Body Worn Camera Technology Review

And

Minimum Performance Specifications

Whitepaper for Consideration Criteria

V.2.5 Aug 6 2015

1.0 Preamble: A primer on body worn cameras from a neutral perspective: a view from the United States of America:

For police body cameras, big costs loom in storage. The storage expenses — running into the millions of dollars in some cities — often go overlooked in the debates over using cameras

By Brian Bakst and Ryan J. Foley, Associated Press

ST. PAUL, Minn. — The rush to outfit police officers with body cameras after last summer's unrest in Ferguson, Missouri, threatens to saddle local governments with steep costs for managing the volumes of footage they must keep for months or even years, according to contracts, invoices and company data reviewed by The Associated Press.

The storage expenses — running into the millions of dollars in some cities — often go overlooked in the debates over using cameras as a way to hold officers accountable and to imYet those costs can have a significant effect on city and county budgets, and in some cases may force police chiefs to choose between paying officers on the street or paying yearly video storage fees.

Baltimore Mayor Stephanie Rawlings-Blake already has sounded the alarm over the long-term costs of police body cameras.

In December, she vetoed a proposal that would have required officers to wear cameras because she didn't believe the costs and other details were adequately considered. City officials estimated costs up to $2.6 million a year for (CLOUD[1]) storage and the extra staff needed to manage the video data.

"Knowing how we didn't have a lot of wiggle room with the budget constraints we face, we couldn't afford to get it wrong," said Rawlings-Blake, who intends to present another plan this spring. "Any time you do something on this scale, if you don't take the time up front, you are setting yourself up for failure and disappointment from the community."

In some cities, the AP found that the small cameras worn by beat cops on their uniforms or glasses were obtained at deep discounts when departments inked data-management deals that are far more lucrative over the long run for device manufacturers. Those plans run between $20 and $100 per officer per month, depending on the volume generated.

Demand for the devices is booming after the controversy in Ferguson and would accelerate further if Congress adopts President Barack Obama's request for $75 million to help communities buy 50,000 more body cameras.

Already, cities are wrestling with whether they can afford to equip all their officers and how often the cameras should be turned off to reduce the video recorded.

With an average officer uploading several videos per shift, it doesn't take long for data — and the associated expense to add up.

"It's enormous," said Police Chief Gordon Ramsay of Duluth, Minnesota, where the city's 110 officer-worn cameras are generating 8,000 to 10,000 videos per month that are kept for at least 30 days and in many cases longer. "The more you capture, the more you have to store, which means higher costs."

Duluth initially received 84 cameras and charging bays for less than $5,000 from camera maker Taser International, but its three-year contract and licensing agreement for (CLOUD¹) data storage cost about $78,000.

Other cities are just beginning to struggle with how to pay for body cameras:

— In Wichita, Kansas, the police department has proposed selling a helicopter used to search for suspects in order to fund its body-camera program for hundreds of officers. The cost is estimated at $6.4 million over a decade and includes two employees to manage the program.

— In Berkeley, California, the city manager warned in a memo in January of likely costs of at least $45,000 a year for storing data from 150 cameras and assigning one or two employees. In addition, officers might spend 30 minutes per shift handling the video — the equivalent annual time of five full-time officers, the memo said. The City Council is scheduled to debate the issue next week.

"In our community, that alone would be about $1 million," City Council member Laurie Capitelli told AP, referring to the officers' time. "I want to look at the costs and consider the trade-offs."

— San Diego's five-year contract with Taser for 1,000 cameras would cost $267,000 for the devices — but another $3.6 million for storage contracts, software licenses, maintenance, warranties and related equipment. City officials can scale back the deal if funding dries up.

Digital Ally, which is among several companies trying to get a foothold in the industry, donated cameras and a server to store the data to the police department in Ferguson, where officers began wearing them shortly after the August shooting of 18-year-old Michael Brown by white officer Darren Wilson. Industry giants Taser and VieVu also saw interest in their cameras spike.

Taser's trials in major U.S. cities tripled after the shooting, and its stock price has more than doubled since. The company's Evidence.com unit, which offers the data-management platform, is expanding.

"This is obviously great for business, but I think ultimately this is a great technology to increase transparency between communities," said Taser chief marketing officer Luke Larson.

Supporters of the body cameras say they help prosecutors close cases faster, reduce use-of-force incidents and make allegations of misconduct against officers easier to probe. Both sides in a videotaped encounter behave better, they say, leading to fewer complaints and legal settlements.

The body-camera funding in the federal budget Obama proposed Monday would be part of a three-year plan and does not distinguish between hardware and storage costs. The proposal will go before a Republican-controlled Congress that is trying to reduce federal spending, and will not be decided for months.

Police officials say they expect the cost of body cameras to exceed the in-car video systems that were widely implemented during the early 2000s. Some departments say it's been hard to find money to maintain those systems as they age. Body-worn cameras are expected to produce even more videos and more requests from lawyers, journalists and the general public for access to what they show.

Mindful of costs, police forces with cameras are limiting when officers use them, what they store and for how long. But many can't avoid adding servers and reassigning or hiring extra staff.

Some officials are warning the ongoing costs could mean tax hikes or service cuts later.

"Everybody is screaming, 'We need body cameras.' But nobody is saying, where is the money coming from? What are you going to do with all the data? Who is going to manage it?" said Sgt. Jason Halifax of the Des

Moines Police Department, which is struggling to identify a funding source for $300,000 to start a program. "Are we going to cut personnel? Are we going to increase taxes?"

With all the recent “hype” about funding by the U.S. Federal Government of late for Body Worn Cameras (BWC), in-car video recording systems have been used successfully for over 2 decades. Our expertise comes from the in-car video market as to the capture, storage and management of video/audio/images and data, and in developing many of the current day techniques and technologies used since 1991.

Many BWC manufacturers are pushing cloud storage for housing police videos as this is a recurring revenue stream for them. Bid specifications published as of late read in some instances like a promotional brochure for a competitive product. Based on our experience, cloud storage is not suggested due to an agency’s lack of control over its cost.

2.0 OUR PERSPECTIVE AS A PIONEER IN COLLECTION AND MANAGEMENT OF DIGITAL AUDIO AND VIDEO DATA SINCE 1991.

Body worn cameras and their resulting data storage is affordable and deployable if consideration is made in understanding the technology

Most Agencies experiences with digital data have been related to in-car recorders and police interceptor “chases” and not the daily interaction with civilians.

The media push has seen many Agencies blindly seeking a cloud based storage system to store their recorded data as they believe the publications and sales presentations presented by serval of the Body Worn Camera (BWC) manufacturers. In some cases, manufacturers have even given away body cameras while still seeing a 70-100% profit due to cloud storage costs.

At the onset of purchasing BWCs, many Agencies do not realize the amount of data that is to be collected. As such, many agencies racked up cellular in-car data wireless costs that, in some cases, exceeded entire maintenance budgets of fleet vehicles within months. Agencies realized very quickly that cloud storage is an expensive proposition, and quickly sought out more easily managed and less expensive local and secure storage systems with cellular data terminal connections for data uploads.

Our solution is for video downloads to be initiated at the precinct or substation level by simply connecting the BWC to a docking station via a USB cable. The system will automatically extract the day’s video files first to a secure local computing device, then is transferred and authenticated to a server and redundant storage device.

Many BWCs don’t offer enough internal storage to hold a full day’s worth of data. As such, Officers are forced to download their BWC’s video files after nearly every incident. This can leave the data’s integrity at risk as the Officer is then in-charge of what data is being uploaded to the in-car storage unit before it being wirelessly or otherwise transmitted elsewhere for permanent storage. This defeats the purpose of the integrity of the data. Data should be downloaded without any special human intervention to a secure collection device. Only once downloaded and then encrypted or “hashed” should the Officer then proceed to do any monitored and audited redaction, annotation, etc.

Irrespective, sending data from 100 Body Cameras via a data channel topically using a cellular network from an in car is overly expensive, and slow. The costs alone to do this may exceed Police Operating budgets, as would a cloud based storage system.

We, as well as other industry peers, are successfully providing generic information that is vital to the selection of a Body Worn Camera System. In this attempt of providing a neutral review of data capture and storage and use, we feel positive that our end-to-end solution can meet the needs of any Public Safety Agency or other entity requiring storage, “hash/authentication” storage, redaction and annotation with an affordable, user friendly, affordable end-to-end system.

3.0 Understanding the Technology

3.1 Pre-requisites of any Body Worn Camera (BWC) solution:

3.1.1 Ideally, a BWC system should not allow the Officer to decide when or when not to record any encounter.

3.1.1.2 While continuous recording is suggested based on an established SOP that stipulates the secure upload of all data and using a technology driven “set of a second set of eyes,” the secure storage local server, there is no way for anyone in the field to redact any data.

3.1.1.3 If Pre-Event recording is set, did this setting record “everything that the Officer saw”, or was the entire encounter or other critical information in fact “collected?”

3.1.1.4 Never should an Officer in the field be able to edit, annotate, save or transmit the data by human intervention or interaction. Data should be automatically uploaded to a secure initial server at the precinct or sub-station level, then be “hashed” or “encrypted” before the Officer or anyone else authorized to do so may review, annotate, redact or copy the data.

3.1.1.4.1 The BWC should feature a log that is maintained until an Administrator decides to erase the log from the BWC, and upload the data relating to the performance of the BWC (when it was turned on, when it was turned off, if there were any technical issues such as a BWC “reboot”), and make all audit logs available for review.

3.1.2 The BWC should have a built-in camera, not a camera that is mounted on a pair of prescription glasses, sunglasses or fake glasses as these known cameras are quite often subject to disturb an Officer’s concentration, and adversely affect the Officer’s personal safety.

3.1.3 The BWC should not have any “visible to the public” indicator lights of any sort. This is vital to keeping Officers safe when operating covertly or at night.

3.1.4 The BWC should be self-contained with no additional cables for battery packs, GPS antenna units, or external cameras.

3.1.5 The BWC should have the exact field of view of the Officer: 170 deg (W) x 140 deg. (H) (corresponding to the combined field of view of view of the human eye(s).

3.1.6 The BWC should feature a battery gauge on the recorder, allowing as a SOP for the Officer to verify quickly and easily the battery level before the start of the shift.

3.1.6.2 Available memory space for video/audio/images.

3.1.6.3 State of the Battery's charge.

3.1.6.4 Use of only Officer seen indicators as to the status of the BWC, its operation, etc.

3.1.7 As to flexibility:

3.1.7.2 Use of the BWC as a replacement of two way radio accessory speaker microphone.

3.1.7.2.1 The BWC can be used as a two way radio accessory, therefore eliminating one additional device that the Officer or user needs to manage or have mounted on his/her person.

3.1.7.3 To reduce the cost of ownership, the BWC should feature a removable, replaceable battery similar to a portable two-way radio.

3.1.7.3.1 No need to use a USB cable or power supply to charge a BWC's internal, non-removal battery as is the case with many manufactured and present BWC's. This charging process, no matter the manufacturer, takes between 4-6 hours. With a removable battery, as is the case with our BWC, a fresh fully charged one can be installed at change of shift or in the field as needed, and see the exhausted battery placed in a charger for recharge. In this case, BWC's can be shared rather than dedicated to the Officer. This feature can be an Agency decision, and is an option not present with most BWC manufacturers.

3.1.7.3.2 As is the case with a portable two way radio transceiver, the Officer or User may in fact carry a second spare, fully recharged battery in his or her "Sam Brown" should an extended period of operation occur.

3.1.7.3.3 As a result, the recorder should be able to operate for 8-10 hours on a single charge and record audio with video at a minimum of 720 p resolution for 12-16 hours.

3.1.7.4 To maximize a return on investment, a BWC should have the capability to be installed in the vehicle (on the dashboard), be charged from the vehicle's electrical system, and to power the unit as well as see the BWC leveraged as an in-car video/audio recorder.

3.1.7.5 For night time operation:

3.1.7.5.1 The BWC should feature a built in IR-Cut filter to allow for lowlight operation, thus changing the BWC's color daytime operation to lowlight operation without the use of any infrared illuminators.

3.1.7.5.2 The BWC should also have the built-in capability of recording in total darkness (and, depending on the scene of view (absorption/reflection), between 13 and 26 feet distance.)

3.1.7.6 The BWC should be capable of being mounted on either a vest, pocket, lapel, etc., with ease of adjustment.

3.1.7.7 The BWC with change in height position should still provide installation/fixation flexibility, all the while maintaining the BWC's 140 deg (H) field of view.

3.1.7.8 The BWC should allow the data (or event at the time of happening) to be marked for ease of retrieval later during the playback (on LCD or on the playback software) for ease in the authorized and logged redaction process.

3.1.7.9 The BWC should feature a built in LCD for test of performance as determined in an SOP and playback of any recorded data.

3.1.7.10 The rechargeable battery should be capable of being recharged by:

3.1.7.10.1 Connection to the BWC by a USB data cable

3.1.7.10.2 Connection to an appropriately configured two-way radio and accessory cord if used as a speaker microphone, drawing power from the two-way radio battery if so enabled, or simply operating as a speaker microphone for the portable two-way radio transceiver.

3.1.7.10.3 By removing the rechargeable battery from the BWC and placing it into a single battery charger.

3.1.7.10.4 By removing the rechargeable battery from the BWC and placing the exhausted battery into a multiple battery bank charger.

3.1.7.10.5 By charging the BWC and its battery (which is inside the BWC without removal) using a USB cable connected to any source of 5 VDC: Via an AC adapter, solar panel, USB powered port, cell phone battery bank, etc.

3.1.7.11 The BWC should be capable of recording video/audio, images (pictures) or audio.

3.1.7.12 In video mode, the BWC should be capable of recording snapshots.

3.1.7.12.1 Video is recorded in H.264 video compression standard.

3.1.7.12.2 Audio is recorded in .wav format

3.1.7.12.3 Images are recorded in .jpeg format

3.1.7.12.4 GPS data is recorded in .txt format

3.1.7.12.4.1 All files are authenticated and watermarked during the recording process.

3.1.8 The BWC initially authenticates its data during the recording process by way of watermarking.

3.1.9 The BWC should when connected to collection device:

3.1.9.2 Validate the BWC and its registration.

3.1.9.3 Upload data to the collection device without Officer or human intervention, and display the process on the collection terminal's screen.

3.1.9.4 Synchronize the time to the collection device's network server.

3.1.9.5 Erase the data in the BWC after successful data upload.

3.1.10 The collection device then "hashes" / "authenticates" the collected and recorded data from the BWC.

3.1.10.2 Once downloaded at the collection workstation, the data is then mirrored to one or more storage servers composed of hard drives.

3.1.10.3 Only then may Officers or other authorized personnel log on as needed and redact the video, make annotations, etc.

3.1.11 In continuous record mode:

3.1.11.2 An entire shift may be handled without any interruption of the Officer's time. This is to maintain Chain of Custody and Video Authentication.

3.1.12 The BWC should have an Administrator or delegate-controlled hard coded serial number that attaches itself to the recorder and recording, with or without any Officer Name, ID number, etc.

3.1.13 No one may manipulate, erase, redact or otherwise tamper with the BWC data until it is first uploaded to a secure storage server.

3.2 As to reliability and in-service usefulness:

3.2.1 Operating temperature range of -26 deg C to +55 deg C

3.2.2 Minimum IP-54 ingress rating

3.2.3 Survive a drop test from 1.3 m in height

3.2.4 Warranty exchange program to be provided

3.2.5 18 month warranty

3.2.6 Available extended warranty

3.3 As to BWC operating features:

3.3.1 Electronic live zoom

3.3.2 In hand playback on built in LCD of video, audio, images

3.3.3 Noise cancelling pre-amplified built-in microphone

3.3.4 Visual indication of separate available record times for video, audio, images

3.3.5 GPS lock indicator

3.3.6 LCD screen shutdown timer

3.3.7 Low battery alert

4.0 Details on the Body Worn Camera / Review Software Application integration & automatic import process. Handling data recorded is critical. A complementary software suite is supplied to download the data from the BWC. This is accomplished by connecting a USB cable to the BWC. There are certain security checks that need to be performed before any data is downloaded, then purged from the BWC, then hashed. The configuration may be simple: 1 cable, one PC, one BWC, or a multi BWC collection station capable of 12, or 20 or multiples of 12 or 20 BWC simultaneous downloads to a secure hard drive, mirrored or not. Review as follows:

4.1 The data collection station at the Precinct or Sub-station is a self-contained secured computing device with local hard drive storage equipped with 12 or 20 USB cables and a user interface terminal.

4.1.1 Single USB cable with complementary software also available.

4.1.1.1 Note where the BWC has an associated software suite that allows one to program the unit, download and view files. The transfer program portion may be used as a stand-alone application, and then use other software suites to manage the downloaded data if the user has other compatible suites.

4.2 Operation

4.2.1 The BWC is plugged into a USB cable and powered on by the User.

4.2.2 The BWC Review Software Application Suite captures the new device notification and attempts to authenticate with the BWC device's password.

4.2.3 In case of Device authentication failure:

4.2.3.1 The failure is logged.

4.2.4 Next, the BWC Manufacturers' default password is attempted.
4.2.4.1 Failure
4.2.4.1.1 This is logged and notification is sent to a system administrator.
4.2.4.2 In case of Device Authentication Success and for court admissibility and data authentication purposes:
4.2.4.2.1 The BWC is first considered as an "unregistered device" and is assigned a device ID and password.
4.2.4.3 Continue with step 4.5.2

4.3 Device authentication success
4.3.1 Continue with step 4.5.2.
4.3.2 Time on device is synced with Server time.
4.3.3 BWC is put into mass storage mode.
4.3.4 BWC watermarked and BWC authenticated recorded Files are transferred individually and erased from the BWC device after each individual file transfer is confirmed with no errors.
4.3.5 Provisions are designed to detect removal before all files have successfully transferred.
4.3.5.1 Files are not deleted unless they have been successfully transferred.
4.3.6 File transfer progress for each recorder is displayed on the import system's display (terminal screen).
4.3.7 When file transfer has completed, the device is ejected from mass storage mode.
4.3.7.1 Until it is physically removed, the system will indicate that file transfer is completed. The device will continue to charge over USB, however there is no way to detect battery level from the terminal screen.
4.3.7.2 The unit is then ready for battery swap or can remain in bay for charging.

4.4 With data now collected at the various collection points:
4.4.1 The file import into Review Software Application Enterprise Server is identical to the current Review Software Application import method.
4.4.1.1 Once a device is removed, the officer will be prompted to associate that removed camera with an individual officer within the system.
4.4.1.2 The system can track who is assigned which device.

4.4.2 The Review Software Application import method:
4.4.2.1 File is copied to the local Review Software Application working directory.
4.4.2.2 File is hashed SHA-512 (SHA2 512 bit digest) client side.
4.4.2.3 The hash value is sent to the server where it is stored in the database.
4.4.2.3.1 The sever may be set up as a redundant mirrored device.
4.4.2.4 The file transport method is initiated.

4.4.2.5 File transport to server completes.
4.4.2.6 There are provisions to detect file transfer failures.
4.4.2.7 File is hashed server side using SHA-512, and the resulting hash value is compared against the value sent by the client.
4.4.2.8 Mismatch generates a notification to the system administrator.
4.4.2.9 Upon successful hash match, the file is mirrored to a secondary storage location and the client is notified of a successful transfer.

4.5 Hash verification – Review Software Application has an on-demand function to individually verify that the hash of a file matches that which is stored in the database.

4.6 Review Software Application Export:
- 4.6.1 Users with sufficient export rights to files or cases may export files to optical disc (CD/DVD/Blu-ray) or USB media (flash drive or external hard drive).
  - 4.6.1.1 User that initiated the export is logged.
  - 4.6.1.2 Resulting export contains a player/file viewer.
  - 4.6.1.3 Includes case Metadata.
  - 4.6.1.4 Recording notes (optionally can be excluded).
  - 4.6.1.5 Capable of verifying the hash value.

4.7 Review Software Application data retention policy:
- 4.7.1 Configurable data retention policy.
- 4.7.2 Off by default.
- 4.7.3 The system can automatically delete files older than a set date (i.e. 3 years) depending on department policy.
- 4.7.4 Individual files can be excluded from the retention policy.

4.8 Automatic Database backup – the Review Software Application database is automatically backed up each day to the secondary storage location.
- 4.8.1 The system may be configured for long term off-line storage using DVD library.

4.9 Video Review: Once a BWC has downloaded its data to a storage system by way of 12/20 BWC collectors, then and only then may an Officer use Review Software Application software to make annotations etc.

- 4.9.1 Before any download: Officers in the field may playback the recorded data on the BWC’s built-in LCD screen.

5.0 Collected Data: Software Design Specifications, Integrity of Video Assets

With now secure data stored and backed up: Once annotated with a CR Number, incident type, etc. by the Officer, only Management can erase any video not deemed important.

TO NOTE:

OUR COMPLEMENTARY REVIEW SOFTWARE APPLICATION SOFTWARE SUITE FOR OUR BWC MAY MANAGE ANY RECORDED DATA FROM ANY SOURCE; VIDEO, CAMERA, ETC.

IMPORTANT FEATURES ARE EMBEDDED IN OUR SOFTWARE SUITE AS TO SECURITY, MAINTENANCE OF THE CHAIN OF CUSTODY, DATA HASH AND AUTHENTICATION. LISTED BELOW ARE FEATURES THAT MEET ACCEPTED JUDICIAL STANDARDS AS TO HOW DATA IS ACCESSED, INTERVENTIONS LOGGED, AUDITED, ETC..

5.1. Security:

- 5.1.1 A definition of User Groups shall be provided and shall include definitions of authority and permitted actions.
- 5.1.2 Pre-defined operational user groups.
  - 5.1.2.1 User defined user groups.

5.2 Logging:

- 5.2.1 All user actions will be logged by the system and be made available for administrators to view and report on.
- 5.2.2 Export log to file.

6.0 User Groups:

- 6.1 A definition of User Groups shall be provided and shall include definitions of authority and permitted actions.
  - 6.1.1 Pre-defined operational admin group.
  - 6.1.2 User defined user groups.

7.0 Group Establishment, Association:

- 7.1 The System shall allow groups to be established at different levels to compartmentalize videos.
  - 7.1.1 The ability of different groups to be able to view all, some, or none of the videos is paramount to this system.

8.0 Video Reproduction and Marking:

- 8.1 The System shall allow the client to limit each group's ability to reproduce the video through means of an optical disc (CD/DVD/Blu-ray) as well as to save the video to a jump drive, local computer hard drive or other type of storage system, mirrored back up system, cloud system, and will log such actions.
- 8.2 The System shall allow the person watching the video to "mark" a specific point in the video by means of inserting a marker. The marker can further allow a "note" to be associated with that marker.
  - 8.2.1 The marker shall be applied on a video record during a recording or a playback.

- 8.3 The System shall allow a copy of the video to be made:
  - 8.3.1 The system shall enable the authorized users to review and/or update the metadata for any of the captured videos.

8.3.2 The system will log changes and provide audit capabilities for all changes to the metadata for each video.
8.3.3 The authorized users shall be able to review these histories.

8.4 The system will allow the local storage to transfer the files to a system Server.

8.5 The System shall have the ability to import outside video/audio files and mark said files with the same metadata as defined above.

9.0 Storage:
9.1 Time limit function for length of retention of recordings.
9.2 Recordings will inherit parent case's permissions unless overridden:
9.2.1 View
9.2.2 Edit
9.2.3 Delete
9.2.4 Burn
9.2.5 Modify Permissions
9.3 Case permissions can be modified by user group.
9.4 Recordings must continue without error while the PC making the recording is under lock and unlocked.

10.0 Importing media files:
10.1 The system will allow users to import video, image and audio files.
10.2 The systems shall verify that the file is a valid media file before attempting to import into the system.
10.3 A SHA-512 hash of the media file will be generated upon import.
10.4 User shall be able to add interviewer and interviewee records to the file.
10.5 Imported media files shall have the same properties as video files.

11.0 Playback:
11.1 Playback functions shall be the same for recorded video files and import media files.
11.2 Access to recorded assets will be controlled by group security.
11.3 Notes can be added, edited or deleted.
11.4 System will allow for the downloading of videos to users with proper security on authorized machines.
11.5 Videos can be burned to an optical disc, stored locally for review, or copied to thumb drive.
11.6 Playback on devices other than authorized Review Software Application computers will be provided by an Review Software Application playback program disk. This program will verify the integrity of the video and allow access to the recording notes.

12.0 Video clips
12.1 The system will allow users to make shortened clips of full-length recordings for export.
12.2 This may be effected through third party software.

13.0 Security:
13.1.1 Set system password criteria
13.1.2 Add users/groups
13.1.3 Assign security access to groups
13.1.4 Assign user permission/security settings:

13.1.4.1 Assign to group
13.1.4.2 User password settings
13.1.4.3 User login hours

13.2 Events:
13.2.1 Email Servers:
13.2.1.1 Name (friendly name)
13.2.1.2 Server (SMTP)
13.2.1.3 Port
13.2.1.4 Authentication User Name
13.2.1.5 Authentication Password
13.2.1.6 Use SSL checkbox
13.2.1.7 Test button
13.2.2 Actions:
13.2.2.1 Event
13.2.2.2 Email From
13.2.2.3 Email To list
13.2.3 Watchdog Notification:
13.2.3.1 Email From
13.2.3.2 Email To list

13.3 Storage Settings:
13.3.1 Storage path
13.3.2 Maximum recording length
13.3.3 Minimum Free Space
13.3.4 Server storage retention length
13.3.5 Only purge when storage is low checkbox
13.3.6 Local storage retention length

14.0 System Updates:
14.1 Server:
14.1.1 Server shall be able to check a website for information regarding new updates available.
14.1.2 The update information retrieval function shall be called upon server startup.
14.1.3 The update information retrieval function shall be called upon a specified interval such as every hour.
14.1.4 The update information retrieval function can be called manually from within the server application.
14.1.5 The server will provide updates to the clients.

14.2 Client:
14.2.1 The client shall check the server for updates upon startup.
14.2.1.1 If the update is mandatory, it shall update immediately.
14.2.1.2 If the update is optional, it shall updated upon program termination.
14.2.2 The client update function can be called manually from within the client application.

14.3 The update functions on both the server and client shall clean up and not leave orphaned files behind.

15.0 Watchdog Application:
15.1 The system shall be capable of registering itself with the common KRC watchdog application.
15.2 The server shall monitor and report the watchdog connection status.
15.3 The server shall be capable of launching the watchdog application.

16.0 Licensing:

16.1 The Review Software Application server and clients shall be licensed through K&A-KRC.

16.2 The server shall manage server licensing and manage client licensing.

16.2.1 Server license will be generated from a machine code.

16.2.2 Server shall have the ability to install and update licenses from:

16.2.2.1 Internet

16.2.2.2 License file

16.2.2.3 Manual paste of license code

16.2.3 Server management of client licensing:

16.2.3.1 Client licenses are not machine specific but available on request from the pool of available licenses.

16.2.3.2 Make total number of licenses and available licenses known to client.

16.2.3.3 Deny login and alert client when all licenses are in use.

16.2.3.4 Clients marked as offline shall consume a license until returned to the system.

17.0 Database:

17.1 The Review Software Application system will use MS SQL as a database.

17.2 The Review Software Application server will connect to the database.

17.3 Review Software Application clients will not be able to connect directly to the database.

17.4 The server will allow for database backup and restore.

18.0 For Cost analysis:

Local Storage (redundant) or Cloud based, which to use?

Overview:Cloud based storage is not affordable, has questionable security and immediate access in case of catastrophic network or off remote site management and failure is always an issue. Many cloud based BWC manufacturers actually reduce the resolution of the original recording to save on storage space, bandwidth, and data transmission related costs. These recordings may not be enhanced to the same degree as would be the original recording.

24.1 Common denominator: BWC Calculations of Data for one month:

Quantity of 100 BWC x 30 days of storage per BWC x 10 GB/ day recording data storage space = 30,000 GB = 30 TB

24.2 Assumption: Consider where only 10% of data collected will be retained after one month: retainage 3 TB per month.

24.2. 1Total Storage for 1 year: 30 TB overhead (buffer) plus 12 months X 3 TB per month = 66 TB.

24.2.2 Data after one year may be transferred and stored on less expensive media.

(DVD). Then archived.

24.2.3 For Redundant Secure RAID server Storage: Industry price for 66 TB storage system with back up: (storage cost alone): $36,500 with back up. One time purchase. No annual recurring charges. BWC connect directly to storage system. (USD)

24.2.4 Industry price for cloud based Read-Access Geographically Accessed redundant Storage: $6,600 per month: First year $79,200.00 Added: 0 .00036 cents every time data is accessed. (USD)

24.3 Example: Financial Model: If data collected in the first year is estimated to be 150,000 hours. At our BWC recording rate this would require 300 TB of on line redundant storage.

Using the example above: the cost of hardware for 300 TB of redundant storage is approximately $197,000 purchase price, versus a cloud based R-A GAS system of $30,000 per month or $360,000 for the year, plus access charges, using of course our compression and high resolution.

24.3.1 Recommendations for cost reduction and data management: Recommended is where we transfer data after one year except for vital elements and incidents which shall reside on the hard drive storage, immediate access, on-line, with all other captured data copied to DVD for perpetual, low cost, off-line storage.

19.0 Review:

While the BWC camera hardware is easy to understand and can be selected for performance and function, feature set, based on understanding the above hardware review and its implications, the falsehoods of Cloud Based storage solutions are just that- revenue generation for the BWC supplier. There is no advantage of a Cloud Based system which is managed by a third party over a redundant storage system easily secured by and for the Agency. In fact, there are many issues with Cloud Based topology other than being significantly more expensive with added yearly recurring costs.

Proof of the matter: No reduction of recorded resolution is needed with a non-cloud based recording solution.

IF and SHOULD a cloud based storage solution be needed, the BWC described in this document will not see its resolution reduced for any cloud storage as the H.264 compression bandwidth is more efficient than other BWC products available.

With a secure redundant in-house system there are no access charges as is the case with a cloud based system.

The end result is where we will still have lesser storage costs with an in house secured redundant storage system (suggested where the redundant Raid located off site in another City or Agency related or other deemed secure site/building), and where a DVD library is used to create archived files once a determination has been set when files should become “near on-line” as to “near to immediate access, on-line”.

26. Summation: From the preamble and preceding article from Police One quoting the Associated Press, you will discover several matters: digital storage as mentioned throughout this response is massive.

Many BWC manufacturers because of this and the limitation of their BWC as to compression proposes an SOP where a BWC records only an incident that has been determined of importance by the Officer (either event or pre-event mode). While the BWC that we manufacture has this feature, this aspect contradicts the intent and purpose and resolve to an Agency of what a Body Camera actually is: a holder of visual record, a second set of eyes, automatic, with limited Officer Control. As has been the experience with in-car video systems used worldwide either on city busses, in car applications, or inside or outside mounted CCTV cameras, the camera catches everything in its field of view when turned on, sometimes outside of the view of the Officer or User, and reviewed or alerted to or captured for review only after the fact sometimes days, weeks, months later.

The Body Cam purported to be part of the specification due to its compression technique used CAN RECORD as suggested and recommended an entire day of video or of an entire shift on its internal memory. Of course personal matters, lunch and break times etc. are handled by turning the BWC off, but where the audit log of the BWC maintains this for administrative purposes and review if needed.

As a result of the aforementioned BWC technology and software administration suite, our BWC is being promoted by way of this whitepaper for consideration to be represented and sold without the concept of an “Officer Controlled” start and stop.

To this added where in Aurora, Colorado, media have reported where an entire event involving a City Official’s wife was not captured by 6 officers equipped with BWC’s , all were turned off. In this situation and with these Officers involved, all were either too busy to start the recorder or their knowledge of the BWC going back in time by 30 seconds (pre-event mode) which knowing this sees them concentrate on whether to record or not, or not to bother at all, or potentially redact the recording in the MDC before sharing and data. Our BWC has been designed to be capable of recording all that the camera sees affordably.

In this format we felt it important to provide a generic review of digital video recording as it relates to BWC’s and to then discuss afterwards in more detail our end to end solution.

Most if not all BWC devices do not have the “back end” system, with audited access and access levels and where most if not all do not offer the mandated “hash” and “hash validation” needed for court admissibility purposes as does our offering. Additionally when there are many BWC deployed, they must be uploaded securely, quickly and with some visual information to the user

as to the process and completion with little or no training. Something that our 12/20 BWC upload station does. They also may be grouped together uploading in multiples of 12 and 20 BWC's simultaneously.

Our end to end solution meets all judicial requirements as to the maintenance of chain of custody and integrity of the recordings and evidence, allows flexibility for authorized redaction and annotation, as well as search by database, in either a redundant or not, cloud based or not storage and archival system.

27.0 Compliance to DOJ (USA) and (UK) Home Office BWC Standards

Technical Guidance on Procurement-Compliance to the US DOJ Standard for BWC's as it relates to the K&A-KRC BWC Hardware and Software

In order to maximize the usefulness of BWC technology, it is suggested where in support of the foregoing document describing BWC's, priority consideration should l be given to manufacturer's that incorporate the following functions for 18 core operating characteristics in their procurement of BWC technology.

Below are the characteristics as established by the "Home Office Center for Applied Science and Technology, Home Office Centre for Applied Science and Technology, *Body-Worn Video Technical Guidance*, published May 2014",(UK), and as adopted by the U.S. Department of Justice 6/2/2015, OMB # 1121-0329 as their BWC standard.

The product offering manufactured by K&A/KRC meets this requirement.

Statement of Compliance

Recording:
Video and audio to record and export in a standard open, nonproprietary format, such that it can be replayed in freely available software (ex. VLC Player) without processing or conversion. Standard formats should be used for interoperability. Data formats that can only be viewed within manufacturer specific replay software are not recommended.
The offering meets this requirements as well as provides watermarking during the recording process within the BWC, and a hash applied when the data has been securely transferred to a server.

Video Resolution,
selectable
VGA (640 x 480)
HD 720P (1280 x 720)
HD 1080 HD (1920 x 1088)
720P is selected for 12-16 hours of recording on 32 GB of BWC internal memory

Video Record Compression: H.264

Frame Rate 30 fps

Horizontal Minimum Field of View: Minimum of 90 degrees: Nominal human vision is 170 deg H

Minimum focus:
Device should be able to focus on all objects from about 1 foot away to infinity. Continuous autofocus or fixed focus should be employed for usability. Manual settings should be avoided as they can distract the user. Motion jitter and blur can be significant when the camera is moving. Automatic image stabilization can reduce this effect.

Audio Quality:
The system is capable of clearly capturing conversational speech at a distance of 3 feet without wind or excessive background noise.
Added where the system features noise suppression built-in.

Recording/Triggering:
Cameras could record continuously or be user-triggered or event-triggered. Cameras take time to start recording video after being powered on and after recording is initiated. This recording latency period should be minimal.

Night-time, low light functionality:
Quality of video footage recorded in low light or night conditions should be useable. Visible flash and infrared illumination can increase the quality of video taken at night but will affect battery life. Low-light filtering, infrared, near infrared, and other low-light compensation technologies or mechanical filters can increase the quality of video taken in low light and severe weather conditions but can affect scene and motion detail.

Synchronization and Metadata:

The device is capable of recording audio simultaneously and time synchronized with video. Consider the additional information that should be collected with the recorded material. Automatically generated data about the wearer, location, date, and time can be collected and packaged in the video format. Device clock must be synchronized with an external universal clock, either GPS or another source, when the unit is plugged in for absolute time of day to ensure accuracy. All Data is then watermarked.

Tamper Resistance:

The device prohibits recordings from being edited or deleted and should not overwrite existing data before they have been transferred. Systems that can export a hash value of files being transferred may provide an enhanced capability to demonstrate tamper resistance. Only once recorded data from the BWC has been uploaded and received a hash value can any authorized person then view, annotate, redact etc. the data.
The hash maintains the meta data watermark file.

Data Transfer from BWC:
Meets the standard USB2/USB3 compliant connection (mini/micro) for charging and/or data transfer. USB3 is preferred as speeds are considerably faster. The connections should be standard on both the device and on any docking station. Data connections that use a proprietary form factor are not recommended. As noted, replaceable rechargeable batteries

reduces significantly the time that the BWC is out of service and the total charging time over use of a USB cable.

Data Export:
Device exports all recorded footage to data archiving or data management system in its original file format and without loss of quality or associated metadata with minimal human intervention or PC skills. Preferably once a USB connection is made to the BWC and is detected by the collection station, this then starts the upload process with no user intervention A fuel gauge on the collection station indicates to the user of upload status. Device should record an audit log which should include information such as device serial number and device events—e.g., on/off, start/stop recording, restart, remaining storage capacity, etc.. As added security when the data is exported the data is then hashed and then sent to both main and or redundant storage server.

Onboard Storage:
Storage can be integrated into the device or provided on removable industry standard memory cards. Removable media has utility in terms of versatility and expansion but comes with security risks. While the BWC is available in two models, recommended is the model where there is no physical access to the storage medium with the BWC providing enough storage to record a full shift by the officer wearing the device, such as 8-12 hours.

Durability:
Device should withstand considerable and repetitive pressure, vibration, and mechanical shock. It should operate within a temperature range from very cold to very hot and be resistant to common environmental hazards, such as dust, condensation, water splashes, and RF interference.

Weight and Form Factor:
Device should not distract or hinder the officer wearing the device from performing other job functions, especially ones related to officer safety. Cameras are designed with widely varying mounting methods and options. Device should be selected for maximum usability and safety. No cables to connect to cameras, batteries, GPS receivers.

End to end solution: The supplier of the BWC also supplies its free viewer software and any integration services as needed to existing departmental systems.

28.0 Product Specifications:
Body Cam with 32 GB TF Internal, Inaccessible Memory,with built-in GPS.

Battery located in user accessible compartment with 5MP CMOS Sensor;

Records video/audio, still images; audio.

Comes with built in LCD monitor.

Has USB connection to upload data as well as upload firmware upgrades.

Functions/Features: Continuous video or pre 15 second event video record. Video Resolution Settings:1920 x 1080/30fps,1280 x 720(30-60fps), 720 x 480 (720p)/(30-60 fps). Default: 720 x 480,(720p) 30 fps.

Video compression/format: H.264 video compression; AVI/MP4 format with synchronized audio and video, continuous record mode.

Continuous record file segments: adjustable: 5, 10, 15, 30 minute segments.

Files are watermarked during record. Data encrypted (hashed) by data Kollector station when data is transferred from BWC to server.

Built-in Camera viewing angle: V/170°,H/140°;
Electronic shutter with mechanical IR filter: 1/2 – 1/2000s; Auto white-balance.

Still image capture resolution selectable: 5/8/12/14 MP with 8X digital zoom, JPG format.

OPERATIONAL FUNCTIONS: Built in invisible to the eye, 4 LED Infrared LED array, 23-26' illumination in reflective scene; IR illumination with IR cut filter to B/W with Manual or Auto IR control.

Audio: High-sensitivity noise cancelling mic, may record audio only as a personal audio recorder, WAV file.

IN HAND, ON SCENE PLAYBACK: Video/audio files may be reviewed on the built-in LCD screen, may be also viewed in the field when connected to a laptop or other device via USB 2.0/3.0 connection.

For USB connection: password needed when USB cable from the recorder is connected to a PC for authorization.

Data Kollector does not require user intervention. User password: can only view the data file. Administrator password: to view, export, edit and delete data.

OTHER: IP-55 rated;
6-position, rotatable clothing/lapel/belt/pocket clip;
Built-in flashlight;
Integrated Multi-pin connector on base of unit: for two way radio connection using the body cam as a speaker-microphone and for power dock or use as in car docking station for use as in car video recorder;
Available external power bank;
Dual multi-colored LED's on top of unit for Unit Status hidden from view of public / actors.;
Built -in Indications via LCD display: Calculates available storage, remaining storage and record times for all modes, battery use. Battery gauge, visual/audible low battery alarm (3.6V);
Recording at 720 p 32 GB 12-16 hrs. Rate: 19 minutes/ 1 GB of video at 1080P resolution, 32 min. at 720P, 69 min. at D1. Varies with motion and lighting conditions.
18 Month Warranty. 2 year warranty extension available.See warranty statement for details.
NO ACCESS TO INTERNAL TF MEMORY CARD.

For more information:

Contact:

USA:Charles Kirmuss, Kirmuss & Associates/Kelly Research Corp., BWC Division:

Tel 303 263 6353 Email: ckirmuss@frontier.net

Canada: Randy Brown, V-Sec Systems

Tel: 204 694 3665 Email: rwb@mymts.net