according to security best practices and standards, and employs a defense-in-depth approach to protect against a wide array of threats. We ensure the physical security of our data centers, implement strong authentication and access controls to safeguard infrastructure and services, and encrypt data at rest and in transit to protect privacy and prevent unauthorized disclosure.

Request For Information Police Body Worn Cameras Pennsylvania Chiefs of Police Association

Company Background- Organization and Experience

Municipal Emergency Services is one of the largest providers of Public Safety goods and services in the United States with well over 25,000 customers across the country. Our 375 people manage a business that is in excess of \$227M (2016 Revenue) and have delivered some of the largest public safety programs in the US in the police, fire and EMS trades.

MES and its Law Enforcement business, Lawmen Supply Company, have 45 years of combined experience in Public Safety. MES is a leading supplier to the Public Safety trades while LSC is a leading Police Supplier with our 375 Public Safety professionals across the country with an average of 25+ years of experience in the trades.

Listed below are key contact reference names for BWC programs built and deployed by MES and VisioLogix, technology provider for your solution. The most important element of the solution is the software and that has been pressure tested in large deployments on a scale with the PCPA BWC program as described.

Customer	Vendor	Contact Name:	Address:	Phone:	Email:	Camera Count
Rochester Police Department	MES and HD Protech/VisioLogix	Lt. Mike Perkowski	185 Exchange St. Rochester, NY 14614	585-428-8831	mp0963@cityofrochester.gov	508
Chinese Police in Shenzhen	HD Protech/VisioLogix	Rita Wang	Win-Win Development Technology Co Floor 4, Plant 112, Jindi Industrial Zone, Futian District, Shenzhen, China.	Cell: +86 181 2707 3684	wangr@sector2dev.com	12,000
ALSI-ASIA-PAGE Ltd.	VisioLogix leading project.	Alexandr Ponomarev	Head of Security Solutions Department 34a, Zhandosov st, Almaty, Kazakhstan	Phone: +77272971016 Mob: +77019077131	Alexander.Ponomarev@alsi.kz	2,000
Allied Universal Protection Services	MES and HD Protech/VisioLogix	Mr. Mark Meredith, General Manager	10680 Trenea Street, Suite 450 San Diego, CA 92131	(858) 322-6206 Direct	Mark.Merideth@aus.com	85
Atlantic County (NJ) Department of Corrections	MES and HD Protech/VisioLogix	Lt. Bruce Carber	5060 Atlantic Ave. Mays Landing NJ. 08330	609-909-7577	carber_bruce@aclink.org	48

Regarding our relevant experience, VisioLogix, the lead technology BWC and Video Management Software provider for the proposal, has experience with a number of large agency deployments over the past 4 ½ years. Key expertise in integration of hardware and the VisioLogix, C3 Sentinel Mission Management software. The recap of agencies and size of deployment is as follows:

Installation of Units by Size of Deployment

up to 5 BWC Units	6 - 100 BWC Units	101 - 500 BWC Units	501 - 1000 BWC Units	1000+ BWC Units
51 agencies	68 agencies	18 agencies	4 agencies	4 agencies

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

The following is a portion of our reference list, please feel free to call anyone on the list.

Reference List

Rochester Police Department MES/Lawmen and VisioLogix Services complete 2/28/17
Lt. Michael Perkowski Michael.Perkowski@CityofRochester.Gov
Research & Evaluation Section
185 Exchange Blvd
Rochester, NY 14614
Phone: 585-428-8831

Allied Universal Protection Services MES/Lawmen and VisioLogix
Mark Merideth Mark.Merideth@aus.com
General Manager
Allied Universal Security
10680 Treena Street, Suite 450
San Diego, CA 92131

Atlantic County (NJ) Department of Corrections
Lt. Bruce Carber carber_bruce@aclink.org
Training Unit Supervisor
Atlantic County Dept. Public Safety
5060 Atlantic Ave.
Mayslanding NJ. 08330
609-909-7577

Greenwich Township Police Dept. MES/Lawmen and VisioLogix Services complete 2016
Captain Kevin Nastasi knastasi@greenwichpd.com
421 W. Broad St.
Gibbstown, N.J. 08027
Desk 856-423-6576
Office 856-423-4206

Win-Win Development Tech. for the Chinese Police VisioLogix leading project.

Rita Wang wangr@sector2dev.com
8/F Building B1 Block Five
Honghualing Industrial Park
Taoyuan Street Nanshan District, Shenzhen, China
Cell: +86 181 2707 3684

**Request For Information Police Body Worn Cameras
Pennsylvania Chiefs of Police Association**

Rochester (NY) Police Department

Our largest US reference customer is Rochester Police Department with over 500 BWC's deployed. Rochester is a complex organization with 8 remote locations and a myriad of security protocols. The MES/VisioLogix team worked closely with RPD to establish a robust and high performance BWC mission. When the entire industry was heading to a Cloud Based environment, RPD took the more challenging and significantly less expensive approach of using its own storage infrastructure. RPD has also collaborated with our development teams to create a best in class software and operating environment that has translated nicely from just a BWC environment into a full digital evidence management platform.



Chinese Police

VisioLogix has managed a challenging installation of over 12,000 BWC's and a highly complex and distant operation. With a solid software foundation, VisioLogix was able to navigate through the numerous roadblocks of a foreign operating environment. This project has helped VisioLogix to scale at the highest levels. The SQL database was successfully pressure tested with 12,000 cameras and even more users. This project has helped the organization to establish protocols for managing the largest of customers.

Kazakhstan Police

VisioLogix has managed a similar large program with the police in Kazakhstan. This deployment features in excess of 2,000 Body Cameras across a fast-moving environment. The main challenge that VisioLogix has faced is that the software is required to manage multiple different body worn cameras. Meeting this challenge has helped the VisioLogix team to create a hardware agnostic environment which is unique in the industry.

January 30, 2019

ATTN: Christopher J. Braun
Pennsylvania Chiefs of Police Association
3905 N. Front Street,
Harrisburg, PA 17110

Dear Mr. Braun:

Axon Enterprise, Inc. (Axon) is pleased to submit the enclosed proposal for a body-worn camera solution to the Pennsylvania Chiefs of Police Association (PCPA) and the State of Pennsylvania. This proposal describes Axon's top-tier body-worn camera program.

The system you select should meet your objectives to provide a solution to purchase implement an effective body-worn camera solution for Pennsylvania's over 30,000 sworn officers working in over 1200 police departments. Axon is the leading provider of law enforcement technology; our primary purpose is to help you achieve your goals and advance the efforts of public safety agencies through technology wherever possible.

Our comprehensive body-worn camera program offers rugged and reliable cameras, the **Axon Body 2** and **Axon Flex 2**, with numerous mounting possibilities. Axon's body-worn camera systems also extend beyond hardware, consolidating all Axon-captured evidence in Evidence.com, Axon's cloud-based and CJIS-compliant digital evidence management software (DEMS).

Some additional benefits you can receive as an Axon partner today are:

- Regular hardware refreshes
- Expert deployment, training, and support
- A Dock & Walk workflow
- Evidence.com DEMS and native data management tools
- Axon View and Axon Capture mobile applications
- Monthly software upgrades
- Unlimited cloud-based storage
- Immediate video access
- Proven CAD/RMS integrations



17800 N 85TH STREET
SCOTTSDALE, ARIZONA 85255

AXON.COM

Axon has developed, expanded, and enhanced its technology over time to build a fully integrated platform with direct input from law enforcement agencies around the world. To date, we've partnered with over 7,500 agencies to deliver industry-leading digital evidence capture solutions and our offerings will only get stronger as we continue developing new products and features to meet the evolving needs of the law enforcement and public safety community.

If you have any questions regarding our proposal, pricing or products, please contact our Proposal Manager, Debashree Nag at 425.589.1963 or dnag@axon.com. Thank you for your consideration; we look forward to continued conversation with the PCPA.

Sincerely,

Robert Driscoll

VP, Associate General Counsel

Axon Enterprise, Inc.

REQUEST FOR INFORMATION POLICE BODY WORN CAMERAS PENNSYLVANIA CHIEFS OF POLICE ASSOCIATION

Submitted by:

Axon Enterprise, Inc.



**17800 North 85th Street
Scottsdale, AZ 85255
800.978.2737
January 30, 2019**

TABLE OF CONTENTS

INFORMATION REQUESTED.....	1
----------------------------	---

INFORMATION REQUESTED

The information requested includes the manufactures, vendors or resellers of specific products and services that meet Pennsylvania Laws, standards and regulations that allow them to develop the necessary polices required. In addition, cost and discounted price are requested. Please provide at least the following information:

- **How does your non-vehicle-mounted mobile video recording systems and technology meet Pennsylvania's published requirements?**

The **Axon Body 2** is a self-contained audio-visual body-worn camera unit with no external wires. We offer numerous mounting options, some optimized for security (Z-Bracket, Molle, and Magnet mounts) and others built for versatility (Shirt pocket, Clip, and Velcro mounts). Mounts can accommodate uniforms, belts, outerwear including jackets, and tactical and SWAT vests (without any alteration).

The Axon Body 2 was designed specifically for law enforcement use in tactical policing situations. Activation of event recording is simple and accessible, making it easy for officers to operate the device in high-stress situations. Recordings are initiated with a single "Event Button" located on the front of the device, so an officer can easily reach it with one hand.



The Axon Body 2 mounted on an officer's chest

Features & Benefits

- **HD Video:** The industry's best low-light video records in 1080p HD
- **Full-shift Battery:** Lasts for a full shift (over 12 hours)
- **Configurable Pre-Event Buffer:** Capture up to 2 minutes before an event
- **Dual-Channel Audio:** Camera records two audio channels
- **Axon Signal Wireless Activation:** Cameras start recording automatically based on pre-defined triggers
- **Optional Mute:** Disable audio in the field to support dual-party consent
- **Mobile Application:** Tag and replay videos from the field with Axon View
- **RapidLock Mounts:** Versatile mounts are designed for versatility and comfort, while keep the camera steady

Technical Specifications

- **Field of View:** 143 Degrees
- **Recording Capacity:** Up to 70 Hours Depending on Resolution
- **Video Quality:** 30 frames per second; resolution spanning 480p - 1080p
- **Battery:** Rechargeable lithium-ion polymer battery (3000 mAH capacity)
- **Weather Resistance:** IEC 60529 IP67 (dust, water); MIL-STD-810G (Salt fog)
- **Humidity:** 95% non-condensing
- **Operating Temperature:** -4 °F To 122 °F [-20 °C To 50 °C]
- **Drop Test:** 6 Feet – camera is housed in high-impact polymer
- **Dimensions:** 3.42 in x 2.76 in x 1.01 in (slightly larger than a pack of cards)
- **Weight:** 5.0 oz.

The **Axon Flex 2** is a point-of-view camera that provides multiple options for wearing the camera to suit your officers' needs in the field. The 120° field of view lens captures events as experienced by the wearer.

The camera is connected to a controller, which houses the battery, with one cable. The Axon Flex 2 camera can be mounted on Oakley Flak Jacket® glasses, ball caps, uniform collars and epaulettes, a lowrider headband, on a vest, and motorcycle and SWAT helmets.



Officer in the field using the Axon Flex 2 camera with the Oakley Flak Jacket® mount

Axon Flex 2 Features & Benefits

- **HD Video:** The industry's best low-light video records in 1080p HD
- **Full-shift Battery:** Lasts for over 12 hours covering an entire shift
- **Configurable Pre-Event Buffer:** Capture up to 2 minutes before an event
- **Dual-Channel Audio:** Camera records two audio channels
- **Axon Signal Wireless Activation:** Cameras start recording automatically based on pre-defined triggers
- **Optional Mute:** Disable audio in the field to support dual-party consent
- **Mobile Application:** Tag and replay videos with the Axon View mobile app
- **RapidLock Mounts:** The system uses versatile mounts designed for versatility and comfort, while keep the camera steady

Technical Specifications

- **Field of View:** 120 degrees
 - **Recording Capacity:** Up to 70 Hours depending on resolution
 - **Video Quality:** 30 frames per second; resolution spanning 480p - 1080p
 - **Battery:** Rechargeable lithium-ion polymer battery (3600 mAH capacity)
 - **Weather Resistance:** IEC 60529 IP54 (dust, rain); MIL-STD-810G (Salt fog)
 - **Humidity:** 95% non-condensing
 - **Operating Temperature:** -4° F to 122° F [-20° C to 50° C]
 - **Drop Test:** Up to 6 feet – devices are housed in high-impact polymer
 - **Dimensions:** Controller: (D1) 0.94 in, (D2) 1.14 in, (W) 2.45 in, (H) 3.0 in;
Camera: (L) 2.9 in, (H) 0.75 in, (W) 0.74 in
 - **Weight:** Controller: 4.4 oz., Camera: 0.88 oz.
- **Have you submitted your non-vehicle-mounted mobile video recording systems to the Pennsylvania State Police for certification?**

Yes, the Axon Body 2 and the Axon Flex 2 cameras are in the list of PA State List of certified body-worn cameras.

- **Is your non-vehicle-mounted mobile video recording systems already certified by the Pennsylvania State Police?**

Yes, Axon Body 2 and Axon Flex 2 cameras are certified by the Pennsylvania State Police.

- **Are you offering a storage solution?**

Yes, Axon's Body-worn cameras are paired with Axon Evidence (**Evidence.com**), a robust end-to-end solution that not only allows agencies to store data, it also enables new workflows for managing and sharing that data securely from anywhere.

Officers and command staff can upload content from Axon and TASER devices or other systems easily, manage it simply with search and retrieval features, and then collaborate effortlessly with prosecutors and other partners by using powerful sharing features. When storage needs increase, the cloud-based system allows agencies to scale instantly and cost-effectively.

Many agencies today are taking advantage of our unlimited data offering to best protect the agency from escalating costs over the course of a program.

- **Will you offer storage solutions bundled (no line item distinction) with the cost of each camera purchased?**

Evidence.com is licensed on a per user basis; a license is required for each camera. As a hosted application, there is no limit to the number of users your agency can add, should administrators or staff without body cameras need access to the system.

A license is what allows a user to access either Basic or Pro Evidence.com features. License counters appear on the administrator's view of the Dashboard, and the Roles page to help you keep track of your licenses. Users in the Lite tier do not count toward your agency's total licenses.

Basic Tier

The Basic tier is the lower of the two paid tiers on Evidence.com. Basic tier users are people who need to upload and manage their digital evidence, but do not need access to advanced features such as automated redaction and group monitoring.

Pro Tier

The Pro tier is the higher of the two paid tiers on Evidence.com. Pro tier users are people who need access to advanced features, such as automated redaction, group monitoring, agency analytics and reports, and human transcription services, among others.

Licenses Tiers

✓ indicates functionality included in the cost per license. Costs for additional features are indicated on a per license basis.

Evidence.com License Tier Features	BASIC	PRO
Secure File Storage	✓	✓
File & Case Sharing	✓	✓
Video Clips & Markers	✓	✓
Custom User Roles & Categories	✓	✓
Automatic File Deletion Schedules	✓	✓
Bulk Reassign, Share, Edit	✓	✓
Single Sign-On (SSO)	✓	✓
Video Redaction		✓
Group Monitoring		✓
Agency Usage Reports		✓
Advanced Device Analytics		✓
Human Paid Transcription		✓
Multicam Playback		✓
Restricted Evidence		✓
Axon Citizen 1:1		✓
Redaction Studio		✓

Evidence.com License Tier Features	BASIC	PRO
Included Storage	Includes 10 GB of storage for non-Axon Fleet video	Includes 30GB of Storage for non-Axon Fleet video

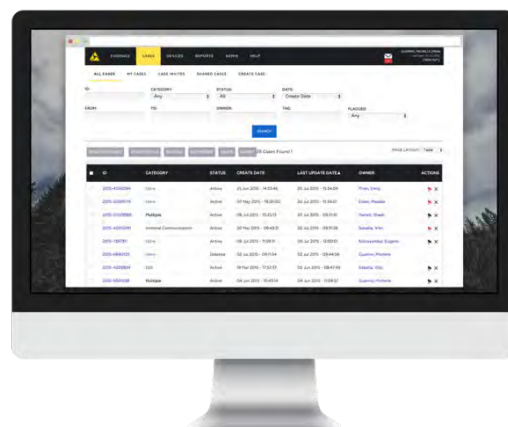
- **How does your storage solution meet Pennsylvania's published requirements?**

Evidence.com is a robust end-to-end solution that not only allows agencies to store data, it also enables new workflows for managing and sharing that data securely - from anywhere.

A SCALABLE SOLUTION

Officers and command staff can upload content from Axon and TASER devices or other systems easily, manage it simply with search and retrieval features, and then collaborate effortlessly with prosecutors and other partners by using powerful sharing features. When storage needs increase, the cloud-based system allows agencies to scale instantly and cost-effectively.

Many agencies today are taking advantage of our unlimited data offering to best protect the agency from escalating costs over the course of a program.



Control Access with Roles and Permissions

Each Evidence.com user is assigned a role. Roles determine a user's permissions, which control levels of access to features and functions in Evidence.com. Information access via Evidence.com is controlled through a robust "Access Control System" managed by the Administrator and that features comprehensive audit trails. Access to information is governed by the agency-defined access control system built into Evidence.com.

Access is controlled according to:

- Pre-defined roles
- Pre-defined individuals (i.e., who has access to what data feed)
- User account-specific passwords

Active Directory

Evidence.com can interface with a federated **Active Directory** to support user login with their agency credentials. Using the industry-standard SAML protocol, officers no longer need to juggle multiple usernames and passwords. With Active Directory

federation, Evidence.com uses the agency's network to authenticate users. Agency credentials are never sent to Evidence.com. This means that if a user changes their password on Active Directory they will log in with that new password.

Simplified Evidence Categorization

Evidence.com uses category types to organized stored video, simplifying the search process for your agency users. All categories are set by your agency to reflect your policies and desired structure. This categorization also facilitates database management by automatically ensuring that only relevant evidence is retained in the system. Every event that is captured and uploaded to Evidence.com can be assigned a category to determine how long it is retained in the system. Proper categorization is important to ensure that incidents remain in the system for the appropriate amount of time. Categories include policy settings for evidence retention and restricted access for especially sensitive evidence.

Evidence Retention Policies

Storage Set-Up Options and Automatic Deletion

For proper management, agencies must create a set of agency-specific Categories large enough to properly segregate evidence by type for retention-setting and search functionality. This list should not be so large that it becomes an impediment to efficient field use by users. Categories can be edited or added later within Evidence.com by users with appropriate access. The category assigned to a video file determines the retention policy associated with that piece of evidence. The evidence retention policy determines:

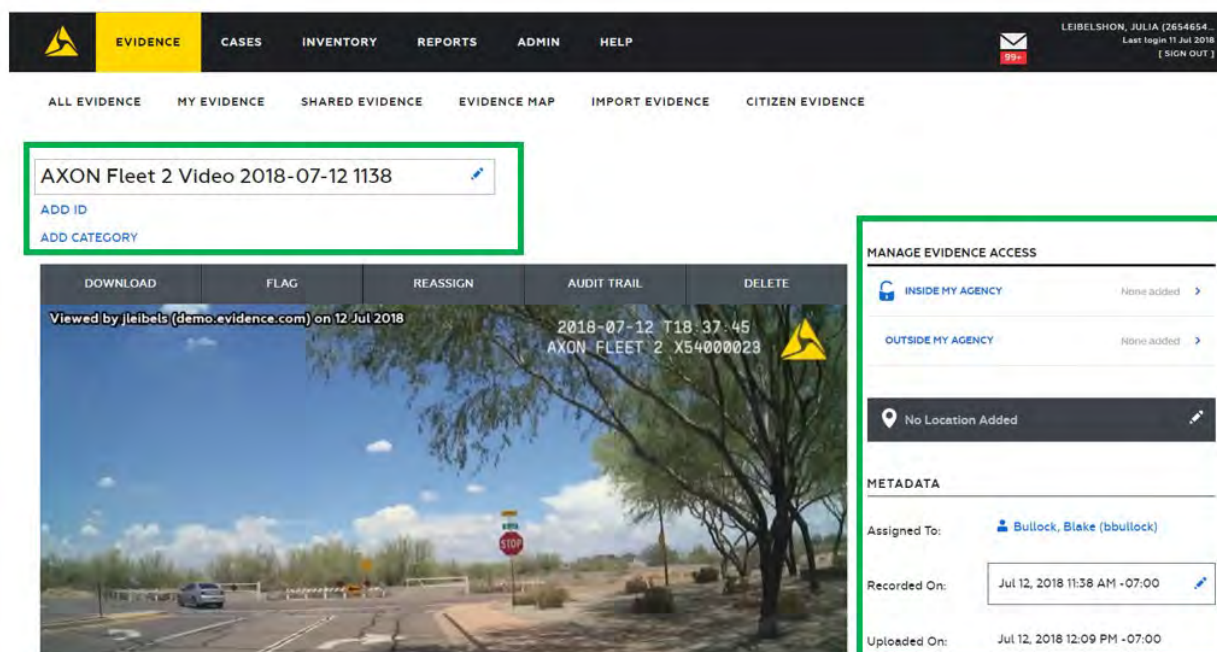
1. Whether the system will initiate automatic deletion of evidence assigned to the category.
2. How long the system waits before initiating the deletion of evidence that is not included in a case. Axon video deletions are based on the recording date. Deletion of all other evidence is based on the upload date.

Remorse Periods for Retrieving Deleted Files

To protect against accidental deletions, administrators can recover files up to 7 days after they are queued for deletion. This policy applies to evidence only. Cases are never deleted automatically. Evidence included in a case is exempt from deletion until it is removed from the case. If evidence is in multiple categories, the longest retention time will be used. This 7-day remorse/recovery period and approval workflow is designed to protect evidence and chain of custody. After the remorse period, the file is expunged.

Managing Your Digital Evidence

Evidence.com was designed to provide users with easy, straightforward ways to review and manage digital evidence. Once a user has located the desired file, he or she can perform the following actions (all actions will be recorded in the evidentiary audit log).



- **Edit Title and ID**
- **Add or Remove Tags** – Tags are labels that can be applied to evidence. Tags can be added to evidence for easy locating in the future. Evidence searches allow users to filter the search results by tags.
- **Edit Location** – The specified location for evidence determines where the pin representing the evidence appears on evidence maps.
- **Add, Edit and Delete Notes** – Notes can be posted about evidence. In addition to the text of the note, Evidence.com shows the author of the note and the date and time that the note was created and updated.

Users can also perform the following actions as part of the streamlined search process:

- **Edit Description** – Descriptions of the evidence can be added or edited.
- **Edit Recorded Date and Time**
- **Download Evidence File** – Data can be exported to external media such as CD-ROMS, flash drives, and external hard drives.
- **Flag or UnFlag Evidence** – Evidence can be flagged to make it easy to find in the future. Evidence searches allow users to filter the search results by the flag status of evidence.

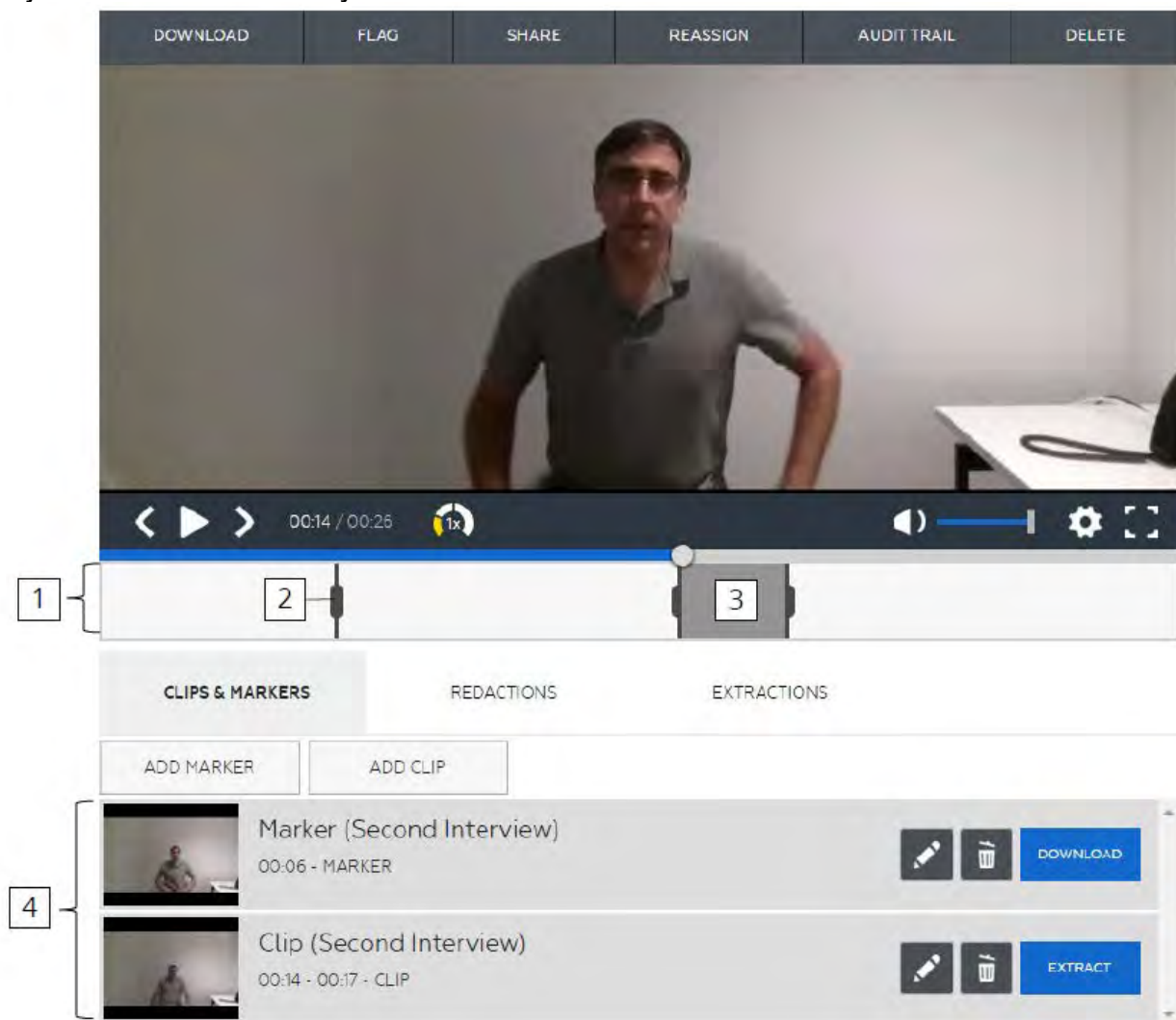
- **Add to or Remove Evidence from a Case** – Users can add or remove evidence to one or more cases.
- **Reassign Evidence** – Users can assign evidence to a user. The user to whom the evidence is assigned becomes the owner of the evidence.
- **View Evidence Audit Trail**
- **Delete Evidence** – Users can manually initiate the deletion of an evidence file. Deleted evidence is added to a deletion queue for 7 days. This helps prevent deleting evidence unintentionally.
- **Restore Deleted Evidence** – If evidence has a status of Queued for Deletion, users can restore the evidence, which removes it from the deletion queue.
- **Assign and Un-Assign Categories** – For evidence that is not assigned to a case, changing the categories that the evidence is assigned to may change the scheduled deletion date. If the scheduled deletion date has already passed, the evidence will be added to the deletion queue.
- **Extend Retention Period** – If evidence is scheduled for deletion, users can extend how long the system retains the evidence before adding it to the deletion queue. The period of time that the retention is extended is equal to the length of the retention policy currently in effect for the evidence. The category assigned to the evidence determines the retention policy. If more than one category is assigned to evidence, the longest retention policy is applied.

Working with Video and Audio Evidence

- **Play, Pause, Rewind, and Fast Forward**
- **View Source** - For video uploaded from an Axon device managed by an Evidence.com agency, the View Evidence page lists the evidence source on the right side of the page. The serial number and model of the recording device are listed.
- **Show and Hide Clock**
- **Rotate the Video** - Users can rotate the video player image 90, 180, or 270 degrees clockwise. This feature is for convenience while viewing a video only. For example, the camera itself may have been on its side or upside down while recording. The rotation does not affect the original video file and is not saved in any way.
- **Markers** - Users can use markers to indicate key moments or highlight important aspects of a video or audio evidence file. For video markers only, users can download markers as image files. Prior to downloading the marker, users can specify options such as whether the title and description appear on the downloaded image. Users can control whether the scrub bar, located below the video image, shows red icons for each marker.
- A **clip** is a continuous segment of an evidence file that you can define. You can create a clip for any segment of an evidence file and assign the clip a title and description. For example, if a 10-minute video includes a 30-second segment that captures important actions and audio, you can create a clip for the important segment.

Marker and Clip Controls

The following image highlights the main Evidence.com video player interface and each major feature available to your users.



Marker and Clip Controls	
1 — Timeline	3 — Clip handles
2 — Marker handle	4 — Markers and clips list

- **Magnify Zone** - Users can use the zone magnification tool to zoom in on a portion of a frame as needed to view details in the video. Users have the option of converting a magnified zone into a marker.
- **Show and Hide Thumbnails** - Thumbnails provide an easy way to preview parts of a video. They appear at the bottom of the video image. Users can move the mouse pointer across them to see each thumbnail.

- **View Video Frame by Frame** - Below the video player, the frame-by-frame scrub bar appears. Each segment of the bar represents a video frame. Use the frame-by-frame features as needed:
 - To preview frames
 - To navigate quickly to a specific frame, and;
 - To skip backwards or forwards

Video Redaction Capabilities*

Evidence.com provides the ability to redact what can be seen and heard in video evidence files. The redaction tools enable you to create redacted versions of video evidence files without affecting the original file.

A *redaction* is a set of information that tells Evidence.com what to redact in a video. You can create a redaction with either Evidence.com redaction tool:

- Manual redaction
- Assisted redaction featuring Smart Tracker technology

When you have completed creating or editing a redaction, you can extract a redacted video. You can create and maintain many redactions for each video evidence file. This enables you to create different redacted videos for different audiences or different purposes.

An extracted video is a video evidence file that Evidence.com creates from a clip or a redaction. Evidence.com never alters the original video evidence file when you create a clip or a redaction.

The clips and redactions features complement each other. If you have a long video and need to share a redacted segment, it is recommended that you first create a clip, extract a video from the clip, and then redact the extracted video.

Redacting a Single Video: The process of redaction involves placing one or more masks in the video. Users can specify precisely which video frame a redaction mask applies to. The redaction mask types are the following:

- **Vector** – Redacts a portion of video frames, in a shape, color, and opacity specified by the user.
- **Blackout mask** — Replaces video frames with a solid black frame.
- **Filter mask** — Obscures entire video frames with either a blur filter, an outline distortion filter, or a segmentation filter.
- **Audio mask** — Remove audio from the frames to which user applies the mask.
- **Skin Blurring** — When using this feature, the user selects the level of skin blurring. Then, during processing, the redaction algorithm searches for skin tones throughout the video and blurs them to the selected level.

Pennsylvania Chiefs of Police Association
Request For Information for Police Body Worn Cameras

Users will also have the option of redacting audio for the duration of a video mask.

Bulk Video Redaction: Public disclosure and FOIA requests can be time consuming, especially when large volumes of videos must be reviewed and potentially redacted. To aid with these large requests, the Bulk Redaction feature allows you to queue video evidence for bulk redaction.

Evidence.com will redact the videos and bundle them into a file. We will email with a link to download this file when it's ready. This link will be active for 3 days.

ORDER SUMMARY

Evidence - 3 files
Request Date - 27 Jul 2015 - 12:22:43 (GMT-0700)
Estimated File Size - 16.95 MB

DOWNLOAD FORMAT

☐ ZIP
☒ ISO

BLUR LEVEL

☐ LOW
☒ MEDIUM
☐ HIGH

AUDIO

☒ MUTE AUDIO

Bulk redaction creates a copy of the original video and a blur filter over the entire video. It can also remove audio for the duration of that copy as well. The blur over the entire video allows requestors to see what happened in the video without potentially revealing personally identifiable details such as faces, addresses, or license plates. This presents an opportunity for agencies to fulfill mass public disclosure requests in the least amount of time.

*Video Redaction is a feature available with Pro licenses (not available with Basic licenses).

- **List the products and services that are already available on State Contract or PA CoStars.**

Axon Enterprise, Inc. is on PA CoStars with the following product groups:

- Electroshock Weapons & Accessories
- Duty Belts, Holsters & Pouches
- Body and Vehicle Cams

- **List your costs for products and services you offer.**

Please find our prices of products and services listed under Appendix A.

- **Will you offer a discount of those prices if multiple police departments group together to buy your products and services?**

Axon may consider a discount from our standard prices. Discounts will be negotiated at the individual agency level.

APPENDICES

- A. Axon Camera Agency Pricing_2019
- B. Axon Body 2 Specifications
- C. Axon Flex 2 Specifications
- D. Axon Interview Specifications
- E. Axon Fleet Specifications
- F. Axon Signal Specifications
- G. Evidence.com Specifications
- H. Evidence.com for Prosecutors Specifications
- I. Evidence Sync Specifications
- J. Axon View Mobile Application Specifications
- K. Axon Citizen Product Card



17800 N. 85th St. Scottsdale, AZ 85255-6311

800.978.2737 Toll Free • 480.991.0791 Fax

www.axon.com • Sales@axon.com

2019 Law Enforcement Agency Pricing – Axon Systems

Axon Flex 2 Camera Hardware and Accessories

Model	Product Description	Agency Price
11528	Axon Flex 2 Camera (online)	\$449.00 ea.
11529	Axon Flex 2 Camera (offline)	\$649.00 ea.
11532	Axon Flex 2 Controller	\$250.00 ea.
11544	Oakley Flak Jacket Kit, Axon Flex 2	\$164.00 ea.
71037	Low Rider Headband, Axon Flex 2	\$29.00 ea.
11545	Collar Mount, Axon Flex 2	\$41.00 ea.
11554	Clip, Oakley, Axon Flex 2	\$23.00 ea.
11546	Epaulette Mount, Axon Flex 2	\$30.50 ea.
11547	Ballcap Mount, Axon Flex 2	\$29.00 ea.
11555	Mount, Ballistics Vest, Axon Flex 2	\$31.00 ea.
11548	Universal Helmet Mount, Axon Flex 2	\$27.00 ea.
11549	Tactical SWAT Kit with ARC Rail, Axon Flex 2	\$65.00 ea.
11533	Cable, Coiled, Straight to Right Angle, 48", Axon Flex 2	\$17.50 ea.
11534	USB Sync Cable, Axon Flex 2	\$10.50 ea.
73082	Wall Wart	\$14.95 ea.

Axon Body 2 Camera Hardware and Accessories

Model	Product Description	Agency Price
74001	Axon Body 2 Camera System (online)	\$499.00 ea.
74004	Axon Body 2 Camera System (offline)	\$699.00 ea.
74006	Axon Body 2 Battery Pack	\$39.00 ea.
11553	USB Sync Cable	\$10.00 ea.

Axon Body 2 Camera and Flex 2 Controller Mounts **

Model	Product Description	Agency Price
74018	Z-Bracket, Men's, Axon RapidLock	\$29.95 ea.
74019	Z-Bracket, Women's Axon RapidLock	\$29.95 ea.
74020	Magnet, Flexible, Axon RapidLock	\$29.95 ea.
74021	Magnet, Outerwear, Axon RapidLock	\$29.95 ea.
74022	Small Pocket, 4" (10.1 cm), Axon RapidLock	\$29.95 ea.
74023	Large Pocket, 6" (15.2 cm), Axon RapidLock	\$29.95 ea.
71026	Reinforced Flexible Magnet Mount, Axon RapidLock	\$29.90 ea.
71038	Reinforced Flexible Magnet Mount, Back Plate	\$13.00 ea.
74028	Wing Clip Mount, Axon RapidLock	\$29.95 ea.
11507	MOLLE Mount, Single, Axon RapidLock	\$29.95 ea.
11508	MOLLE Mount, Double, Axon RapidLock	\$39.95 ea.
11509	Belt Clip Mount, Axon RapidLock	\$29.95 ea.

** Two mounts are included (a la carte) for \$0; \$29.95 for each additional mount.

Axon Signal Hardware & Services

Model	Product Description	Agency Price
70112	Axon Signal Vehicle unit (1 per car/motor)	\$279.00 ea.
Service	Axon Signal Vehicle unit installation and/or training	Variable
70116	Axon Signal Performance Power Magazine (SPPM)	\$100.00 ea.
varies	Axon Signal Sidearm	\$10 per user per month (60-month term required)



Axon Dock Hardware

Model	Product Description	Agency Price
11536	1-bay + Core Axon Dock for Axon Flex 2	\$375.00 ea.
11537	6-bay + Core Axon Dock for Axon Flex 2	\$1,495.00 ea.
11538	1-bay for Axon Flex 2	\$99.00 ea.
11539	6-bay for Axon Flex 2	\$1,195.00 ea.
11541	1-bay T&E Dock for Axon Flex 2	\$0
11542	6-bay T&E Dock for Axon Flex 2	\$0
74009	1-bay + Core Axon Dock for Axon Body 2	\$375.00 ea.
74008	6-bay + Core Axon Dock for Axon Body 2	\$1,495.00 ea.
74011	1-bay for Axon Body 2	\$75.00 ea.
74010	6-bay for Axon Body 2	\$1,195.00 ea.
70027	Axon Dock Core, compatible with all 1-bays and 6-bays	\$300.00 ea.
70033	Wall mount, Axon Dock	\$42.00 ea.
70040	Desk plate, Axon Dock	\$35.00 ea.

Customer Care Extended Warranty

Model	Product Description	Agency Price
85070	TASER Assurance Plan Axon Body 2 annual payment	\$240.00 ea.
85054	TASER Assurance Plan Axon Flex 2 annual payment	\$348.00 ea.
87026	TASER Assurance Plan Axon Dock 6-Bay annual payment	\$336.00 ea.
80118	2-Year Extended Warranty Axon Flex 2 Camera	\$299.95 ea.
87029	2-year Extended Warranty Axon Body 2 camera	\$199.95 ea.
87030	2-year Extended Warranty Axon Dock for Axon Body 2, single bay + core	\$129.90 ea.
87031	2-year Extended Warranty Axon Dock for Axon Body 2, 6-bay + core	\$499.90 ea.
80124	2-year Extended Warranty Axon Dock for Axon Flex 2, single bay + core	\$129.90 ea.
80125	2-year Extended Warranty Axon Dock for Axon Flex 2, 6-bay + core	\$499.90 ea.

Axon Evidence (Evidence.com) Services

Model	Product Description	Agency Price
87001	Basic Axon Evidence license: 1 year	\$180.00 ea.
89001	Pro Axon Evidence license: 1 year	\$468.00 ea.
80022	Pro Axon Evidence License Annual Payment	\$468.00 ea.
85100	Axon Evidence integration license, annual payment	\$180.00 ea.
85123	Axon Evidence Unlimited Plan annual payment*	\$948.00 ea.
85130	Officer Safety Plan annual payment**	\$1,308.00 ea.
85035	Axon Evidence storage (GB): 1 year	\$0.75 ea.

* This license tier is only available for 3-year or 5-year terms

** This license tier is only available for 5-year terms.

*** Axon Evidence storage not included with the Basic Package. A-la-carte storage is required.



Axon Professional Services

Model	Product Description	Agency Price
n/a	Basic remote support	Free
85055	Axon Full Service	\$17,000 ea.
85144	Axon Starter	\$2,750 ea.
85146	Axon 1-Day Service	\$2,000 ea.

Axon may change pricing or product offerings at any point in time. The committed pricing is based on each Axon Quote provided to the Agency.

Freight Policy Freight is the responsibility of the purchaser. All taxes, duties and customs, where applicable, are the responsibilities of the customer.

Pricing Pricing for Law Enforcement/Correctional Agencies Only. Must be a sworn law enforcement officer to purchase.

Order Lead Time 4 to 6 weeks ARO. **ALL SALES ARE FINAL.**

For delivery status or information on how to place an order, call our sales department at 800-978-2737, fax: 480-991-0791

Axon Enterprise, Inc.'s Sales Terms and Conditions for Direct Sales to End User Purchasers apply to all sales and are available at <http://www.axon.com/sales-terms-and-conditions>.

Flak Jacket is a trademark of Oakley, Inc.

▲, ▲ AXON, Axon, Axon Body 2, Axon Evidence, Axon Flex, Axon Flex 2, Axon Fleet, Axon Signal, Axon Signal Sidearm, Axon Signal Vehicle, and TASER are trademarks of Axon Enterprise, Inc., some of which registered in the US and other countries. For more information, visit www.axon.com/legal. All rights reserved. © 2019 Axon Enterprise, Inc.



YOU'RE JOB ISN'T ALWAYS PRETTY.

Come rain, shine, blood or sweat—our products will be there, toughing it out alongside you. Because when it comes to safety, security, and your agency, looks don't matter – reliability does.



800-978-2737 axon.com/body2

AXON BODY 2 FEATURES AND BENEFITS

RETINA HD VIDEO: The industry's best low-light video now records in HD.

FULL-SHIFT BATTERY: 12+ hours

PRE-EVENT BUFFER: Configure your pre-event buffer time to capture up to 2 minutes before an event.

WIRELESS ACTIVATION: Axon Signal reports events, like when you open the car door or activate the light bar, so your camera can detect them and start recording.

OPTIONAL MUTE: Ability to disable audio in the field to support dual party consent.

IN-FIELD TAGGING: Add a marker to important points in your video.

UNMATCHED DURABILITY: Built to withstand extreme weather and brutal conditions.

RAPIDLOCK MOUNTS: Versatile mounts keep the camera steady during tough situations.

MOBILE APP: Stream, tag, and replay videos right on your phone with Axon View.

MULTI-CAM COMPATIBILITY: Review up to four videos, including Axon Body 2, Axon Flex 2 and Axon Fleet footage, on one screen through Evidence.com.



APP AVAILABLE FOR
APPLE AND ANDROID



AXON BODY 2 SPECIFICATIONS

VIDEO RESOLUTION: Configurable up to 1080p

WEATHER RESISTANCE: IP67 (IEC 60529)

CORROSION RESISTANCE: MIL-STD-810G
METHOD 509.5 (SALT FOG)

FIELD OF VIEW: 143 degrees

OPERATING TEMPERATURE: -4 °F to 122 °F
-20 °C to 50 °C

DROP TEST: 6 Feet

HUMIDITY: 95% non-condensing

WARRANTY: 1 year from date of receipt with
extended full five-year warranty options

RECORDING CAPACITY: Up to 70 hours
depending on resolution

Android is a trademark of Google, Inc., iOS is a trademark of Cisco Technology, Inc., and Apple, the Apple logo, iPhone, iPad and iPod touch are trademarks of Apple, Inc. The Android robot is reproduced or modified from work created and shared by Google and used according to terms described in the Creative Commons 3.0 Attribution License. Wi-Fi is a trademark of the Wi-Fi Alliance.

▲, ▲ AXON, Axon, Axon View, Axon Body 2, Axon Flex 2, and Evidence.com are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information, visit www.axon.com/legal. All rights reserved. © 2017 Axon Enterprise, Inc.



GAIN A NEW PERSPECTIVE

THE LEADING POINT-OF-VIEW CAMERA, EVOLVED

Unmatched Durability | Best-in-Class Image Quality | Optimum Wearability

Gain a new perspective with the Axon Flex 2 camera. It brings point-of-view video to the next level, boasting a rugged industrial design, new mounts, and advanced capabilities like unlimited HD and a 120-degree field of view. Plus, it belongs to the growing Axon network of devices and apps that work together so you can focus on what matters - your job, not your technology.

AXON FLEX 2 FEATURES AND BENEFITS

BEST-IN-CLASS IMAGE QUALITY: The leading point-of-view camera now records in HD.

DUAL-CHANNEL AUDIO: Reduce ambient noise for improved sound quality.

WIDER FIELD OF VIEW: Capture more at the scene with a 120-degree field of view.

FULL-SHIFT BATTERY: Lasts for 12 hours of battery.

PRE-EVENT BUFFER: Configure your pre-event buffer time to capture up to 2 minutes before an event.

ENHANCED MOUNTS: Designed for versatility and optimum comfort.

UNMATCHED DURABILITY: Built to endure extreme field and weather conditions.

WIRELESS ACTIVATION: Axon Signal reports events, like when you open the car door or activate the light bar, so your camera can detect them and start recording.

MOBILE COMPATIBILITY: Stream, tag, and replay footage right on your phone with the Axon View app.

EVIDENCE.COM INTEGRATION: Easily manage, retrieve, and share videos online.

MULTI-CAM COMPATIBILITY: Review up to four videos, including Axon Flex 2, Axon Body 2 and Axon Fleet footage, on one screen through Evidence.com.



APP AVAILABLE FOR
APPLE AND ANDROID

AXON FLEX 2 SPECIFICATIONS

WEATHER RESISTANCE IEC 60529 IP54 (dust, rain); MIL-STD-810G (Salt fog)

HOUSING High-impact polymer

FIELD OF VIEW 120 degrees

OPERATING TEMPERATURE -4 °F TO 122 °F [-20 °C TO 50 °C]

DROP TEST 6 feet

VIDEO MPEG-4 (MP4); H.264

HUMIDITY 95% non-condensing


WARRANTY 1 year from date of receipt

RECORD TIME Up to 70 hours depending on resolution

ENCRYPTION 256-bit AES

Apple and  are trademarks of Apple Inc. and  and Android are trademarks of Google Inc.

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

 AXON, Axon, Axon View, Axon Body 2, Axon Flex 2, and Evidence.com are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information, visit www.axon.com/legal. All rights reserved. © 2017 Axon Enterprise, Inc.

MPC0250 REV F





CAPTURE AND PROTECT YOUR VIDEO INTERVIEW EVIDENCE

Axon Interview allows agencies to capture video of witness and suspect interviews, tag it with descriptive metadata, and automatically transfer it to Evidence.com. Featuring world-class security and large-agency support, it is a full interview room video solution that provides critical, defensible evidence for the prosecution.

PROTECT THE TRUTH

A full video record of the interrogation process helps protect officers against claims of abuse, coercion, and perjury.

INCREASE CONVICTION RATES

Interview room video provides stronger evidence for the prosecution, leading to fewer pre-trial motions and improved evidentiary record on appeal.

SECURE YOUR INTERVIEWS

Data is encrypted, and the system includes automated audit trail capabilities for tracking chain of custody.

CUSTOMIZE YOUR DEPLOYMENT

Axon Interview works for any-sized agency with support for multiple simultaneous interviews, decentralized monitoring and remote camera sites.

ELIMINATE DATA SILOS

Completed interviews are securely stored and managed alongside all other types of digital evidence at your department. All interview metadata is retained on the Evidence.com platform for efficient search and retrieval.

AXON INTERVIEW FEATURES & BENEFITS

REDUNDANT RECORDING: Ensure the confession is captured every time.

24/7 BUFFERING OPTION: Capture forgotten interviews and let nothing slip through the cracks.

METADATA MANAGEMENT: Flexible customer-defined metadata.

PRE AND POST-EVENT RECORDING: Customize pre and post-event windows of up to 7 minutes.

TOUCH-SCREEN SOFTWARE: Quickly enter metadata with high accuracy.

HIGH-DEFINITION: Produce industry-leading audio and video for the prosecution.

MASKING: Preserve attorney-client privileges without sacrificing video continuity.

MOTION-BASED TRIGGER: Supports DWI/DUI rooms for when officers' hands are full.

AXON INTERVIEW SPECIFICATIONS

TAMPER-PROOF TECHNOLOGY SHA-2 hashing algorithm and chain of custody including standard reports

VIDEO ENCODING H.264 baseline and main profile (MPEG-4 part 10/AVC), streaming compliant

CAMERA SECURITY HTTPS encrypted communication to the camera, IEEE 802.1x network access control

SUPPORTED PROTOCOLS IPv4/v6, FTP, CIFS/SMB, SMTP, Bonjour, UPnP

POE SUPPORT Power over ethernet IEEE 802.3af/802.3at type 1

COVERT OR OVERT CAMERAS Support for either style of camera to best fit your needs



Axon Fleet 2

THE NEXT GENERATION OF IN-CAR HITS THE ROAD



| TAKE YOUR VIDEO TO THE NEXT LEVEL

Offload Anywhere | Plug & Play Functionality | Multi-Cam Playback

In-car systems haven't changed in decades. Until now. Featuring improved front and rear cameras, Axon Fleet 2 is a breakthrough video system that unlocks the power of Axon's network. Offload video anywhere. Watch up to four videos at once on Evidence.com. Axon Fleet 2 is upgraded continuously behind the scenes, so you'll always have the latest, greatest in-car tech connected to the Axon network of people, devices, and apps.

| FLEET 2 FEATURES AND BENEFITS

LICENSE PLATE READABILITY: Up to 4X digital zoom make license plates readable at up to 30 feet (9.1 meters).

WIRELESS MIC: Capture audio up to 1,000 feet (305 meters) away.

NIGHTTIME VISABILITY: Capture what happens inside the car at night with Axon Fleet 2's infrared capability.

WIRELESS ACTIVATION: Compatible with Axon Signal, which reports events like when you open the car door or activate the light bar, so that your nearby cameras can detect them and start recording.

WIRELESS OFFLOAD: Offload video evidence anywhere using LTE or Wi-Fi.

PRE-EVENT BUFFER: Capture up to two minutes before an event.

MDT APP: Stream, tag and replay any camera's videos, plus write notes and upload footage, right from your MDT with Axon View XL.

MULTI-CAM PLAYBACK: Review up to four videos simultaneously before sharing footage on Evidence.com.

UNPRECEDENTED PRICE: Build an upgrade into your Axon Fleet program to ensure you have the latest tech.

CONTINUOUS UPGRADES: Full-featured solution that receives new capabilities via regular software upgrades.

LTE is a trademark of the European Telecommunications Standards Institute, and Wi-Fi is a trademark of the Wi-Fi Alliance.

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

▲ ▲ AXON, Axon, Axon Fleet 2, Axon Signal, Axon View XL, and Evidence.com are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information, visit www.axon.com/legal. All rights reserved. © 2018 Axon Enterprise, Inc.

REV B





YOUR CAMERA'S FOCUSED RIGHT WHEN YOU ARE

Axon Signal is a technology that enables certain Axon cameras to sense events up to 30 feet away and start recording. Whether you're driving your vehicle, using your TASER CEW, or drawing your sidearm, Signal operates effortlessly, allowing you to focus on what matters most.

AXON SIGNAL PRODUCTS



AXON SIGNAL VEHICLE: Enables events like opening the car door or activating the light bar to alert your cameras to start recording. Ideal for cars, SUVs, and motorcycles.



AXON SIGNAL PERFORMANCE POWER MAGAZINE (SPPM): Capture critical footage when using your TASER X2 or X26P Smart Weapon. The SPPM reports to your camera when your weapon is armed and logs the moment that the trigger is pulled and arc is engaged.

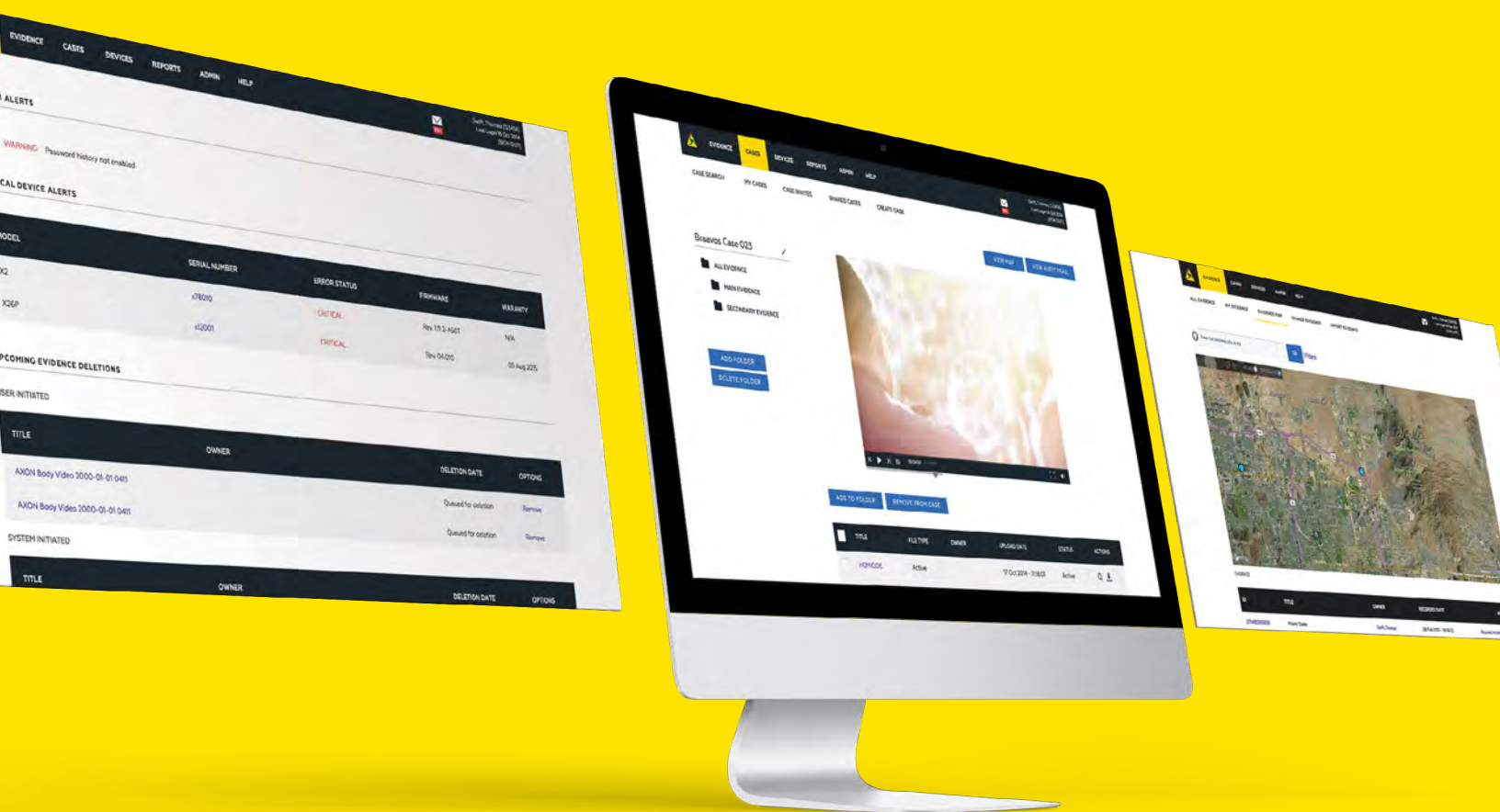


AXON SIGNAL SIDEARM: This easy-to-install smart sensor attaches to the large majority of sidearm holsters. Axon cameras within 30 feet can detect the removal of your sidearm from its holster and start recording via a wireless signal, so you can act with confidence in the field.

Axon Signal Vehicle Unit SKU: 70112

800-978-2737
Get early access at axon.com/signal

AXON, Axon, Axon Signal, X2, X26P, TASER, and  are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information, visit www.axon.com/legal. All rights reserved. © 2017 Axon Enterprise, Inc.



MANAGE ALL OF YOUR DIGITAL EVIDENCE FROM CAPTURE TO COURTROOM

Evidence.com is a scalable, cloud-based system that consolidates all of your digital files, making them easy to manage, access and share while maintaining security and chain of custody.

UNIFY YOUR DIGITAL ASSETS

Eliminate data silos and manage all types of digital media from capture to courtroom, all with one secure system.

FASTER WORKFLOWS

Achieve the fastest speed of evidence processing through automation. Save time and money with industry-leading redaction technologies and secure digital sharing tools.

SCALABLE TECHNOLOGY

Enable deployments of any size with active directory integration, groups, reports, CAD/RMS Integration, automatic retention schedules and more.

THE AXON ADVANTAGE

Start immediately with no hardware to set up. Choose between plans with fixed or unlimited storage, and adjust instantly if needed. Stay up to date with free, automatic updates every month.

800-978-2737 axon.com/evidence

EVIDENCE.COM FEATURES AND BENEFITS

LOWEST TOTAL COST OF OWNERSHIP:

Evidence.com eliminates the cost of an in-house data center and the time associated with manual processes.

AVAILABILITY: Hosted securely in the cloud, Evidence.com can be accessed anytime, anywhere.

ONE-CLICK SEARCH: Search by officer name, incident ID, location and other tags to find files quickly.

CONFIGURABLE RETENTION: Schedule automatic retention periods based on incident type or crime severity.

CASE MANAGEMENT: Quickly view and share all digital files related by case number.

REDACTION SUITE: Save time with automated redaction, bulk redaction, clips, markers, thumbnails and more.

CAD/RMS INTEGRATION: Automate Axon video tagging by pulling in the correct metadata from existing systems.

PROSECUTOR WORKFLOW: Connect digitally with the prosecutor using the most scalable sharing solution available.

MOBILE INTEGRATION: Store and manage files captured with mobile devices in the field.

ANALYTICS AND AUDIT TOOLS: Monitor system usage, from total videos uploaded to who has reviewed, shared and deleted files.

EVIDENCE.COM SECURITY FEATURES

CJIS-COMPLIANCE

Evidence.com is fully CJIS compliant.

AUDIT TRAIL AND CHAIN OF CUSTODY

Data is tamper-proof and all access events are reported in a secure audit trail.

CUSTOMIZABLE USER PERMISSIONS

Administrators can determine what files can be viewed by users and groups of users.

DATA ENCRYPTION

All information is fully encrypted in transit and at rest.

For more information, visit axon.com/security.



EVIDENCE.COM FOR PROSECUTORS

MANAGING EVIDENCE FROM CAPTURE TO COURT

As body camera footage and other forms of digital evidence become more prevalent, law enforcement agencies are faced with an unprecedented amount of data. That's why we offer Evidence.com for Prosecutors, a free evidence management solution that streamlines your workflow, making it manageable to handle agencies' growing amounts of evidence without having to grow your staff.

SHARE EVIDENCE WITH EASE

Evidence.com is easy to use. With a few clicks, you can add evidence to cases and share them with relevant parties, cutting a weeklong sharing process down to just minutes. Evidence.com also requires no ramp-up time to implement, and because of its instantly scalable, cloud-based system, increasing storage capacity is seamless.

KNOW YOUR DATA IS SECURE

We employ industry-leading security practices that have earned us the trust of thousands of agencies on our platform. Data is encrypted, and all actions are recorded in an audit log to ensure chain of custody and authenticity. That way, evidence managed through Evidence.com is still admissible in court.

DON'T BREAK YOUR BUDGET

We understand that attorneys don't always have the budgets that law enforcement agencies may have for new technology. Our standard plan lets you share cases, receive files from multiple agencies, upload digital data, instantly provide e-discovery, and more—for free. Plus, you won't have to hire additional staff to accommodate the influx of evidence. You can also redact footage, eliminating costs for external consultants.

STANDARD FEATURES

- Receive shared cases and share evidence externally for discovery
- Upload any type of digital data
- Add evidence to cases
- Create video clips and markers
- Customize user roles and permissions
- Set automated deletion schedules
- Bulk reassign, edit, and share

WANT TO LEARN MORE?

Contact us to hear about your options and to start your trial.

EVIDENCE.COM PROSECUTOR LICENSES

PLAN	STANDARD	PRO
PRICE PER USER	FREE	\$39/Month
STORAGE OF SHARED EVIDENCE	Unlimited	Unlimited
ADDITIONAL STORAGE PER MONTH	6.25¢/GB/Month	6.25¢/GB/Month
Receive Shared Cases	✓	✓
Share Evidence Externally for Discovery	✓	✓
Upload Any Type of Digital Data	✓	✓
Add Evidence to Cases	✓	✓
Create Video Clips and Markers	✓	✓
Customize User Roles and Permissions	✓	✓
Automated Deletion Schedules	✓	✓
Bulk Reassign, Share, Edit	✓	✓
Redact Videos		✓
Generate Agency Usage Reports		✓
Export Search Results to CSV		✓
Create Organizational Groups		✓
Single Sign-On		✓





EVIDENCE Sync

- ▶ **Desktop Evidence Control** - Allows management of digital evidence and TASER® products from any computer with an internet connection, including an MDT.
- ▶ **Any File, Any Source** - Upload any audio, video, photo or other files currently on CDs, memory cards, servers or a hard drive to EVIDENCE.com.
- ▶ **Handsfree Transfer** - Select the data to upload to EVIDENCE.com, then log out and walk away while the app keeps working.

The newest version of EVIDENCE Sync makes your workflows easier and saves you time. Use Sync to preview, annotate and upload digital evidence from any source to EVIDENCE.com, plus manage your agency's TASER products and update firmware. And as always, your data is secure and easy to access at any point.

EVIDENCE.COM

▶ scan this QR code to learn more





FEATURES & BENEFITS



Upload Any Digital Evidence

Upload any format and size of photo, video or audio recording.



Manage TASER Products

Collect evidence, change settings, assign, and update firmware for your CEWs or AXON® cameras.



Add Metadata

Tag evidence with Title, Event ID, and Category, and assign evidence at upload.



Schedule Uploads

Select a folder or file on your hard drive or network to upload at set times.



Upload from Servers

Upload interview room or dash-cam videos from shared drives.



Upload from Camera, CD, or SD Card

Upload crime scene photos from any source.



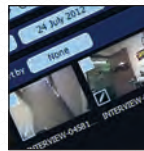
Upload from the Field

Run the app from your MDT and access from the field.



Walk Away During Uploads

Log out while uploads keep going in the background.



View Files in a Gallery

Quickly manage photos and videos using thumbnails.



Search Easily

Find any file and search by title, date, keyword or other fields.

EVIDENCE.COM

► scan this QR code to learn more



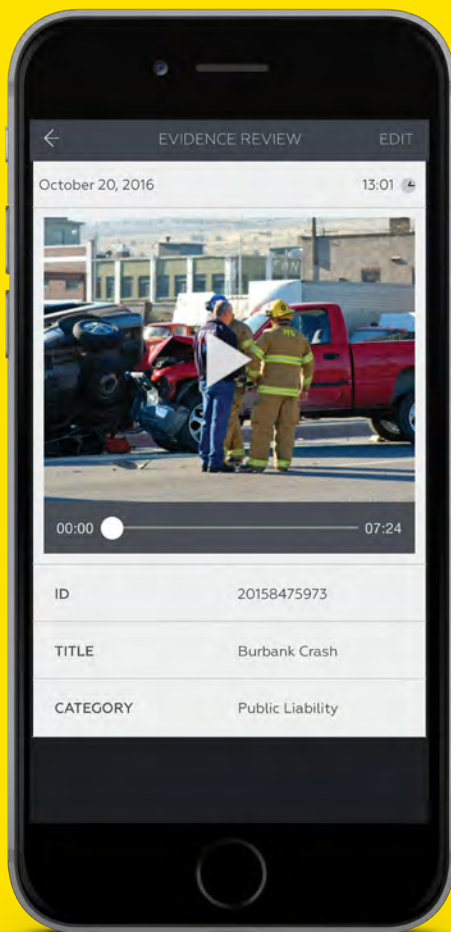
✉ Help@EVIDENCE.com

☎ 1.877.270.0553

📍 Scottsdale, Arizona, U.S.A.



INSTANT VIDEO PLAYBACK IN THE FIELD



AXON VIEW

See what your camera sees

TURN ROUTINE VIDEO INTO VALUABLE EVIDENCE

Live Feed | GPS Tagging | Metadata Input

Axon View is a mobile application that wirelessly connects with your Axon camera to provide instant playback of unfolding events in the field. Axon View automatically maps video with GPS data and allows real-time tagging of metadata, such as Case ID and Category, from your phone. Before you set foot in the station, your video is automatically filed into the correct case report and retention schedule.

800-978-2737 axon.com/view

AXON VIEW FEATURES & BENEFITS

INSTANT REPLAY: Prevent frivolous disputes over recorded events

MOBILE TAGGING: Input data on the scene for easy searching and accurate retention

GPS: Map video evidence automatically

LIVE STREAMING: Achieve optimal camera placement

SECURE STORAGE: Information is viewed but not stored on the mobile device



APP AVAILABLE FOR
APPLE AND ANDROID

AXON VIEW SPECIFICATIONS

IOS:

Compatible with Apple iOS 8.0 and above on iPhone, iPad, and iPod touch

Size: 29.5 MB

Language: English, Spanish, and French

ANDROID:

Compatible with Android Devices Version 4.1 and above

Size: Varies by device

Language: English, Spanish, and French

Android is a trademark of Google, Inc., IOS is a trademark of Cisco Technology, Inc., and Apple, the Apple logo, iPhone, iPad and iPod touch are trademarks of Apple, Inc. The Android robot is reproduced or modified from work created and shared by Google and used according to terms described in the Creative Commons 3.0 Attribution License.

AXON, Axon, and Axon View are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information, visit www.axon.com/legal. All rights reserved. © 2017 Axon Enterprise, Inc.



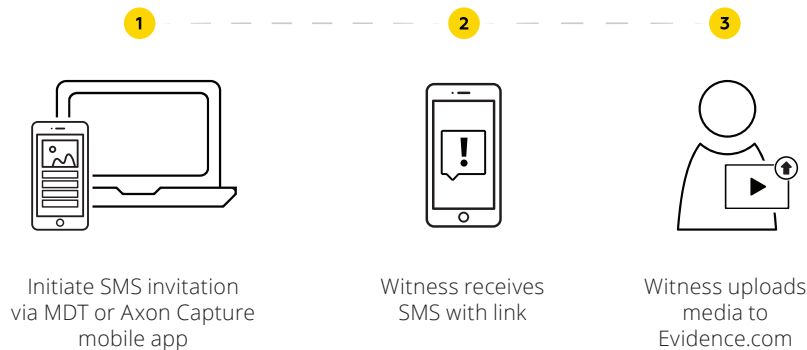
COMMUNITY EVIDENCE, NOW PART OF THE AXON NETWORK

For too long, agencies have struggled to securely receive evidence from the community and determine what content is useful for an investigation. Axon Citizen, makes it easier for community members to submit photos and videos of an incident and for your agency to manage that media in Evidence.com, helping lead to more prosecutions.

HOW IT WORKS

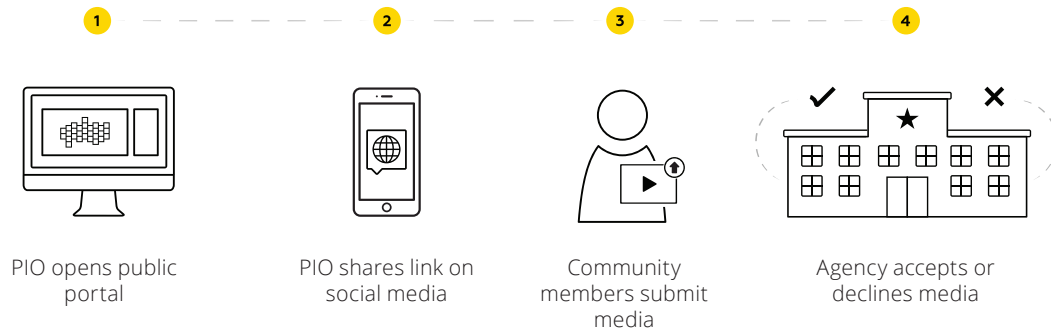
CITIZEN FOR OFFICERS: ONE-ON-ONE EVIDENCE COLLECTION

When you respond to a scene, you should be able to collect photos and videos from witnesses without worrying about the chain of evidence. With Axon Citizen, you can invite witnesses to securely send their media through the Axon Capture mobile application or Evidence.com on your MDT. Once collected, their submissions go straight into Evidence.com and are immediately logged in the audit trail instead of sitting on your camera roll or in your email.



CITIZEN FOR COMMUNITIES: PUBLIC EVIDENCE COLLECTION

You always want help from the community — but you don't want to be overwhelmed. Axon Citizen simplifies the collection process, letting you create public portals where community members can upload photos and videos, which are immediately screened for viruses. Then, your agency can review the media as fast as possible to accept or reject submissions. All submissions are instantly categorized and searchable.



AXON CITIZEN FEATURES & BENEFITS

CENTRALIZES YOUR EVIDENCE: Submissions go straight into Evidence.com with your agency's other files, eliminating any need to download media, print it or transfer it to a USB drive, and submit it to the evidence locker.

PROTECTS THE CHAIN OF CUSTODY: Axon Citizen utilizes Evidence.com's secure audit trail to show which officer initiated the collection, for which incident, at what time and place, and from which community member.

ACCELERATES THE REVIEW PROCESS: Axon Citizen's triage tool allows the officer reviewing submissions to quickly decide which submissions to accept or decline.

STREAMLINES SEARCHING: All submissions will be automatically categorized and searchable within Evidence.com to simplify case building.

OFFERS NETWORK RELIABILITY: Axon Citizen manages all the infrastructure and tools needed to support large volumes of submissions, so your agency can remain confident that the service will work during large-scale events.

AXON CITIZEN SPECIFICATIONS

COMPATIBILITY:

Citizen for Officers: Axon Capture (Android and iOS) or Evidence.com

Citizen for Communities: Evidence.com

Citizen Submission: Any web-enabled smartphone

UPLOAD METHOD

Upload data via any 3G or 4G data connection, or via a Wi-Fi connection

ACCESS

Officers must log in to their active Evidence.com account to use the application

STORAGE

The application will only upload data to Evidence.com secured storage

LANGUAGE

Available in English

Android is a trademark of Google Inc.; Apple, iPhone, and iPod touch are trademarks of Apple Inc.; iOS is a trademark of Cisco, and Wi-Fi is a trademark of the Wi-Fi alliance.

▲, ▲ AXON, Axon and Evidence.com are trademarks of Axon Enterprise, Inc., some of which are registered in the US and other countries. For more information, visit www.axon.com/legal. All rights reserved. © 2017 Axon Enterprise, Inc.





PROTECTION • SECURITY • INTEGRITY

Prestige II Camera

Description

1296P Full HD Resolution Video Quality

The Prestige II Body Worn Camera features 32 megapixel recording for outstanding still recording or burst mode which can capture 30 frames in one second. The built in microphone also records audio. The ultra wide angle lens covers 140 degrees. Waterproof, the Prestige II Camera can withstand drops of up to 1 meter. Storage capacity is either 32G or 64G. Continuous video recording up to 13 hours.

Night Vision Recording

The Prestige Camera automatically turns on the infrared light when conditions require it. Large and powerful infrared light can reach up to 15 meters in pitch black darkness.

32 Megapixel Camera

Arriving at the scene of an accident or crime the Prestige II camera enables the officer to quickly snap photo images even while the unit is recording video in both night vision and full color mode. The Prestige II features a maximum 32 megapixel camera with an available burst shot option. With the built in 32 or 64 GB memory the recorder can store thousands of high quality images instantly.

WiFi

With support for optional built-in WiFi, the Prestige II allows you to connect to a smart phone or remote. This app can turn your smart phone or tablet into a live video remote offering full control of all functions and settings.

GPS

The optional GPS function indicates on playback the exact location of the camera, as well as the time and date.

- 1296 Full HD Video
- Over 12 hours recording
- Night Vision Mode
- Audio/Voice Recording
- Instant Playback
- GPS Function
- WiFi Function



Prestige II Camera Specifications

Hardware

CMOS Sensor	4MP OV4689
Lens	140-degree Wide Angle
Screen	2-inch LCD
Storage	Built-in 32G/64G
Battery	Built-in 3200mAH Lithium-ion Battery
Weight	4.6 oz. / 130 g
Size	3.11 x 2.24 x 1.06 in. / 79 x 57 x 27 mm (HxWxD)
IP Rating	IP66
Infrared LED	Up to 15 Meters Working Range
Interface	USB 2.0 for Data Transfer and Charging
Working Temperature	-40° - +140°F / -40-+60 °C
Storage Temperature	-4° - +131°F / -20-+55 °C

STANDARD ACCESSORIES

USB Cable, Wall Charger, Universal Metal Clip, Software CD, Manual

OPTIONAL ACCESSORIES

Built-in GPS, Built-in WiFi, External Camera, Suction Cup Bracket, Epaulette Clip, Drop In Dock

Battery Performance

Continuous Recording Time	12 hours at 1080P @30fps; 13 hours at 720P @30fps;
Battery Status	Screen Display
Low Battery Warning	Beep Alert
Charging Time	3.5 hours

Software

Password Protection	Input password to enter menu and playback (Optional)
Data Protection	Password required to check data in camera
Pre-recording	30 Seconds
Post-recording	5/10 Seconds, 10/20/30 Minutes
Watermark	User ID (7-digit Device ID and 6-digit Police ID), Date/Time Stamp
Snap Shot	Capture Picture While Video Recording
One Button Recording	Support
Burst Mode	Available
Digital Zoom	Available

Video / Image / Audio

Video Format	. MOV (Compression Format: H.264
Video Resolution	2560x1080p@30fps; 2304x1296p@30fps; 1920x1080p@30fps; 1440x1080@30fps; 1280x720@30fps; @60fps; 848x480@30fps
Image Format	.JPEG
Image Resolution	34M (7808x4392); 23M (6400x3600); 18M (5632x3168)13M (4800x2700); 9M (4032x2268); 6M (3200X1800); 4M (2688X1512)
Audio Input	Built-in Microphone
Audio Format	.MP3





PROTECTION • SECURITY • INTEGRITY

Protector II Body Camera

Description

Real Time Video Streaming

The Protector II Body-Worn Camera, with 4G LTE technology, has the capability of direct transmission of live video, audio and GPS locations in real time, day or night, to police headquarters. This provides situation awareness to observing security personnel and gives them the ability to make critical assessments and decisions to assist the officer in the field. This is accomplished while simultaneously recording the video on the camera itself. With 4G LTE or WIFI live video streaming is accomplished without the involvement of or need for smartphones and can be activated by the control center.

21 Megapixel Camera

Arriving at the scene of an accident or crime the Protector II camera enables the officer to quickly snap photo images and video even while the unit is transmitting video in both night vision and full color mode to headquarters. The Protector II features a 21 megapixel camera. With the built in 32 GB or 64 GB memory the recorder can store high quality images instantly.

Night Vision Recording

The Protector II Camera features night vision capability up to 10 meters with visible face detection.

Audio / Voice Recorder

The Protector II police camera also has a built in voice recording for recording and transmitting audio when no video is needed. Perfect for recording victims or witnesses statements.

Instant Playback

The Protector II police camera provides instant playback allowing the officer to playback videos and images anytime on the 2 inch color LCD display. Videos can be paused, rewind and replayed.

GPS

The GPS function indicates on playback the exact location of the camera, as well as the time and date.

Two-Way Audio

The Protector II has the capability of built-in real-time communication with the control center.



- **1440 Full HD Video**
- **Date and Time Stamp**
- **Night Vision Mode**
- **One Button Recording & Streaming**
- **GPS Function**
- **WIFI Function**
- **2x Infrared Light**
- **1x Laser Light**
- **Audio Voice Recording**
- **Instant Playback**

Protector II Camera Specifications

Recording

Sensor	5MP CMOS
Chipset	Ambarella A12A55
Max pixel	21 Megapixels
Video Resolution	2560 x 1440 30p / 1920 x 1080 30p / 1280 x 720 30p /
Live Streaming Resolution	1280 x 720 x 30p
Video Format	h.264 .AVI/MPEG4
Fast Forward	2X, 4X, 8X, 16X, 32X, 64X
REW	2X, 4X, 8X, 16X, 32X, 64X
Audio	High Quality Built-in Microphone
Audio Format	AAC2/MP3
Water Mark	User ID, Time and Date Stamp Embedded into Video
Camera	21 Pixel Camera
Camera Format	JPEG
Snap Shot	Capture Photos During Video Recording
Recording Time	Continuous: 9 hours with fully charged battery, IR closed, resolution ratio 1920 x 1080
Storage Capacity	32G/64G/128G
Storage Level	Visual Indicator
Record LED	Red
One Button Recording	Support One Button Recording
Activation Prompt	Audible, Visual, and Tactile Vibration Confirm Activation of Record and Stop
Pre-record Function	>10s Pre-record
Last-record Function	>10s Last-record
Video Quality	Best / Better / Normal
Video Section	5 min/10 min/15 min/30 min/45 min
Burst	2/3/5/10/15/20 shot burst picture taking
Red IR Switch	Auto / Manual
Motion Detection	Auto / Manual
Audio Guide	Support
Chime	Support
GPS	Built-in
Language	English

4G	LTE/FDD Mode, Real Time Live View Stream, Point to Point
Streaming Video Time	5 Hrs.
Screen Protection	30s / 1 min / 3 min / 5 min
Timing Photography	5/10 Seconds
Brightness	Low/High
Auto Turn Off	30 sec / 1 min / 3 min / 5 min
Key Tone	Support
Sound Volume	Support

Video Image Review

LCD Screen	2 in. TFT-LCD High Resolution Color Display
Audio Playback	Yes
Video Output	HDMI 1.3 support 1080
Video Transfer	USB 2.0

Camera

Recording Angle	Wide Angle 140 Degrees
Night Vision	Up to 10 Meters with Visible Face Detection
Waterproof	IP67
Clip	High Quality Metal Clip with 360° Rotation
PTT	Can Connect to Different Types of Radios

Battery

Type	Built-in 3500mAH Lithium
Charging Time	4 Hours
Battery Life	8 Hours
Battery Level	Visual Indicator

Others

Unique ID Number/Unit	Include 5 digit device ID and 6 digit police ID
Password Protect	Support
Dimension	96mm x 62mm x 34mm (3.78" x 2.44" x 1.34")
Weight	160g (5.64 oz.)
Working Temperature	-40 / +60° C (-40 / +140° F)
Storage Temperature	-20 / +55° C (-4 / +131° F)

Accessories

Standard Accessories	USB Cable, Charger, Manual, Driver CD, Universal Metal Clip, Drop-In Dock
----------------------	---



Protector II

32 Gigabytes

With 4G LTE, WIFI and GPS - \$695

64 Gigabytes

With 4G LTE, WIFI and GPS - \$730



Prestige II

32 Gigabytes

Without WIFI or GPS - \$360

With either WIFI or GPS - \$390

With both WIFI and GPS - \$420

64 Gigabytes

Without WIFI or GPS - \$390

With either WIFI or GPS - \$420

With both WIFI and GPS - \$450