

CITY OF MINNEAPOLIS

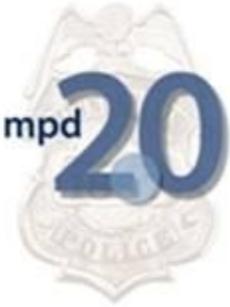
MPD Body Worn Camera Test and Evaluation

Project Review

MPD's results of its body worn camera test and a look at project scope, results, policy, software, hardware, training and data retention/redaction considerations.



7/8/2015



MPD Body Camera Test and Evaluation

1. Project Initiation

Background

In an effort to improve accountability and citizen confidence in the police department, Chief Harteau elected to have the Minneapolis Police Department (MPD) evaluate the use of body worn cameras by officers. At the request of Chief Harteau, MPD formed a Body Worn Camera Steering Committee. The committee is comprised of personnel from Patrol, Minneapolis IT, Training Unit, Internal Affairs Unit, and Mayor's staff, Police Federation, City IT and the MPD Business Technology Unit. Several sub-groups worked on separate issues; legal and finance, policy, operation and IT considerations.

Staff researched and conducted a product search for body worn cameras. Research included the gathering of information on policies, best practices, required infrastructure, devices, costs and operational support. The goal of the test and evaluation project is to assess policy considerations, camera hardware/software functionality and the BWC product/professional services.

Project overview

MPD officers from three police precincts tested BWC products/services from Taser and VieVu over a six month trial period. The test began in November 2014 and continued until mid-May 2015. The test and evaluation was scheduled during winter through spring to test cold weather deployment and determine if there were any performance issues related to extreme weather conditions. The BWC policy was also validated. BWC policy, modeled after the MPD in-squad policy, was examined areas for strengths and identified areas of weakness which may need more development.

Officers captured over 7,000 BWC videos. The videos recorded police officers having making contacts with citizens, enforcing arrests, issuing citations, and the day to day activities of law

enforcement. Notable videos include officers performing CPR, helping the unfortunate and the capture of gun-wielding double murder suspect.

The BWC software was evaluated for ease of use, data download, data management, review, and annotation features. Administration tested cloud and local storage of digital video images. Also evaluated was secure cloud sharing of videos with the City Attorney Office and County Attorney's Office for prosecution.

Procurement

Initial research was completed and in accordance to the City's procurement process, a Request for Proposal (RFP) was issued April 24, 2014. The RFP asked for qualified companies to provide a proposal for a six month or longer trial of body worn cameras and a digital video storage solution. Minimum requirements were set for BWC camera functionality, wear ability and durability. Vendors were asked to comply with video storage requirements and Service Level Agreements (SLA). SLA's guarantee that configuration; installment, maintenance and support can be delivered according to the City's requirements. Vendors' proposals were due May 24, 2014.

10 vendors responded to the RFP. A BWC Evaluation Panel made of members of the City of Minneapolis reviewed each proposal. A qualitative review process was used and respondents were evaluated on; ease of the solution's use, ability to meet requirements of the RFP scope of services, maintenance, and training & support offerings, cost of services and acceptance of City's RFP Terms and Conditions. Two companies meet the City's requirements. Taser and VieVu were selected based on their responses to the RFP and proposed solution.

Product Selection

In general, a final selection of a vendor and their product/services will be reviewed after both phases of the test and evaluation is complete. BWC will be evaluated as to functionality, wear ability and durability. Software and storage solution will be studied for ease of use, organization, and ability to manage video files for redaction, court and investigations. Pricing is a factor, but the Department is committed in finding the best fit for the Department and officers.

MPD has applied for Federal Grant BWC funding. Core BWC product and functionality requirements from the grant have been incorporated into the final MPD product selection process. Grant or independent City project, these 18 requirements are the minimum standards which should be met by a BWC vendor. Other desirable options include; CAD Integration, Bluetooth capability, Redaction, Wi-Fi integration, Voice to Text, and Digital Multimedia Evidence Management capacity and Buffer Recording.

| Operating Characteristics | | Functionality Description | |
|---------------------------|----------------------------|--|---|
| 1 | Recording Format | <p>Video and audio to record and export in a standard, open, non-proprietary format, including both Codec and Container, such that it can be replayed in freely available software (e.g., VLC player) without processing or conversion. Standard open formats should be used for interoperability. Examples include MP4 and MKV. Data formats that can only be viewed within manufacturer-specific replay software are not recommended.</p> <p>VGA, HD 720P, and 1080 HD are predominant standard resolutions. The higher the resolution, the more storage is needed. Estimates below were created assuming H.264 compression with medium to high motion at 30 frames per second (fps) derived using a heuristic formula widely used in industry. Actual storage utilized is dependent on scene complexity and the motion of the video captured. Consider what sort of analysis may be conducted on the video before selecting a resolution.</p> | |
| 2 | Video resolution | VGA (640 X 480) | 550-1,100 MB per hour (0.55-1.1 GB) |
| | | HD 720P (1280 X720) | 1,650-3,325 MB per hour (1.65-3.325 GB) |
| | | 1080 HD (1920 X 1088) | 3,750-7,550 MB hour (3.65-7.55) |
| 3 | Video Encoding/Compression | <p>Use of the lowest possible amount of compression in order to maximize the amount of information available to law enforcement. Consider what sort of analysis may be conducted on the video before selecting video encoding or compression. Examples include MPEG-4, H.264, and H.265. H.264 is an improvement over MPEG-4 compression. H.265 is a new standard which further reduces storage needs while</p> | |
| 4 | Frame rate | <p>30 frames per second (fps) is a standard video frame rate. Higher recording speeds capture more motion detail but require increased storage. Frame rates lower than 25 fps suffer from increased motion blur.</p> | |
| 5 | Horizontal Field of View | <p>Adequate to capture a majority of activity at a reasonable distance. This would likely require at least a 90 degree field of view. Wide angle lenses capture more of a scene, but distort the view and lose detail towards the edges of the frame. Software tools may be required to properly analyze or view the video from extremely wide angle video.</p> | |
| 6 | Camera Focus | <p>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.</p> | |
| 7 | Audio Quality | <p>The system is capable of clearly capturing conversational speech at a distance of 3 feet without wind or excessive background noise.</p> | |

| | | |
|----|--|--|
| 8 | Separate Audio and Resolution and Encoding Compression | If the device will be used in a mode to record audio only, compressed audio requires less storage than video (4-60 MB per hour per microphone depending on desired quality). If high speech quality is needed, a sampling rate of at least 22 kHz with at least 24-bit capture is suggested per microphone. Higher values might be necessary to capture increased fidelity at a distance. Standard open encoding with speech quality resolution suggested. Examples include MP3 and WMA. |
| 9 | 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. |
| 10 | 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. |
| 11 | Synchronization | 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. |
| 12 | 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. Standard encryption such as AES can be employed to protect data and improve the management of lost devices and memory cards. |
| 13 | Data Transfer | Recommend 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. |
| 14 | 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. Device should record an audit log which should include information such as device serial number and device events—e.g., on/off, charging, start/stop recording, remaining storage capacity, etc. |
| 15 | 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. Consider whether enough storage should be available to record a full shift by the officer wearing the device, such as 8-12 hours of non-volatile onboard storage. Loss of power must not cause data to be lost or corrupted. |

| | | |
|----|------------------------|---|
| 16 | Battery Life | Consider whether the battery should provide enough power to record a full shift by the officer wearing the device, such as an 8-12 hour battery life. Devices that do not run on rechargeable batteries are not recommended. |
| 17 | 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. |
| 18 | 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 |

(Department of Justice, 2015)

2. Project Implementation

Testing Approach

Scope: The test and evaluation concentrated strictly on product review and policy validation.

Out of Scope: Complaint reduction, use of force reduction and officer policy compliant were not studied and are out of scope of this report.

Selection of testing sites: Three of the five police precincts were selected to be body camera test sites. The 1st, 4th and 5th Pct. each has a unique demographic make-up. These precincts have differences in racial, social economic factors and levels of urbanization density. These precincts also offer a variety of calls for service, as well as call load. A test across the three neighborhoods was a good social barometer to measure the response from citizens and officers to the implementation of body worn cameras.

Selection of evaluation officers: MPD tested Taser products first. An administrative staffing requirement of the test based on the first vendor trial was to have to have 12 officers in each precinct. This was driven by logistics; each Taser multi-docking station has six-docking bays. Each precinct commander asked for volunteers and selected 12 officers from those who were interested in participating in the project. The volunteer group has a mix of officers work days, middle and night shifts.

There were some staffing changes during the project. Promotions, transfers, and on-duty injuries required several new volunteers to replace staff. Throughout the project there was a core group of 29 evaluators.

Administration: This project is a small scale test across multiple locations. BWC program administration was centralized in the MPD's Business Technology Unit (BTU). The test was

scheduled to run six months if there are no delays/complications. Evaluation officers continue to report to localized precinct patrol supervisors for all 911 response issues. In matters relating to body camera use, training and support, officers report findings back to BTU. A patrol officer, formally assigned to the Training Unit and familiarized with Taser products has been assigned to BTU as the department body camera liaison. Project support is provided by the BTU operational sergeant and project management by the BTU commander. Day to day content and operation of BWC program is monitored by BTU.

BTU configured video retention schedules and video categories. Device assignment, roles & permissions, and responsibilities were also configured by BTU within Evidence.com and VERIPATROL Administration applications. Unless the digital evidence was critical to an important case, mistakes in categorizing videos or not labeling were not amended by BTU. This restraint was deliberately taken to measure the rate of categorizing task failure and to gauge future supervisory review.

Camera distribution: MPD elected to provide each of the evaluation officers a body camera. Some cities like Los Angeles “will transfer the cameras to the next shift in order to maximize the number of officers utilizing the camera” (Goff, J. 2014). This practice is not a good fit with MPD business model. Past Department equipment management practices has demonstrated individual device assignment leads to increased accountability.

Three types of body worn camera were tested. VieVu has one camera model. A VieVu LE3 camera unit was paired with each officer. Taser has two camera models; Taser Axon (body camera worn center mass) and Taser Flex (worn in multiple configurations; glasses, epaulet, neck, and hat). Both devices are integrated to the same software and web-storage solution, Evidence.com. Each testing precinct was assigned six Taser units of both devices for their teams to test. Officers selected their device, first come first serve. The devices were not equally divided across precinct shifts. Only one vendor’s product was tested at a time to prevent running dual infrastructures supporting two BWC programs at the same time.

Infrastructure

Data Connections: In the first phase of the test, two additional data line drops were added to the three test precincts to accommodate data transmittal from the Taser multi-docks to cloud storage. Moving forward, both vendors would need significant increases in accessibility and bandwidth to transmit data. Depending on the vendor selected, each precinct would need 8 to 20 new data line drops. The Metro Optical Ethernet (MOE), the means which transmits data from location to location, needed a bandwidth increase at each police precinct.

In the second phase, data was stored locally in a server. There was no other additional infrastructure needed. If local storage is selected, then the MOE will need to be increased between the local networks. Each site and each solution was tested before the start of the test &

evaluation project.

The Department used existing computers to provide Taser a secondary/back-up means of uploading data/video. The same computers were the primary means of data transmittal for the VieVu trial. There were no additional infrastructure additions. There will be a need for additional switches, Ethernet connection and/or computers when the Department proceeds with BWC deployment

Both BWC have the capacity to integrate with the squads MDCs. This option was not used due to logistical considerations. It would not have been feasible to retro fit 240 squad cars for the sake of 36 users. It is still an option to consider if the Department selects VieVu or Taser products.

Camera warehousing No special accommodations, cabinets or structural changes were needed to house either BWC at each precinct. There was unused and available space to store the cameras between officers' shifts. When the Department expands the use of BWC throughout the Patrol Division, there will be more demand for racking, device storage, and power & data access considerations. MPD will need to house 100-130 cameras at each of 5 precincts requiring 7 to 18 multi-docks (depending on selected vendor). A space feasibility study will be needed to be completed before further installations.

Policy

The following review of BWC policy is concentrated on operational effects of policy regarding the capture of BWC data. Privacy, chain-of-custody, data requests, and jurisdictional consistency need further research. These topics will be addressed by MPD's implementation team. MPD used a written Standard Operation Procedure (SOP) developed by Police Administration, Training, Patrol and Police Federation (Union). The same SOP was used in the Taser BWC trial and no modifications or changes were made. The SOP is incident based, but allows some latitude as to when an officer could turn the BWC on or off.

Strong policy drives data collection. Clear policy directs officers when to activate and when to deactivate a BWC. A review of three policies makes evident how explicit policy for activation can influence the amount of data collected and increase expected storage costs. Similarly, policy on deactivation has influence on data accumulation can have the same effect. Deactivating a BWC too soon, may render content meaningless. Deactivating too late, may produce volumes of data with no evidentiary value and add to overall costs.

| Alameda Co. G.O. 8.17 | Minneapolis PD SOP | Denver PD 111.11 |
|---|---|--|
| <p><i>Staff</i> shall make every effort to record all enforcement contacts, such as arrests or citations. <i>Staff</i> shall make every effort to record non enforcement contacts should they become confrontational, assaultive, or enforcement orientated.</p> <p>General Order 8.17 Page 2 of 3</p> <p>D. It is recommended that <i>Staff</i> record pedestrian contacts, interviews, and other events when the recording has value as evidence, to limit liability, to resolve citizen complaints, or as a training tool.</p> <p>(Brosi, A. 2015)</p> | <p>Officers should manually activate the PVR to Record Mode when reasonably safe and practical in the following situations:</p> <ul style="list-style-type: none"> • Traffic stops • Suspicious vehicle stops • Suspicious person stops • Priority responses • Vehicle pursuits • Arrest situation • Work-related transports • Vehicle searches • Physical confrontations • Crimes in progress <p>In any situation that the officer feels appropriate when taking a statement and/or gathering information from a victim, suspect or witness</p> <ul style="list-style-type: none"> • Any Significant Incident (see definitions) • When advising an individual of their Miranda rights • When ordered to do by a supervisor • Any time an officer feels it is appropriate to preserve audio or visual evidence consistent with the purposes stated in this policy. <p>(Minneapolis, 2014)</p> | <p>All officers will place the BWC into event mode prior to any officer initiated field contacts involving actual or potential violations of the law including:</p> <ol style="list-style-type: none"> 1. Traffic stops 2. Pedestrian and/or vehicle contacts <p>b. All officers will place the BWC into event mode when responding to the following calls for service and/or in the following situations:</p> <ol style="list-style-type: none"> 1. While en-route to any in-progress, just occurred and/or any other call for service where the fleeing suspect and/or vehicles may be captured leaving the crime scene 2. All calls requiring the presence of a Crisis Intervention Team (CIT) officer 3. When responding to calls reportedly involving weapons or violence 4. All calls involving suspected suicidal and/or suicidal individuals 5. When engaging in a foot chase, provided the activation does not interfere with officer safety or the safety of others 6. When emergency or pursuit emergency driving response is required (See OMS 112.08) 7. While executing warrantless searches of individuals, vehicles, buildings and other places <ol style="list-style-type: none"> A. The BWC will be utilized to record the request and consent when practical. This recording is intended to enhance a documented consent however, it is not intended to replace the use of any form used to gain and/or record the consent to search without a warrant. 8. While advising an individual of their Miranda rights <ol style="list-style-type: none"> A. The existence of a recorded advisement will be documented in the officer's statement. 9. All arrests and/or citations, provided the activation does not interfere with officer safety or the safety of others 10. While taking statements from subjects, victims and witnesses (See OMS 302.11) <ol style="list-style-type: none"> A. Consideration may be given to a victim who requests not to be recorded or when circumstances warrant. 11. If not already, the BWC will be activated to record any encounter that becomes adversarial or in any situation that the officer believes use of the BWC would be appropriate or would provide valuable documentation. <p>(Leuthauser, J. 2015)</p> |

Alameda Sheriffs Department of CA deploys 160 VieVu BWC in the field. Their officers record on the average 2.3 GB per month/ device (A. Brosi, 2015). The amount of data is nearly half the amount collected by MPD during its VieVu test and evaluation (4.5 GB per month/device). Denver PD used 106 devices in a BWC test. Their staff reports DPD officers collected 9.4 GB

per month/device (J. Leuthauser, 2015). There is a clear progression of administrative/policy retirements and responsibilities which influence the frequency of BWC activation. Alameda SO policy is a collection of recommendations. MPD SOP guilds officers to when they should activate a BWC. Denver PD is the most direct. The policy declares officers will “place the BWC into event mode prior to any officer initiated field contacts (J. Leuthauser, 2015)” under proscribed conditions. Indeed there are other factors which will influence activation/deactivation including: environmental conditions, calls for service numbers community expectations and supervision. Policy, without supervision and accountability is ineffective.

In the Taser and VieVu test and evaluations, MPD officers did not continuously record their entire work shift. Battery life limits continuous recording. While standby battery life is 12-72 hours depending on the device, BWCs can only continuously record 4-5 hours at standard definition. The Department could lower video quality of a BWC and capture more video at lower resolution. This setting change would be off-set by battery degradation in cold weather use by a Taser BWC. Neither vendor has a BWC with an exchangeable battery pack. A BWC recording every minute of an officer tour of duty would generate 50 to 70 times more billable data. Continual recording would also create some separation of evidence issues, as police calls are incident driven and handle from start to finish.

Training

With each vendor, four two-hour training sessions were conducted to provide evaluation officers, project administration, Records, Crime Lab and court personnel the skills to operate the devices, software and web-base access. MPD conducted a brief overview of the body camera SOP. Staff demonstrated client-based access and taught the skills to load, retrieve, review, copy, annotate video files. Once trained, officers were able to record immediately in the field.

Additional training was provided in Phase 1 of the test and evaluation. The Department issued smart phones to all evaluation officers. The smart phone was used to Bluetooth connect to a BWC and utilize Taser apps for evidence management. VieVu LE3 does not currently have this option, but will have a similar Wi-Fi connection in a future product release. The set-up of smart phones encountered some training challenges. Not everyone had the same skill set or knowledge level of smart phone operation, required intensive assistance and additional individual training was needed by some to have the smart device operational. The actual use of the smart phone in the field also presented some trials. Some officers already had personal smart phones and were unwilling to carry two. A few officers installed the Taser Apps on their own phone and did not use the issued smart phone.

If smart devices are used in future deployment, it is suggested to have a separate training session for each group of officers. The combination training of BWC and smart phone enrollment is too much knowledge to transfer in one class. Smart phones do pair with the BWC without issues, but the maintenance and monthly billing are additional support items to be considered in the

overall budget for a body camera program. Smart devices, such as an iPod, can also pair with the BWCs.

3. Project Initial Data Results

Data Captured In the six month BWC evaluation, MPD officers recorded 7,077 videos loaded into either Evidence.com or local storage. They took 2,367 still digital photos, all loaded into Evidence.com. Officers uploaded 712 GB of data, of which 99% of the data is video evidence and less than 1% is digital photo data. Over 740 hours videos were recorded.

In a full patrol deployment of 615 BWC (with policy changes, seasonal differences in calls for service and recording at the same rate/definition) it is anticipated the Department could record nearly 440,000 BWC videos a year (over 1,200 videos a day). The amount of videos is over 40,000 hours of digital recording. Officers would take over 146,000 evidence still digital photos and create in total up 65 terabytes of data (66,240 GB). The projected amount of video is 3 times more than all in-squad video recorded per year (134,000).

An importance consideration is video file format. VieVu records in a different BWC file format than Taser and the rate of capture is 1.5 greater than Taser. The Department would need significantly more storage space available if it used VieVu’s solution. This would increase one-time setup costs and ongoing operations expenses. It is somewhat offset with data allowance for cloud storage (discussed in pricing options).

| MPD’s Test and Evaluation BWC File Format Comparisons | | |
|---|------------------------|----------------------------|
| VieVu | 1 hour video = 1.57 GB | 1 GB = 0.63 hours of video |
| Taser | 1 hour video = 0.76 GB | 1 GB = 1.30 hours of video |

Category Types: The BWC data captured is arranged in categories. There are no preset factory/industry video categories. Collections of videos can be configured by the Department. Some police departments have over 100 categories and various retention schedules. MPD staff is already experienced with digital video categories used within the in-squad camera program. The BWC operation mirrored those categories to shorten the learning curve and have some uniformity in video storage. Videos fell into 6 configured categories: significant events, use of force, arrests, citations/traffic, non-evidence events and uncategorized.

| Video Category | BWC Test Total Number |
|-------------------|-----------------------|
| Force | 30 |
| Significant Event | 163 |
| Arrest | 968 |
| Citation/Traffic | 843 |
| Non Evidence | 3,793 |
| Uncategorized | 1,310 |

Use of force events were < 1 % of video entries, significant events 2%, arrests 14%, tags/citations 12%, uncategorized events 18% and non-evidence events were 53% of all recordings.

Data Retention The video event categories were put into retention schedules collections. The same categories and retention schedule was used for both phases of the BWC test. The retention time periods were suggested by the City Attorney Office and are different than other video camera programs operated by City Departments, including MPD. Body camera video retention groups are:

- Non-evidence and citation videos saved for one year.
- Use of force and arrests events is saved for 7 years.
- Significant events saved until determined.

A noteworthy number of videos were uncategorized (unknown). While every video may not be a call for service, citizen encounter or major event with a case number; every event does fit within in one of the five other categories other than unknown. The non-categorization is not a result of device, software or web-application failure. Officers simply did not do it. There was a significant difference in the rate of non-categorization with the different BWC products tested. In the Taser test, 13% of the videos were uncategorized (unknown retention). In the VieVu test 22% of the videos were uncategorized (unknown retention). This is a 65% increase in the rate of uncategorized videos. The non-categorization of video has direct financial considerations. BWC cloud storage is set at a fixed rate per device and any data overages will be billable per GB/year. Also, if officers do not label incidents (case numbers) it will take more time and possibly more staff to retrieve video when needed.

The increase number of uncategorized videos is directly linked to the method officers entered event categories and labeling into the video file. In the Taser test officers had the ability to Bluetooth directly into the BWC device, provide a case number, make comments and select a retention category. This could be done in the field right after the event was captured on the BWC. VieVu cameras currently do not have a Bluetooth/ Wi-Fi capability to use a smart device to annotate and categorize videos. Staff would need to return to the precinct after the event and use a designated computer to enter data. Or an officer could wait until the end of the shift to enter data. In the VieVu trial this workflow while less convenient than field entry, did not present operational obstacles. Only 2 or 3 officers per shift would entry data at the test precincts. In practice, staff did not categorized videos because it was difficult to do so in a timely fashion, hence the 65% increase in uncategorized videos.

If MPD does not employ any Bluetooth or Wi-Fi capability to make data connections in the field then MPD will need to overcome some logistical considerations and install equipment in squads that will allow officer to review, annotate and name videos in the field (expected one-time cost

an additional \$100,000). This will prevent excessive downtime and limit possible overtime.

4. Hardware Review and Performance

Security: Both BWC vendors have secure encrypted transmissions of data into the cloud. Taser uses SSL RSA 2048-bit key, 256- or 128-bit ciphers (depending on client browser) for data encryption in transit (Taser. *Security*. 2015). VieVu encryption in transit and rest uses AES-256 (VieVu. *VieVu Solution Whitepaper*.2015).

Taser Axon BWC: The Taser Axon Body camera is an all-in-one one-piece body camera. It has a camera lens, microphone, internal memory and battery pack combined into one unit. Power activation is a slide switch at the top of the device and record activation is a separate push button switch on the center of the BWC. It is worn center mass on the officer's chest. It does have some other mounting options that will allow placement on the pocket of a shirt or pocket on an outer garment. The Axon BWC is paired to the data storage site Evidence.com. It can be accessed by Bluetooth for review, labeling, comments and categorizing of videos. The BWC cannot edit, alter or delete video nor can video be altered by a paired Bluetooth mode.



To activate recording, an officer pushes the raised on/off push button twice. To deactivate recording, an officer pushes and holds the on/off push button for three seconds. The device has a LED light display to inform the officer the device is powered and/or recording. It also has an audible alert when the camera is activated. The BWC has a 30-second buffer recording function. Officers download video off the BWC and the data is then uploaded to cloud storage.

- Below are selected features of the Axon FWC (Taser. 2013)
 - **Storage** 8 GB On-board
 - **Record time** 4-13 hours based on settings
 - **Recharge time** 6 hours
 - **Video playback** Via Phone App
 - **Video resolution** 640 X 480
 - **Video frames per second (FPS)** 30 FPS
 - **Operating Temperatures** -4°F to 122°F
 - **Drop test** 6 feet
 - **Field of View (FOV)** 130°

Axon Performance: The BWC is very sturdy and has several mounting options. It is easy to use

with one hand. The activation and deactivation process is a deliberate act. There were no reports of accidental deactivations and just one report of accidental activation. There were several reports of non-recording of events. The non-recording of an event was corrected by a factor reset and the device was returned to the field with no other issues. Of the 18 Axon units, one was defective and sent back for warranty issues.

Taser Axon Flex BWC: Flex BWC is a multi-piece unit which can be worn in several different manners. The device consists of a video camera/with audio (a lipstick camera) which can be attached to eyewear, a power cord and the controller/battery. The BWC has a 30 second buffer recording function. Officers download video off the BWC and data is then uploaded to cloud storage.

The controller is similar in operation as the Axon camera with the same on/off functions and device alerts. It is connect to the camera by a data/power cord. Power activation is a slide switch and record activation is a separate push button. The device's main feature is a Point of View



camera (POV) because it can gather video from the officer's perspective. The field of view is 75° and the resulting video is tighter, with less distortion. An officer can attach the camera (which also houses the on board 8 GB memory) to eyeglasses, cap, or shirt collar/epaulette. It is paired to Evidence .com for video management. The controller has an audible alert that indicates the device is in the recording mode.

- Below are selected features of the Axon FWC (Taser. 2013)
 - **Storage** 8 GB On-board
 - **Record time** 4-13 hours based on configurable settings
 - **Recharge time** 6 hours
 - **Video playback** Via Phone App
 - **Video resolution** 640 X 480
 - **Video frames per second (FPS)** 30 FPS
 - **Operating Temperatures** -4°F to 122°F
 - **Drop test** 6 feet
 - **Field of View (FOV)** 75°

Flex Performance: Flex BWC has superior clarity and resolution compared to the Axon BWC. It also has greater options in mounting. Even so there were some complaints as to the wear ability of the unit. Officers needed to frequently adjust the components of the Flex camera to ensure optimal operation and comfort. In cold weather, officer wear hats, which sometimes interfered when the unit was worn on a pair of eyewear. In addition, during the course of an officer's shift,

an officer may remove, zip up or put an outer garment on and off again many times during the shift. This required more camera adjustment than the body mounted Axon or VieVu BWC.

Because the camera unit is three pieces, there was a noticed tendency of the equipment to disconnect from itself. This caused several cases of failure to activate or record. The cord from the camera to the battery pack would unseat and cause the non-activation issues. By design, the cord separation is an officer safety feature, separating easily so an officer is not endangered. Yet this safety feature could be problematic when retrieving a critical video related to high profile event, an officer believes in earnest video is recorded, yet none is captured. Further device training can alleviate some of this issue, but it is unique to the Flex camera.

VieVu BWC:

The VieVu LE3 BWC is an all-in-one unibody camera. The BWC is slightly larger than a pager. It has a camera lens, microphone, internal memory and battery pack combined into one unit. There is no buffer recording or an on-board video playback screen. The camera is meant to be worn center mass on the officer. It has a rotating clip which attaches to an officers uniform. It must be worn with the lens topside. The BWC is paired with VERIPATROL Client and VieVu solution for video management.

Power activation and record activation is a single slide switch on the center of the device. When the slide is moved down, the camera turns on and begins recording. When the slide is returned upwards, the camera stops recording and shuts off. When the camera is on and recording the lens is exposed and a green ring is displayed around the lens as an indicator the device is in recording mode.



- VieVu LE3 BWC general product specifications (VieVu 2015):
 - **Storage** 16GB On-board
 - **Record time** Up to 5 hours continuous
 - **Standby time** 72 hours
 - **Video resolution** 1280 X 720 (HD), 848 X 480 (WVGA) (SD)
 - **Video frames per second (FPS)** 30 FPS
 - **Format** MPEG-4, H.624, AVI container
 - **FOV** 68°

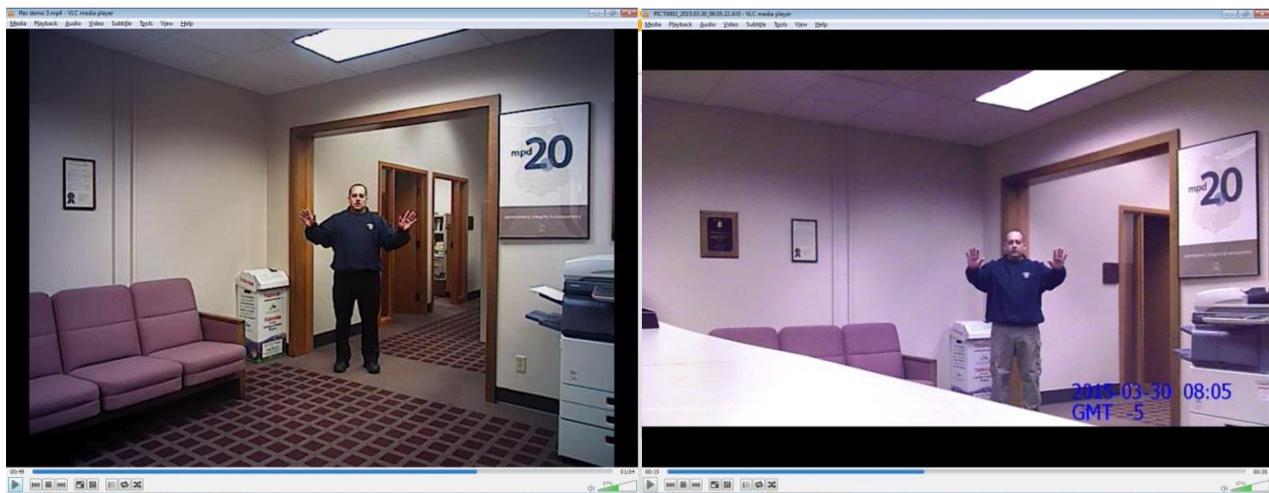
VieVu LE3 Performance: The VieVu LE3 BWC is compact, lightweight and easy to use. Video is downloaded off the BWC and then uploaded to a local storage solution. Officers did not have any failures to activate the BWC. The slide mechanism straightforwardly activates and deactivates the camera. There are no external wires or connections that would tangle in an officer's uniform or work environment. During the trial period, there were only two device

failures. Officers could not download data. The issue was easily resolved with an on-site factory reset of the device. The BWCs were placed back into service without further issues.

Officers did experience many instances of accidental BWC activations. When an officer sat in a squad car and the seatbelt would cross the BWC affixed to the officers' shirt or outer garment, the seatbelt turned the BWC on. The seatbelt would push the activation switch down and the BWC would begin to record. The vendor suggested fix for this issue is a low-tech, but effective solution. An officer would need to place an elastic band or rubber band around the BWC to provide extra tension to prevent accidental recordings.

BWC Field of view (FOV)

Included in the report are three pictures taken at 21 feet. The Taser Flex (head mount) has a narrow 75° field of view. The camera is mounted higher on the body than the Taser Axon. The Flex can also be attached to eyewear and directed exactly to the point the officer is looking at. It does not have any distortion. The VieVu LE3 is worn center-mass, but has a much narrower FOV than Tasers center-mass Axon. Its image is similar with the Taser Flex, as the FOV is only a few degrees different.



Taser Flex 75° FOV

VieVu LE3 68° FOV

Neither BWC will replace the officers own observations or what an officer felt or experienced on scene. While field of view is an important consideration in product review, it should not be the only criteria for selection. Ultimately a selection should be based on what the Department expects from body cameras; an exact representation of what an officer saw or an independent unbiased witness to the events recorded.

The Taser Axon BWC has a 130° field of view. It captures much of the area in an officer's peripheral vision. This FOV range compensates for the lack of mobility of the lens as it is mounted center-mass on the officer wearing the BWC. The recorded videos display a "fisheye"

effect. The barrel distortion is due to the wide lens used to capture images as the officer's torso is difficult to point and shoot



Taser Axon 130° FOV

Which is BWC point of view is better? Unquestionably, the narrower view Taser Flex and VieVu LE3 have better resolution, clarity and detail compared to the Axon BWC. But there are advantages to both FOV applications. Situations on the street are rapidly evolving and complex. A wider point of view can capture more information (such as accomplices' actions) and might be important in the aftermath of a police action. Similarly, if an officer uses deadly force, view from a Taser Flex or VieVu BWC would provide critical and exact detail as to what the officer saw as a threat. Both vendors would benefit by having a 90° FOV BWC as it would provide less distortion and more contextual detail.

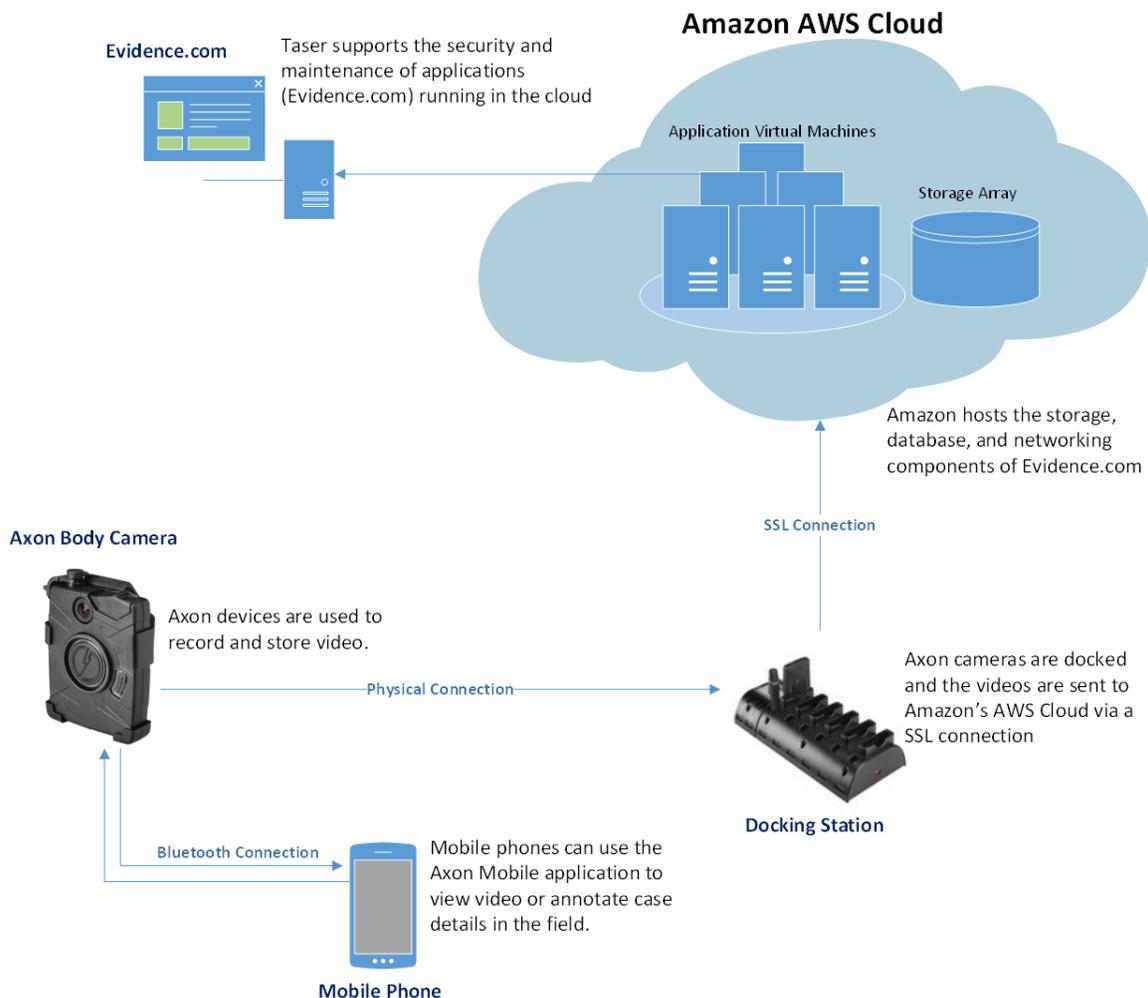
5. Data Storage

Taser Data Storage: Taser does not have a local storage option. All video is stored on the cloud through Amazon Web Service (AWS). Data is delivered timely and is secure. Cloud storage has several advantages. With permissions, video can be retrieved on any device anywhere in the United States. A police department does not need additional software to connect, but it does need licenses for each user to connect the cloud storage. The licenses are tiered in pricing in relationship to amount of video stored and features needed (editing, administration...etc.).

Cloud storage also assists in secure web-sharing of videos. This is a desirable feature in which the Department can provide prosecution office copies of the video/evidence without assigning personnel to access, copy and transport hard copies of video evidence to City and County Attorney's offices.

The diagram below, provided by City of Minneapolis Internal Audit Unit, outlines how data is

currently entered into the Taser storage solution (W. Tetsell, June 9, 2015).



VieVu Data Storage: At the onset of the RFP and prior to purchase, VieVu had two data storage options. The first is localized storage and the other is hybrid cloud storage with Amazon Web Services (AWS). In order to utilize the AWS cloud-storage, the Department would need to employ a staging server. The server would ingest data from the BWC devices and then push the videos to AWS via the intranet. VieVu recently has added a third option; a fully hosted cloud solution.

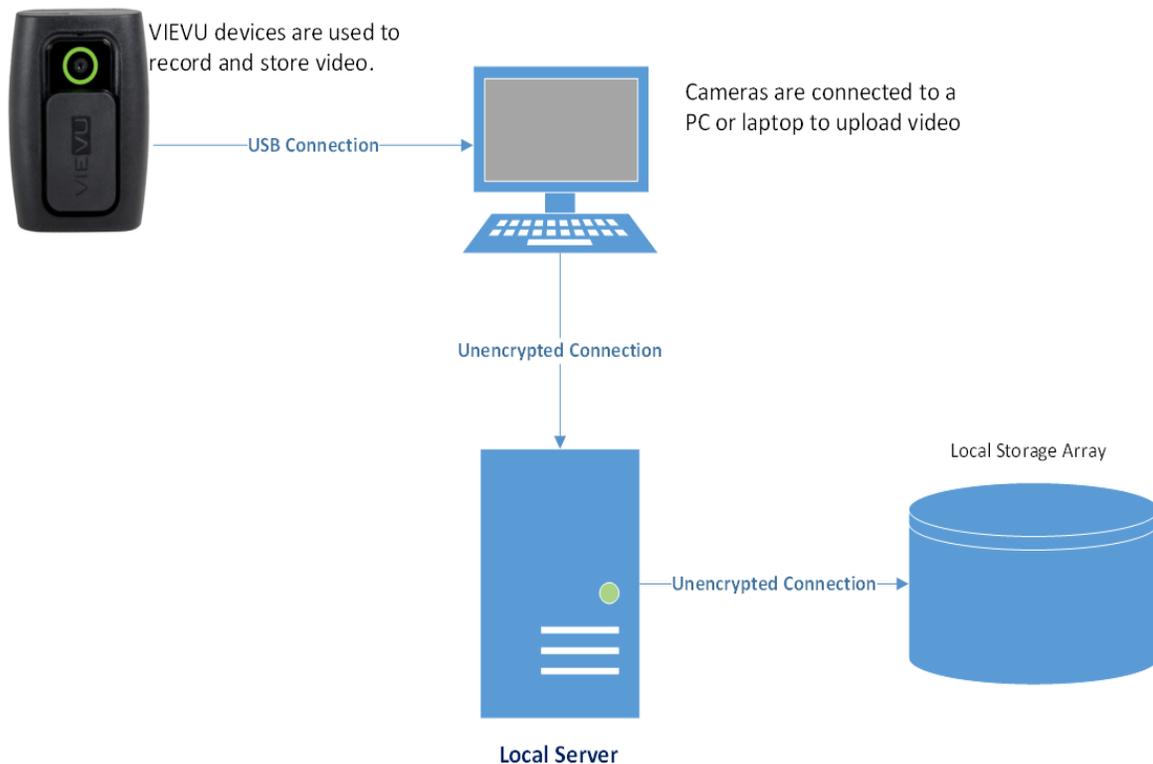
Before the Department took delivery of the BWC devices, VieVu switched cloud storage providers. They selected Microsoft AZURE as the new data storage provider, a government cloud computing community (GCC) option which is marketed as CJIS compliant. The Department researched the GCC option: no current police department was using AZURE for BWC data storage. MPD declined to use GCC storage option; it would have been the first police

department to do so and was considered too great of a risk to take in a test and evaluation project.

MPD stored the BWC data locally. City IT designed and provided a storage solution. The BWC project team estimated the amount of storage needed based on data collected in the Taser BWC 4-month test. MPD Officers collected 100 GB data per month using Taser Devices. A 500 GB storage solution was determined to be the right size to accommodate a three-month test. Midway through the Vie VU test however, the BWC project team discovered that the VieVu cameras recorded in a different file format which resulted in capturing 1.5 times the data for the same amount of video. Data entry and video downloading was suspended two weeks early of the VieVu test rather than increase storage capacity.

The diagram below, provided by City of Minneapolis Internal Audit Unit, outlines how data is currently entered into the VieVu storage solution (W. Tetsell, June 9, 2015). The VieVu fully hosted Microsoft Azure storage solution would be similar in architecture as Tasers hosted storage site.

VieVu Body Camera



6. Taser Software Review

Evidence.com: Video management is done through Evidence.com. Anyone who has access to the web-based application has their level of access defined by pre-determined administration set roles and permissions. BTU configures roles and permission levels to the Department's preferences. Officers can only view their own video. They cannot edit or delete the video with the software. Supervisors can review any non-restricted video and cannot edit or delete videos. BWC Administration and the Crime Lab have the rights to view, lock, delete/edit (redact or shorten) a video. The software always preserves an original copy of the video and can support multiple copies/versions of a video. The application has a very robust audit function and can track who accessed, viewed, shared or deleted a video. BWC Administration can also name categories of videos, set retention schedules and schedule automatic deletion. The application allows searches for videos by date, officer, label, category or type of evidence (video, audio, picture).

Axon.com: Axon.com is an application loaded onto the issued iPhones. Officers use the application to access non-downloaded videos in the body cameras via Bluetooth. An officer can access and review a video, at 5 frames per second. Officers used this application to label, comment and annotate videos and photos in the field. The result is a significant savings in time in the back office because officers can label videos in the field and then drop the camera in a docking station at the end of the shift. No waiting at computers or additional accrued overtime waiting for a camera to completely download video.

Evidence.Sync: The uploading, annotating and categorizing of videos can also be accomplished through installed software Evidence.Sync. The City IT Department vetted and installed Evidence.Sync on the common shared report writing computers in each precinct station. BTU, Administration, Crime Lab and Records Units also had software installed to assist with management of videos. The software links to Evidence.com, a secured cloud base video storage solution accessible by the web.

Evidence.Mobile: Evidence.Mobile is an application installed on the iPhones issued to the test and evaluation officers. It provides officers with additional resources to capture digital evidence. Through the application, officers can record video, audio or take still pictures. In the test, officers used this application over 2,300 times to take still photos. The photos are taken by the camera function in the application, not the software on the smart phone. When the data is downloaded and then uploaded to Evidence.com, the photos are also transmitted. Once data is completely downloaded off the device, the application deletes any photos on the BWC.

7. Taser Software Performance

Evidence.com: Web-based, Evidence.com software was not packaged or managed by City IT.

Once an officer signs in to Evidence.com, they can access videos that have been uploaded into the cloud. Access is password protected. Predictably, officers would forget their password. The software has a password reset and if an officer locked themselves out, it has a 5 minute reset. During the test, Taser updated the software and several search capabilities were enhanced. Users did not report any down time or interruptions. MPD asked Taser to improve software to arrange assigned personnel in groups. Taser made this software change near the end of the test and evaluation. Taser offers live support during normal business hours.

Axon: The software Axon is a mobile application loaded onto smart devices via an Apple iTunes account. Other than using the right iTunes account, there were no reported issues loading the application. Once on the smart device, officers easily used the Bluetooth option to access and add data to the video files. This process worked well and there were no reports of interruptions of service.

Evidence.Sync: This is client based software which was packaged and pushed to designated BWC computers. The software allows a BWC to download data into the computer and then will upload data to the cloud. There were no reported issues with the software or its use.

Evidence.Mobile: This mobile application had two issues that officers discovered. Officers would need to change the settings on their smart device to allow the application to use the on-board camera. This is more of a smart device issue than software problem. When officers used the camera function of the application, the application would take a picture and then pause and ask the operator if they wanted to take another. Officer found this inconvenient as they always wanted to take another picture.

8. VieVu Software Review

VERIPATROL Client: MPD installed VieVu software on City servers which runs the SQL database of VERIPATROL. Every computer used to download videos had an install of VERIPATROL Client. The software allows officer to only download, retrieve, annotate and view their own videos. Supervisors and administrators can view all videos based on preset roles and permissions. The software does not allow any staff to alter, edit or change the video in any way. The software is easy to use by officers. It allows officers to perform only five functions:

- Download
- Add Details (annotate)
- Search
- Copy
- Play

In the test program, officers were not given permission to copy videos. A search for a video with partial information could be enhanced with the software's filtering function. Officers are

able to filter a search by these options; officer, officer ID, category, case number or comment. There is no ability to edit, redact or change a video by officers or by administration.

VERIPATROL Administration: This software was client installed on all machines used for BWC program administration. It has all the functionality of VERIPATROL Client; administrators could view, search, annotate, play and copy videos. VERIPATROL Administration also provides the ability to assign cameras to individual officers and changing assignments as staffing changes. In full deployment the software can integrate with Active Director to authenticate, authorize and manage staffing/assignment changes.

The software provides MPD the ability to set roles and permissions of users (those who would download videos and those who would view videos). MPD can set retention schedules, and change them as directed by state law or the City Attorney's Office. Software also allows MPD to select the video definition of the BWC. HD (High Definition) produces a much better picture, but at a cost of double the data. MPD elected to use standard definition to limit the amount of data collected. The software does provide an audit function. The software also has the ability to document video alteration. VieVu states the system has "a FIPS 140-2 compliant digital signature process is used verify the video has not been altered (VieVu, 2015). Software allows program administration to monitor and prevent unsanctioned access to data.

VERIPATROL Mobil: MPD used Veripatrol Mobil – View Only in a single mock up squad. The VERIPATROL Mobil application allows staff to leverage a data connection with squad computer (MDC) to a BWC to review and input data. Officers can review video on the MDC's full screen at full size, full speed (30fps) and resolution (VieVu, 2015). There are options for a Department to use wireless data transfer from the squad MDC to VERIPATROL sever. This is a separate software package

9. VieVu Software Performance

VERIPATROL Client: MPD did not experience any VERIPATROL Client software failures. Officers were able to annotate add comments to videos as needed. There were several cases when data transfer was slow, but this is an issue with the City's internal infrastructure rather software. It does not have a password reset option. Officers would need to contact administration to have this task completed.

VERIPATROL Administration: VERIPATROL Administration client software provides basic data retrieval tools. There are no internal reports per se, but administration can sort through data by officer, camera, videos and the master log (audit tool). The use of the software could be improved to include the ability to internally or externally sort data in an Excel spreadsheet like fashion.

The VERIPATROL Administration client software does not provide access to Server Setup

configuration menus. A program administrator needs remote access to the local storage server in order to run the VERIPATROL Administration application on the server to be able to access the server setup. This is the only place one can monitor the free disc space on the storage server and view/edit the categories and retention periods.

VERIPATROL software, as tested, did not have any redaction tools or options. The current MPD business model requires highly trained certified video specialists from the Crime Lab Unit to accomplish this task. To redact a video, the Crime Lab must export the video into a third-party software program. Staff must examine the video frame by frame and redact non-public data/images. If used in full deployment, the Crime Lab may need to increase staff.

VERIPATROL Mobil: As tested in a single squad, there was no performance issues notice. The application easily allowed staff to view and annotate videos in the LE3 BWC. Playback was in full screen and full frame rate (30fps). There are however, logistical issues which prevent fully utilizing VERIPATROL Mobil and Remote Data Transfer software. In the current equipment set up of a squad, the MDC lacks a free USB port to plug the BWC into for a data connection to review video. VieVu cabling requires two ports, one for power via POE and the other for data transfer. Additionally, the MDC's are at the end of service life. The Department will begin a multi-year project in 2016 to replace current MDC's. New equipment may have the necessary USB ports for review.

If selected, two free USB connections to an MDC shall be necessary so that officers can view annotated and categorized videos in the field. Failure to do so MPD will sustain increases in overtime costs or officers leaving the field early to download video. It might force staggered shifts times within the Day, Mid and Night work shifts. This staffing option is highly undesirable as it breaks the continuity of command and sharing of information across work teams.

The VERIPATROL application also allows wireless transfer for video file over 4G/Wi-Fi to VieVu Solution Cloud or VERIPATROL. The cloud solution and VERIPATROL Mobile-Remote Transfer were not in scope of the test. If selected, there should be more testing necessary for this additional third-party software package.

Remote access to video footage was not possible unless the user's computer was physically connected to the network. Utilization of a VPN remote connection was not sufficient to access the video.

10. Operational Concerns

Several operation concerns were examined in the test. Equipment and software were tested to ensure that any BWC deployment would be efficient and effective. Failure to address the concerns may jeopardize on-going program and evidence, increase costs and create workflow

bottlenecks. Those concerns include:

- Cold weather deployment
- Redaction
- Docking stations
- Smart Devices
- FOIA Requests
- Staffing

BWC Cold Weather Deployment: Prior to BWC testing, a principal concern about the any BWC model was the effect of cold weather on the cameras usability. There are a few major cities in the same climate zone as Minneapolis to solicit references/experience in this performance factor. It was important to test and monitor this phenomenon. In the MPD Taser test, temperatures often dipped below zero°. An un-seasonally warm winter and spring prevented any cold weather testing with VieVu LE3. Results of the test demonstrate when responding to calls for service, officers would move from a warm environment (a squad car), to a cold environment (outside) and sometimes into another warm environment (a dwelling). On occasions, the camera lens would fog over, blurring the video for a short time. The fogging effect is much like a pair of glasses fogging over due to the transfer of heat. Nevertheless, the fogging effect is short-term and did not occur with every device. There are commercial anti-fogging sprays and applications that can be applied to a BWC. At this time, the fogging issue is infrequent and insignificant and does not warrant further action.

Cold weather also has an effect on the battery life. MPD Patrol shifts are ten hours. Occasionally officers work beyond 10 hours in a shift. The stand-by battery life of a Taser BWC is 12 hours. The standby battery life of VieVu Le3 is 72 hours. In practice, MPD staff found the battery life of a Taser BWC between 9.5 to 10 hours in cold weather. There did not appear to be any notable cold weather battery life issues with VieVu BWC.

Redaction: Certain videos will need video and audio redaction. The current business model directs staff from the Crime Lab to accomplish this task. The process is very time consuming. Once the video has been exported into a third-party software program it needs to be examined frame by frame. One minute of redaction can take over an hour to complete. Example: a body camera records at 30 frames per second. One minute of body camera video has up to 1800 frames. Each frame would need the face of a person(s) blurred and that face/target would move in every frame. While it can be done, under MPD's current business practice model, it requires highly qualified and skilled video technicians to do this



work.

Taser has a solution within evidence.com that can save time and does not require highly skilled staff to the redact data. After a video/audio time segment is identified as needing redaction, staff can apply a blurring effect of the video or removal of audio with a click of a button. In this report there are five identical pictures (one with no redaction, low blur, medium blur and high blur, and last with vector masking). They are examples of the redaction tool in Evidence.com. The redaction effect can be applied to one frame, one second, a batch portion or the whole video. The process is easy to learn and do; it only requires a few minutes of training. Mass copies of the redacted video could be produced in a timely fashion if needed for a public data request.



Low Blur

Medium Blur

High Blur



Vector Mask

VieVu did not have a redaction tool available during the test and evaluation. They have partnered with Microsoft and will have a redaction application in late 2015. It is essential to have redaction tools within the software of both BWC products as this will help in the timely management of FOIA requests for videos. The redaction of certain videos will ensure public information is public and that which is private remains so. An in-software application also allows staff to store a copy of the redacted video for future review and record keeping. Operational costs will increase if the department selects a vendor that does not supply a redaction tool. The Crime Lab would need to hire another staff member to handle requests for redacted video.

Docking Stations: At the end of a patrol shift, an officer is required to transfer data from the

BWC to the cloud or local storage and charge the device. Each provided BWC had cords and individual charging connection to manage this task. In the limited test, BTU attached cords to each designated computer for officer to maintain VieVu LE3 BWCs downloading. In an expanded deployment it would be impractical as there are not enough designated computers or power outlets to accomplish this daily requirement.



Taser Six Bay Multi-Dock



VieVu 15 Bay Multi-Dock

In Phase 1 of the test, Taser provided a six bay multi-docking station. Officers were able to annotate and add comments in the field and at the end of the shift “dock and walk” leaving the device in the docking station. To upload and charge a Taser Axon or Taser Flex BWC, an officer cradles the device in a six-bay multi-docking station. This dock can accommodate either camera or battery pack. Once docked, the camera uploads video/data over the internet to Evidence.com. Upload times depend on amount of data recorded, number of cameras docked and bandwidth/traffic. The expectation is all videos from all cameras will upload before the officer’s next shift. In MPD’s Taser test, uploading was accomplished within several hours of docking a camera.

VieVu now has a 15- Bay Multi-Dock. This device was not available in production during Phase 2 of the trial. VieVu had offered to provide a beta test model, but MPD declined. This device is similar in operation to the Taser docking stations. It can be configured to charge, download a BWC or both tasks.

The dock devices are advantageous to on-going operations. It prevents needless waiting for free computers. The docking stations would require an infrastructure upgrade at each of the five police precincts. The total one-time cost is about \$90,000 for data connections, cabling and racking. The investment will prevent unnecessary overtime costs as officer can leave the BWC in a secure place, confident that data is uploaded and the device is charged and ready for use for the next scheduled shift.

Smart Devices: In the test and evaluation, a smart phone was paired with Taser BWC. Future offerings from VieVu will also offer the ability to pair with their BWC via Wi-Fi. Both

applications will allow officer to remain in the field for calls for service and eliminate the need for overtime at police stations to enter data. The one-expense or on-going phone bill will offset any expected BWC data entry overtime.

Additionally, the continued use of this application, any smart device or iPhone, creates the opportunity to expand on evidence-based prosecutions. Officers are able to use a smart device to capture evidence that normally would not be gathered in the field (photos and interviews). The digital evidence captured by the smart device does not supplant the need for Crime Lab specialists; serious major crimes will still need skilled technicians to gather and provide forensic documentation.

There are many situations where a quick picture or audio recording can provide all that is needed; a look at a broken window, a bent fender or a confession. The cameras paired with smart devices oft times will provide the “first look” at a crime scene and a means to document the Department initial response to a call for service. The use of this paired technology will augment officer reporting and provide “accurate documentation of events, actions, conditions and statements made during arrests and critical incidents (TASER 2014)”. Indeed the application is a supplement and augments the retelling of events, but not a replacement for officer’s first-hand observations, experiences and specialized knowledge.

Freedom of Information Act (FOIA) Requests: Much of the video recorded by body cameras is public data. There are portions that are private and will remain so according to law. But the Department is obligated to release video deemed public when appropriate. Request for videos are from internal and external sources. In the same manner that in-squad videos are used for investigations and prosecutions, so too with BWC videos. Nearly 100 Taser videos and 100 VieVu were requested by the City and County Courts and MPD investigators for use for active criminal investigations.

The first series of public data request were from news/media organizations. Anticipating these requests, the Department selected six videos. After passing legal review for data practices, the videos were released to the media. The procedure was relatively seamless and occurred in a timely fashion. Turn-around from request to order fulfillment was less than a week.

Eight requests were received from the general public for body camera videos recorded during the first 120 days of the trial period (T. Wallace. 2015). Even this low number of requests was problematic for the Department to adequately respond in a expeditious manner. Some of the difficulty lies in adequately training staff to respond. The department also lack adequate equipment needed for redaction. More difficulties lie within the business practice of video review. That procedure is examined latter in this document. It’s not always the sheer number of requests that create issues; it is the content of each and every video that can be troublesome.

A private citizen via a public data request, asked to see the first 25 videos recorded in the field

from the beginning date of the test and evaluation. Staff eliminated test videos and on-going criminal investigation videos. They developed a list of 25 public videos. These were submitted to a city attorney for review. From start to finish, the process took over 10 weeks (J. Kellogg, 2015). Evidence.com has a secured web-based sharing option; these videos were provided one at a time to the requestor. However, the use of the web-based sharing was suspended; the request felt uncomfortable sharing potential identifying data to gain access to the information. Minnesota Data practices do not require person share personal information to receive or view public data. The practice of public data requests shared by secured web-sharing was immediately suspended.

Others asked for any and all public videos. A request of this nature exposes the vulnerabilities of a body camera program. On one hand the Department has an opportunity to improve openness/transparency and on the other, must strongly defend the rights of others to privacy. These concerns are then balanced with adequate staffing to fulfill the requests.

Others have noted that mass requests are challenging to integrity of a body camera program; “the requests threaten to create crippling workload for agencies with limited staff and technology” (Lucia, B. 2014). Some police departments have halted body camera programs over this concern. The issue of massive public records requests may not be an issue that the City of Minneapolis can solve alone. As more and more police departments adopt body camera technology, privacy and data records policies will be examined by the Minnesota Legislature. The goal should be statewide direction on this new form of data collection/retention.

Due to Minnesota Data Practice laws, certain videos will need video and audio redaction. As a result of public data requests for videos, a workflow of the business process to fulfill requests was created. Once a request was filed, the selected video was submitted to a city attorney specializing in data practice requests for review. If the video needed video or audio redaction, those sections in the video were identified and assigned to staff for processing. The Taser Evidence.com software has a redaction option in which portions of the video and/or audio can be redacted. If specialized redaction is needed, the video must be exported out of Evidence.com and redacted frame by frame in another software program by a skilled Crime Lab staff member. The records clerk also needed to look into the police records management system to determine if the case was open closed or under active investigation. The records clerk then would check court records to see if the case had been adjudicated. Once those tasks were completed, the video would be redacted and then reviewed by the Deputy Chief of the Office of Professional Standards. After a final approval, the video was released.

Responding to FOIA requests will significantly drive up costs with increase staff and data storage. In a full BWC deployment, MPD will record an estimated 440,000 videos a year (more than 1,200 a day). There are currently several requests to inspect any and all BWC videos. Even if the Department had adequate staffing to respond to just these two requests, it is physical

impossible to inspect every video in a normal business year yet alone process the video to satisfy the requests. While waiting for a petitioner to view the requested data, the videos age in the retention schedule and approach automatic deletion from the storage system.

The Minnesota Department of Administration Information Policy Analysis Division (IPAD) states that in cases such as this “Records aren't *required* to be destroyed according to the approved retention schedule, they *may* be destroyed. It would frustrate the purpose of Chapter 13 if an entity destroyed data that are responsive to an open request” (J. Hey, 2015). This is a conflict between the spirit of the law and the letter of the law. MPD business practice upholds the spirit of the law; it holds all requested data until it can be inspected, even past city set retention schedules. The consequences for doing so may include never deleting data until it has been inspected. This will significantly increase storage costs.

Simply off-loading video from servers (local or cloud) to other mediums may not reduce costs. The Department would give up the in-house Digital Multi-Media Evidence management system which is embedded in BWC storage software and purchase another.

Current staffing allows for only one records specialist to review all BWC video. This person is also responsible for review and redaction of all other MPD records. Any BWC program will need to include proper staffing and an ongoing review to assure staffing is adequate as the program continues.

Staffing: A police officer was assigned to the BWC project as a full-time trainer, coordinator and quartermaster. BTU supplied a sergeant who worked as a part-time BWC administrator. Project management was provided by the BTU commander. In a full deployment, these roles will not change and most likely will not be increased.

There are several key areas that will see a need for more employees. Internal Affairs will examine video for complaint resolution. In some cases there may be a dozen videos which need review. Even though the Department may dismiss more complaints, it may need more staff to examine each and every video in question. It is anticipated that another investigator may be needed to review video. The increase in available videos will also affect delivery of videos to the Police Conduct Oversight Committee. More general staff maybe need to retrieve copy and transport video to the committee.

As described the current process handling BWC video is fragmented in the Records Information Unit. It has several areas in which work bottlenecks and prevent timely response to data requests. Possible solutions may include more Records Unit staff, or a full time attorney to assist.

11. Taser Advantages and Disadvantages

Below are some pros and cons to using Taser software and the camera devices. The cameras are easy to use. The images are clear and detail (depending on field of view). The software is simple to install, use, configure and search & retrieve videos. In cold weather use, the battery life could use some improvements in performance. If the Department wished to save data locally or with another cloud provider, it is unable to do so as software and storage is proprietary.

| Taser Advantages | Disadvantages |
|---|---|
| Multiple mounting options | Software/storage proprietary |
| Dock and walk capacity | Axon “fisheye” barrel lens effect |
| Unlimited Data Plans | Flex connection cords |
| Bluetooth viewing and annotation | Battery life |
| Video management, configurability, secure web-sharing, & video/audio redaction features | Unable to group camera users by work groups |

12. VieVu Advantages and Disadvantages

Below are some pros and cons to using VieVu software and the camera devices. The BWC is sturdy and reliable. The images are clear. It would be advantageous to have a better mounting clip and more mounting options as the device tends to fall off an officer’s uniform. The BWC is also prone to accidental activations. Many of the noted issues are a reflection on the Departments business process and operations. All of the difficulties in software installation were resolve as the Department eliminated software conflicts with other police applications.

| VieVu Advantages | Disadvantages |
|---|--|
| Ease of use | Prone to accidental activations |
| Light weight | No Bluetooth/Wi-Fi capacity |
| Superior resolution of video at 21 feet | Difficult to manage data in software program |
| Green recording notification | High local storage costs |
| Good sound clarity | No redaction feature |

VieVu’s product line has been rapidly evolving over the last six months. The company has also changed pricing strategies and recently was acquired by Safariland LLC. VieVu will still operate as a standalone company (K. Kiogora. June 2015). On the horizon are software changes which will allow redaction and enhanced video data management. Bluetooth capacity to a smart device is also another option that will be available at a later date. As deployment of officers in the field becomes more mobile and less reliant on officers staging from a central local, the Department should look at the 4G WI-FI upload option. All these services/products will need more study before being put into action.

13. Taser Current Hardware and Storage Pricing

The following is Taser’s current pricing for hardware and storage licenses. The pricing is based on a 5-year contract and is the pre-negotiated rate (D. Fowers, personal conversation, March 3/19/2015).

Hardware

- Axon Body Camera \$399
- Flex Body Camera \$599
- Six-bay Charging/Upload Dock \$1500
- Smart Device \$199

Storage: There is no in-house storage solution. Taser offers a tier storage licensing plan.

| Plan Name | Basic | Standard | Pro | Ultimate | Unlimited | Officer Safety |
|----------------------------------|---|-------------|-------------|---------------------------------|---------------------------------|---------------------------------|
| Price/Month | \$15 | \$25 | \$39 | \$55 | \$79 | \$99 |
| Included Storage/Year | 5 GB | 10 GB | 15 GB | 20 GB | Unlimited | Unlimited |
| Upgrade | | | | Camera upgrade 2.5 years | Camera upgrade 2.5 years | Camera upgrade 2.5 years |
| Additional Storage /Month | \$0.125 per GB (Taser. <i>Priced right for any agency.</i> 2015). | | | | NA | NA + CEW Upgrade/5 yr. |

In addition, Taser recently added a discount license plan for City, State and Federal courts. The data plan is “Freemium” and is at no costs to the host police department or the Court (D. Fowers, personal conversation April 16, 2015). Based on a department’s configured roles and permissions, appropriate court staff will be able to access, retrieve and review body camera digital evidence. The Court will not have the rights to redact, restrict, edit or delete and evidence. Taser also has started a BWC device discount program in April, 2015 which provides departments grants for full deployment of Taser products. The grant amounts vary depending on the accompanying warranty or plan (Taser, *Just announce*, 2015).

- Smart Weapon or Axon camera with extended warranty: \$100 per officer
- Smart Weapon or Axon camera with TASER Assurance Plan enrollment: \$200 per officer
- Officer Safety Plan enrollment: \$400 per officer

Other staff within the department may need to be provided with a lower tiered plan to have access to BWC data. Criminal investigators, internal affairs personnel, records staff...etc, will

not need full access to input video into the system, but will need limited access to pull video from the system for review.

14. VieVu Current Hardware and Storage Pricing

The following is VieVu current pricing for hardware and storage licenses. The BWCs pricing is based on a bundled purchase of BWC and cloud based storage. BWC are priced higher if purchased separately from the storage bundle.

Hardware:

- VieVu BWC \$199
- Non-bundled BWC \$899.95
- 15-bay Charging/Upload Dock \$1500

| Storage Plan | VieVu Straight Shooter 25 (Local) | VieVu Solution (Cloud) | VieVu MPD (Cloud) |
|---|--|-------------------------------|--------------------------|
| Upgrade | NA | Camera upgrade every 3 yr. | |
| License/storage/device | \$25/m | \$55/m | \$99/m |
| MPLS IT system storage/device (R. McGuire, 2015) | 71.86/m | 0 | 0 |
| Extra storage | Every GB @ 6.84/year | \$00 .125 per GB per month | |
| GB include per year/BWC | NA | 60 GB/yr. | 720 GB/yr. |

Local storage: In the test and evaluation, MPD purchased the BWCs and software. MPD was able to install software on any computer/device and did not need to purchase any on-going licenses. Since the MPD BWC test, VieVu has changed its pricing strategy, including local storage options. If the Department selects a bundled plan, software will be included. VieVu's current local storage option is the Straight Shooter 25 plan. It is priced at \$25 per month per device (VieVu, *Straight Shooter 25*, 2015). Local data is also charged back to local storage provider \$6.48 per GB for every GB saved.

Fully Hosted Cloud Storage: VieVu presented two cloud storage options, each with a different pricing plan for cloud storage. The first option is the VieVu Solution. The Department can use either a fully hosted cloud solution or a hybrid cloud solution. Base storage is \$55 per month for each license (VieVu, *LE3 VieVu Solution*, 2015). Each device is allowed 60 GB per year and there are charges of \$1.50 per GB/year for overages in data accumulation/storage.

The second cloud base option is a custom plan designed with MPD's data retention and projected

data accumulation in mind. It offers a 720GB/device allowance. The details include a \$99/month per device license, free device refresh in 3 years and bundled camera purchases (K. Kiogora, July 2 2015). Data overage would be \$1.50 per GB a year. It would be highly unlikely the Department would pay any overages as allowable data is 432 TB per year. Expected cost of the VieVu MPD plan is \$730,620 for 615 devices. Although significantly higher than the other cloud storage plan, it would be a beneficial if the Department is under court order to increase retention schedules or to use BWC for every encounter.

15. BWC Plan Comparisons

| Plan | Taser Unlimited 615 BWC Unlimited (\$79) 100 Basic (\$15) | Taser Ultimate 615 BWC Ultimate (\$55/m) 100 basic (\$15) + 20 % increase per year (y2-7) | Taser Pro 615 BWC Pro (\$39/m) 100 basic (\$15) + 20 % increase per year (y2-7) | VieVu Solution 615 BWC Cloud storage (\$55/m) + 20 % increase per year (y2-7) | VieVu Straight Shooter 25 615 BWC Local storage + 20 % increase per year (y2-7) | VieVu MPD 615 BWC Cloud storage (\$99) |
|-----------------|--|--|---|--|---|---|
| | New device every 2.5 years (\$246,000 value/refresh) | | | New Device every 3 years (\$122,385 value/refresh) | | New Device every 3 years (\$122,385 value/refresh) |
| Y1 | \$601,020 | \$471,270 | \$357,653 | \$450,180 | \$714,860 | \$730,620 |
| Y2 | \$601,020 | \$484,554 | \$372,241 | \$470,106 | \$814,809 | \$730,620 |
| Y3 | \$601,020 | \$497,838 | \$386,829 | \$490,032 | \$914,758 | \$730,620 |
| Y4 | \$601,020 | \$511,122 | \$401,417 | \$509,958 | \$1,014,707 | \$730,620 |
| Y5 | \$601,020 | \$524,406 | \$416,005 | \$529,884 | \$1,114,656 | \$730,620 |
| 5Y Total | \$3,005,100 | \$2,489,190 | \$1,934,145 | \$2,450,160 | | \$3,653,100 |
| Y6 | \$601,020 | \$537,690 | \$430,593 | \$549,810 | \$1,214,604 | \$730,620 |
| Y6 | \$601,020 | \$550,974 | \$445,181 | \$569,763 | \$1,314,553 | \$730,620 |
| 7Y Total | \$4,207,194 | \$3,577,854 | 2,809,919 | \$3,569,703 | \$7,102,947 | \$5,114,340 |
| Extra data | Unlimited | \$1.50 GB per year | | | NA | \$1.50 GB per year |

| Taser Assumptions | VieVu Assumptions |
|--|---|
| <ul style="list-style-type: none"> • 615 BWC issued • Ultimate Plan = 20 GB/yr. allowance per device • Pro plan = 15 GB/yr. allowance per device • Basic Plan = 5 GB/yr. allowance per device • Officers collect 72 GB per year/device • 20% increase in data per current data retention schedule • Unlimited licenses for Prosecution. • Web Storage: extra data charged at \$1.50 per GB/yr. • 100 License to view (Detectives) | <ul style="list-style-type: none"> • 615 BWC issued. • 60 GB/yr. allowance per device (cloud only) • MPD Plan = 720 GB/yr allowance per device • Officers collect 108 GB per year/device. • 20% increase in data per current data retention schedule. • Web storage: extra data charged at \$1.50 per GB/yr. • Local storage: all data charged at \$6.84 per GB/yr. • Unlimited users (view) • 615 Straight Shooter 25 local storage plan is \$25/month per device (\$184,500/yr.) |
| *Base rates for all plans from Taser, VieVu and City IT | |

16. Expected one-time set-up and on-going expenses

| | Taser Axon | Taser Flex | VieVu Web | VieVu Local |
|---------------------|----------------|----------------|----------------|----------------|
| 615 BWC | 245,385 | 368,385 | 123,000 | 123,000 |
| Rebate/grant | -123,000 | -123,000 | 0 | 0 |
| 30 Spare BWC | 11,870 | 17,970 | 9,000 | 9,000 |
| Smart Device | 145,140 | 145,140 | 0 | 0 |
| Clips/Mounts | 12,300 | 123,000 | 6150 | 6150 |
| Dock | 154,500 | 154,500 | 61,500 | 61,500 |
| Cabling | 84,700 | 84,700 | 84,700 | 64,500 |
| Racking | 5,000 | 5,000 | 5,000 | 5,000 |
| Total | 535,895 | 775,695 | 289,350 | 269,150 |

Assumptions:

- Taser currently has the ability to pair with a smart device, VieVu does not.
- BW storage will require some type of racking or carpentry work to accommodate 100-130 BWC stored at each precinct.

On-going expense other than storage

| | Taser Axon | Taser Flex | VieVu Web | VieVu Local |
|----------------------|----------------|----------------|---------------|----------------|
| IT | 30,000 | 30,000 | 30,000 | 30,000 |
| Computers | 0 | 0 | 0 | 122,400 |
| Phone Service | 354,240 | 354,240 | 0 | 0 |
| Total | 384,240 | 384,240 | 30,000 | 152,400 |

Assumptions:

- Taser currently has the ability to pair with a smart device, VieVu does not. If a smart

phone is used rather than a Bluetooth or Wi-Fi device then there will be on-going phone bills.

- As tested, VieVu will need more computers for data management. This expense will be mitigated if the department uses 15-day multi-docking station.

17. Risks

Audit: The City of Minneapolis Internal Audit Department is detailed to identify and examine the risks involved in with the implementation of officer worn body camera program. The audit team meets bi-weekly with the BTU staff to help highlight the risks of data collection, security, storage, access and other such risks that impact the feasibility of the body camera program. Risk types are divided into categories; operational, compliance, technical, privacy, and financial. These risk types are rated medium to high.

Some areas of concerns have been identified in the test and evaluation. Storage costs, retention, privacy, policy and State data practices are topics that will need closer attention before there is further body camera deployment in the Department (W. Tetsell. March 23, 2015). Once identified, work can be done on the area of concerns before they potentially threaten the project. A full BWC audit report will be issued to Minneapolis City Council in late July 2015.

18. Community Engagement

The City of Minneapolis Police Conduct Oversight Commission (PCOC) will be hosting three public-listening sessions to solicit public comment on policy and operational aspects of the BWCs. The PCOC will be providing the department with their report in Spetember.

19. Further Study

Product: VieVu's product line has been rapidly evolving over the last six months. The company has also changed pricing strategies and recently was acquired by Safariland LLC. VieVu will still operate as a standalone company (K. Kiogora. June 29, 2015). On the horizon are software changes which will allow redaction and enhanced video data management. Bluetooth capacity to a smart device is also another option that will be available at a later date. As deployment of officers in the field becomes more mobile and less reliant on officers staging from a central local, the Department should look at the 4G Wi-Fi upload option. All these services/products will need more study before being put into action.

The camera, software and pricing options have changed since the Department began the test. It would also be beneficial to test in-production items to make a better assessment of product selection

20. Federal Grant

Grant Funding: The city has elected to submit for a federal matching grant for BWC hardware purchase. The funding opportunity came after the testing of BWC was completed. The Body-Worn Camera Pilot Implementation Program Application was submitted in June 2015 and announcement of acceptance will be made in 4Q 2015. The expectations of the grant include;

Successful applicants will develop and implement policies and practices required for effective program adoption, and will address program factors including the purchase, deployment, maintenance of camera systems and equipment, data storage and access, and privacy considerations. BJA expects the BWC programs to make a positive impact in the quality of policing in these jurisdictions and to inform national efforts to improve the use of BWCs more broadly. While BWC equipment may be purchased under this program, successful applicants must demonstrate a commitment and adherence to a strong BWC policy framework, including comprehensive policy adoption and requisite training (U.S. Department of Justice, 2015).

The Department could qualify for \$600,000 in a matching grant for BWC equipment purchases. The Department is leveraging work already done and will use the knowledge gained from its BWC test and evaluation program to satisfy the requirements of the grant (if awarded). Once an announcement is made, the Department will move forward with its plan for a full BWC implementation program.

21. Next steps

Next steps include:

- Community engagement
- BWC selection
- Grant notification
- Meet with PRC
- Contract negotiation
- Council presentations and approval
- Upgrade infrastructure
- Policy review
- Training
- Implementation
- Project monitoring
- BWC Project Review
- Cost Benefit Analysis

22. BWC Project Timetable

Below is a proposed work schedule for a full deployment of 615 BWC in Patrol. Much of the work in months 1-5 has been completed and can be leveraged to help the City if it receives a federal grant or continues on its own for full BWC deployment.

| MPD BWC Full deployment Implementation Timeline | | | |
|---|--|-----------------------|--------|
| | Deliverables | Responsible Staff | Months |
| 1 | Define scope, goals, stakeholders and objectives | Steering Committee | 1 |
| 2 | Establish work groups | Steering Committee | 1 |
| 3 | Identify projected costs | BTU/City IT | 1-3 |
| 4 | Identify possible funding sources | Finance | 1 |
| 5 | Provide project manager | BTU | 1-24 |
| 6 | Review hardware, software and storage requirements | BTU/City IT | 1 |
| 7 | Research and policy development on video storage/redaction/expungement and release | City legal/RIU | 1-3 |
| 8 | Develop policy | Policy committee | 1-3 |
| 9 | Community and stakeholder engagement | MPD administration | 1-24 |
| 10 | BWC product/vendor review | BTU/City IT | 2-3 |
| 11 | Procurement | BTU/City IT/Finance | 4-5 |
| 12 | Develop training plans | Training | 3-4 |
| 13 | Site and infrastructure development | BTU/City IT | 4-5 |
| 14 | Release policy to stakeholders | Administration | 5 |
| 15 | Training pilot officers/ courts/administration and support teams | Training | 5-6 |
| 16 | Implement pilot project | BTU/1st Pct. | 6-8 |
| 17 | Begin tracking program expected outcomes and officer performance metrics | IAU | 6-24 |
| 15 | Assess pilot and policy application, adjust as necessary | Administration | 8 |
| 16 | Expanded deployment | Pct(s). 2-5, SWAT, K9 | 9-18 |
| 17 | Administration support /monitor and compliance | BTU | 6-24 |
| 18 | Over all program evaluation | Administration | 24 |
| 19 | Report on outcomes and goals | IAU | 24 |
| 20 | Continued operation and support | BTU | TBD |

23. MPD BWC Test and Evaluation Summary

The test and evaluation of BWC demonstrates MPD staff can integrate personal worn recording devices into everyday 911 police services provided by MPD staff. The BWC are easy to use and do not compromise officer or citizen safety. Environmental conditions are negligible and do not limit the use of BWC in cold weather. Data collected can provide useful evidence for prosecution, assist in training and help resolve complaints. Digital Multimedia Evidence management software shall greatly help in the processing of the expected hundreds of thousands of videos to be copied, shared or redacted as needed. Other findings are:

Policy: BWC technology needs a strong, accountable and clear policy for use and guidance. The tested policy allows officers some latitude in turning the BWC on or off. Current BWC policy should be revised to reflect actual MPD business practices, State law and the City's expectations of service. Policy and accountability will drive data collection and retention.

Logistics: Does the City choose a BWC that fits the Department or does the Department change to fit the BWC? MPD will need to overcome some logistical considerations and install equipment in work places and squad cars to assist in the operation of a fully deployed BWC program. These modifications will prevent excessive downtime away from patrol service and limit possible overtime.

Data Collection Once collected, video data must be stored. Local BWC storage is not currently feasible for MPD. Local BWC data storage is nearly twice as expensive as a fully hosted cloud or hybrid cloud solution. Data storage providers such as Microsoft or Amazon Web services can provide cloud storage services that are cheaper, more accessible than and as secure as local storage.

Data Retention: Existing data retention policies are set by the City Clerk's Office to reduce exposure to litigation. There is no current State law that specifically addresses BWC data retention, but that does not preclude future State legislation. Both are trumped by FOIA requests to inspect any or all BWC videos. The City is obligated to retain videos under these requests until they are received or inspected. It will be physically impossible to inspect the anticipated volume of 440,000/yr. BWC videos. Unless there are legislative or state IPAD changes, an unlimited BWC data storage plan provides accessibility to the data and offsets increased costs associated with material & staff required to download video from local or cloud storage to another storage medium.

Smart devices: A smart device paired with a BWC can provide better customer service as

officers gather photos for evidence, insurance claims or needed reports. Officer can store those photos in the embedded Digital Multi-media Evidence management system in the BWC software/storage solutions. Using Bluetooth or Wi-Fi capability, officers can annotate, name and make comments to videos in the field and remain in service longer and avoid anticipated overtime costs for data entry. Using a phone will increase yearly costs by \$354,000.00.

Staffing: Adequate staffing exists for BWC administrative management, training and quartermaster duties. Exact numbers are not yet known, but the City will need more staff assigned for BWC data management in several work areas tasked with new BWC duties. Additional staff may be redirected or new-hires. The expected outcome of BWC is a reduction in complaints and use of force. The Police Department's review process, including Internal Affairs and the PCOC, will need to review many more videos. Additional staff will help them make informed determinations on complaint resolutions. MPD Records Information Unit currently handles 2,000 requests for information per week. The expected volume and content of BWC videos (440,000/yr.) requires extensive time to find, copy, review and redact for satisfaction of FOIA requests. There should be a full-time city attorney and/or a data practice manager assigned to BWC data review.

Bibliography

1. A. Brosi, (personal communication, June 24, 2015)
2. Department of Justice, Body worn pilot implementation program FY 2015 competitive grant announcement. Retrieved from <https://www.bja.gov/%5CFunding%5C15BWCsol.pdf>
3. Goff, K. (2014). *Officials report positive reviews of LAPD's on-body cameras*. Los Angeles, CA. Los Angeles Daily News. Retrieved from <http://www.dailynews.com/general-news/20140311/officials-report-positive-reviews-of-lapds-on-body-cameras>
4. D. Fowers. (personal conversation, April 16, 2015)
5. J. Hey, (personal communication, July 6, 2015)
6. K. Kiogora, (personnel communication, June 29, 2015)
7. J. Leuthauser, (personal communication, June 26, 2015)
8. Lucia, B. (2014). *Massive public records requests cause some police to hit the pause on body cam programs*. Seattle, WA. Crosscut Media. Retrieved from <http://crosscut.com/2014/11/body-cams-washington-seattle-privacy-disclosure>
9. R. McGuire, (personnel communication, June 24, 2015)
10. Minneapolis Police Department SOP. (2014). Minneapolis, MN. *MPD body camera SOP*. Retrieved from <http://www.ci.minneapolis.mn.us/www/groups/public/@mpd/documents/webcontent/wcms1p-133495.pdf>
11. Taser (2015). *Just announced: the standard issue grant program*. Retrieved from http://info.taser.com/sig.html?mkt_tok=3RkMMJWWfF9wsRogvaXMZKXonjHpfsX74uouW6a2lMI%2F0ER3fOvrPUfGjI4ATsVnPa%2BTFAwTG5toziV8R7bNKc1p3doQXhXh
12. Taser. (2015). *Priced right or agencies of any size*. Retrieved from <http://www.evidence.com/pricing>
13. Taser. (2015). *Security*. Retrieved from <https://www.evidence.com/security>
14. Taser. (2013). *Taser axon flex*. Scottsdale, AZ.
15. W. Tetsell, (personal communications, March 23, 2015)
16. W. Tetsell, (personal communications, June 9, 2015)
17. T. Wallace (personal communications, April 4, 2015)
18. VieVu. (2015) *LE3*. Retrieved from <http://www.viewu.com/viewu-products/hardware/>
19. VieVu. (2015) *LE3 VieVu Solution* Retrieved from <http://www.viewu.com/plans/plans#viewu-solution>
20. VieVu (2015) *LE3 Straight Shooter 25*. Retrieved from <http://www.viewu.com/viewu-products/software>
21. VieVu. (2015). *VieVu Solution Whitepaper*. Retrieved from <http://storage.viewusolution.com/documents/VIEVU%20Solution%20Whitepaper.pdf>

This page intentional left blank