

# Body-Worn Camera Workgroup Findings and Recommendations



*Integrity...Fairness...Service*

Prepared April 2015

THIS INTERAGENCY MEMORANDUM  
HAS BEEN CREATED FOR THE PURPOSE OF  
PROVIDING RECOMMENDATIONS DESIGNED  
TO ASSIST WITH INTERNAL DECISIONMAKING  
REGARDING POTENTIAL POLICY DEVELOPMENT.

Forward

Law enforcement personnel selflessly risk their personal safety every day to keep our citizens safe and preserve a high quality of life in our communities. Police are given great authority by citizens and must use this authority in a manner that follows our legal construct and protects every individual's rights.

Authority brings with it the responsibility to enforce laws fairly, without compromising the public trust. Our community counts on law enforcement to maintain the highest levels of honesty and integrity; without it, there can be no trust.

The Baltimore County Police Department has long enjoyed a high level of community confidence. The agency's values of **Integrity**, **Fairness**, and **Service**, have been guiding principles for decades, and we believe they have served everyone well. Our leaders have a strong belief in those values and understand the need to maintain community confidence, while providing the highest levels of service.

In achieving our mission, we take our role as custodian of community-granted resources seriously. At a time when resources are limited, we seek to provide law enforcement services as efficiently as possible, and we recognize that technology can help achieve that goal.

We also understand that technology requires careful consideration. To that end, our workgroup was formed to explore the possibility of implementing a body-worn camera program. The members of the workgroup contributed their valuable time to conduct research and to provide recommendations. We hope that these recommendations support the needs of the community and Department members alike, and that they will help us move forward in achieving our mutual public safety goals.

Major Mark J. Warren, Workgroup Chair

## Table of Contents

Executive Summary.....	6
Introduction.....	8
Background.....	11
Consideration for this Technology.....	11
Current State of the Field.....	13
Program Benefits, Challenges, and Limitations.....	16
Perceptions vs. Reality.....	16
Impact on Community Relations.....	16
Complaint Reductions and Resolution.....	18
Impact on Police Management.....	19
Impact on Case Prosecution.....	20
Financial Impact.....	21
Technological Limitations.....	22
Legal Implications.....	25
The Maryland Wiretap Act.....	25
Other Operational Considerations.....	33
Records Access and Maintenance.....	36
Additional Legal Discussions.....	39
General Policy Issues.....	42
Program Implementation.....	42
Equipment Deployment.....	42
Key Policy Components.....	44

General Deployment Guidelines.....	45
Notification Guidelines.....	46
Recording Activations, Prohibitions, and Stoppages.....	47
Officer Discretion.....	47
When Recording Is Appropriate.....	48
When Recording May Not Be Appropriate.....	50
When to Deactivate or Reactivate a Recording.....	51
Memorialization of Recording Activations and Stoppages.....	53
Review and Reporting of Recordings.....	54
Review of Recordings.....	54
Reporting of Recordings.....	56
Recording Collection, Storage, and Retention.....	57
Upload Guidelines.....	57
Labeling Recordings.....	57
Retention Guidelines.....	58
Evidentiary Implications.....	60
Data Maintenance, Management, and Analysis.....	61
Custodianship and Security.....	61
Access for Copying, Redactions, or Deletions.....	61
Quality Control and Data Analysis.....	62
Equipment Specifications and Recommendations.....	63
Human Resource Implications.....	65
Training Implications.....	65

Use in Performance Evaluation.....	67
Staffing Needs.....	68
Expected Program Cost Estimates.....	69
Community Awareness and Education.....	71
Final Workgroup Findings and Recommendations.....	73
Workgroup Position and Support Discussion.....	73
Recommended Actions Prior to an Initial Program Decision.....	76
Recommended Actions Prior to Program Implementation.....	76
Recommended Actions After Pilot Program Implementation.....	77
Recommended BWC Program Policy and Procedures.....	78
Appendices.....	80
Abbreviations Guide.....	81
References and Citations.....	85
Technical Subcommittee Report.....	90
Acknowledgements.....	128

## Executive Summary

This exploratory workgroup dedicated a great deal of time to understanding issues related to body-worn camera (BWC) technology. Workgroup members have read and critiqued the available literature on BWCs, witnessed demonstrations, met with stakeholders and intensely and thoughtfully debated the issue.

Before summarizing our conclusions, we feel it is important to remember why a national conversation about BWCs exists. What problem do we want cameras to solve?

In too many communities across the country the relationship with local law enforcement is tainted by distrust and disrespect. The last year has taught us that there still are places where citizens do not trust police to provide a complete and faithful rendering of controversial events. In such communities, the body-worn camera has emerged as a necessary tool to help create more transparent, more accountable law enforcement.

We feel confident that Baltimore County is not one of these places. Here, police *do* enjoy the trust and support of our communities – the result of a longstanding belief in transparency and the free flow of information; of commitment to a skilled, diverse workforce; and a focus on neighborhood outreach and understanding. These elements of a healthy police-community relationship are more powerful than any tool or technology. They – not cameras or any other technology - must remain the centerpiece of the mission to build and maintain trust.

This is the context in which this workgroup explored the issue of body worn cameras. We believe our Department offers the accountability that other communities want cameras to provide. At the same time, we do not take our good relationship with the public for granted. We do not presume immunity from conflict with our communities, and we are interested in new tools that may help us better serve our citizens.

We have discovered that this particular tool involves incredibly complex issues with enormous legal and fiscal ramifications. Research shows that benefits and challenges both are attached to BWC programs.

The perceived benefits include:

- Increased transparency and accountability.
- Reductions in use of force, complaints against officers, and lawsuit costs.
- Enhanced quality and efficiency of prosecution.

The potential challenges include:

- Technological limitations of the BWC equipment.
- Significant cost of equipment purchases and additional staffing; storage solutions and data maintenance; and increased public information requests.

- Loss of contact between officers and the public due to administrative requirements related to BWC usage.
- Chilling effect on the police-citizen relationship due to privacy concerns.

The workgroup concluded that at this time the cost of a BWC program outweighs the expected benefits. Even if the costs were less, the workgroup did not view BWC use as necessary or efficient at this time due to the:

- Lack of empirical data indicating systemic problems relating to use of force or complaints related to police activities.
- Lack of demand from the community for a BWC program.
- Lack of data about the true fiscal impact of BWC programs.
- Complexity of BWC use under the current Maryland Wiretap Act as it relates to oral interceptions.
- Impact of requests for BWC recordings, including the redaction process.

In meetings with community representatives, we found a lack of understanding about:

- How BWC technology works and what can be expected from the recordings.
- Implications of audio and video interceptions and the impact on privacy issues.
- The impact of broad public access to BWC recordings under the Maryland Public Information Act (MPIA).
- The short- and long-term costs of such a program.

The community representatives made it clear to us that there should be far more discussion with our communities before a BWC program is implemented. All but one representative refused to advocate for BWCs without a greater understanding of the issue; none provided any compelling reason for program implementation now.

**With this information in hand, and without a compelling need for the technology, our workgroup concluded that the decision to implement a BWC program should be delayed pending additional research and resolution or mitigation of the hurdles related to BWCs.** (Note that our agency recently instituted a voluntary pilot program involving the use of TASER cameras, and evaluation of that program will likely yield valuable information to assist with decisions related to BWC use.)

We must remember that data regarding the true impact of BWC programs is limited. This technology is relatively new and still evolving, but may become more cost-effective in the future. Legislative changes must be made to protect law enforcement agencies and officers using BWCs. The fact is that law enforcement remains tentative about BWC use; some agencies that initially embraced BWCs have retreated from or minimized BWC use after realizing the consequences.

If this agency decides to move forward with a BWC program, this exploration of equipment and policy issues will remain relevant. Additional research and testing will be necessary, but the agency would be able to pick up where the workgroup left off.

## Introduction

The Police Executive Research Forum (PERF) noted that Sir Robert Peel, founder of the London Metro Police, said “Police must recognize always that the power of the police to fulfill their functions and duties is dependent on public approval of their existence, actions, and behavior and on their ability to secure and maintain public respect.” We recognize that the community provides us legitimacy, and that their approval is conditional. Our agency must meet community expectations and do so with appropriate transparency. Baltimore County Executive Kevin Kamenetz, decided to explore the potential use of body-worn cameras to help us meet those obligations. To that end, our Chief of Police, James W. Johnson, commissioned an exploratory workgroup to examine the issue.

### Workgroup Composition and Structure

Major Mark Warren of the Criminal Information and Analysis Division was given the charge of developing and leading the Body-worn Camera (BWC) Workgroup. The workgroup was comprised of representative leaders within the Baltimore County Police Department and other key County agencies. They included:

- Mr. Scott Shellenberger                      State’s Attorney’s Office
- Sheriff R. Jay Fisher                              Sheriff’s Department
- Captain Dennis Delp                              Patrol Division
- Captain Don Roby                                  Criminal Investigations Division
- Captain Andre Davis                              Community Resources Bureau
- Captain Joseph Conger                            Technology and Communications Section
- Director Vickie Wash                              Legal Section
- Director Elise Armacost                           Media and Communications  
Section
- Lieutenant Michael Norris                       Internal Affairs Section
- Supervisor Chris Kollmann                      Forensic Services Section
- Sergeant Vincent Luther                          Planning and Crime Analysis Section
- Officer Mike Koffenberger                       Planning and Crime Analysis Section
- Mr. Robert O’Connor                              Office of Information Technology
- Mr. Chip Hiebler                                    Office of Information Technology
- Sergeant Dave Rose                               Fraternal Order of Police Lodge #4
- Sergeant Steve Comegna                          Fraternal Order of Police Lodge #4
- Corporal Kathy Greenbeck                       Fraternal Order of Police Lodge #4

This internal workgroup met weekly throughout early 2015 to begin reviewing known materials and to discuss numerous issues relating to this complex technology. Once the internal workgroup identified the key issues and developed potential policy

positions, several community representatives were invited to meet with the Chief of Police and selected members of the workgroup to discuss their concerns. This meeting took place in February 2015 and included representatives from the following organizations:

- National Association for the Advancement of Colored People (NAACP)
- American Civil Liberties Union (ACLU)
- National Alliance on Mental Illness (NAMI)
- Towson University (on behalf of Hispanic/Latino groups)
- Northwest Citizens Patrol (NWCP)

The meeting participants were provided with a technical demonstration of how BWC equipment works, and given legal clarification about what police can and cannot record under the law. During the meeting the community representatives discussed their perspectives relating to BWC use; those perspectives are noted in the “Background” section of this document.

#### Goals and Objectives of the Workgroup

The primary focus of the workgroup was to make preliminary recommendations to the Chief of Police regarding the potential use of BWCs. The Chief himself made it clear to the workgroup that no decision has been made about whether to begin use of BWCs, and that the workgroup's findings and recommendations would help shape that decision.

Due to time constraints, the workgroup adopted the following goals and objectives:

- Determine whether the agency should implement a BWC program.
- Ensure key stakeholders a voice during the research process.
- Review existing literature to ensure best practices are considered.
- Provide a legal perspective on all facets of potential program implementation.
- Provide policy recommendations that satisfy administrative and criminal investigative needs, as well as stakeholder expectations.
- Develop technical specifications that support implementation and long-term compatibility of BWC equipment.
- Provide recommendations for data collection and analysis that support program evaluation and officer accountability.

We believe we have achieved these preliminary goals and objectives. The Chief of Police will have much to consider. As other workgroups have learned, the issues surrounding BWC programs are far too complex to address in a hasty manner. Once decisions have been made on the program's future, additional work must be done, and some of those issues are addressed later in this document.

## Literature Review

Although research into the area of BWCs is somewhat limited, several recent documents were considered by our workgroup. These documents are relatively fresh and allow us to avoid having to “reinvent the wheel” on many associated issues.

Among them are:

- Implementing A Body-Worn Camera Program, PERF/COPS
- Police Officer Body-Worn Cameras: Assessing The Evidence, Michael D. White, PhD (OJP/DOJ)
- Workgroup on the Implementation and Use of Body Worn Cameras by Law Enforcement, GOCCP
- Body-Worn Cameras For Criminal Justice: Market Survey, NIJ/NLECTC

The document we most relied on is the comprehensive implementation program document authored by PERF. PERF sent BWC surveys to 500 agencies; 254 responded, giving PERF a great deal of relevant data. In addition to the survey, PERF directly interviewed 40 law enforcement chief executives who either implemented BWC programs or were considering doing so. Finally, PERF held a conference in late 2013 to discuss BWCs, including over 200 law enforcement executives and other criminal justice experts.

The information gleaned by PERF was helpful in our time-constrained effort to frame issues, understand trends, and increase our chances for success, should we decide to implement a BWC program.

In addition to those think-tank documents noted above, we also reviewed policies, concept papers, and program implementation evaluations from several agencies, including:

- International Association of Chiefs of Police
- Rialto, California Police Department
- Mesa, Arizona Police Department
- Phoenix, Arizona Police Department

Note that policies and programs from Rialto, Mesa, and Phoenix, were often cited in the aforementioned think-tank documents, as they are in this document. We also reviewed policies from other agencies. Those policies and program evaluations, as well as other documents we reviewed, are noted in the appendices at the end of this document.

## Background

### Consideration for this Technology

Like most law enforcement agencies, our Department tends to consider new technologies in an open-minded, but conservative, manner. While we have been looking at body-worn cameras (BWCs) for several years, recent events have provided a sense of urgency.

At the national level, the death of Michael Brown put a focus on policing not seen since the Rodney King incident in Los Angeles. As we know, Michael Brown was an 18-year-old African-American shot by a white police officer in Ferguson, Missouri. The officer did not have a BWC or an in-car camera, and there was no footage available from other sources. The incident sparked intense civil disobedience in Ferguson, and outrage from around the country, as citizens became more outspoken about their distrust for law enforcement and the increased need for transparency.

In Ferguson, many called for the use of cameras to record interactions between citizens and police officers. Such a recording may have been helpful in the Michael Brown case, but camera usage is not necessarily a panacea for all high-profile incidents. A good example is the New York City case of Eric Garner, another African-American who died proximate to the use of force by a white police officer. While there was plenty of good camera footage of the use of force, many still felt that the criminal justice system let them down when the grand jury chose not to indict the officer criminally after a review of all of the evidence.

So while a camera recording is not the “end all” in terms of evidence, it clearly can have an impact on perception (as discussed below). Soon after the grand jury announcements were made in the Brown and Garner cases, a shooting occurred in Berkeley, Missouri, a community neighboring Ferguson. In that instance, 18-year-old Antonio Martin, also African-American, was shot by a white police officer who had a BWC available but did not deploy it. There was footage from a business camera that, although a bit distant, seemed to support the officer’s need for the use of force. So despite the geographic proximity to Ferguson, and the chronological proximity to the grand jury decisions in the Brown and Garner cases, Berkeley did not suffer the same community reaction seen in nearby Ferguson.

Within Baltimore County, we have not had recent high-profile incidents resulting in a specific hue and cry for body-worn cameras. We believe we enjoy a good relationship with the community. Baltimore County crime is at its lowest levels in decades. Potential indicators of an erosion of trust in our community are also low. We reviewed data provided by our Internal Affairs Section for the last 10 years (2005-2014) and found that:

- Citizen-based complaints for the last five years were lower than the 10-year average, and the number of complaints during 2014 was the lowest of the decade.
- Sustained findings in citizen-based complaints dropped from a 15 percent average from 2005-2007 to less than six percent from 2008-2012. (2013-2104 data is incomplete but equally promising.)
- Administrative-based complaints for six of the last seven years were below the 10-year average, and the number of such complaints during 2014 was the lowest of the last decade.
- Excessive force complaints for four of the last five years were below the 10-year average, and the number of such complaints during 2014 was the lowest since 2005. Note that fewer than one percent of these complaints were sustained.
- Use of force (UOF) incidents for both 2013 and 2014 were lower than the 10-year average, and the number of incidents during 2014 was the lowest since 2006.
- Police-involved shooting incidents for six of the last eight years have been below the 10-year average, and the numbers of incidents in 2014 was equal to or lower than seven of the other nine years.

We also reviewed our complaints to determine the number that would be considered race-based, although this is a highly interpretive effort. The term “race-based” is somewhat subjective, as is the application of that term against the context of the alleged complaints. Complicating matters, the computer system used to track cases and extract data was replaced halfway through the last decade, making it impossible to do comparative data analysis. In the context of these limitations, however, we found that in six of the last 10 years, fewer than 10 race-based complaints were filed. More importantly, only two cases of a race-based nature were sustained against officers in the last decade. None of this data indicates that our agency is systemically acting improperly in terms of general performance or use of force. Further, it does not appear to demonstrate a compelling need to implement BWCs for oversight purposes.

Despite these promising statistics, our agency has seen protests at the local level, both within the County and in the surrounding jurisdictions. Some communities are voicing their demand for more transparency from their law enforcement agencies, and the use of BWCs may be a way to move towards that goal. The Howard County Police Department report cited a survey done by a private company, Brickhouse Security. In the survey, almost three-quarters of respondents felt officers should use BWCs, and over 80 percent felt that filming of interactions was not an invasion of privacy and that it would prevent the use of excessive force by police. In addition, a recent Daily Beast article reported on surveys done last December by CBS (Columbia Broadcasting System) and the Washington Post that found citizen support for BWCs at 91 percent and 86 percent, respectively.

As noted earlier in this document, we met with some community representatives to get a better sense of the local perception of body-worn cameras and their impact on communities. After briefs on associated legal and technology issues, we spent almost

two hours discussing BWC program implications. Much of the discussion related to legal issues, and the ACLU representative shared his experiences as a participant in the Baltimore City BWC program initiative. During the meeting the representatives noted several things:

- Little outreach had been done to their organizations or constituents regarding the impact of BWC use.
- It was a far more complex issue than they had originally thought.
- The participants leaned towards citizens having discretion to request the camera be turned off in sensitive situations or in areas with an expectation of privacy, rather than leaving officers with that discretion.
- An announcement of recordings was preferred.
- There was concern that language barriers and cultural competency could affect a citizen's decision to allow recording.
- They had little understanding of the impact of public information laws and access to recordings.

The participants felt that many of the issues still needed to be fleshed out and that there should be additional discussion directly with the community about the potential impact of the program. One issue is the fiscal impact on the community, which we were not able to discuss in depth due to time constraints. Interestingly, by the end of the meeting, most of the participants would not take an official position about whether we should move forward with the BWC program due to the complexity of the issue, but they definitely wanted more opportunity to discuss it.

The impact of the public's perception of the need for BWCs has seeped into political opinion and activity. As a result we see more potential for federal, state, and local legislation. For example, the website RollCall.com recently reported that Congressional representatives might put forth a BWC bill. Even President Obama weighed in on BWCs, asking Congress for \$75 million in grant funding for BWC equipment purchases and program implementation.

Regardless of public perception, the reality is that there are potential positives and negatives in using such a technology. Those benefits and limitations need to be part of future discussions with the community and may re-shape citizen perceptions. We discuss those issues in greater detail later in this document.

### Current State of the Field

Needless to say, a great deal of technology is available to law enforcement. Law enforcement uses TASERs, in-car vehicle cameras, closed circuit television (CCTV), license plate readers – the list goes on and on. Law enforcement always looks to use technology to accomplish our mission in a more efficient manner.

Scott Greenwood of the American Civil Liberties Union (ACLU) is a frequent guest at law enforcement think-tank conferences. According to PERF's study, Greenwood

seems to feel that the use of body-worn cameras is inevitable. Citizens can easily record events on phones and there are fixed cameras at more public locations than ever, so it makes sense that police officers should record citizen interactions from their own perspective.

The ACLU now has a smart phone application called “Police Tape,” to make it easier for citizens to record interactions with police. Such recordings appear to occur more frequently. A citizen-initiated recording during a police interaction with our agency made the news just last year. In that instance, an Auxiliary Team member attempted to stop a citizen from recording the interaction; the recording went viral and received national attention, most of it negative.

Even if law enforcement does not want to embrace BWCs, we might not have a choice. Courts appear to be looking at BWCs as an answer to “stop and frisk” allegations against agencies. In the State of New York, for example, a judge recently ordered the local police to begin wearing BWCs to prevent racial profiling. According to White, the decision has been temporarily stayed by a federal appeals court, but we could see more legislation from the bench.

So Greenwood’s position may be right; BWC use may be inevitable. Although our agency has not implemented a BWC program, at the time of this report we have implemented a pilot program for the use of TASER-mounted cameras. While TASER cameras may assist us in certain use of force situations, they will not capture the vast majority of our interactions with citizens.

That being said, the use of BWCs is a relatively new phenomena. Unlike the in-car camera, BWCs didn’t become particularly relevant until about a decade ago. In 2005 the United Kingdom (UK) introduced the concept via a small pilot study. Within a few years, over 40 UK areas had them in use.

Here in the United States the Rialto Police Department in 2012 did one of the first well known domestic studies of BWCs. Two years later, the Associated Press stated that about one in six law enforcement agencies used BWCs. Such use appears to be growing. In November 2014, digital news media source “Vocativ” claimed to have reached out to police agencies in the 100 most populous cities in the United States. Vocativ found 41 agencies in which at least a portion of their officers used BWCs; 25 others have plans to do so. Only 30 agencies claimed to have no plans to use BWCs, but that may be changing since the federal government announced that millions of dollars in grant money may be available for agencies to purchase them.

So at the national level, it appears that the use of BWCs may be gaining momentum. For example, the Los Angeles Police Department recently announced that it would purchase 7,000 BWCs for its personnel. Some larger agencies already using body-worn cameras include Oakland, Dallas, Denver, Detroit, and Miami.

That does not mean every law enforcement agency is sold on the idea. When PERF issued its survey in July, 2013, over 75 percent of the respondents indicated they did not have a BWC program at that time. There is no indication that PERF interviewed those agencies to determine why. There are many different reasons why agencies have been slow to implement BWC programs. In our research we found that in:

- Auburn, Washington the Police Department is avoiding BWCs due to the impact of public information requests generated from use of in-car cameras.
- Grand Rapids, Michigan, the Chief of Police has several concerns related to the constant filming of officers and citizens.
- Riverside, California the sheriff's union is suing to stop BWC use, arguing it is a negotiable term and condition of employment.
- Wichita, Kansas, they have considered selling, or at least grounding, a helicopter to pay for the BWC program.
- Berkeley, California, officers spend about 30 minutes per shift handling the recordings – the annual equivalent of the cost of five full time officers.
- Minnesota there is a state representative pushing a bill to keep BWC footage private; he is an ex-police officer.

In Maryland, we have not seen a great deal of use of BWCs, but we are aware that some agencies are considering them. We surveyed 98 Maryland agencies with the primary responsibility for law enforcement in their jurisdiction. We found that 18 of the 98 currently use a BWC, but many more are considering the technology. This ratio of BWC use at the state level mirrors the AP position that about one in six agencies use BWCs nationally.

The Baltimore City Police Department does not yet have BWCs but is looking seriously at them. The AP recently reported that Mayor Stephanie Rawlings-Blake initially “vetoed a proposal that would have required officers to wear cameras because she didn’t believe the costs and other details were adequately considered.” In part it may have been the “\$2.6 million a year for storage and the extra staff needed to manage the video data.” Nonetheless, she recently stated that she hopes to have BWCs in use by the end of the year.

For those in Maryland who do use BWCs, many just started their programs, and three of the 18 agencies consider themselves in a pilot phase. It is worth noting that most of the 18 agencies using BWCs tend to be smaller in size, serving less populous communities. That is not surprising; the smaller the size of the technology deployment, the easier it is to finance and implement the deployment in a controlled fashion.

## Program Benefits, Challenges, and Limitations

The benefits, challenges, and limitations of body-worn cameras (BWCs) have been written about at length in several research documents. Many of the concepts will be universal and will have an impact on any agency implementing a BWC program, regardless of size or type. Despite the fact that these concepts have been covered *ad nauseam*, we felt it necessary to restate them as a starting point for program consideration.

### Perceptions vs. Reality

In a review of program implementation evaluations, the use of BWCs appears promising, but not without cost in terms of social and financial capital. The think-tank documents we reviewed frequently cite the program results in Rialto, California; Mesa and Phoenix, Arizona; and two agencies in the United Kingdom. The results indicate many perceived benefits from the use of such technology. There have also been challenges noted as well and, in an attempt to manage expectations, we discuss these issues below.

Outside of program implementation evaluations, the use of BWCs generally has been viewed more positively than negatively, in part due to the significance of the perceived benefits. In a recent study, GOCCP noted that BWCs have the potential to enhance public safety and improve relations between police and members of the public by reducing misconduct, facilitating resolution of incidents, and improving officer training. GOCCP cited broader potential advantages such as enhancing public confidence in the criminal justice system and reducing exposure to civil liability. Despite this common viewpoint, there are challenges that need to be considered.

Note that many of the documents we reviewed have a section dedicated to “perceived benefits” and a separate section for challenges or limitations. We found that many of the benefits and challenges were frequently interrelated via common threads such as community relations or prosecutorial impact. Below, we have chosen to present these issues from the perspective of those common threads so the pros and cons of each issue can be weighed against each other; this is an informal cost/benefit analysis, if you will. The only exception is technical limitations, discussed at the end of this section.

### Impact on Community Relations

In general, the sources we reviewed claimed that the use of BWCs would improve the relationship between law enforcement and the community. They cited better behavior by citizens and officers, as well as increased transparency as the reason for that improved relationship.

With regard to behavioral changes, PERF concluded that when the parties know they are being recorded, everyone tends to conduct themselves better. White, in his study, noted that there was not much research about citizen perceptions of BWCs, but an early UK study found that over two-thirds of the crime victims surveyed believed that the use of BWCs was beneficial to their interactions with police. That study also noted that during interactions with police over 80 percent of crime victims felt safer because of the presence of a BWC. All in all, the sentiment is that cameras produce better behavior, which leads to increased police accountability and increased trust in the police by citizens.

From a transparency standpoint, PERF stated that BWC use provides more accurate documentation of interactions between police and the community. The GOCCP study noted that BWC use goes beyond transparency - in that it provides “clarity” to citizen encounters such as “stop and frisk” events, field interviews, and even arrest situations. White goes on to add that increased transparency results in police “legitimacy.”

Giving citizens greater access to police recordings also increases transparency. Various state and federal laws regulate access to public information. Interest in recorded information is likely to be greater than ever.

The GOCCP study provided an overview on the Maryland Public Information Act (MPIA). Some key issues related to the MPIA are discussed in the “Legal Implications” section of this document, but it is worth highlighting a few things here. The MPIA clearly states that public records include films and recordings, and that public access should occur without unnecessary cost and delay. Some recordings may be held back if clearly connected to an active investigation, but many will have to be made available at some point.

As other jurisdictions have found, attempting to increase transparency via public access to recordings can be extremely costly and time consuming. One reason is the demand for the recordings themselves; broad requests are often made, requiring a great deal of human resources to review and redact the recordings in accordance with law and policy. The other reason relates to the data tied to the recordings; the community will expect empirical analysis of the BWC program, and will make similar requests to access that data.

The recording collection and data analysis that comes with such a program presents other issues. The GOCCP study noted that the public may be wary of law enforcement-compiled information, viewing this as “Big Brother” oversight for such purposes as facial and voice recognition. The public recently expressed similar fears about license plate reader (LPR) technology and the retention period for the data. While the early purging of LPR data might reduce such concerns, there could be a negative impact on our efforts, as the recordings and data may be necessary for use as evidence in criminal investigations. Even in non-evidentiary settings, what an officer was or was not doing at a particular time may be crucial to a claim, so the retention of the BWC recording in that situation may still be important.

Beyond oversight concerns, the use of a BWC may have a chilling effect on citizens' willingness to speak with police officers. The GOCCP study cited the "officious and legalistic tone to police/citizen interactions" as the reason. Agencies may need to strike a balance in BWC use so it does not interfere with efforts to gather useful intelligence. This was a concern in Oakland and Mesa, where the lack of officer discretion with regard to recording undermined information gathering efforts. Policies need to be developed to allow for a continued free flow of information. In the end, the GOCCP study indicated that the potential benefits of the BWC outweighed the concerns and that community surveys and participation in implementation of the program might help curb those concerns.

### Complaint Reductions and Resolution

Most documents cited the potential for reduction and resolution of complaints, including use of force incidents, as a significant benefit of BWC use. With regard to complaint reduction, the IACP cites a study noting that in some instances, citizens opted against filing a complaint once they knew a recording existed. Mesa's study found officers using a BWC experienced 40 percent fewer complaints than those without; similar results were found in Rialto, which used a control group for validation. In addition, White found that even when a complaint is filed it tends to be less frivolous when a BWC is present.

White and the IACP also found the BWC extremely useful in resolving citizen complaints. As GOCCP noted, investigation of citizen complaints are often credibility issues involving the word of the officer against that of the citizen. BWC recordings may provide "clarity" and "objectivity" to the situation and even help investigators ask better questions of the parties involved, leading to a quicker resolution.

This concept of complaint reduction and resolution extends to use of force (UOF) incidents, which tend to be more serious from the perspective of both the community and law enforcement. Rialto found that the officers using BWCs had half as many UOF incidents as those without BWCs. Mesa saw a 75 percent reduction in UOF complaints during their pilot study. In Maryland the Laurel Police Department reported a 30 percent UOF reduction since beginning a BWC program. While these findings are promising, such lofty expectations must be tempered by contextual differences. For example, our agency has roughly 18 times more sworn personnel than Rialto and we have different policies and procedures. Considering that our UOF rate is roughly one-quarter that of Rialto, it is unlikely that we would see similar reductions in UOF.

PERF concluded that BWCs provide protections for officers who conduct themselves properly, but generate a large number of complaints due to a high level of activity or frequent contacts. They also found that in most cases BWCs support the officers' accounts of events. The Oakland Police Department echoed this, finding that in the overwhelming majority of cases the footage indicated the officers' actions were appropriate. So more often than not, the recordings help to exonerate officers. But

even when recordings are used to hold officers accountable, as GOCCP noted, such use should facilitate “faster and more effective” complaint resolution that benefits all parties.

### Impact on Police Management

Management’s ability to use resources and technology effectively is crucial to serving the community. As GOCCP noted, there is no evidence to indicate that use of BWCs would reduce productivity; indeed, BWCs may increase efficiency.

One efficiency issue is the impact on police performance. The IACP’s position is that BWCs can help evaluate officers’ performance in “a more complete and fair manner.” There is a belief that random auditing of recordings may identify potential problem areas or training deficiencies for correction; it also provides an opportunity to observe our officers doing things right. While some view such an audit as a “fishing expedition,” GOCCP feels management needs to be able to review performance, especially if an officer has a history of prior citizen complaints.

As noted above, training deficiencies may also be identified by recording review. PERF felt that review of the recordings would be a useful training tool; White, however, noted that more research needs to be done about the effectiveness of BWCs as training tools. Nonetheless, White noted that the Miami Police Department has been using BWCs since 2012 at its Training Academy; BWCs are used as training tools in the UK as well.

There could certainly be a benefit to using BWCs at the Academy and at in-service training, and for remedial training involving ongoing performance issues. In any setting, the opportunity for an officer to review the recording and get immediate feedback from an instructor or supervisor could be valuable. BWC recordings would be an important tool in scenario-based training by giving officers the perspective of both the third-person (instructors) and their own.

BWC training would also provide an opportunity to educate officers about safety issues related to BWC use. There are safety concerns about the actual wearing of the body camera. For example, some felt that BWCs worn around the neck could cause an injury due to the weight of the camera. Such hazards can be mitigated to increase safety, and educating the officers on those concerns is crucial.

Conversely, officers need to know that BWC use likely will improve their safety. Officer safety should improve if hostilities between the police and citizens decrease. The UK study implied that BWC wearers were only one-third as likely to be assaulted as those who did not wear BWCs. If management can mitigate the concerns of officers and if BWCs are used effectively, we can expect officer injuries to decrease, along with time lost and money spent on absenteeism due to the injuries.

It is important to note that BWC programs carry the potential for a chilling effect on the relationship between officers and management. As discussed above, some officers

may fear BWCs will be used for fishing expeditions to identify inappropriate behavior, or that the recordings will be used to constantly second-guess the officers' actions. If officers view BWCs that way, they may avoid engaging citizens. The GOCCP report noted that the "same argument was raised with respect to the use of dashboard cameras, but there is no data to show that the presence of the dashboard cameras reduced police productivity." To address this issue, agencies have been using a collaborative approach to implement their programs, and that approach shows promise.

Finally, management must be aware that the use of BWCs may be a collective bargaining issue. The IACP noted that the police union in Las Vegas threatened to sue the department because use of the BWCs constitutes a change in working conditions. This also became an issue of "meet and confer" in San Jose, California, and likely has affected other jurisdictions implementing BWC programs.

### Impact on Case Prosecution

There is a strong belief that having BWC recordings available for court will enhance the quality of prosecution cases, and speed up case resolution. The IACP noted that there are few things as compelling as having the judge or jury seeing the suspect and hearing his or her own words. They indicated that recordings made at scenes can provide investigators, prosecutors, and juries with "detailed, accurate, and compelling evidence." GOCCP's study cited a survey of prosecutors that found that 96 percent improved their ability to prosecute cases when in-car camera footage was available; one expects a similar result with BWC usage.

The GOCCP study went on to say that recordings would help prosecutors better evaluate the credibility of witnesses and case resolution options. The IACP added that prosecutors surveyed found "the greatest value of video evidence is its ability to refresh the officer's memory and to verify the accuracy of written reports and statements." White and others noted that recordings would improve evidence documentation for specific situations such as domestic violence cases and accident scenes.

Cases involving BWC use could also be resolved more quickly. White noted that studies in the UK show that cases with accompanying BWC evidence were 70 to 80 percent less likely to go to trial than similar cases without BWC evidence. If the BWC can help resolve cases short of trial, it follows that there would be reductions in "police overtime for court appearances and...pending case backlogs in the courts," as noted by GOCCP.

The use of BWCs has an impact on discovery, especially with respect to the challenge of making Brady material available to the defense. The GOCCP study noted that it is much easier to review documents for relevant material than recordings. Decisions would have to be made about who would search the recordings for exculpatory information; it could fall to court personnel, prosecutor's offices, or the police officers involved in the case. Either way it becomes "labor intensive and expensive" to conduct such a search. GOCCP suggested a solution – having the recording officer somehow

tag segments of the recording for the prosecution. But even that takes time, and we are unsure if that is technically possible.

That cost of time and money also extends to redactions, as noted in the “Community Impact” section of this document. The issue here, however, would be editing required as part of defense motions, victim or witness safety issues, or orders from the court. The prosecutor’s office would likely be required for redacting discovery and court recordings without assistance from court or police personnel.

### Financial Impact

As mentioned earlier, implementation of a BWC program comes with a great cost, and some of that is discussed in other areas of this document. It is worth noting that PERF reported that 39 percent of survey respondents who did not use BWCs cited cost as the primary reason.

The cost of such a program includes one-time costs, such as the initial purchase of equipment, and long-term costs such as staffing and recording storage solutions. Evidence indicates that BWCs are less expensive in comparison to in-car cameras, but as PERF noted, many of the law enforcement agencies consulted for the study still spent between \$800 and \$1,200 per camera.

The cost of storage solutions can be “crippling” according to Chief Aden of the Greenville (NC) Police Department. One PERF respondent reported spending \$2 million per year in recording storage solutions for 900 cameras. Unfortunately, there is not much long-term data on the costs of storage solutions, but enough evidence exists to show that the costs are substantial.

The cost of staffing to handle BWC program requirements - such as coordinating information requests, making copies of recordings, and redactions of recordings - could be far more than agencies have anticipated. That last task, the redaction of recordings, may be extremely costly. As the GOCCP study noted cameras are still new technology, and there is no way to know how expensive redacting will become in the future.

There are other potentially significant costs such as overtime expenses related to report writing. As the Phoenix evaluation found, the use of a BWC does not save time on reports because officers have to review the recordings to ensure the written reports are accurate. We must also be concerned about unfunded mandates from well-intentioned legislatures.

On the other hand, there are potential areas for cost savings, such as shorter retention periods for recording storage, less overtime for court appearances, and even linkages from the BWC to the records management system to auto-populate report information, saving officers time during the recording upload.

But the largest savings may be through better risk management and the expected reduction of civil liability.

Multiple sources noted the likelihood of such reductions, and White cited a 1995 study of in-car cameras in which such reductions were realized. With evidence that BWC usage has reduced use of force incidents and misconduct complaints, such savings could be significant. There could be fewer lawsuits, and even when lawsuits are filed, they may be resolved more quickly, with less expensive settlements or damage awards. Fewer complaints could allow a resultant reduction of staffing in our Internal Affairs Section providing additional cost savings. If a BWC program were implemented here in Baltimore County, the real costs associated with the BWC program should be compared to the historical costs the jurisdiction has paid out in civil judgments over the years.

It is possible that failure to implement a BWC program could expose the jurisdiction to more risk. In the Mesa program evaluation, there were concerns that failure to adopt accessible technologies like BWCs could result in a greater risk of civil litigation and liability; whether these concerns are valid remains to be seen.

### Technological Limitations

There are many commentaries about the technological limitations of BWCs. It is important that they be discussed to mitigate the “CSI Effect.” Many citizens, especially those who serve as jurors, feel forensic techniques should solve every crime in a rapid manner. They may believe that BWCs will explain every facet of an interaction; some law enforcement officers may believe that as well.

We know that there are limitations to any evolving technology; we have summarized many of them below. Most of this material comes from the Force Science Institute, a research body focusing on the use of force by police officers. In 2014 they published a newsletter that outlines 10 limitations of BWCs. Dr. Bill Lewinski, executive director of the Force Science Institute, notes that in law enforcement interactions “[BWCs] can't provide all the information needed to make a fair and impartial final judgment. There still may be influential human factors involved, apart from what the camera sees.” To that end, we've listed those 10 limitations below, much of it taken word-for-word from the newsletter.

- *A camera doesn't follow the individual's eyes or see exactly as they see.* Cameras track broadly but can't document what an individual sees in a given instant. There is a visual perception disconnect between the individual's field of view and that of the camera. Simply glancing away can drastically change what might be occurring “right before one's eyes.” In addition, the impact of physiological and psychological stress may result in one's brain suppressing some incoming visual images that seem unimportant in a life-threatening situation.
- *Some important danger cues can't be recorded.* For example, “resistive tension” may be sensed by the officer and acted upon as a preemptive measure, but on camera it may look like the officer made an unprovoked attack, because the

sensory cue you felt doesn't record visually. In addition, the officer's prior knowledge and experience may heighten that sensitivity to those cues, but the camera cannot interpret that.

- *Camera speed differs from the speed of life.* BWCs often record at high speed but it's theoretically possible that something as brief as a muzzle flash or the glint of a knife blade that may become a factor in a use of force case could still fail to be recorded. This is also affected by the individual's reaction time which will certainly be slightly behind the event as it unfolds. In review of the recording, the reaction time must be considered; without doing so the reviewer is not likely to understand how an officer can unintentionally end up firing additional shots after a threat has ended.
- *The camera may see better than the individual in low light.* The high-tech imaging of BWCs allows recording with much better clarity in low-light settings, so the camera recording may provide elements of the scene in sharper detail than the individual would perceive at the time the BWC was activated. So in dim light, the officer becomes more dependent on context and movement in assessing and reacting to potential threats. In that environment, a suspect's posturing will likely mean more to the officer at the time than some object the suspect is holding. This would mean that whether the suspect was holding a cell phone versus a gun may not be as evident to the officer in real time as it is during a review of the recording. Conversely, the transition from high light to low light situations (or vice versa) may result in the camera temporarily blocking images altogether.
- *The officer's body may block the view of the BWC.* This may be dependent on the officer's location and angle, such as when officers "blade" their stance for safety purposes. Critical moments during an event that the officer may see could be missed entirely by the BWC, obscuring what a reviewer may need to see to make a fair judgment.
- *Cameras only record two-dimensionally.* BWCs don't record the depth of field that the naked eye may see, so judging distances in footage may be difficult. Without a proper sense of distance, a reviewer may misinterpret the level of threat an officer was facing, making the officer's use of force seem inappropriate.
- *The absence of sophisticated time-stamping may prove critical.* Time-stamping is sometimes measured minute by minute, but to fully analyze and explain an officer's perceptions, reaction time, judgment, and decision-making it may be critical to break the action down to units of one-hundredths of a second or even less. A reviewer's ability to see how quickly suspects can move and how fast the various elements of a use of force event unfold can change their perception of what happened and the pressure forcing officers to act.
- *One camera may not be enough.* With more recordation of a use of force event, there is a greater likelihood that uncertainties may be clarified. What looks like an egregious action from one angle may seem perfectly justified from another. The example of multiple camera use in the National Football League (NFL) tends to validate this position. Ideally police officers deserve the same consideration.
- *A camera encourages second-guessing.* This despite the landmark use of force *Graham v. Connor*, where the Supreme Court noted that "an officer's decisions in

tense, uncertain, and rapidly evolving situations are not to be judged with the '20/20 vision of hindsight." The officer has to assess what he was experiencing while it was happening and under the stress of his life potentially being on the line. That disparity can lead to far different conclusions for a reviewer.

Conversely, officers should be allowed to see their recordings and others taken at the scene but only for informational purposes; not to supplant a firsthand memory of the incident.

- *A camera can never replace a thorough investigation.* A recording should be weighed and tested against witness testimony, forensics, the involved officer's statement, and other elements in a fair, thorough, and impartial investigation that takes human factors into consideration. The recordings have great value, but should not be given undue, if not exclusive, weight in the judgment of an officer's actions.

While these limitations are significant, the law enforcement value of recordings may justify efforts to educate the public and the police regarding the capabilities and limitations of BWCs.

## Legal Implications

### Legal Implications of Body-Worn Cameras

The first issue is whether a body-worn camera (or any piece of equipment with video and audio capability), which is used to intercept the images of and words spoken between a law enforcement agent and a citizen(s), violates Title III of the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510 et seq. (hereinafter “Title III”) or Maryland Annotated Code, Courts & Judicial Procedures Article §§ 10-401 et seq. (West 2014) (hereinafter “Wiretap Act”)?

The US Constitution, and more specifically the Fourth Amendment, constrains electronic surveillance by the police and other government agents. See *Katz v. United States*, 389 U.S. 347, 88 S. Ct. 507, 19 L.Ed.2d 576 (1967)(electronic surveillance of pay telephone by FBI was search and seizure subject to Fourth Amendment standards; “the Fourth Amendment protects people not places”).

However, whereas the Fourth Amendment does not constrain the actions of private individuals, the Wiretap Act constrains *any* individual - citizen and law enforcement officer alike.

### The Maryland Wiretap Act

There are 12 states that have wiretap statutes similar to Maryland (California, Delaware, Florida, Hawaii, Illinois, Kansas, Massachusetts, Michigan, Montana, New Hampshire, Pennsylvania, and Washington).

The exact language of the Maryland statute, in pertinent part, is:

- Except as specifically authorized in the statute, *an individual* may not “willfully intercept...or endeavor to intercept, any wire, *oral* or electronic *communications*.” Md. Code Ann., Courts & Judicial Procedures §10-402(a)(1) (West 2014) (emphasis added).
- Further, it is unlawful to willfully use or disclose the contents of communications obtained in violation of the Wiretap Act. § 10-402(a)(2)-(3).
- Thus, illegally obtained communications will also be excluded from any court proceeding. § 10-405.

The Wiretap Act defines “oral communication” as “any conversation or words spoken to or by a person in *private* conversation.” § 10-401(13)(i) (emphasis added). The term “private conversation,” however, is not defined in the Wiretap Act. The ultimate question then becomes - what constitutes a private conversation?

## *Lawful Interception*

The Maryland Wiretap Act requires that all parties consent to the interception of the oral communication (also referred to as “two-party consent”). Cts. & Jud. Proc. § 10-402(c)(3). This is one feature of the Maryland Wiretap Act that is more protective of privacy than its federal counterpart, Title III, which permits one-party consent for the purpose of interception. 18 U.S.C.A. § 2511(2)(c)–(d) (West 2014).

There is, however, an enumerated crimes exception in the Wiretap Act that allows for the interception of a communication when there is one-party consent, pursuant to the investigation of certain crimes: murder, kidnapping, rape, sexual offense in the first or second degree, child abuse in the first or second degree, child pornography, gambling, robbery, a felony under Title 6, Subtitle 1 of Criminal Law Article (e.g., arson, burglary), bribery, extortion, dealing in a controlled dangerous substance, a fraudulent insurance act, an offense related to destructive devices, a human trafficking offense, sexual solicitation of a minor, obstructing justice, sexual abuse of a minor, abuse of a vulnerable adult, a theft scheme over \$10,000, conspiracy or solicitation of the above described offenses, and a barricade situation involving hostages. Cts. & Jud. Proc. § 10-402(c)(2). The enumerated exception is not likely to be applicable to the vast majority of law enforcement encounters with citizens on a daily basis.

Further, there is also a statutory carve-out, commonly referred to as the “dash cam exception,” that was added to the Wiretap Act in 1991. This provision relates specifically to a police officer who audio records as part of a video recording while lawfully detaining a vehicle in the course of a criminal investigation or traffic enforcement. Although a vehicle detention is undoubtedly a *public* encounter between a police officer and an individual, the dash cam exception requires the officer to identify himself as a law enforcement officer before initiating an interception, and inform all parties that the recording is being made as part of a video tape recording at the beginning of the interception. Cts. & Jud. Proc. § 10-402(c)(4). It is important to note that this “identify and announce” provision does not require, however, that the law enforcement officer obtain consent to the recording.

Notably, again in 2008, the General Assembly crafted another exception to the Wiretap Act. Section 2-403 of the Criminal Procedure Article exempts from the provisions of the Wiretap Act the audio or audiovisual recording of a custodial interrogation of a criminal suspect made by a law enforcement unit. Unlike the dash cam exception, there is no requirement that the law enforcement officer identify himself as such, announce the recording, or obtain consent to the recording.

It is critical to recognize that the General Assembly was, in the past, inclined to legislate two very specific exceptions to enable police to intercept both audio and video of an oral communication with a private citizen, when both of the exceptions would seemingly capture conversations that could not be less private (vehicle stop, which would occur on a public thoroughfare; custodial interrogation, which would occur between a law enforcement officer who advises the defendant that anything he says will be used

against him in court). **Therefore, it seems prudent to have unequivocal legislative authority before moving forward with a body-worn camera program.**

### *Consequences for a Wiretap Act Violation*

In addition to the exclusion of evidence, a Wiretap Act violation carries the potential risk of criminal and civil penalties. It is important to note that for purposes of the Wiretap Act, the “willful” interception of an oral communication does not require knowledge on the part of the officer that his action is unlawful. *Deibler v. State*, 365 Md. 185, 776 A.2d 657 (2001). The penalties are as follows:

- Criminal – felony carrying a penalty of up to five years and \$10,000 fine. Cts. & Jud. Proc. § 10-402(B).
- Civil – award for actual damages, but not less than liquidated damages computed at the rate of \$100 a day per violation, punitive damages, and reasonable attorneys fees and litigation costs incurred by the individuals whose communications were intercepted. Cts. & Jud. Proc. § 10-410.

### *Evaluating Oral Communication*

As previously stated, the Wiretap Act defines “oral communication” as “conversation or words spoken to or by a person in private conversation,” but fails to further define the term “private conversation.”

It goes without saying that police encounters with citizens are subject to occur virtually anywhere, to include a public street, a public park, a neighborhood bar, a person’s home or apartment, or a private or public business. The types of police encounters run the gamut from a simple neighborhood business check, a call for service, a witness interview, a field interview, a *Terry* stop, service of a search and seizure warrant, to a hostage barricade, etc.

This begs the question: during a police encounter (other than a traffic stop), do the words exchanged between the officer, subject(s), and anyone else present, constitute “private conversations” that trigger the protections of the Wiretap Act, such that intercepting them would be a violation?

If these conversations are indeed deemed “private,” the Wiretap Act would require the consent of all parties in order for the officer to lawfully obtain an audio recording using a body-worn camera.

Arguably, since the statute fails to define “private conversation,” without a clear legal definition or an explicit Wiretap Act exemption, the law enforcement officer would be placed in the untenable position of determining whether a particular verbal encounter is a private conversation. Simply identifying himself as a law enforcement officer and announcing the audio recording would likely be insufficient to comply with the Wiretap

Act, as the statutory carve-out exception for vehicle stops would not apply to these types of encounters.

In light of the vaguely defined terms (“oral communication” and “private conversation”) in the Maryland Wiretap Act, Maryland courts have construed “oral communication” to incorporate the reasonable expectation of privacy (REP) standard, set forth under the Fourth Amendment of the U.S. Constitution. *Fearnow v. Chesapeake & Telephone Co. of Maryland, Inc.*, 342 Md. 363, 376, 676 A.2d 65, 71 (1996). The seminal case concerning REP is the Supreme Court case, *Katz v. United States*, wherein Justice Stewart opined in the majority opinion, “What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment analysis.” 389 U.S. 347, 351, 88 S. Ct. 507, 511, 19 L.Ed.2d 576 (1967).

### *Two-Part Reasonable Expectation of Privacy (REP) Analysis*

In order to invoke the protections of the Wiretap Act, at least one of the parties must have a reasonable expectation of privacy (REP) in the intercepted communication. There is a two-step analysis for determining whether a speaker has a REP in relation to particular communication:

- Subjective expectation - First, the speaker must exhibit an expectation that his words are being conveyed in private. If not, the inquiry ends, and the communication is not protected by the Wiretap Act. *Katz*, 389 U.S. at 361, 88 S.Ct. at 516.
- Objectively reasonable - Second, the speaker’s subjective expectation of privacy must be objectively reasonable under the circumstances. Said another way, society must be willing to protect the communication as private. Otherwise, notwithstanding the speaker’s subjective expectations, intentions or desires, the communication may be lawfully intercepted without a warrant. *Id.*

The question then becomes, under what circumstances is an expectation of privacy objectively reasonable? In general, conversations conducted in a private location are presumed to be private. When a person is in his own home, that fact alone raises a reasonable inference that he intends his conversations to be private. *Malpas v. State*, 116 Md. App. 69, 84, 695 A.2d 588, 595 (1997). Similarly, conversations are not considered private when they are conducted in a location accessible to the public or open to public view. See *Gibson v. State*, 138 Md. App. 399, 771 A.2d 536 (2001) (Police observations of defendant during their early morning surveillances did not implicate in any way any Fourth Amendment protection enjoyed by burglary defendant; in those wee morning hours, defendant voluntarily conveyed to anyone who wanted to look his suspicious meanderings through the yards and neighborhoods of the county).

Examples of locations where conversations are generally considered private include:

- In one’s home or apartment.
- In a hotel room.

- In a small public restroom.
- At a workstation or other areas of a business set aside for private activities.
- In a telephone booth.

Examples of locations where conversations are generally not considered private include:

- On a public street, or in a person's public movements.
- In the company of others, *i.e.*, in a restaurant.
- In a school classroom or on a school bus.
- On premises open to the public.
- In a boat on a public waterway viewable by the public.

However, the private nature of a conversation can be extinguished when it is knowingly exposed to public observation. When a conversation is conducted in a manner that allows it to be overheard by anyone who happens to be standing about, the speaker cannot reasonably expect his statements to remain private. For example, a person shouting on the telephone so loudly that his neighbor in the adjoining apartment can overhear and record him, has no reasonable expectation of privacy in his statements, despite speaking inside his own apartment. See *Malpas v. State*, 116 Md. App. 69, 695 A.2d 588 (1997) ("The risk of being overheard by an eavesdropper, lawfully in position to hear, is one we necessarily assume whenever we speak").

By the same token, it is also possible to conduct a private conversation in a public place, *e.g.*, a couple whispering "sweet nothings" on a park bench, or a meeting between a confidential informant (CI) and a narcotics detective in a dimly lit restaurant to discuss drug activity. In both examples, the participants clearly are seeking privacy despite the public nature of their meeting location. Does society, however, recognize these conversations as private?

Some of the factors considered in determining whether a conversation is private (existence of REP) are the:

- Volume of the communication or conversation.
- Proximity or potential of other individuals to overhear the conversation.
- Potential for communications to be reported.
- Affirmative actions taken by the speakers to shield their privacy.
- Need for technological enhancements to hear the communications.
- Place or location of the oral communications as it relates to the subjective expectations of the individuals who are communicating.

These factors are not exclusive and the determination will be made on a case-by-case basis. In other words, the evaluation is very fact driven, and therefore, subject to interpretation.

It is important to delineate the distinction between an expectation of “non-interception” (expectation that a person’s communication is not subject to being recorded) and a reasonable expectation of privacy (REP) in an oral communication (expectation that person’s conversation is entitled to remain private). In other words, the Wiretap Act does not protect any and all spoken words from unwanted interception; it only protects words spoken in privacy.

*Private Conversation in the Context of a Law Enforcement Encounter – Attorney General Guidance*

**2000 Attorney General Opinion and the 2010 Attorney General Letter of Advice**

Prior to 2015, the Office of the Attorney General touched on the issue at hand, though not squarely. In 2000, an Attorney General Opinion was requested by Charles Moose, Chief of Police for the Montgomery County Police Department and was written by then Chief Counsel of the Advice and Opinions Division of the Attorney General’s Office, Robert N. McDonald. See 85 Opinions of the Attorney General 225 (2000) (hereinafter, 2000 AG Opinion). The central issue was whether an officer who inadvertently records the audio portion of a videotaped interview without consent is violating the Wiretap Act. The resulting opinion was that an inadvertent interception is not a “willful” interception as required for a Wiretap Act violation. However, footnote 8 of that opinion provides a glimpse into how the Attorney General analyzes an oral communication between police and citizens. In footnote 8, McDonald offers these instructive remarks:

It is also notable that many encounters between uniformed police officers and citizens could hardly be characterized as “private conversations.” For example, any driver pulled over by a uniformed officer in a traffic stop is acutely aware that his or her statements are being made to a police officer and, indeed, that they may be repeated as evidence in a courtroom. It is difficult to characterize such a conversation as “private.”

85 Md. Op. Att’y Gen. at 234 n.8.

A 2010 Advice Letter from Robert N. McDonald to Delegate Samuel Rosenberg more closely addressed the issue at hand. The issues presented were “Whether the Wiretap Act applies to situations where citizens record public activities of police officers,?” “Whether Police Activity Involves an ‘Oral Communication?’,” “Does an arrest or stop of a citizen by a police officer involve a ‘private conversation?’” See Letter from Robert N. McDonald, Chief Counsel, Opinions & Advice, Office of Md. Att’y Gen., to Samuel I. Rosenberg, Md. House of Delegates (July 7, 2010) (hereinafter, 2010 AG Advice Letter). (Note: A Letter of Advice does not carry the same weight as an Opinion of the Attorney General. An Opinion goes through many more layers of review within the AG’s office than a Letter.)

After examining the 2000 AG Opinion, relevant case law, and wiretap laws of various states, McDonald determined that, in a nutshell, a communication between a citizen and a police officer is not likely private.

The 2010 AG Advice Letter references footnote 8 of the 2000 Attorney General Opinion in an attempt to resolve the issue of whether a citizen who intercepted oral communication between himself and a police officer is violative of the Wiretap Act. The 2010 AG Advice Letter proceeds to say that the reasoning of that excerpt (footnote 8), which suggested that a police officer would not face prosecution or liability under the Act for recording an arrest or traffic stop in a public place, would apply equally to a citizen recording a police officer. *Id.* at 6.

Turning to case law, the 2010 AG Advice Letter quotes several cases, including an unpublished Fourth Circuit opinion, which suggests that for purposes of the federal and state statutes, a suspect does not have a reasonable expectation of privacy in his statements while he is seated in a police car. *Id.*; *See, e.g., United States v. Rodriguez*, 998 F.2d 1011 (4<sup>th</sup> Cir. 1993) (unpublished).

McDonald further explains, “subsequent decisions of the Maryland courts...as well as the authorities cited in the 2000 AG Opinion indicate that, in most cases, the conversation between the officer and citizen who is arrested or detained by the officer is not likely to be considered a ‘private conversation’ protected by the Act.” 2010 AG Advice Letter to Samuel I. Rosenberg at 7.

Finally, McDonald assessed the wiretap laws of other jurisdictions. In particular, the Washington state statute is akin to Maryland’s in that it prohibits the interception or recording of a “private conversation,” yet does not define the term. The Washington Court of Appeals examined the meaning of ‘private conversation’ in *State v. Flora*, 845 P.2d 1355 (Wash. App. 1992), in which a defendant recorded a conversation with the police during his arrest on a public street. The court concluded the arrest was “not entitled to be private” because the officers’ statements were “uttered in the course of performing their official and public duties”. *See* 2010 AG Advice Letter to Samuel I. Rosenberg at 8 (citations omitted). Thus, the officers “could not have reasonably considered their words to be private”. *Id.*

McDonald concluded by identifying three possible outcomes when analyzing whether statements made by a police officer during an encounter with a citizen were part of a “private conversation” and therefore fell within the definition of an oral communication covered by the Wiretap Act. Two of those outcomes are relevant here. First, it seems unlikely that a court might find, in most cases, that a particular encounter between police and citizens involves a “private conversation,” particularly when they occur in a public place and involve the exercise of police powers, so as to qualify as an oral communication under the Wiretap Act. Second, it is likely that a court would hold that a police stop of an individual necessarily is not a “private conversation,” and therefore does not involve an oral communication covered by the Wiretap Act. This seems to be

the most likely outcome in the case of a detention or arrest, and is the most consistent with the 2000 AG Opinion and the majority holdings of other states courts. *Id.* at 10.

The 2010 AG Advice Letter was seemingly requested as a result of the Anthony Graber case, which involved a motorcyclist who used a helmet camera to video and audio record a traffic stop made by a Maryland State Police Trooper. Graber posted the video on YouTube, for which he was subsequently arrested and charged with violations of the Wiretap Act (among other charges). Relying heavily on the 2000 AG Opinion and 2010 AG Advice Letter, Harford County Circuit court judge, Hon. Emory Plitt, dismissed the count charging Graber with violation of the Wiretap Act. See *State of Maryland v. Anthony John Graber, III*, Case No. 12-K-10-647 (Sept. 27, 2010).

It should be noted that the 2010 AG Advice Letter is written in the context of the citizen/defendant recording the police which is the inverse of the body-worn camera fact pattern in question. Neither the 2000 AG Opinion or the 2010 AG Advice Letter addresses the circumstance where the police are intercepting the oral communication, outside of the willful interception analysis of the statutory carve out of the Wiretap Act, which specifically allows the interception during a traffic stop (given that police comply with the other requirements of the carve-out).

### **2015 Attorney General Letter of Advice**

In seeming anticipation of the 2015 General Assembly Legislative Session and the introduction of several “body-worn camera” bills, Delegate Rosenberg again solicited the Attorney General’s opinion concerning the application of the Wiretap Act to the use of body-worn cameras. See Letter from Jeremy M. McCoy, Assistant Attorney General, Office of Counsel to the Gen. Assembly, Office of Md. Att’y Gen., to Samuel I. Rosenberg, Md. House of Delegates (January 14, 2015) (hereinafter, 2015 AG Advice Letter). Writing for the Attorney General’s Office of the Counsel to the General Assembly, Assistant Attorney General, Jeremy M. McCoy opined:

Less clear is whether an individual may have a reasonable expectation of privacy in a communication with a law enforcement officer in a non-public place, such as in a suspect’s or witness’s home, or whether an officer’s body camera may lawfully intercept a communication between two or more third parties in a public or private setting. The reasonableness of any expectation of privacy in those circumstances may depend on the context of the communication, such as whether the officer has legal justification to be present in the location and to interact with the individual, or whether the individual interacting with a police officer wearing a body camera on duty and has reason to believe the camera is recording may reasonably expect any such interaction to be private.

2015 AG Advice Letter to Samuel I. Rosenberg at 4.

The 2015 Advice Letter, and particularly this excerpt, captures so many of the questions that the workgroup has explored and struggled to answer. Under the current state of the law, clarity is evasive as McCoy so aptly notes, especially in light of the number of variables that are present in any given police encounter and the fact that the encounter is oftentimes dynamic, and by its nature, continually subject to change, sometimes complex, highly unpredictable, and often potentially dangerous.

In further exploring the significance of the location or setting in evaluating the conversation, McCoy proffered that, “The most significant factor in determining whether the interception of an individual’s oral communication with a law enforcement officer appears to be whether, under the two-part subjective and objective test, the individual has a reasonable expectation of privacy in the conversation, based on the factual circumstances of the interaction.” *Id.* at 5.

Although the 2015 Advice Letter does not specifically address this, it merits discussing that while victims and confidential informants may have concerns about the recording of a conversation (and the subsequent disclosure), the critical inquiry is whether or not society is willing to recognize that conversation as private. Both individuals, presumably, may very much want to remain anonymous, and in some instances, that may be possible or even desirable. Ultimately, however, the mission of a law enforcement agency and its responsibility to the community to prevent crime and apprehend and prosecute those who are responsible for criminal acts must be balanced with the citizen’s right to privacy.

And, finally, on the question presented as to specifically whether an exception to the Wiretap Act was necessary in order for the state to mandate the use of body-worn cameras by law enforcement, McCoy ultimately concluded that, “Depending on the desired scope of the authority to intercept oral communications with law enforcement officers, within constitutional limitations, specific authorization for certain types of interceptions may help provide clarity to the application of the Act.” *Id.* at 8.

Again, as stated previously, the legislature has essentially signaled the necessity of a wiretap exception for the interception of law enforcement communications with citizens despite the foregoing Attorney General Opinions and Letters of Advice. Having said that, several bills have been introduced in the 2015 session of the General Assembly that attempt to address the body-worn camera issue.

## Other Operational Considerations

### *Video Recordings*

Video surveillance by a law enforcement agency is subject to the requirements of the Fourth Amendment. Neither the Wiretap Act nor Title III restrict the use of a video camera that records only images and not oral communications. *Ricks v. State*, 312 Md. 11, 537 A.2d 612 (1988). There are other laws that impose restrictions on video recording in certain circumstances, but none of these apply to the recording of a public

encounter between a police officer and a private citizen. See, e.g., Md. Code. Ann., Crim. Law §§ 3-901 et seq. (West 2014) (concerning “crimes relating to visual and camera surveillance in private places”).

The Fourth Amendment, on the other hand, imposes similar warrant requirements on the government's use of video surveillance as the wiretap statute imposes upon the use of audio surveillance. See generally, *United States v. Nerber*, 222 F.3d 597 (9th Cir. 2000). Warrantless videotaping by a law enforcement officer implicates the Fourth Amendment, and its state counterpart, Article 26 of the Maryland Declaration of Rights, when it invades an individual's reasonable expectation of privacy. See *Malpas v. State*, 116 Md. App. 69, 695 A.2d 588 (1997). Thus, determining whether a warrant is required for nonconsensual video recording entails a REP analysis.

“Video surveillance is inherently intrusive because... a video camera sees all, and forgets nothing.” *Brannum v. Overton Cnty. Sch. Bd.*, 516 F.3d 489, 496 (6th Cir. 2008) (Videotaping by school officials of students changing in locker room was unreasonable Fourth Amendment search) (alteration in original) (internal quotations omitted). Yet warrantless videotaping does not, in and of itself, violate a reasonable expectation of privacy (REP). Rather, a person must believe his movements are undertaken in privacy, and will remain private. His subjective belief/expectation must also be one society accepts as reasonable.

As previously discussed, a critical factor in evaluating REP is location. Although the Fourth Amendment protects persons, not places, “the extent to which the Fourth Amendment protects people may depend upon where those people are.” *United States v. Gonzalez*, 328 F.3d 543, 547 (9th Cir. 2003) (quoting *Minnesota v. Carter*, 525 U.S. 83, 88, 119 S.Ct. 469, 142 (1998)). For example, it is well settled that when an individual is in public, he has a significantly diminished reasonable expectation of privacy. Further, it is generally accepted that the police are permitted to record what they normally may view with the naked eye from a vantage point they lawfully occupy. See e.g., *United States v. Jackson*, 213 F.3d 1269, 1280 (10th Cir.) (“The use of video equipment and cameras to record activity visible to the naked eye does not ordinarily violate the Fourth Amendment.”), *vacated on other grounds*, 531 U.S. 1033, 121 S.Ct. 621, 148 L.Ed.2d 531 (2000); *United States v. Mclver*, 186 F.3d 1119, 1125 (9th Cir.1999) (“We reject the notion that the visual observation of the site became unconstitutional merely because law enforcement chose to use a more cost-effective ‘mechanical eye’ to continue to the surveillance.”). For unlike conversations, a person cannot maintain privacy in his physical image or movements while exposed to public view. Consequently, videotaping of suspects in public places, such as banks, does not violate the Fourth Amendment. *Gonzalez*, 328 F.3d 543. It stands to reason that issues with warrantless video recording will arise, more often than not, when it occurs in a presumptively private location, like a private home or office.

In a Maryland Court of Special Appeals case, *Donaldson v. State*, Baltimore County homicide detectives videotaped and audiotaped a defendant's statement without his knowledge or permission. 200 Md. App. 581, 28 A.3d 129 (2011). The court held the

police did not need permission from Donaldson before recording the interviews in the police interrogation room. Relying on Florida case, which found that a defendant has no reasonable expectation of privacy in a police interview room, the court reasoned “appellant was not led to believe that his statements would not go beyond the interrogation room, the police interviewers did nothing to foster any particular sense of privacy in the interviews, and it was not reasonable for appellant to have assumed otherwise.” 200 Md. App. 581 at 594, 28 A.3d at 196 (2011).

### *Enhanced Recording Devices*

There will likely be Fourth Amendment issues with a body-worn camera system that is capable of enhanced recording beyond the observations of the police officer, particularly if such a recording occurs within a constitutionally-protected area.

The prevailing majority of courts recognize that “technologically unaided or unenhanced overhearing of statements does not constitute a search under the Fourth Amendment.” *Malpas v. State*, 116 Md. App. 69, 84, 695 A.2d 588, 595 (1997). Likewise, “to observe what is open and patent either in daylight or in artificial light” is not a search. *Petteway v. United States*, 261 F.2d 53, 54 (4th Cir. 1958). Many courts have drawn these conclusions based on the reduced expectation of privacy in public places or the plain view exception. It would defy logic that an officer “should be precluded from observing as an officer what would be entirely visible to him as a private citizen.” *Texas v. Brown*, 460 U.S. 730, 740, 103 S. Ct. 1535, 1542, 75 L. Ed. 2d 502 (1983) (Officer’s use of flashlight to illuminate interior of defendants car during traffic stop did not implicate Fourth Amendment.). See also, *United States v. Williams*, 902 F.2d 678, 680-81 (8th Cir. 1990) (use of ultraviolet light is not a search).

However, the reasonable expectation of privacy does include protection against unreasonable visual intrusions. See *United States v. Capps*, 435 F.2d 637, 641, n. 7 (9th Cir. 1970) and *State v. Bryant*, 287 Minn. 205, 177 N.W.2d 800, 803 (1970). Visual intrusions can interfere with an individual’s right to be left alone just as powerfully as the eavesdropping at issue in *Katz*. *United States v. Kim*, 415 F. Supp. 1252, 1254 (D. Haw. 1976). Thus, many courts have held that visual devices that allow observation into a residence is a Fourth Amendment violation. *Williams v. City of Lancaster, Pa.*, 639 F. Supp. 377, 382 (E.D. Pa. 1986).

### *Body-Worn Cameras in Schools*

A body-worn camera recording that captures images or audio of juveniles in a school environment would be subject to the provisions of the Maryland Public Information Act (MPIA) as a record of the Baltimore County Police Department. The MPIA prohibits disclosure of police records concerning juvenile offenders, victims of suspected child abuse, and sexual assault, thereby shielding the juveniles’ identities protecting their privacy. See Gen. Provis. § 4-301; Cts. & Jud. § 3-8A-27; Human Serv. §§ 1-201 to -203. The statute does not prohibit disclosure of (or mandate the protection of) a child’s identity when the child is a victim of any other crime, or when the child is merely a

witness. Nevertheless, there is a strong public policy interest/rationale in protecting the privacy of children in these instances as well.

In the vast majority of cases, the public would not gain any meaningful benefit from disclosure of a child's identity (a child's identity will be of no legitimate concern to the public). Disclosure is unlikely to further the public's understanding of the events recorded; it is also unlikely to further the purpose of the MPIA, which is to shed light on "the affairs of government and the official acts of public officials and employees". Gen. Provis. § 4-103. In comparison, redaction of the child's identity would protect any private details of a child's life that are captured on the recordings, and which can be of no legitimate concern to the public. It would also limit the child's exposure to potentially negative attention, *i.e.*, bullying, harassment, intimidation, etc. Given the strong societal interest in protecting children, the potential harm resulting from disclosure, and the nominal public benefit, the disclosure of a child's image or identification would be "contrary to the public interest" on most occasions. Nevertheless, except as discussed above, there does not appear to be a provision in any state law that would fully protect these privacy interests.

The Family Educational and Privacy Rights Act (FERPA), which governs inspection and review of education records, would not apply to body-worn camera recordings by School Resource Officers because these recordings are not "education records" under FERPA. See 20 U.S.C.A. § 1232g(4)(a) (West 2014) (defining an "education record" as one "contain[ing] information directly relating to a student" and which is "maintained by an educational agency or institution or by a person acting for such agency or institution").

### Records Access and Maintenance

#### *Record Release and Redaction – Maryland Public Information Act*

As the statute is currently written, the recordings captured by the body-worn camera would be considered public records under the Maryland Public Information Act (MPIA), Md. Code Ann., General Provisions Article, Sections 4-101, et seq., and therefore would be subject to a public information act request by media outlets, inmates, private citizens, etc. Obviously, this invokes seemingly greater concerns about an individual's privacy than the release of paper documents, police reports, or even photographs. "Video surveillance is inherently intrusive because... a video camera sees all, and forgets nothing." *Brannum v. Overton Cnty. Sch. Bd.*, 516 F.3d 489, 496 (6th Cir. 2008).

Recorded images and sounds captured have a far more profound effect on the receiver of them. The potential for some of the most private and emotionally charged life events may be captured by body-worn cameras. See generally, *United States v. Mesa-Rincon*, 911 F.2d 1433, 1442 (10th Cir.1990) ("Because of the invasive nature of video surveillance, the government's showing of necessity must be very high to justify its use."); *United States v. Torres*, 751 F.2d 875, 882 (7th Cir.1984) ("We think it ... unarguable that television surveillance is exceedingly intrusive, especially in

combination (as here) with audio surveillance, and inherently indiscriminate, and that it could be grossly abused-to eliminate personal privacy as understood in modern Western nations.”)

A release of a recording would likely require departmental review by the Office of the Chief, the Media and Communications Section, and the Operations Bureau. Virtually every request would require at least a threshold legal review in order to ensure compliance with the required denials and the discretionary denials delineated by the MPIA and other relevant state and federal laws that restrict release of confidential and privileged information. Such inquiry would include which part of the record, if any, is subject to release, when the record may be released, and to whom the record can be released.

The review and analysis for purposes of determining whether the release of all, part, or none of the record is required will depend, in part, on whether or not the record is an investigatory record. Gen. Provis. § 4-351. While most recordings will fall into this category, this discretionary denial is not a complete bar to release, but rather a “temporary” or partial denial until the investigation is closed. Further, a custodian may use a discretionary denial for part or all of a public record only if the “custodian believes that inspection of a part of a public record by the applicant would be contrary to the public interest ...” Gen. Provis. § 4-343. Within the “investigatory records exception” is a category of persons who have special, presumptive right to access records, *i.e.*, a person in interest. This category represents the individual whose interaction with the police is captured by the recording. There are very specific, limited reasons upon which to withhold this record and this requires yet another level of analysis.

Further complicating the matter is the legal requirement that certain protected information be redacted from records prior to their release, *e.g.*, medical information, personal information, information relating to juveniles, etc. As an example of the burden this may impose, under an Attorney General’s Opinion addressed to former County Attorney Jay Liner, a person in interest’s statement that she is bleeding would likely need to be redacted as a medical record.

In addition, the actual physical component of the redaction itself will be a labor intensive and cumbersome process. The necessity to redact audio and/or video would undoubtedly require additional human resources dedicated to the legal review, compliance, and fulfillment of the requests for the release of body-worn camera recordings, including technical assistance from the Forensic Services Section to execute the legal requirements of the law. In as much as there are thousands of requests for police reports each year, it is reasonable to anticipate an influx of requests for body-worn camera recordings. Clearly, the decision to institute the use of body-worn cameras will have the unintended impact of increasing the Department’s administrative/fiscal burden of fulfilling these requests. How much these additional MPIA requests will impact an already overburdened Department is unknown, but if the Seattle Police Department’s experience (a massive amount of information requests threatening to derail plans to outfit officers with body-worn cameras) is any indication of

the potential, serious consideration must be given to what modifications should be made to the MPIA, while still preserving the public's right to have information about the "affairs of government and the official acts of public officials and employees". Gen. Provis. § 4-103.

While the MPIA contains a provision that allows for recovery of reasonable costs for "the search for, preparation of, and reproduction of a public record," this does not include the first two hours of the research. § 4-206(b)-(c). Ostensibly, this would offset some of the additional costs associated with the necessity for additional resources required for the fulfillment of these requests. However, to recoup the true cost associated with the increase of requests and the complexity of work to fulfill them, it is likely that a more thorough cost assessment must be undertaken.

Anecdotally, there is some evidence to suggest that the general public has little or no awareness of the relationship between the MPIA and body-worn camera recordings, such as the likelihood that recordings may be released that portray potentially embarrassing or uncomfortable events or situations in a person's life. It is quite one thing to have a police report released that contains words on paper and yet it is an entirely a different scenario altogether to release an audio recording of an incident (e.g., a domestic violence incident that occurred inside someone's home).

Another consideration is that the camera recordings are subject to potential disclosure under the Maryland Rules of Procedure pursuant to the civil and criminal rules of discovery and the subpoena rules. Again, it is necessary that the Legal Section engage in a legal review, working in conjunction with the Office of Law and the Office of the State's Attorney for Baltimore County to comply with the discovery rules, which will require additional human resource hours to comply.

### *Expungement of Recordings*

Maryland law allows for certain police records to be expunged in limited circumstances.

For arrests or confinements not resulting in a charge, all police records, including photographs, must be expunged within 60 days after receipt of the request. If a law enforcement unit fails to expunge a police record as required, the person entitled to expungement may seek legal redress and recover court costs. Crim. Proc. § 10-103.1. After a charge is filed, a person may obtain a judicial order for expungement when the charge results in an acquittal, *nolle prosequi*, stet, or probation before judgment (PBJ), if the person is found criminally not responsible for certain crimes, or the person receives a pardon for certain crimes. Unless an order is stayed pending an appeal, within 60 days after entry of the order, every custodian of the police records and court records that are subject to the order of expungement shall advise in writing the court and the person who is seeking expungement of compliance with the order. Crim. Proc. § 10-105.

Accordingly, body-worn camera recordings would constitute yet another record for which review and compliance with expungement statutes is required, and which mandate a legal review and therefore would require additional human and technical resources.

### *Record Retention*

Some recordings of law enforcement encounters will become evidence in criminal, civil, or administrative proceedings, or a combination thereof, requiring the Department to maintain them as it would any other piece of evidence subject to retention for evidentiary purposes.

There are various statutes that would impact the necessity to store the body-worn camera evidence and properly document the chain of custody and any modifications made to the original recording. Additionally, appeals, post conviction proceedings, and petitions for writs of actual innocence will require that some of the body-worn camera recordings be kept for decades.

The Department would likely follow the current retention policy, with the understanding that in the instance of body-worn camera recordings, there will likely be the need to redact the recordings in some instances and make any number of copies of a particular recording. Therefore, it will be necessary to always maintain an original, unredacted version of the recording.

### Additional Legal Discussions

#### *First Amendment Impact on Interception of Police Communications*

The First Amendment does not protect most police communication from interception, but does protect a private citizen's speech under the First Amendment and therefore will likely implicate the Wiretap Act in certain circumstances.

The US Supreme Court in *Garcetti v. Ceballos*, ruled that when public employees make statements pursuant to their official duties, they are not speaking as private citizens for First Amendment purposes; therefore, the Constitution does not protect those communications. 547 U.S. 410, 421, 126 S. Ct. 1951, 1960, 164 L. Ed. 2d 689 (2006).

Also worth noting is that the Department of Justice filed a statement of interest in the "Preakness Case," *Christopher Sharp v. Baltimore Police Department*, a §42 U.S.C. §1983 federal claim filed in the District Court of Maryland where officers allegedly took a cell phone containing video of an officer's arrest and alleged brutality of a woman. Police were also alleged to have erased the video. In the letter, the Department of Justice said, "The right to record police officers while performing duties in a public place, as well as the right to be protected from the warrantless seizure and destruction of those recordings, are not only required by the Constitution (First Amendment right to gather information about public officials); they are consistent with our fundamental

notions of liberty, promote accountability of our government officers and instill public confidence in the police officers who serve us daily.” NOTE: Baltimore City’s Motion for Summary Judgment was denied and the case ultimately resolved by way of a Settlement Agreement in 2014.

Contrast the above with the potential for impingement of such constitutionally protected rights of free speech and association of a citizen through the use of body-worn cameras. When citizens engage in free speech activity such as peaceful protests, picketing, demonstrations, political rallies, marches, or attendance at religious ceremonies or functions, the potential exists to capture the speech of law abiding citizens. It’s understood that when the participants are involved or engaged in illegal activity, the same concerns are not at issue. However, the fear that police may track, identify, create a “watch list”, or store recordings of lawful participants as a result of monitoring these events with body-worn cameras could result in a chilling effect on a person’s right to engage in protected activity. It’s critical to reconcile the use of body-worn cameras with these core constitutional rights and values, while also enabling law enforcement to achieve its goals.

### *Policy Arguments*

The availability of video/audio evidence in police misconduct lawsuits against law enforcement would help plaintiffs successfully bring claims (particularly in “he said/ she said” cases) and alleviate the problem of potential juror bias in favor of police in the face of evidence of police wrongdoing. Likewise, the availability of this type of evidence would lessen the load of an already heavily burdened judicial system because frivolous civil rights suits would be dismissed (or not brought) if corroborating physical evidence (audio/video) existed. (See Prince Georges County case involving University of Maryland students celebrating a win over Duke and according to reports, a student confronted officers, verbally provoked them and assaulted them, and then fought with them as they tried to detain him. Video recordings by students showed the officers to be the aggressors.)

Having said that, it is still critical to keep in mind that a body-worn camera will record the events as they unfold only from whatever limited perspective the camera captures, however, it may or may not capture the officer’s perception of the events, which could be a distinctly different viewpoint altogether. In as much as *Graham v. O’Connor*, held that “[t]he ‘reasonableness’ of a particular use of force must be judged from the perspective of a reasonable officer on the scene, rather than with the 20/20 vision of hindsight,” it stands to reason that what the officer perceives is a critical component of the analysis, and therefore, not every use of force case will be resolved on the video alone. 490 U.S. 396, 397 (1989). What the officer reasonably believed to be occurring, and therefore prompted his actions, when “forced to make a split-second judgment[s] – in circumstances that are tense, uncertain, and rapidly evolving – about the amount of force that is necessary in a particular situation,” will undoubtedly, in some instances, result in litigation. *Id.*

## Conclusion

When a law enforcement officer records the communication between himself and a private citizen who is being arrested or detained, or between himself and a witness in an investigation, or during any police encounter, are those conversations private and protected such that they are violative of the Wiretap Act?

The most compelling language contained in guidance from the Attorney General rendered to date seems to suggest that it would be legal for the police to intercept oral communication in most police encounters, because it would not likely be deemed a “private conversation” inasmuch as a citizen is acutely aware that any statements made to a police officer may be repeated as evidence in a courtroom. **However, clear legislative authority is necessary to proceed, even with a body-worn camera pilot program, so that police are not put in the untenable position of trying to ascertain whether or not a conversation is private, such that it can be recorded, in addition to all of the other decisions that they must make, some of which are life and death, split second decisions.**

## General Policy Issues

Most of this section, and others that follow, are contingent on the decision to implement a BWC program.

### Program Implementation

As White noted, because the effects of a BWC program are so far reaching and costs difficult to predict, agencies considering BWC use should proceed cautiously. Howard County's report cited the Albuquerque BWC program - Albuquerque reportedly implemented the program without adequately considering the needed infrastructure; as a result it was unprepared for the overwhelming number of recording requests they received. There have been similar concerns with TASER deployments in large agencies. Recently the Los Angeles Police Department announced they would deploy 7,000 BWCs to personnel, but deployment timeframes are not fully known.

During discussion, our workgroup consensus was that any future BWC deployment should be piloted. This would allow preliminary evaluations before too many financial resources are expended. If the program is institutionalized, deployment should be done incrementally, allowing for necessary adjustments in areas such as training, policy, information requests, etc. Incremental deployment may show that equipment need not be deployed to all personnel in a given assignment. For example, we have found that TASERs do not need to be issued to every patrol officer; strategic deployment has worked with TASERs, and might be suitable for BWCs as well.

### Equipment Deployment

With regard to who should wear the BWC, the workgroup first considered voluntary deployment. The Ocean View, Delaware Police Department uses a voluntary BWC program to supplement their mandatory in-car camera program. A voluntary program may be feasible during a pilot phase, but most agencies that have chosen BWC programs have policies mandating camera use for selected personnel.

PERF noted that, if voluntary use of a BWC is permitted, the policy needs to specify which officers, if any, are required to wear a BWC and when. PERF indicated that any policy – voluntary or mandatory - should state which personnel are assigned or permitted to wear BWCs. Voluntary use may not be a long term issue; as noted in a webinar of the Phoenix program evaluation, in the post-Ferguson era, some officers now ask for BWCs.

PERF noted that agencies have found it helpful to begin BWC deployment with units that interact extensively with the public. To that end, our workgroup agreed that BWCs would be appropriate for virtually all patrol and traffic personnel.

With regard to specialized assignments, BWC usage would depend on function. Our Criminal Investigations Division (CID) should consider situational BWC deployment,

such as during location entries or warrant services. For CID units such as the Regional Auto Theft Task Force or the Warrant Apprehension Task Force, BWCs should be considered for day-to-day use due to the high number of confrontations with suspects. The Violent Crimes Unit may want to use BWCs when interviewing witnesses due to the propensity of such witnesses to change their stories.

On the other hand, possible compromises to case integrity or officer safety may be a factor with covert or undercover CID units; such risks could increase with BWC use. The impact on victims and witnesses – compromising victim confidentiality or a chilling effect on information sharing – may be a concern for some CID personnel.

The workgroup felt that if BWC usage compromises the safety of the operation, negatively impacts intelligence gathering or compromises investigatory techniques, it should not be considered for day-to-day use. The same concerns apply to our Support Operations Division (SOD). The SOD Commander has spoken about potential BWC use to the commanders in each unit, which are diverse in terms of function.

Aside from use with Traffic personnel, BWCs may not be practical for deployment elsewhere in SOD. For the Marine Team or the Commercial Vehicle Safety Team, elements such as water, dirt, and grease may affect the BWC equipment. The Aviation Team already has surveillance capability but little citizen interaction, so BWC use is unnecessary. For the K-9 Unit there are concerns about whether the equipment is resilient enough to withstand the physical nature of the work, which often occurs in rugged environments. For the Tactical Unit, whose members carry 60 or more pounds of equipment, BWCs could compromise officer safety and expose sensitive police tactics. For the Mobile Crisis Team and the Workplace Violence Team, BWC use could escalate situations involving people in mental distress. Clearly, a great deal of testing and evaluation should occur prior to SOD deployment, even for traffic personnel.

School Resource Officers (SROs) come into contact with thousands of students every year. We are aware of only a few agencies that allow SROs to carry BWCs. We would have to collaborate with Baltimore County Public Schools (BCPS) to ensure that usage in schools corresponds to the expectations of police and school personnel, students, and parents.

A parallel situation arose with BCPS several years ago when TASERs were deployed to our field personnel. Although SROs have never been permitted to deploy TASERs, the school system knows that units responding in support of an SRO may be equipped with the TASER, and that TASERs could be used out of operational necessity. We may need a similar policy for BWCs in schools, should the program be institutionalized.

Finally, the group considered usage by supervisors, sworn personnel in administrative positions, and non-sworn personnel in our agency. Our workgroup feels that supervisors should lead by example, wearing BWCs if their personnel wear them; Phoenix uses such a policy. Conversely, the workgroup felt that sworn members in administrative positions, and non-sworn members such as cadets and the Auxiliary

Team, should not wear BWCs due to the nature of their jobs and the lack of operational necessity.

### Key Policy Components

The documents we reviewed cover a broad range of procedural considerations. The IACP started at “square one,” stating that agencies using BWCs “should provide them to all such officers for use in accordance with agency policy” – essentially, there needs to be a policy in effect. PERF’s study found that nearly a third of the agencies surveyed had no written policy in place for BWC usage. GOCCP cited other expected policy components such as rules regarding BWC activation and recording, privacy rights, and data storage and access procedures.

As part of our research, we reviewed policies from more than 20 agencies using BWCs, and identified trends regarding key issues. We found that:

- 42.1 percent prohibit the use of privately-owned BWCs.
- 89.5 percent require the use of BWCs for designated personnel.
- 89.5 percent have prohibitions for BWC use.
- 57.9 percent give officers some discretion to activate the BWC.
- 47.4 percent provide direction about when to stop recording.
- 42.1 percent require notification of the person being recorded.
- 78.9 percent stipulate who can view the recording post-incident.
- 89.5 percent provide direction about how to tag/label the recording.
- 47.4 percent restrict who can edit or delete recordings.
- 57.9 percent provide specific recording retention guidelines.

Interestingly, no single policy component mentioned above was found in all of the policies we reviewed. Such inconsistency may change if agencies are accredited in some fashion. Our agency is accredited through CALEA, the Commission on Accreditation for Law Enforcement Agencies. CALEA standard 41.3.8 applies to in-car recording systems. This is a “mandatory” standard but it only has two requirements and it does not yet apply to BWCs.

Recently CALEA proposed adding BWCs to the accreditation standard and posted a discussion forum with the following potential BWC standard components:

- Policy statement on the purpose and organization philosophy regarding use.
- Requirements and restrictions for activation and deactivation of the device.
- Criminal and administrative use of camera captured data.
- Data storage and retention requirements.
- Equipment maintenance and inspection procedures.
- Training requirements for users and supervisors.
- Requirements for a documented review of camera captured data including frequency and quantity.

We believe CALEA eventually will create a BWC standard, so agencies considering BWC programs should tackle the issues up front. We discuss many of those issues in greater depth throughout this document. As a starting point, we need to address the purpose of this technology and other general issues related to BWC deployment.

### General Deployment Guidelines

The primary purpose of BWCs is to document police interactions and investigations. Our workgroup feels that BWCs should be used only in operational settings. The IACP took the position that BWCs should not be used in administrative settings, and added that the policy should prohibit surreptitious recording of communications with or between officers without the permission of the Chief. PERF suggested a written policy that tells officers when Internal Affairs personnel would access BWC recordings and for what purposes.

A key issue is when and how the BWC equipment can be used. Our workgroup discussed a few of these issues and agreed on the following common sense policy rules, many of which were cited in the PERF and IACP documents:

- Private camera equipment should not be used.
- The Department must own all recordings and controls them appropriately.
- BWCs cannot be used off duty or for non-departmental activities, to include secondary employment.
- Officers should be prohibited from accessing recordings for personal use or for posting to social media and websites.

A few other general deployment issues have been mentioned in the think-tank documents or raised by workgroup members, and they include:

- The IACP's position that officers issued BWC equipment must use it. This would help avoid "second-guessing" whether to record (i.e., the previously mentioned police-involved shooting in Berkeley, Missouri).
- PERF's position that the BWC policy should state how and where on the body the camera is to be worn.
- White's position that officers should be required to start recordings as early as possible so nothing is missed.
- PERF's position that officers should only activate the recorder if doing so does not place themselves or others in danger.
- The FOP's position requiring additional arriving units to activate their recorders; this could lead to additional policy decisions about how to handle multiple recordings of the same incident.

Our workgroup also raised the issue of how to handle the lack of BWC availability. Police officers must be able to do their job even if a BWC is unavailable. If possible, however, officers should attempt to borrow such equipment from a nearby police facility.

In addition, if a BWC exceeds recording storage space in the midst of a shift, provisions will have to be made for the officer to return to a police facility to upload the recordings, rather than risk overwriting existing recordings.

### Notification Guidelines

As GOCCP noted, an issue important to public support of BWCs is determining when and how to notify citizens that they are being recorded. The first consideration is whether notification is legally required. Under Maryland's current two-party consent system, notification and a request for consent must be made to avoid violation of the Maryland Wiretap Act.

The Maryland Wiretap Act includes a legislative carve-out for traffic stops, exempting these stops from consent requirements. Despite how "hyper-public" a traffic stop tends to be, the law still requires police to notify the person being stopped that the interaction is being recorded. Likewise, Baltimore County has considered proposing BWC-related legislation through the Maryland General Assembly that would exempt all citizen-police interactions from consent requirements but still would require notification. We believe that any BWC-related legislation will require notification.

Our workgroup also considered whether notification of a BWC recording should be required by policy if not by law. As noted in the "Key Policy Components" section above, 42.1 percent of agencies surveyed require that police notify the subject that he or she is being recorded. Many see this requirement as a "best practice." PERF felt the practice of notification would help to deescalate situations; PERF and the IACP indicated that in knowing one is being recorded leads to better behavior.

We concluded that the notification of recording should be included in the BWC training program as a de-escalation tool. We did not support mandatory notification because there are situations where notification may be impractical or unsafe. The workgroup felt that officers should use discretion in making notifications, using their judgment to determine when notification would have a positive impact.

If notification is required by policy for all interactions, there likely will be exceptions. A general standard is discussed in the "Officer Discretion" section below. Basically, the provision exempts BWC recording in situations where recording is deemed unsafe, impossible, or impractical. Coincidentally, such exceptions are included in the state legislation under consideration in Annapolis. In such situations, officers could mitigate the lack of initial notification by making notification after the fact.

There are other, more detailed, standards we could implement regarding notification such as requiring notification for non-custodial interviews, for crime victims, or for other specific situations. But it became apparent during our discussions that this workgroup would not reach consensus on individual scenarios. With the possibility of an across-the-board requirement for notification, the workgroup agreed to table the issue until pending BWC legislation is settled in Annapolis.

## Recording Activations, Prohibitions, and Stoppages

### Officer Discretion

Before we can determine when to record, we need to determine whether officers will have situational discretion. This discretion would apply to activation and deactivation of the recording system. The think-tank documents spend a great deal of time discussing the issue, and they strongly support officer discretion.

As PERF noted, the American Civil Liberties Union (ACLU) takes a different position. The ACLU wants “all situations recorded so [the] action is reflexive.” The ACLU believes “activation of the camera should be reactionary for the officer without requiring them to evaluate the situation.” Essentially the ACLU position is that if an incident “goes bad,” the BWC will provide an indisputable record of the event. The ACLU also contends that mandatory recording will actually protect police officers from “allegations of discretionary recording or tampering.” The GOCCP study indicated that reducing officer discretion with respect to what and when to record will not only ensure that relevant events are captured and prevent the loss of relevant evidence, but also protect police officers from accusations of tampering with videos.

The think-tank documents indicate that the law enforcement community, like our workgroup, strongly supports officer discretion. The FOP, in its model policy, stated that an officer must have discretion “to manually activate the system anytime the officer believes it would be appropriate or valuable to document an incident.” A webinar review of the Phoenix program evaluation, emphasized that officers must have the ability to turn off the cameras.

Without discretion to activate or deactivate the camera, PERF noted that the police relationship with the community could be damaged. PERF felt that requiring officers to record all interactions would have a potentially negative impact, as crime victims and witnesses would be reluctant to provide information knowing they were being recorded. PERF and the IACP felt discretion is beneficial, and cited several examples when officers should be able to exercise discretion:

- When recording is unsafe, impossible, or impractical.
- When transporting members of the opposite sex.
- When dealing with aggressive prisoners.
- During informational transactions.
- When speaking with crime witnesses and members of the community who wish to discuss criminal activity.
- During sensitive situations such as interviews with sexual assault victims, or at violent crime or accident scenes.

The need for discretion with recording is no different than in other areas of police work. It applies to situations not explicitly covered in policy but still legitimate from a law

enforcement perspective; no policy can cover every situation. PERF noted that discretion recognizes officers' professionalism and allows for flexibility in gray areas – it also allows for the “best solution in balancing the evidentiary value of a recorded statement against the witnesses' reluctance to be recorded.” As long as discretion is monitored and documented, there should be little abuse.

As a side note, White found that discretion resulted in a large reduction in recording storage – as much as 42 percent in Mesa, AZ - although cost should not be the primary concern. We agree that cost savings are not the primary reason for officer discretion; nonetheless, such savings are important because the saved money could be used to offset program costs or help pay for other areas of police service.

### When Recording Is Appropriate

Should law enforcement adopt the ACLU's position that an officer's entire shift be captured, the guidelines would be simple. However, our workgroup believes officers need discretion, so we address the permissibility of recordings from that perspective.

The workgroup's position that all public interactions need not be recorded is supported by the GOCCP study, which outlined several reasons:

- Increased data storage costs and upload time, as well as the creation of large amounts of unimportant data that must be searched to find important information.
- A reduced comfort level for officers is likely to affect morale.
- Situations an agency may not want to record (e.g., officer breaks, interactions with informants or victims of certain crimes, etc.).
- The need for additional power sources and other cost-related reasons.

In any case, the GOCCP workgroup believes agencies should have a policy clearly stating when officers must activate recording devices. The FOP's model policy provides a simple starting point; the BWC should be activated only for legitimate law enforcement purposes.

There are other recommended general thresholds for camera use. In the Phoenix program evaluation webinar it was recommended that BWCs be used for all enforcement activities. The IACP takes a broad approach as well, recommending that officers activate their BWC whenever they make contact with a citizen in the performance of official police business. PERF recommends recording all encounters that become adversarial.

PERF noted the most common approach is “to require officers to activate their cameras when responding to calls for service and during law enforcement-related encounters and activities.” PERF said that the policy must clearly define the terms “law enforcement-related encounters and activities.” PERF's analysis indicates that many policies have officers activate the BWC when in doubt about whether to do so – thus giving them discretion. The FOP and GOCCP also leave room for discretion,

essentially recommending BWC use for any “legitimate law enforcement contact where the officer believes that a recording of an incident would be appropriate.”

The FOP model policy and the GOCCP study listed similar situations for consideration in any BWC activation policy. They generally felt that BWC use for all “field contacts involving actual or potential criminal conduct within video and audio range” was appropriate, to include:

- Traffic stops of virtually any type, including simple assistance of motorists, as well as traffic-related activities like vehicle searches, DWI investigations, and field sobriety tests.
- Domestic violence calls.
- Physical or verbal confrontations, and all use of force situations.
- Emergency responses and back up responses.
- Pursuits, both vehicular and on foot.
- Suspicious vehicles and persons calls.
- Consent to search situations and search warrant services.
- Arrests, to include warrant services, and arrestee transports.
- Special weapons and tactics (SWAT) operations.
- Pedestrian checks, field interviews, and stop and frisk situations.
- Statements made by individuals in the course of an investigation or complaint.
- Advisement of Miranda rights.
- Seizure of evidence.

This list is comprehensive if not all-inclusive, and it covers the most likely recording scenarios, including self-initiated enforcement and all calls for service. Our workgroup, however, felt that compiling such a list would have a chilling effect on the use of officer discretion, a critical component of the BWC program.

The workgroup discussed this issue at length and concluded that generalized guidance is appropriate. After several discussions the workgroup settled on the following language as a starting point for discussion, with the caveat that additional consideration be given before final policy implementation:

*“Body-worn cameras will be used for all enforcement actions; for calls of a potentially criminal or adversarial nature; and for any other law enforcement contact that the officer believes appropriate.”*

The workgroup felt that this language strikes a balance between the pursuit of transparency and the agency’s needs, and the need for officer discretion. A few workgroup members suggested the words “emergency” and “suspicious” should be considered in the language. In general, workgroup members felt that the language represents the basic intent for BWC use, but that the language should be supported by additional guidelines relating to prohibitions and officer discretion as it relates to activations, deactivations, and reactivations. Future discussions with focus groups involving citizens and officers may reshape this language.

This language, as proposed by our workgroup, conflicts a bit with the position of some of the think-tank documents. The GOCCP study, for example, notes that “reducing officer discretion with respect to what and when to record will not only ensure that relevant events are captured and prevent the loss of relevant evidence, but also protect police officers from accusations of tampering with the videos.” A primary reason for a BWC program is increased transparency, yet transparency may suffer if the recording policy is too discretionary.

The use of discretion led to another issue: Whether the officer should start with the BWC “off” and use discretion to activate it, or whether to start with the BWC “on” and then use discretion to deactivate it. The majority concluded that the latter was preferable. If the BWC is on by default, there is a recording of some duration that might explain an officer’s decision to deactivate the BWC. This would better serve the goal of transparency. A dissenting opinion held that such a policy would be wasteful and costly because it would produce so many recordings of little value. Some workgroup members felt that not recording at the beginning of an interaction that becomes adversarial is necessary because the officer may not have the opportunity to activate the BWC later. This could result in a challenge to the integrity of the officer and the agency.

While the workgroup could not reach consensus on this issue, it generally supports a high level of discretion with regard to BWCs, but recognizes that officer discretion must be balanced against agency needs and community expectations. This is a key policy issue that, we feel, requires additional discussion after the workgroup submits its findings.

#### When Recording May Not Be Appropriate

There are several operational reasons why a BWC should not be used. As noted above, officers should not use a BWC in situations where recording is unsafe, impossible, or impractical. We agree that an officer’s safety should not be compromised by the use of a BWC. One example cited by White involves incidents with possible explosive devices. Law enforcement has long standing prohibitions about using electronic equipment around explosive devices - police radios, cell phones, etc. BWC use should also be prohibited in such situations.

Other prohibitions relate to the potential to compromise investigations. PERF and the IACP recommend against BWC use by undercover officers; when dealing with confidential informants; and during conversations between officers about case tactics or strategies.

BWCs should also not be used in an abusive manner. As cited by the FOP model policy, BWCs should not be used for “the purpose of intimidating an individual or to discourage an individual from observing police activity, making appropriate inquiries of

an officer, or making a complaint.” Prohibitions against potential abuse or the compromise of criminal investigations should be included in the policy.

There is gray area with regard to sensitive situations that support the need for officer discretion. The FOP model policy raises the issue of BWC use in medical facilities. White feels that sensitivity should be shown in incidents involving faith or religion, and religious facilities. PERF and the IACP caution against BWC use in places where there is a high expectation of privacy or, more specifically, in places where nudity is a factor – in restrooms and locker rooms or during strip searches, sex crime investigations, etc. The IACP added that, when possible, officers should avoid “filming” juveniles and bystanders (although that standard should apply to audio recording as well). Our workgroup generally agrees that while use of BWCs in these scenarios is not ideal, it cannot be ruled out if the Department decides BWCs are an operational necessity. Officers will need to use discretion in such situations.

Regarding the general recording of victims, suspects, and witnesses, PERF indicates that officers should “take into account the evidentiary value of recording and the willingness of the victim to speak on camera.” PERF noted that some agencies require victims to consent to the recording and that generally, people are concerned about retaliation for cooperating with law enforcement. Our workgroup agreed that citizens may refuse to cooperate if forced to be on the record. PERF noted that one way around such concerns is allowing the camera to be “pointed away if the person is reluctant to talk,” implying that we could still record audio. White’s position was simpler - if “the victim is unsure or uncomfortable, we should not record.” That may not be practical from an investigative standpoint since recordings could be used as evidence in false report cases. On the other hand, our Criminal Investigations Division (CID) does not always compel written statements from suspects or witnesses, so CID could work without the recordings if necessary. The workgroup felt officer discretion must be used in such situations.

The workgroup discussed concerns related to employee-related BWC recordings. The FOP’s position is that BWCs should not be used to record “conversations of fellow employees during routine, non-enforcement-related activities without their knowledge or during rest or break periods...unless an active preexisting investigation is underway and authorized by law.” PERF agrees with this position. The FOP went on to add that BWCs should not be used to record non-work-related personal activities or areas with a reasonable expectation of privacy, such as restrooms. Our workgroup agrees that such guidelines should be included as prohibitions in the policy.

#### When to Deactivate or Reactivate a Recording

A recording has two portions: audio and video. Some think-tanks conclude that audio and video components are not necessarily “part and parcel” to each other. The workgroup generally agrees. When we discuss recording stoppages (below) we generally refer to a stoppage of both audio and video, but we recognize that there may be exceptions.

Regarding deactivations (stoppages), we first considered the general duration of a recording as determined by policy. We found differences of opinion in the think-tank documents. For example:

- The FOP model policy stated that once the BWC is activated, it should stay activated until the conclusion of an investigative event or enforcement contact.
- The IACP model policy stated that once the BWC was activated, the recording should continue without interruption, essentially implying the BWC should run until the end of the event.
- PERF felt that once the BWC was activated it should continue recording until the conclusion of the incident; or until the officer has left the scene; or until a supervisor has allowed deactivation on camera.

Our workgroup discussed those recommendations and other potential parameters. This includes recording from arrival to departure of an incident scene; until a scene is secure or non-confrontational; until an arrestee arrives at a police facility; and others. PERF noted that some agencies require officers to keep the BWC running until the location is secure, at which point it could be deactivated.

The third dot point above, as suggested by PERF, falls a bit short because it does not mention officer discretion; what happens if the supervisor cannot be reached to authorize the deactivation? The FOP model policy addressed this problem by saying that if approval could not be obtained, the officer should document the reason for the deactivation. The workgroup encourages supervisory involvement in such situations, but does not believe it will be practical in every case. Officers must retain discretion.

Discretion is required when an individual requests that a recording be stopped. When consent is an issue, such as in an area with an expectation of privacy, the IACP leaned towards not recording without permission of the person being recorded. In its model policy concept paper, the IACP noted generally that if an officer needs to ask permission to enter premises, they need to ask permission to record. The IACP complements that position by noting that if the officer has a legal right to enter the dwelling against the resident's wishes then filming should continue. PERF said that "many law enforcement agencies have taken the position that officers have the right to record inside a private home as long as they have a legal right to be there."

If consent is an issue, the recording officer may have to honor the individual's request to stop recording. But even if proposed legislation exempts our officers from consent requirements, there will be times when our officers may want to grant a request to stop recording; the officer should have discretion to do so. Honoring a request to stop recording must, however, be conditional. The officer should have the discretion to resume recording if the situation changes.

## Memorialization of Recording Activations and Stoppages

There are two standard ways to memorialize recording activations and stoppages: During the recording itself and in the incident report. The IACP felt both were appropriate - regardless of whether the activation/stoppage was intentional or accidental, or because there was no recording due to a mandated prohibition.

The IACP model policy noted that in addition to documenting a stoppage in the report officers should record an announcement on tape that they are stopping or resuming a recording; this protects against accusations of selective editing. This would likely involve a verbal justification for the action. The FOP model policy recommends that if supervisory approval for deactivation could not be reasonably obtained, the officer will document on the BWC and the report the reason for termination, noting the date and time.

The issue of memorialization drew mixed reactions from the workgroup. Some felt steps to document activations and stoppages were prudent, while others felt they complicate matters unnecessarily. Some noted that if a subject requests a recording stoppage, the request itself is documentation. Others noted that there is no way to document on camera an accidental stoppage.

The workgroup noted that there will be many recordings for which there is no report, so documenting the activations and stoppages in those situations would not be possible. The workgroup viewed such documentation as time-consuming and cumbersome, with a negative impact on police work. Contrary to the FOP's policy recommendation, the workgroup did not feel supervisory approval should be required to activate or deactivate a recording, and did not feel that documentation of that decision in an incident report should be a requirement.

## Review and Reporting of Recordings

### Review of Recordings

A major issue is whether the recording officer should be permitted to review the recording prior to writing the incident report or associated statements. There are two schools of thought. As PERF noted there is a concern that the review may influence the officer's perception of the incident if it does not agree with the recording. On the other hand, failure to allow review may highlight differences between the recording and the statement, potentially creating a "false impression of dishonesty" on the part of the recording officer.

In PERF's interviews with police executives, most advised that they were in favor of allowing officers to review the video prior to making a statement. A minority contingent of executives felt the officer's credibility would be better served if an officer is not permitted to review the recording, as it reflects the officer's perspective at the time of the incident. In the end, PERF recommended allowing a review of the BWC recording prior to report writing. The Phoenix program evaluation webinar noted that "the facts are the facts" and the recording is only part of the incident; Phoenix allows the review of the recording prior to report writing.

Another issue is whether review of the BWC recording should be universal or restricted in police-involved shootings and other uses of force. The IACP model policy recommended that the agency reserve "the right to limit or restrict an officer from viewing the video file" in situations involving suspected wrongdoing or serious uses of force, such as officer-involved shootings. The FOP position was the opposite – members involved in a use of force incident or accident causing injuries should be permitted to review their own BWC recording prior to providing a recorded statement or completing reports.

Some members of the workgroup felt it could be prudent to reserve the right to restrict the viewing of recordings; others felt there is no scenario that would justify such a restriction. The State's Attorney's Office (SAO) is part of our workgroup, and it sees no need to restrict viewing of BWC recordings. Knowing such restrictions are not in our TASER camera policy, the workgroup agreed that restrictions should not apply to BWCs either.

The workgroup discussed the potential to taint the officer's perception of the event by reviewing the BWC recording prior to making a statement or writing an incident report. As stated previously, PERF found a minority contingent of police executives who felt that review prior to writing the report could hurt the officers' credibility; if the officer saw or heard something on the recording that he did not perceive at the time of the incident, his credibility could suffer.

The workgroup's SAO representative recognized that officer credibility could be a concern and agreed that the officer's perception at the time of the incident is crucial to prosecutorial process, especially in use of force situations. The workgroup's Strategic Planning Team contingent suggested that officers should include in their statements and reports their perception of the event both before and after reviewing the recording. Our SAO representative agreed. Such documentation would allow a balance between the need to understand the officer's perception at the time of the event and the need for a full accounting of the event. Recognizing that the SAO's needs for successful prosecution help drive departmental policy, the workgroup supported dual documentation in use of force incidents, if the Department allows the officer to review the BWC recordings.

Officers may also need to review the BWC recordings made by another officer. The SAO said that when there are multiple BWCs at an incident, all officers required to file reports should be able to review all BWC recordings. In addition to these additional officers, others will eventually review the recordings during the criminal investigation: Follow-up investigators, the State's Attorney's Office, the suspect's counsel, to name a few. Administrative reviews by professional standards personnel may also be required. Supervisors should be able to review recordings at the time of the incident to ensure case accuracy, and also for the purpose of performance evaluations in limited situations (discussed later in this document). PERF recommends that the policy "clearly describe the circumstances in which supervisors will be authorized to review" an officer's BWC recording. Our workgroup feels that provisions mentioned above should be included in the policy.

Review of BWC recordings will extend to administrative investigations as well. The FOP model policy recommends that "whenever an officer is subjected to internal administrative investigation, discipline, or questioning during an internal administrative investigation, the officer and his or her representative or legal counsel shall be given an opportunity to review all relevant recordings prior to being questioned." The GOCCP position paper was a bit different, noting that "watching BWC images prior to providing a statement during a misconduct investigation may give the officer an advantage not available to a civilian complainant." GOCCP went on to say that giving the officer such access "may prevent an investigator from having an opportunity to assess the accuracy and completeness of the officer's version of events."

Our workgroup feels that the officer should also be able to review BWC recordings he or she made prior to an interview with Internal Affairs personnel. In addition, and as noted in the "General Deployment Guidelines" section above, PERF indicated that there should be a written policy that tells officers when Internal Affairs personnel will access BWC recordings and for what purpose. That policy should specify when Internal Affairs and the recording officer would be able to review the recording.

## Reporting of Recordings

Memorialization of a BWC recording in the officer's incident report is important. As the IACP noted, recordings are not a replacement for a written report and the existence of a recording should be noted in the report. PERF agreed. The workgroup, in the interest of simplicity, suggested that a dropdown menu option or "check-box" indicating the presence of a recording be added in the agency's Field-Based Reporting (FBR) system; this may eliminate the need to write about the recording in the report narrative. This would save time for officers and make the system searchable for data analysis purposes. Mesa created a similar solution that allows information to be auto-populated into their report management system.

As noted in the "Memorialization of Recording Activations and Stoppages" section, the workgroup found several scenarios where information relating to BWC use could be considered for inclusion in the incident report. They include:

- All activations, deactivations, and reactivations (recommended in several documents).
- Delayed activations (recommended by FOP model policy).
- Failure to record when required by law or policy (recommended by PERF and GOCCP).
- Accidental recordings.

Many of the think-tank documents recommended noting activations and stoppages in the incident report, along with the justification for them. While these recommendations have merit in terms of transparency, the workgroup did not feel the need to memorialize such decisions in the incident report.

The workgroup is aware that there will be many recordings for which there is no report, and that documentation of activations and stoppages would not always be possible. Even when there is no report, at the time of upload the recording officer will be able to connect a call for service to the recording, providing accountability.

The workgroup viewed documentation of activations and deactivations in the incident reports as time-consuming and cumbersome with a negative impact on police work. Excessive documentation takes time that officers could spend in positive interactions with citizens. The workgroup felt that with adequate supervision, questions about discretionary activations and deactivations can be handled outside of the incident report, reducing potential for errors and abuse.

## Recording Collection, Storage, and Retention

### Upload Guidelines

When the recording officer completes a review of the recording, the recording must be uploaded to the storage servers. As PERF and the IACP noted, this transfer of data must include measures to prevent data altering, deletion, and copying. Both noted that the recordings should generally be uploaded by the end of the shift during which the BWC was used. This would help prevent accidental loss of data or unintentional viewings of the recordings and is especially important in situations where multiple individuals have access to the same BWC.

It would be ideal if the uploads were automatic (i.e., wireless); this would help save time during the upload, tagging, and even report writing. This would also save time at the end of the shift when multiple officers would attempt to upload recordings. Short of an automatic upload, a manual upload will be required. In Phoenix, as with many other jurisdictions, the recording officer performs the upload and labeling of the recording (see below). PERF recommends the same process with the caveat that in exceptional circumstances such as officer-involved shootings or in-custody deaths the officer's supervisor or investigator should upload and label the BWC recording.

In general, the upload should occur at the officer's permanent assignment, although circumstances may dictate otherwise. Since we favor increased discretion in terms of what is or is not recorded, all recordings should be uploaded, regardless of evidentiary value. The only exception might be an accidental recording. With proper review and approval from the Legal Section, we could entertain requests for deletion, just as we do within the TASER camera guidelines.

### Labeling Recordings

The labeling or "tagging" of recordings is critical. As PERF noted, the recordings should be categorized correctly to ensure they are held the proper length of time. PERF said the recording should be classified according to event type or other subcategory designation that represents the incident captured. Proper tagging allows effective searches of the recordings for quality control and data analysis.

White noted that in Mesa, the officers failed to properly label the recording about 60 percent of the time. Initially, Mesa added a "check" box to the report writing program to indicate that a recording was available. Their officers had to notify dispatch that a recording was made so the existence of a recording could be noted in the call remarks in the computer-aided dispatch (CAD) system. In addition, an evidence "voucher" was created linking their storage solution to the case information in the report management system. Mesa officers felt that these steps unreasonably increased their workload. Eventually, auto-population solutions shortened the process.

We probably would not have an auto-population solution for tagging at the time of program implementation. BWC recordings would be labeled manually, another reason to support officer discretion about whether to record. Tagging recordings would be dramatically more time consuming if all interactions are recorded without exception.

Phoenix and Mesa use CAD data or radio codes (our version of “situation found” or “SF” codes) to connect to the event number. Once a storage system is identified, the exact method can be developed based on technological capabilities. Multiple layers of labeling may be needed because of the impact on retention requirements.

### Retention Guidelines

As noted by PERF and others, retention guidelines are critical because a balance must be struck between the value of the recording from an evidentiary standpoint versus the costs associated with recording storage and public information requests. Longer storage means more cost and more transparency; failure to retain the recordings could result in failed prosecutions and lost appeals cases.

Retention of any evidence can be a complex issue, but especially so for BWC recordings. Factors for retention may include whether an arrest was made, whether there was a use of force, whether there will be a post-conviction appeal, potential civil litigation, etc. These factors shape the retention schedules recommended by the agency, the State’s Attorney’s Office, and the County Office of Law.

As the IACP notes, legislation may mandate preservation. Such legislation could include evidentiary and public information laws. As discussed in the “Legal Implications” section of this document, there are no current requirements for BWC recording retention under Maryland law as it relates to evidence generally or to public information; there may be in the future, if BWC use becomes more prevalent.

Without legal mandates, the Department must determine its own retention schedule. Those retention periods will likely be much longer for recordings with evidentiary value and will have to be finalized during our post-workgroup follow-up and after collaboration with our stakeholders. Our workgroup’s legal representatives recommend that for BWC recordings we follow the same retention guidelines as for other types of evidence, with a minimum retention of 42 months to address potential civil litigation. Failure to retain records for that length of time puts us at risk in future legal proceedings.

Recordings of non-evidentiary value can be handled much differently, although what constitutes non-evidentiary recordings must be defined. PERF notes that confrontations captured during the recording should always be considered evidence; we as an agency must define what “evidence” means - regardless of the retention schedule we develop.

PERF’s analysis found recording retention times varied from 60 to 90 days for recordings of non-evidentiary value. Others had much shorter retention periods; in Fort

Collins, Colorado, footage that does not depict contact with citizens is discarded after only seven days.

One consideration for our agency is the legal requirement related to the filing of brutality complaints by citizens. Brutality complaints are governed by Maryland law and must be notarized and filed within 90 days of the incident. Our workgroup believes that 90 days should be more than enough time to allow for the filing of these and other complaints. We cannot ignore the potential for civil litigation if a recording has some evidentiary value not discovered at the onset; again, we need a 42 month retention period.

Based on these discussions, we are looking at a minimum of 42 months before recordings could be purged, regardless of evidentiary value. That period could be mitigated if our risk managers felt that the cost of storage outweighed the potential for civil litigation. In any case, once the retention guidelines are finalized, PERF recommends that agency policy include specific retention times. Further, our agency should consider educating the public about these retention periods.

## Evidentiary Implications

Once a recording has been collected, labeled, and stored, consideration must be given to the use of the recording as evidence. As noted earlier in this document, recordings can be valuable in the prosecution of criminal cases and defense of civil litigation, and may help to limit the number of cases that actually go to trial.

To maximize that value in both types of legal proceedings, we must understand the importance of the chain of custody of this relatively new tool. The GOCCP study cited the reasons for a proper chain of custody:

- Protecting integrity of recordings for their use in investigation and court proceedings.
- Guaranteeing that the recording is not being used inappropriately, such as for commercial or entertainment purposes.
- Laying a foundation for court admissibility.
- Establishing whether witnesses have reviewed the recording before providing a statement or testifying in court.

These are common sense issues. With regard to evidentiary value and protection of the chain of custody, the NIJ noted that once a recording is admitted as evidence in court “the question of admissibility can be linked to whether an officer can authenticate the audio/video recording as a true and accurate depiction of the events.” The NIJ went on to emphasize the need for “time and date stamp/identifiers...imprinted on the media either in the video images directly or in the underlying metadata information of the data files.”

Our State’s Attorney’s Office (SAO) workgroup representative agrees with GOCCP and the NIJ. The SAO representative and our workgroup are confident that the officer making the BWC recording will be able to confirm in court that it is the “true and accurate depiction of the events.” With regard to retaining the integrity of the metadata and the data files, we already have the technical capability and processes to ensure we have master copies of evidentiary recordings - so called “gold copies” - that can withstand legal challenge. This is known as “hash authentication” and is recommended in the Technical Subcommittee report. We agree that it is imperative that an un-redacted and unchangeable original recording be preserved.

The SAO representative and the workgroup feel that as long as the appropriate technology is in place, the BWC recordings will be treated similar to recordings we currently process as evidence, there should be no negative impact on court cases or the chain of custody. There should be no need for special certification or documentation, and no need to change the medium used to present the recordings for court purposes. Our workgroup’s Legal Section representative feels the same holds true with regard to the impact of BWC recordings on potential civil litigation.

## Data Maintenance, Management, and Analysis

### Custodianship and Security

Designation of a custodian of the BWC data is critical. Due to the importance of retaining the integrity of the data, we recommend that technically proficient personnel within the Digital Multimedia Evidence Unit (DMEU) of the Forensics Services Section (FSS) serve as the official custodian of the records.

The DMEU is already responsible for recordings made during the deployment of TASER cameras. The DMEU will ensure that recordings are not altered (redacted) or deleted without approval, and that recordings are managed by appropriate evidentiary standards. The DMEU will also ensure a reliable backup system is in place.

The DMEU must set clear policy related to prevention of unauthorized access to or the release of BWC data. This must be done in conjunction with our Technology and Communications Section (TCS), which will control administrative rights and settings related to the selected recording storage solution. As part of its oversight, the TCS will monitor the access of those with permission to download the recordings and associated data. Managing such access is a key to protecting the integrity of the recordings and the data. The parameters for access to the data should be clearly stated in policy.

### Access for Copying, Redactions, or Deletions

The DMEU will also have to oversee the tedious and complex process of recording redactions and deletions. The first, time-consuming step of the process involves identifying what will be redacted. In Mesa the redaction request is first sent to the officer who made the BWC recording. The officer identifies people and items that should be redacted and forwards that information to the unit that will conduct the redaction. Depending on the final redaction guidelines, our Legal Section feels it could handle most redaction decisions without consulting with the recording officer; however, it is impossible to know if this will be true in practice. In some instances, only the BWC operator will know the actors in a recording. Depending on the volume of requests and the need for input from officers, redaction consultations could result in officers missing time from regular assignments and incurring overtime costs.

As demonstrated to our workgroup illustrated, the technical process of redaction is tedious and time consuming. Our DMEU representative in the workgroup found that redaction generally takes about 30 times longer than the recording itself. Mesa's evaluation produced a similar finding. One reason for the lengthy redaction process lies with the fact that some BWC recordings contain as many as 30 frames per second. Another reason is the complexity of the technical redaction process and equipment, which requires well-skilled personnel.

Redactions or copying of recordings related to criminal proceedings could be done by personnel from the State's Attorney's Office (SAO) or by the DMEU (at the SAO's direction). With regard to general information requests, redactions would be done solely by the DMEU in cooperation with our own Legal Section, which will have final authority over redactions.

The issue of deletions is equally important. There must be input from the SAO and the Legal Section regarding regularly scheduled purges of recordings, as well as deletions made by specific request (such as expungement). Our research indicates that the purging of recordings should be part of the policy, and consideration should be given to multi-layer review of non-standard deletion requests. PERF suggests contacting both the Legal Section and State's Attorney's Office before deletion occurs. Our workgroup feels the State's Attorney's Office should be contacted first regarding criminal cases. Even then, the Legal Section should make the final determination, regardless of whether the recording has evidentiary value.

### Quality Control and Data Analysis

Access to recordings should be granted for quality control. The IACP recommends that recordings be "randomly checked at least monthly," and more frequently for officers with performance issues. Phoenix allows a lieutenant to conduct random quality control reviews. PERF recommends that Internal Affairs personnel, rather than an officer's supervisor, perform such audits. Our Accreditation and Inspections Team is trained to conduct audits, but our workgroup feels we could control quality better at the "local" level through monthly or quarterly line inspections.

These quality control personnel should make routine review of recordings part of the standing inspection process. An administrative officer from each unit could randomly check a minimum number of recordings during a set time period. This review could be conducted as part of currently required inspections of other police records. The reviewing officer would make the appropriate administrative notations within the inspection documentation, and should bring any deficiencies to the attention of the unit commander for corrective action. Our Legal Section workgroup representative emphasized that once the deficiency is identified, it must be addressed.

Finally, access to recordings should be considered for periodic reporting of data trends. The unit responsible for trend identification and data analysis will depend on the evidence solution chosen. Some evidence solutions have better search capabilities than others. We feel it would be useful to know how and when the BWCs are used, the length of recordings, frequency of deactivations, etc. The data could help with quality control and corrective actions, long-term budgeting, and even grant funding requests. Even if our chosen evidence solution has limited search capabilities, our Scanning and Forecasting Team may be able to conduct additional limited searches through our existing records management system, which has indexing capability.

## Equipment Specifications and Recommendations

Due to the complexity of BWC technology, a sub-committee within the workgroup was assigned to address equipment specifications and recommendations. The Appendices include a comprehensive report on technological specifications that should be considered in evaluating any potential police body-worn camera program. Recommendations and expected cost estimates are provided when possible.

### Executive Overview

The most significant recommendation of the sub-committee is that BWC programs should be approached at the “enterprise” level. This means identifying a “single source” solution that covers everything from the BWC device itself to the digital file management system and all components in between. An enterprise solution provides a single point of administration for devices, users, files, redaction, chain of custody, and dissemination. It also provides the fewest possible dependencies for multiple providers, support mechanisms, manual processes, and system interfaces.

Another significant recommendation is the need to engage a cloud storage service provider. Hosted solutions offer redundant storage with system uptime and security levels that typically exceed those attainable by individual municipalities. Total cost of ownership is typically lower because staffing, electrical service, environmental controls, facility space, and scalability requirements are handled by the provider in a consolidated model. Additionally, hosted solutions offer robust features including role-based security, redaction/reproduction tools, and full auditing.

One of the largest quantifiable considerations is the fiscal investment required for implementation and maintenance. The report contains a range of fiscal investments based on assumed operational models and projected capture and storage. The report relies heavily on the cost estimates of enterprise solutions that constitute total system pricing packages.

These estimates place first-year investment figures from about \$0.6 million to \$1.2 million. The fourth-year estimates range as high as \$8.5 million, counting the aggregation of recording storage over time. Full illustrations of investment ranges are included in the “Technology Fiscal Investment” section of the sub-committee report.

Device selection requires consideration of many unique specifications. The chosen device should limit intrusiveness in field encounters, and its environmental protection standards should assure reliable field use. Minimal user controls and features are recommended for simple field operation. The standards for capture specifications are reasonable, with a video resolution of 640X480, recording speed of 30 frames per second, and a lux rating of 1-0.5. Observational enhancements such as night-vision or long range audio are not recommended. Battery life, recording life, and storage capacity should support continuous 12-hour operation.

The sub-committee has no strong recommendation for a BWC mounting position; each position has technical limitations. Point-of-view mounted systems – often attached to the user’s head or eyeglasses - provide the closest available approximation of the police officer’s perspective, but are more intrusive to field interactions due to their appearance. Torso-mounted solutions are generally more passive in appearance, but are easily obstructed or moved out of position, depending on the officer’s physical orientation. The sub-committee recommends devices that offer flexible mounting options. It suggests that an operational pilot group conduct additional analysis.

Additional detailed information about each technical specification is found in the Appendices.

## Human Resource Implications

### Training Implications

For BWCs, as with any new technology, significant time must be dedicated to training and education. Many personnel would need to be trained, including:

- Officers using the BWCs in any capacity.
- Supervisors and commanders overseeing operational functions.
- Criminal investigative personnel responsible for follow-up activities.
- Professional standards personnel, including the Internal Affairs Section and Accreditation and Inspections Team.
- Technical staff supplying support to the end users; this includes those in our Technology and Communications Section and the Office of Information Technology.
- Technical staff acting as custodian of recordings, such as those in our Forensics Services Section.
- Records management personnel, due to the presence of BWC information in our incident reports and their role in fulfilling public requests for police reports.
- Media and Communications Section personnel who will need to coordinate informational inquiries.
- Legal Section personnel responsible for coordinating public information requests and decisions relating to copying/redacting/deleting recordings.
- State's Attorney's personnel responsible for prosecution of criminal cases and redactions of recordings as the result of legal motions.
- Office of Law personnel responsible for defense in civil litigation and development of future legislation.
- Any oversight personnel, such as those in elected positions, budget-related positions, County-level communications positions, etc.

Training may be needed for neighboring law enforcement agencies such as the Baltimore County Sheriff's Department or other police departments so they know what to expect when we have joint operations. In addition, and as noted in another section of this report, this education must also extend to our community members.

Depending on the audience, multiple types and styles of training will be necessary. Technical demonstrations and classroom instruction will educate on the complexity of the laws and policies governing BWC use. A scenario-based component would be of great value to all audiences because it lets the user to see the difference between his or her perception of the event and what is actually captured in the recording.

For non-BWC users, exposure to BWCs is needed for awareness and understanding. We expect this training to take a few hours at most and to provide it in a variety of venues.

For BWC users, a specialized training course would be necessary. (Police recruits should receive the training during their Recruit program at the Training Academy.) Initial BWC training would likely take a full day, especially if it includes a scenario-based component. There would have to be provisions for BWC users and their supervisors to receive refresher training periodically. This refresher training could be performed at In-Service training or during roll call. PERF recommends that the training be done at least once a year. In addition, BWCs users and their supervisors should have access to related procedures via a training manual or other hard copy, on mobile data terminals, and through our agency's Intranet.

Initial training on the use of the BWC would require at least a full day because the training extends beyond the BWC. The presence of the BWC will change the way officers "do business" in many aspects beyond the use of the camera itself. As the NIJ noted, "training should not only be for use of the BWCs but also for the officer's perceptions of the camera." BWC users will have to be as skilled as possible since their actions will be closely scrutinized. It would be impractical to conduct such important training in just a few hours.

We believe the BWC user training should include components on how the equipment functions and all oversight policies associated with the BWC. Other components should include:

- Technical training on how the equipment works, including testing, operation, upload procedures, etc.
- Legal awareness regarding wiretapping laws, privacy issues, consent and notification issues, etc.
- Enhanced verbal skills training to improve effectiveness and avoid inappropriate language.
- Implementation of new language to instruct citizens and officers about the presence of a BWC during an interaction.
- Education about the impact on officer safety from BWC use, and ways to mitigate potential hazards.
- Scenario-based training that encompasses all the training components and gives the users a sense of the impact of BWC usage.

From an operational standpoint, the most important component may be the need for enhanced report writing skills. BWC usage will require greater detail in incident reports to support what is in the recordings. BWC users may wish to comment in the body of the report about decisions related to activation, deactivation, and reactivation of the BWC, even if not required by policy. In addition, and as noted by our SAO and Strategic Planning Team workgroup representatives, officers may need to document in the report both pre-recording review perceptions and post-recording review findings. Further, officers need to understand that despite the BWC use, they still must obtain written statements as they have always done, as BWC recordings are not a substitute for report documentation.

One other important consideration is the need for user buy-in for BWCs. This issue was covered in many of the think-tank documents. As the NIJ noted, “one of the most challenging issues an agency may face is officer acceptance.” White noted that in Mesa’s initial survey, only 23 percent of the officers polled thought they should have BWCs, and less than half felt that other officers would welcome the presence of a camera at the scene.

To overcome this hurdle, the positives of the program must be highlighted and explained clearly. White emphasizes the NIJ position that the officers should understand that the primary purpose of BWCs is for evidence collection and officer safety. White stressed the value of the BWC as a tool. He felt that an effort must be made to break down the officers’ fear of technological complexity and the inundation of technological tools, and to stress the value of BWCs in improving the citizens’ view of officer professionalism.

As part of this buy-in process, BWC users need to know the empirical basis for the program. The IACP noted that one study of in-car cameras showed officers were exonerated 93 percent of the time when a recording existed. In Phoenix officers became more active because they had video to support the fact that they were acting legally.

#### Use in Performance Evaluation

Use of recordings for performance evaluation was discussed at length. Recordings can be valuable tools for enhancing performance. Some workgroup members noted that reports are reviewed routinely, and since BWC recordings are integral to the report, they should be reviewed as well. Others spoke to the impracticality of reviewing all recordings; this is noted in a previous section in this report.

Partly due to limitations of the technology, the review of recordings cannot replace personal observations by supervisors. If there are performance deficiencies, supervisors need to observe and correct them as soon as possible. As one workgroup member noted, we should not ask supervisors to routinely review BWC recordings after the fact, a practice we would discourage among the public. The workgroup felt that if supervisors are going to use recordings for performance evaluations the review should occur in conjunction with personal observations, and only when cause exists – for example, when a documented performance enhancement program is in place.

The workgroup saw value in using recording review in training settings at the Academy and in field training scenarios, where the Field Training Officer (FTO) could perform a peer-to-peer review of the recordings. Again, recording review would need to occur in conjunction with personal observations by the FTO.

The workgroup agreed with the IACP that officers should be allowed to view their own videos for self-training and to evaluate performance. The workgroup did not feel that recording review should be used for promotional or transfer packages due to the

impracticality of making copies. In limited circumstances our Awards Review Board may find such a review helpful.

### Staffing Needs

Staffing is one of the most challenging issues related to BWCs. As noted in a previous section, many agencies shy away from BWC programs due to the cost of associated staffing requirements. This has been a hard lesson for agencies that implemented programs but were unprepared for just how costly they could be.

In Mesa, police expect to exponentially increase duties, and add personnel to manage the program. Mesa stated it needs to add training and program management coordinators at the district level, among other new staff. The evaluation indicated that a failure to provide adequate and effective oversight of the program could expose “the department to increased liability.”

Many of the units and functions that would require increased staffing were represented in the workgroup, including the:

- Legal Section, which would need additional personnel to handle the public information requests.
- Forensic Services Section, which would need new technicians to handle copying, redaction, and deletion requests.
- Technology and Communications Section, which would need additional personnel to handle equipment maintenance and administrative oversight.
- Training Section, which will need at least one additional instructor to handle initial and annual refresher training.
- Media and Communications Section, which would need an additional coordinator to handle an expected increase in requests from media and other stakeholders.
- State’s Attorney’s Office, which would need new technicians to handle the anticipated response to legal motions.
- Office of Information Technology, which will need multiple personnel to assist with storage solutions and the parallel role they share with the Technology and Communications Section in administrative oversight.

Every one of the units mentioned above must have at least some staffing in place before a program is implemented. If the BWC program is phased in, staffing augmentation can be done incrementally. Training personnel will take time, just as training BWC users takes time. There may even be a need for personnel certifications, if required by accreditation agencies. Failure to have at least some of these personnel trained at the time of program implementation could put the agency in a backlog situation for a long time to come.

## Expected Program Cost Estimates

Listed below are estimated program costs, based on general assumptions. These costs are driven by technical decisions about BWC equipment and recording storage, and by unresolved policy decisions that will have a fiscal impact. When those decisions are made we are still unlikely to be able to determine specific costs; more likely we will identify an expected cost range. This is due, in part, to the fact that technology constantly changes, translating to potential cost increases, although there are factors which could mitigate costs. Depending on the final program determinations, the estimates could be greater than estimated below; they are unlikely to be less. Our assumptions:

- BWCs would be issued to 1,200 police officers, corporals, and sergeants.
- Ten percent of the deployment would occur during the first year pilot. The remaining 90 percent deployment would occur in a two-year rollout during the second and third years of the program.
- Rollout costs (below) are accrued over the two-year rollout period, not yearly.
- Annual costs (below) apply to the post-rollout period, beginning in the fourth year of the program and occurring in perpetuity (but without cost increases considered).
- The implementation would include an “enterprise solution,” which would absorb annual BWC and ancillary equipment maintenance and replacement costs.
- Training costs only apply to the 1,200 sworn personnel receiving a full day of training. It covers neither refresher training nor training for others requiring some alternative BWC training.
- Equipment costs do not include basic computers, desks, chairs, etc., for new personnel.

<i>Fiscal Encumbrance</i>	<i>(Costs)</i>	<i>Pilot</i>	<i>Rollout</i>	<i>Annual</i>
BWCs and ancillary equipment	= (min) (max)	\$50,000 \$120,000	\$500,000 \$1,200,000	N/A N/A
Recording storage/maintenance	= (min) (max)	\$120,000 \$120,000	\$1,500,000 \$8,500,000	\$2,750,000 \$8,500,000
Departmental staffing	=	\$664,300	\$2,121,600	\$1,060,800
Other agency staffing	=	\$287,300	\$1,198,600	\$599,300
Training costs	=	\$32,000	\$288,000	N/A
Totals	= (min) (max)	\$1,153,600 \$1,223,600	\$5,608,200 \$13,308,200	\$4,410,100 \$10,160,100

Some of our assumptions regarding staffing costs:

- Staffing estimates are based on what is needed to get the program running in the first year, followed by likely annual staffing needs based on the deployment schedule noted above.
- Salaries are based on 10 years of service, with a 30 percent fringe cost built in.

<i>Likely Staffing Costs</i>	<i>Initial</i>	<i>Annual</i>	<i>Salary</i>
Police Corporal (TCS)	1	1	\$97,500
Police Officer First Class (TCS)	2	3	\$89,700
Police Officer First Class (Training)	1	1	\$89,700
Forensic Services Technician (FSS)	1	4	\$67,600
Criminal Records Processor (IRMU)	1	1	\$54,600
Attorney (Legal Section)	1	2	\$104,000
Public Information Specialist (MCS)	1	1	\$71,500
Evidence Specialist (SAO)	1	5	\$78,000
Network Engineer (OIT)	1	1	\$91,000
Desktop Technician (OIT)	1	1	\$52,000
Report Writer/Programmer (OIT)	1	1	\$66,300
Subtotals	12	21	N/A

## Community Awareness and Education

Managing public expectations will be critical to the success of a body-worn camera program. This is true of any program announcement, but especially so with BWCs because of the complexity of the issue and the many misconceptions and assumptions about BWCs. This was confirmed in our meeting with community representatives – they did not fully understand the impact of constituents being on camera.

The public release of this advisory report could be a significant first step. The report itself will raise public awareness of the upside and downside of BWCs and of the way Baltimore County likely would approach such a program.

The Media and Communications Section, in conjunction with the County Executive's Office of Communications, will provide information about the report and its findings using community outreach, official County web-based tools, and mainstream media channels.

### Guidelines for Awareness Program Launch

The launch of a BWC program from the outset should specify the reasons for the program, what we hope to accomplish, and how the program will work. As PERF noted, the public is likely to be “more accepting of the BWC if agencies are transparent about their camera policies and practices.” To that end, issues that must be addressed for the public include:

- The type of BWCs to be used.
- The number and assignment of officers who will wear BWCs.
- When the BWCs will be activated or deactivated, and the role of officer discretion in those decisions.
- The fact that the camera is worn facing outward, meaning citizens will be filmed.
- The fact that filming may occur in private homes.
- An awareness of consent laws and whether a citizen can refuse to be recorded.
- The role of recordings in an investigation.
- The role of recordings as evidence.
- The recording's status as a public record under the Maryland Public Information Act (MPIA), to include investigatory or other exceptions which might preclude release of the recording.
- How MPIA requests for BWC video will be handled, to include redactions.
- An expectation regarding initial and ongoing operational costs.
- The data retention period for recordings.
- The limitations of BWCs; i.e., they do not tell us what the officer perceived, where his attention was focused or what his thought processes were. They only show the point of view of the BWC.

This last point – the limitations of BWCs – is critical. We must convey that cameras are not a panacea. Especially in use of force incidents, they cannot answer the question of what an officer perceived or why he took a certain action. The camera is a tool designed to provide additional information about an incident or event; the information provided by the camera is not the only, nor is it necessarily the most important, evidence.

Our BWC public outreach plan should include:

- A media event to introduce and explain the BWC program.
- Web-based information about the BWC program (to be prepared in advance of the media event).
- Sharing of web-based information through official social media channels.
- Personal outreach to specific stakeholders.
- A print piece (tri-fold or handbill) summarizing the BWC program and its purpose, for distribution at the community level.

Educational outreach about the BWC camera program should be ongoing and should take place routinely after use of force incidents and other controversial police incidents. This ongoing outreach to the public also gives us an opportunity to stress that, despite some limitations, the goal of the BWC program is to foster transparency and accountability while protecting civil liberties and privacy interests. This positive approach to awareness should result in the social capital we need from the community to be successful.

## Final Workgroup Findings and Recommendations

This section is comprised of two parts. The first section outlines the workgroup's position about whether a BWC program should be implemented at this time; it includes a discussion of the support for that position. The second section is a set of recommendations that should be considered if the decision is made to implement a BWC program.

### Workgroup Position and Support Discussion

After a great deal of discussion and research, the 18 members of the workgroup were polled anonymously about whether our agency should implement a BWC program. Each member was asked to provide up to three reasons supporting their position. The results of the poll were as follows:

- *Three members felt a BWC program should be implemented.*
- *Two members felt a BWC program should not be implemented.*
- *Thirteen members felt the decision to implement a BWC program should be delayed.*

Two of the three members who felt a BWC program should be implemented took that position conditionally. The first condition was that program implementation should only occur with legislative changes protecting officers and the agency from unintended violations of the Maryland Wiretap Act. The second condition was that the program must begin as a pilot, with a thorough evaluation of the pilot before full deployment.

One of the three members recommending program implementation did so partly because a BWC program seemed inevitable. The member felt that it would be better to develop the terms of our own program rather than having the state legislature dictate those terms. Other reasons for supporting a BWC program included:

- Increased accountability to citizens, resulting in a return by police to a more service-oriented profession.
- Potential reduction of frivolous complaints and lawsuits initiated by citizens.
- The BWC's value as a training aid.
- An expected positive impact on prosecutions due to the evidentiary value of recordings.

In contrast, 15 workgroup members did not support BWC program implementation. Two members of the workgroup felt a BWC program should not be implemented at all. Thirteen said that a decision whether to implement a BWC program should be delayed, and many said they took this position because they felt that a BWC program was inevitable. Otherwise, these members said, they would have recommended against BWCs altogether.

The 15 members not in support of BWC program implementation, despite positional nuances, often cited similar reasons for their position:

- *The departmental problems and community pressures that have led other agencies to move toward BWCs at this time are largely nonexistent here.* Twelve members said there have been no significant incidents or systemic problems resulting in a call from the community for this technology; a BWC program may be seen as a solution to a problem that doesn't exist – and that given the cost and complexity of the program it would be a mistake to move forward at this time. In our meeting with community representatives, we heard no demand for BWC use. Workgroup members noted that we enjoy a good relationship with the community, unlike some agencies that recently have adopted BWCs; many have done so in response to a public outcry for additional oversight due to perceived problems relating to use of force, racial profiling, etc. Our internal data shows downward trends regarding use of force and complaints, and we have very few officers suspended for departmental violations. Our agency has been involved in only a few lawsuits related to use of force in the past several years, most related to TASER usages – an issue recently addressed by the pilot program for TASER cameras. It was noted that the Department sought out TASER camera technology on its own; there has never been a call from the community for TASER cameras or in-car cameras.
- *Legislative changes need to be made in the Maryland Wiretap Act.* Ten members felt that we need to protect our agency and its members from unintended violations of the wiretapping statute; indeed, this is a “must” to be able to operate the equipment with clear policy direction. Failure to make legislative changes would require a complex set of rules regarding notification and consent; this could harm operational efficiency and officer safety.
- *Legislative changes need to be made regarding access to BWC recordings under the Maryland Public Information Act (MPIA).* Nine members felt that failure to limit releases will have a significant impact on operational needs and our policy/procedure, and create a huge financial drain on the County.
- *The expense of a BWC program could be astronomical.* Eight members felt this true not only for equipment and maintenance, but especially for storage space and additional staffing. Such costs would be passed on to the taxpayer. We have yet to see evidence that the cost of BWC use in Baltimore County would be offset in savings from fewer lawsuits, a benefit noted in other studies. Once in place, the BWC program would be difficult to terminate or even scale back, leaving the County with a significant, permanent fiscal obligation and little financial payoff. It is noteworthy that TASER recently cited recordings storage as a huge growth area for its company; we know other agencies avoided BWCs for this reason.
- *Far more discussion is required with communities to educate them and manage expectations.* Seven members noted that the public has little understanding of the impact of laws related to police recordings, and that we have not had nearly enough time to discuss this with them. Community representatives echoed this concern at a recent meeting with members of the workgroup. Workgroup

members felt that citizens will have concerns about privacy issues and the public release of recordings; this could result in a chilling effect on communications with law enforcement. Several members expressed concern that BWC equipment is marketed to the public as a tool that shows what “truly occurred” during a police interaction - despite what we know about equipment limitations and the complexity of police perception at the time of the event.

- *Data from other programs is limited, so the true impact of BWC programs is still difficult to forecast.* Four members felt we should wait and see how other programs perform and learn from their experiences. Two of those four members noted that we are especially interested in the experiences of larger agencies, few of which have BWC programs at this time. The GOCCP study also cited the benefits of learning from early adopters.
- *Other future legislative mandates may impact BWC programs.* Two members felt that – beyond issues related to consent and records access - key legislative requirements involving notifications of recording, data retention, etc., may be on the horizon. These members felt we should wait for these decisions.
- *The redaction process is still evolving, technologically and procedurally.* Two members felt that, before starting a BWC program, we should see how the redaction process changes in the future.
- *The use of BWCs likely will adversely affect operational productivity.* One member felt the effect could be significant, especially with regard to the administrative time needed to perform uploads, labeling and tagging, etc.

The 15 members who recommended denying or delaying a BWC program decision expressed their opinions in great detail and with passion. The three responses supporting program implementation offered brief, concise responses. This indicates that workgroup members who opposed a BWC program at this time felt strongly.

The last time the workgroup met it discussed the results of the meeting with community representatives. We also discussed our internal survey findings. Workgroup members were encouraged to summarize their thoughts. Some reiterated concerns that BWC use would lead to judiciousness on the part of officers; officers may unconsciously withdraw from citizen contact, harming community policing efforts.

Others observed that new technology usually acts as a “force multiplier,” making policing safer and more efficient. BWCs, however, may take time away from our interactions with citizens. This is the first technology considered by our agency that could cost police additional administrative time. These two observations – the potential for overly judicious policing and the drain on the officer’s time – led many workgroup members to conclude that BWCs could hinder efforts to serve the community - the antithesis of what we seek to achieve.

At the end of the final workgroup meeting, members were given the opportunity to change their initial survey position regarding BWC use. At the time of this report, none chose to do so.

### Recommended Actions Prior to an Initial Program Decision

In our research, the workgroup identified tasks that should be completed prior to a final decision regarding BWCs:

- Conduct analysis to determine if an empirical need to use BWCs exists; this should include a cost/benefit analysis related to use of force in our agency and lawsuits defended by the County.
- Conduct extensive outreach to the community so citizens have a thorough understanding of legal issues related to BWCs, and the likely fiscal impact on citizens as a result of such a program.
- Conduct post-outreach citizen surveys to see if citizens broadly support BWC implementation.
- Review additional BWC program evaluations to see if the results from these agencies are consistent with the few available to us thus far.
- Perform extensive testing and evaluation of selected BWCs, in lab and field conditions.

### Recommended Actions Prior to Program Implementation

If the County decides to move forward with a BWC program, prior to program implementation the agency should:

- Seek legislative changes at the state level providing protections for the agency and its officers from unintended Maryland Wiretap Act violations.
- Seek a legislative compromise at the state level regarding the release of BWC recordings that balances the need for transparency against the fiscal and operational impact of release requests.
- Consult with other agencies regarding their experiences with BWC implementation.
- Conduct a focus group at the patrol officer level, seeking input by likely BWC users.
- Collaborate with the Baltimore County Public School system on potential BWC use in schools.
- Develop a BWC implementation team that includes a cross-section of agency members.

- Formalize all policy issues through a standard command review process.
- Construct a BWC pilot program with incremental deployment.
- Acquire BWC equipment with a high level of recording capability and quality.
- Implement a comprehensive equipment program to minimize administrative support needs.
- Engage a cloud storage service compatible with our equipment selection.
- Provide an adequate infrastructure, to include appropriate staffing, to ensure appropriate support for the program from its inception.
- Provide adequate training to all personnel in a position to use BWCs or review BWC recordings.
- Conduct an awareness campaign designed to inform citizens and manage their expectations regarding a BWC program.
- Develop feedback mechanisms for BWC users, oversight entities, and citizens.
- Develop memoranda of understandings with external agencies (SAO, OIT, etc.) regarding access and oversight issues.

#### Recommended Actions After Pilot Program Implementation

Once the pilot program has ended, and prior to formal program institutionalization, the agency should:

- Conduct post-implementation surveys and interviews with citizens, officers, and supervisors to determine the initial impact of the program.
- Conduct a full pilot program evaluation to determine whether the program should continue.
- Determine likely cost for agency-wide implementation based on actual costs from pilot program.
- Develop additional legislative recommendations, if necessary.
- Make necessary policy adjustments.

## Recommended BWC Program Policy and Procedures

Whether the BWC program is in pilot status or formally institutionalized, the policy and procedures should state the following:

- BWCs will be deployed to patrol and traffic assignments, where the greatest number of police interactions with citizens occurs.
- BWCs will not be deployed to specialized units, unless there is a demonstrated need and operational compatibility.
- BWC equipment and recordings are the property of the Department.
- BWC use should be prohibited during off-duty or secondary employment status, in administrative settings, and during non-departmental activities.
- Officers assigned BWCs must use them on duty when available.
- BWC use is not required if impractical or unsafe to do so.
- Officer discretion is permitted in determining when a BWC should be activated or deactivated.
- Generally the BWC should be activated at the beginning of police-citizen interactions involving enforcement, calls of a potentially criminal or adversarial nature, or any other contact that that officer believes appropriate.
- Notification of a citizen regarding BWC recording is discretionary (unless required by statute).
- Officers may review BWC recordings before completing incident reports or providing statements.
- The existence of a BWC recording must be noted in some fashion in the incident report.
- The officer's perception of the event prior to and after reviewing a BWC recording must be noted in the incident report.
- Prior to the end of their shifts, officers must upload and label recordings they initiated.
- BWC record retention guidelines will set retention periods that acknowledge the difference between recordings of evidentiary and non-evidentiary value.

- Specialized evidence handling procedures must be used to ensure a proper chain of custody.
- An original unedited version of the recording must be held in a secure location to ensure that it cannot be altered or deleted.
- Custodianship of BWC data will be assigned to a specific unit.
- Inappropriate access and use of BWC recordings and data is prohibited.
- Editing and deletion must involve the Legal Section and the DMEU.
- Certain pre-determined units are authorized to access BWC recordings and data for administrative investigations and quality control.
- Use of BWCs is permitted in pre-determined training or performance enhancement settings.
- Certain requirements must be met with regard to initial and annual BWC training and certification.
- Equipment inspection and maintenance is required at certain pre-determined intervals.

## Appendices

Abbreviations Guide

References and Citations

Technical Subcommittee Report

## Abbreviations Guide

ACLU – American Civil Liberties Union

AEC – Advance Encryption Standard

AG – Attorney General

AP – Associated Press

BCOPD – Baltimore County Police Department

BCPS – Baltimore County Public Schools

BWC – Body-worn camera

CAD – Computer-aided dispatch

CALEA – Commission on Accreditation for Law Enforcement Agencies

CBS – Columbia Broadcasting System

CCTV – Closed circuit television

CC# - Central Complaint Number

CD- Compact Disc

CID – Criminal Investigations Division

CJIS – Criminal Justice Information System

COPS – Community Oriented Policing Services

CSI – Crime Scene Investigation

DMEU – Digital and Multimedia Evidence Unit

DOJ – Department of Justice

DWI – Driving While Intoxicated

FBR – Field-Based Reporting

FERPA – Family Education and Privacy Rights Act

FOP – Fraternal Order of Police

FSS – Forensic Services Section

FTO – Field Training Officer

GB – Gigabyte

GOCCP – (Maryland) Governor's Office of Crime Control & Prevention

GPS – Global Positioning System

IACP – International Association of Chiefs of Police

IRMU – Information and Records Management Unit

LED - Light Emitting Diode

LPR – License plate reader

MCS – Media and Communications Section

MPEG – Moving Picture Experts Group

MPIA – Maryland Public Information Act

NAACP – National Association for the Advancement of Colored People

NFL – National Football League

NIJ – National Institute of Justice

NLECTC – National Law Enforcement and Corrections Technology Center

OIT – Office of Information Technology

OJP – Office of Justice Programs

PBJ – Probation Before Judgment

PERF – Police Executive Research Forum

PIA – Public Information Act

REP – Reasonable Expectation of Privacy

SAO – State’s Attorney’s Office

SD – Secure Digital

SF – Situation Found

SOD – Support Operations Division

SRO – School Resource Officer

SSL-RSA – Secure Socket Layer – Private Encryption Key

SWAT – Special Weapons and Tactics

TCS - Technology and Communications Section

UK – United Kingdom

UOF – Use of force

US – United States

USB – Universal Serial Bus

WiFi – Wireless Network

WLAN – Wireless Local Area Network

WPAN - Wireless Personal Area Network

WWAN – Wireless Wide Area Network

WWLAN - Wireless Wide Local Area Network

## References and Citations

- Albuquerque (NM) Police Department. 2013. *Use of Tape/Digital Recorders Policy*.
- Anderson, Joanna. January 26, 2015. *Democrats Plan Police Body-Camera Legislation*. [www.rollcall.com](http://www.rollcall.com). 1/28/2015 Accessed Online.
- Alexander, Keith L. January 25, 2015. *Lawyers See New Benefit to D.C. Police Body Cameras – As Evidence for Trials*. The Washington Post. 1/26/2015 Accessed Online.
- Alexander, Rachel. December 7, 2014. *Body Camera Use Abuts Privacy Issues*. The Spokesman-Review. 1/20/2015 Accessed Online.
- Aransas Pass (TX) Police Department. 2014. *Mobile Audio Video Policy*.
- Arizona Department of Public Safety. 2012. *Field Video and Audio Program*.
- Associated Press. July 13, 2007. *Britain Straps Video Cameras to Police Helmets*. NBC News. 3/26/2015 Accessed Online.
- Bakst, Brian and Ryan J. Foley. February 6, 2014. *For Police Body Cameras, Big Costs Loom In Storing Footage*. Associated Press – [www.ap.org](http://www.ap.org). 2/2/2015 Accessed Online.
- Bernstein, Maxine. February 5, 2015. *Portland Police Chief Wants to Add Tech support Jobs to Help with Body Camera Program*. The Oregonian. 2/5/2015 Accessed Online.
- Briscoe, Tony. December 1, 2014. *Chicago Police to Begin Testing Body Cameras on Officers In 60 Days*. Chicago Tribune. 12/4/2014 Accessed Online.
- Burnsville (MN) Police Department. 2014. *Mobile Video Recorder System Policy*.
- Caldwell County (NC) Sheriff's Office. 2014. *On-Body Recording System (OBRS) Policy*.
- Cassidy, Megan. January 22, 2015. *Phoenix Police: Body Cameras Beneficial But Costly*. The Republic. 1/23/15 Accessed Online.
- Chang, Cindy. September 21, 2014. *L.A. County Sheriff's Deputies Test 4 Types of Body Cameras*. LA Times. 12/4/2014 Accessed Online.
- Ciaramella, CJ. February 23, 2015. *Privacy Activists Fight Police Bodycams*. The Daily Beast 2/25/2015 Accessed Online.

City of Baltimore (MD). 2015. *Mayor Rawlings-Blake's Working Group on the Use and Implementation of Body-Worn Cameras*.

City of Norman (OK) Police Department. 2014. *Request for Proposals Digital In-Car Video/Audio System and Integrated Body Worn Video/Audio Solution*.

Edmonton Police Service (AB). 2013. *Body Worn Video Pilot Project Interim Report*.

Farrar, William. 2013. *Self-Awareness to Being Watched and Socially-Desirable Behavior: A Field Experiment on the Effect of Body-Worn Cameras and Police Use-of-Force*. Washington, DC: Police Foundation.

Foley, Ryan J. and Jim Salter. February 6, 2015. *Cities and Departments Face a Budget Dilemma in the Rush to Put Cameras On*. Associated Press - [www.lawofficer.com](http://www.lawofficer.com). 3/24/2015 Accessed Online.

Force Science Institute. December 1, 2014. *Survey Officer Attitudes Before Issuing Body Cams, Researchers Urge*. [www.policeone.com](http://www.policeone.com). 12/9/2014 Accessed Online.

Force Science Institute. September 23, 2014. *10 Limitations of Body Cams You Need to Know for Your Protection*. [www.policeone.com](http://www.policeone.com). 12/8/2014 Accessed Online.

Fox45. December 16, 2014. *Laurel Police See 30% Reduction in Use of Force With Body Cameras*. WBFF Fox Baltimore. 12/17/2014 Accessed Online.

Fox News. January 21, 2015. *Minnesota Bill Would Keep Body Camera Footage Private*. [www.foxnews.com](http://www.foxnews.com). 2/2/2015 Accessed Online.

Fraternal Order of Police, Grand Lodge. 2014. *Body-Worn Camera (BWC) Recommended Best Practices*. Columbus, OH: FOP Labor Services Division.

Governor's Office of Crime Control and Prevention (MD). 2014. *Workgroup on the Implementation and Use of Body Worn Cameras by Law Enforcement*.

Gurman, Sadie. March 10, 2015. *Denver Body Cams Didn't Record Most Use of Force Cases*. Associate Press. 3/24/2015 Accessed Online.

Hartford (CT) Police Department. 2012. *Body Worn Audio/Video Recording System Policy*.

Hermann, Peter and Rachel Weiner. December 2, 2014. *Issues Over Police Shooting in Ferguson Lead Push for Officers and Body Cameras*. Washington Post. 12/4/2014 Accessed Online.

Hickory (NC) Police Department. 2015. *Body Worn Cameras General Order*.

Hill, Kashmir. November 5, 2014. *A Future in Which Every Police Officer Wears a Body Cam Isn't Entirely Rosy*. Forbes. 2/3/2015 Accessed Online.

Howard County Police Department (MD). 2014. *Body-Worn Video Devices: Research Findings*.

International Association of Chiefs of Police. 2014. *Body-Worn Cameras: Concepts and Issues Paper*. Alexandria, VA: IACP National Law Enforcement Policy Center.

International Association of Chiefs of Police. 2014. *Body-Worn Cameras: Model Policy*. Alexandria, VA: IACP National Law Enforcement Policy Center.

Johnson, O’Ryan and Erin Smith. December 3, 2014. *Boston Brass, Police Union Fear Body Cams on Cops*. Boston Herald. 12/4/2014 Accessed Online.

Kaste, Martin. January 22, 2015. *Police Departments Issuing Body Cameras Discover Drawbacks*. [www.npr.org](http://www.npr.org). 1/22/2015 Accessed Online.

Katz, Charles, Mike Kurtenbach, David Choate and Justin Ready. 2014. *Evaluating the Impact Of Officer Worn Body Cameras in the Phoenix Police Department*. Washington, DC: Bureau of Justice Assistance.

Koehn, Josh. December 4, 2014. *Police Union Challenge Halts SJPD Body Camera Program*. San Jose Inside – [www.sanjoseinside.com](http://www.sanjoseinside.com). 12/10/2014 Accessed Online.

Lake Havasu City (AZ) Police Department. 2014. *Audio-Video Recording Policy*.

Las Vegas (NV) Police Department. 2015. *Body Worn Cameras Policy*.

Laurel (MD) Police Department. 2013. *Wearable Video Recorder General Order*.

Lochhead, Colton. November 12, 2014. *400 Officers Involved in Metro Body Camera Study*. [www.reviewjournal.com](http://www.reviewjournal.com) 12/4/2014 Accessed Online.

Lopez, German. January 13, 2015. *Why Police Should Wear Body Cameras – and Why They Shouldn't*. [www.vox.com](http://www.vox.com). 3/26/2015 Accessed Online.

ManTech Advanced Systems International, Inc. 2012. *A Primer on Body-Worn Cameras For Law Enforcement*. Washington, DC: National Institute of Justice.

Mather, Kate. November 4, 2014. *LAPD Moves One Step Closer to On-Body Cameras for Officers*. LA Times. 12/12/2014 Accessed Online.

Merced (CA) Police Department. 2014. *Portable Video Recording System Policy*.

Mesa (AZ) Police Department. 2014. *On-Officer Body Camera Program Policy*.

Mesa Arizona Police Department. 2013. *End of Program Evaluation & Recommendations: Axon Flex*.

Miller, Lindsay, Jessica Toliver, and Police Executive Research Forum. 2014. *Implementing a Body-worn Camera Program: Recommendations and Lessons Learned*. Washington, DC: Office of Community Oriented Policing Services.

Modesto (CA) Police Department. 2012. *Portable Video Recording System Policy*.

National Institute of Justice. 2014. *Body-Worn Cameras for Criminal Justice: Market Survey*. Washington, DC: United States Department of Justice.

New Orleans (LA) Police Department. 2014. *On-Officer Video Recorder (OVR) Policy*.

Newport News (VA) Police Department. 2013. *ADM-570 In-Car Mobile Video Cameras and Axon Body Cameras Policy*.

Pearce, Matt. September 27, 2014. *Growing Use of Police Body Cameras Raises Privacy Concerns*. LA Times. 2/3/2015 Accessed Online.

Phoenix (AZ) Police Department. 2013. *Body Worn Video Technology-Pilot: Operations Order*.

Puente, Mark and Luke Broadwater. February 18, 2015. *Test Body Cameras on 100 Baltimore Officers, Task Force Says*. Baltimore Sun. 2/19/2015 Accessed Online.

Raftery, Jillian. November 12, 2014. *Man's Requests for Thousands of Police Body-Cam Videos Boggling Down Departments*. Mynorthwest.com 12/4/2014 Accessed Online.

Ramirez, Eugene P. 2014. *A Report on Body Worn Cameras*. Los Angeles, CA: Manning & Kass, Ellrod, Ramirez, Trester LLP.

Rialto (CA) Police Department. 2014. *Body Worn Video Systems Policy*.

Richinick, Michele. December 4, 2014. *Eric Holder: Cleveland Police Engage in 'Excessive Force'*. [www.msnbc.com](http://www.msnbc.com) 12/5/2014 Accessed Online.

Rokos, Brian. January 28, 2015. *Riverside County: Sheriff's Union Sues to Stop Body-Camera Use*. The Press Enterprise – [www.pe.com](http://www.pe.com). 2/2/2015 Accessed Online.

Roy, Allyson. 2014. *On-Officer Video Cameras: Examining the Effects of Police Department Policy and Assignment on Camera Use and Activation*. Arizona State University.

San Diego (CA) Police Department. 2009. *Taser Axon Audio/Video Policy*.

San Jose (CA) Police Department. 2009. *Taser Axon Policy*.

Sarasota (FL) Police Department. 2014. *Body Worn Camera Video Systems Policy*.

Stross, Randall. April 6, 2013. *Wearing a Badge, and a Video Camera*. The New York Times. 12/5/2014 Accessed Online.

Sullivan, Jennifer. December 18, 2014. *New Uniforms, New Cars, New Way of Policing: SPD Tests Body Cams*. The Seattle Times. 12/29/2014 Accessed Online.

Sullivan, Jennifer. November 21, 2014. *Man Drops Massive Records Request, Will Help Seattle Police With Video Technology*. The Seattle Times. 3/24/2015 Accessed Online.

Susman, Tina. December 3, 2014. *NYPD Officers to Wear Body Camera in Pilot Program*. The Los Angeles Times. 12/4/2014 Accessed Online.

Tracy, Abigail, EJ Fox and Ryan Walsh. November 15, 2014. *Is Your Police Force Wearing Body Cameras?* [www.vocativ.com](http://www.vocativ.com). 1/12/2015 Accessed Online.

Walker, Heather. October 30, 2014. *GRPD Chief Says No to Body Cams*. Woodtv.com. 2/3/2015 Accessed Online.

Wheeler, Timothy B. March 3, 2015. *Counties Urge Curbs on Releasing Police Body Camera Videos*. The Baltimore Sun. 3/4/2015 Accessed Online.

Whelan, Aubrey. December 1, 2014. *Philadelphia Police to Test Body Cameras for Six Months*. [www.philly.com](http://www.philly.com). 12/4/2014 Accessed Online.

White, Michael D. 2014. *Police Officer Body-Worn Cameras: Assessing the Evidence*. Washington, DC: Office of Community Oriented Policing Services.

Wyllie, Doug. August 15, 2014. *Following Ferguson, A Body Camera on Every Officer?* [www.policeone.com](http://www.policeone.com). 12/8/2014 Accessed Online.

Yimam, Bofta. February 5, 2015. *Action News Investigates: Police Body-Worn Cameras and Your Rights*. [www.wtae.com](http://www.wtae.com). 2/6/2015 Accessed Online.

# BALTIMORE COUNTY

## POLICE BODY-WORN CAMERAS

Research Project, March 2015



### TECHNICAL SUBCOMMITTEE REPORT

Baltimore County Police Department  
&  
Baltimore County Office of Information Technology

## Technical Subcommittee

Although there are many legal, operational, and procedural aspects to police body-worn cameras, the technical specifications are certainly a very large part of this project. A technical subcommittee was formed with representatives of the Baltimore County Police Department and the Baltimore County Office of Information Technology for the purpose of reviewing the technical solutions, limitations, and considerations. It included:

- Captain Joseph D. Conger, BCOPD - Technology and Communications Section Commander
- Mr. Robert O'Connor, OIT - Chief Technology Officer
- Mr. Christopher Kollmann, BCOPD - Digital & Multimedia Evidence Supervisor
- Mr. Chip Hiebler, OIT - Senior Project Manager
- Corporal Jean P. Slattery, BCOPD - Technology Projects Supervisor
- Officer Timothy White, BCOPD - Technology Projects Coordinator

## Purpose and Scope for Technical Document

While the overall purpose of the Body-Worn Camera Workgroup is to review the technology and determine if Baltimore County should move towards adoption, the purpose of the technical subcommittee is to review available device specifications should the committee recommend that the County move forward. These specifications would be appropriate for both evaluating if the County should move towards adoption of this technology, as well as for how to best adopt this technology if the decision is to move forward.

## Business Process Assumptions

In order to evaluate the available features and specifications of body-worn camera devices, the technical committee needed to establish a general assumption of the business process goals for this technology. The Technical Subcommittee researched devices offered by several companies, reviewed studies by other police agencies, and participated in the larger Body-Worn Camera Workgroup.

While many potential areas of benefit were identified for body-worn cameras, the driving goal was generally stated as to capture the best approximation of the perspective of the police officer. This does not negate the values of other benefits, but a main objective was required when considering specifications that were subject to competing priorities.

The contents of this document contain the evaluations and recommendations of this subcommittee as a result of abstract research. Although some hands on device and system research were included, this was very limited. All evaluation and recommendation from this document would be subject to modification in the review of an operational pilot program, which is the recommended course of action for further evaluation.

## Executive Overview

This document provides a comprehensive report on the technological specifications that should be considered in evaluating any potential police body-worn camera program. Recommendations are provided where available.

The most significant recommendation of this report is that body-worn camera programs should be approached at the “enterprise” level. This means identifying a single source solution that covers everything from the body-worn camera device to the digital file management system and all components in between. An enterprise solution provides a single point of administration for devices, users, files, redaction, chain of custody, and dissemination. It also provides the fewest possible dependencies for multiple providers, support mechanisms, manual processes, and system interfaces.

The second most significant recommendation is the engagement of a cloud storage service provider. Hosted solutions offer redundant storage with system uptime and security levels that typically exceed those attainable by individual municipalities. Total cost of ownership is typically lower because staffing, electrical service, environmental controls, facility space, and scalability requirements are all handled by the provider in a consolidated model. Additionally hosted solutions offer robust mature features including role-based security, redaction/reproduction tools, and full auditing.

One of the largest quantifiable consideration points is the fiscal investment required for implementation and maintenance. This document contains a range of fiscal investments based on assumed operational models and projected capture and storage. The report relies heavily on the cost estimates of enterprise solutions which constitute total system pricing packages. These estimates place year one investment figures on a range from about \$0.6 million to \$1.2 million. The year four estimates can range as high as \$8.5 million when accounting for the aggregation of video storage over time. Full illustrations of investment ranges are included in the Technology Fiscal Investment Section.

Device selection requires consideration of many unique specifications. Device form factor should limit device intrusiveness in field encounters, and environmental protection standards should assure reliable field use. Minimal on-device user controls and features are recommended for simple field operation. The standards for capture specifications are reasonable, with video resolution 640X480, recording speed 30 frames per second, and lux rating 1-0.5. Observational enhancements such as night-vision or long range audio are not recommended. Battery life, recording life, and storage capacity should support continuous operation for 12 hours.

The mounting position of the device has limited technical recommendations. Point-of-view mounted systems provide the closest available approximation of the police officer’s perspective, but are more intrusive to field interactions by virtue of their appearance. Torso-mounted solutions are generally more passive in appearance, but are easily obstructed or mispositioned according to the officer’s physical orientation. The

recommendations in this area are to consider devices that offer flexible mounting options, and to conduct further analysis through an operational pilot group.

Additional detailed information about each technical specification and area of consideration follows in the remaining sections of this document.

### Physical Device Attributes

The physical attributes of the camera devices themselves have significant impacts to the practical field operation of the device, the intrusiveness to police citizen interactions, the durability and reliability, and the security of the recorded data.

#### *Device Mounting*

There are generally two types of mounting options available for body-worn cameras. These are torso-mounted devices, and point-of-view mounted devices. These are general classifications, and not absolute categories.

Torso devices come with a variety of mounting options related to the officer's main torso area from the waist to the shoulders. Mounting options include shirt clips, pocket clips, shirt pins, necklaces, and even some that require special modifications to the uniform shirt. Mounting locations generally vary from the shirt pockets, to the center of the chest, and to the front of the shirt below the shoulder. This type of mounting is generally less obtrusive and less likely to become a focal point for the citizen during police encounters. Torso-mounted devices may also experience higher police officer acceptance levels by being fairly passive in appearance.

Torso-mounted devices are the most common type of devices currently available and in use. The limitations of this mounting are largely related to the position and angle of view. Torso-mounted devices are effective when the police officer is directly facing the citizen or area of interest. The device becomes less effective when the officer is not directly facing the citizen or area of interest. For example, officers who blade their body to present their non-weapon body side towards a person would have the camera facing away. The same goes for bladed shooting stance. For officers who do not use body blade postures, strong two handed hold of service weapons and conductive electrical weapons commonly obstruct the camera field of view. Officers involved in assault or shooting situations are also trained to seek cover and concealment to protect them from assaulting suspects. In doing so, officers try to position most of their body behind an obstruction from the threat. This would also likely obstruct the torso-mounted devices. When seated in a motor vehicle, the field of view is commonly obstructed by the steering wheel and dash board, limiting the ability of the camera to record the vehicular police response. Finally torso-mounted devices do not move with turns of the officer's head. So an officer who turns their head to one side when scanning an area, facing multiple adversaries, checking for back up, etc., will not have those perspectives captured, and in fact will capture video from a forward perspective that the officer could not actually see at the time of recording.

Point-of-view devices come with a variety of mounting options related to the officer's head and neck. Mounting options include eyeglass frames, hat/helmet attachments, head bands, collar bands, and shoulder epaulette attachments. This type of mounting is generally more obtrusive and could become a focal point for the citizen during police encounters. Attaching to eyeglass frames can be problematic when officers need to transition in and out of sunglasses, and hat mounting presents similar concerns. Point-of-view devices may also experience lower police officer acceptance levels based on a perceived aggressive appearance.

Point-of-view systems generally provide a wider range of mounting locations from the head to the neck and shoulder within a single device type. These devices have a higher point of view than torso-mounted devices in all cases, making them less likely to be obstructed by the use of weapons, cover and concealment, or vehicle dash boards while driving. Mounting on the head also allows the camera to turn with the officer's attention when scanning an area, facing multiple adversaries, checking for back up, etc. Body blade posture is also not an issue since these stances keep the head and face focused forward to the citizen or area of interest. The limitations of these mounting positions are less related to the camera point of view and more related to the officer's personal physical comfort and operational acceptance. Another consideration with point-of-view systems is that the camera perspective is still not exactly the same as the police officer's perspective. The officer can still turn their eyes without moving their head, as well as close their eyes; the recorded video would not account for these in either mounting solution.

In conclusion, the point-of-view devices provide a closer resemblance to the police officer's perspective than torso-mounted devices, but they still have limitations and may be significantly obtrusive and unaccepted by the users. A pilot program is required for further evaluation of the mounting options.

### *Vehicle Dash Mounting*

Some body-worn camera devices offer the ability for the officer to mount the device in an optional dash mount for use as an in vehicle dash-cam. This allows a device that is otherwise obstructed by the steering wheel and dash to better captures the front view from the vehicle while traveling. The down side of this option is that it requires the officer to move the device between the body mounting position and the vehicle dash mount. This makes it a less passive device and requires more time and attention for the officer at each transition into and out of a vehicle.

In conclusion, vehicle mounting brackets are unnecessary and impractical accessories.

### *Device Dimensions, Weight, and Appearance*

Most body devices are comparable in size to a thick modern smart phone, with the longest side ranging from two to four inches. Weights range from two ounces to 10

ounces, but most typically around four ounces. Most devices are black or dark in color to blend in with the uniform or other equipment.

Point-of-view mounted devices are generally smaller in size than torso-mounted devices, but may require a tethered battery supply or other device that is about the size of a torso-mounted device.

In conclusion, both cases allow the cameras to be mounted on the officer as a mostly passive device, and have limited impact to the officer's normal range of motion in the field environment.

### *Device Components and Form Factor*

Torso-mounted devices generally have a single form factor for the entire device. This eliminates concerns with wire connections on the body of the police officer that could become entangled or could be used as a weapon by an assailant.

Point-of-view devices commonly have a two piece unit with a wire connecting them. In the event the device has a wire connecting two components, that wire needs to be reliably attached with suitably high tensile strength to prevent interruption of recording. At the same time, that wire must have a suitably low tensile strength to prevent it from being a danger to the officer by either entanglement or by an assailant using it as a weapon. The potential for damage to the wire connection also requires it to be field serviceable and replaceable so that cameras sustaining wire damage can be quickly returned to service.

In conclusion, while a single form factor is simpler to operate, the viewing angle benefits of a point-of-view device outweigh the wiring concerns when appropriate tensile strength and support needs are satisfied.

### *Device Environmental/Durability Ratings*

Police officers work in highly mobile roles within the community. These include activity in all types of weather and conditions. These also result in significant contact with criminal suspects. Any device selection would have to consider appropriate hardware ratings for shock, vibration, temperature, moisture, dust, and other common environmental variables. Multiple standards have been established and published related to environmental protection ratings.

In conclusion, the manufacturer should provide certification of an appropriate environmental protection rating.

### *Device Buttons and Controls*

Devices come with a wide variety of user buttons and controls on them, enabling the police officer to use various device features. These can include on/off buttons, video settings, audio settings, night vision modes, playback controls, video tagging, and more.

Many of the on-device buttons and controls manage features that this document would otherwise recommend against using for the field officers. Therefore since more basic and universal features are generally recommended, these advanced controls should not be included on the device.

Buttons and controls on the device are also potential points of failure based on their location on the device, sensitivity to movement, and types of features managed. Buttons and controls on the body side of the device may be activated through contact with the body, and would likely have unintended effects on the video. It is also not likely the officer will know that the buttons have been accidentally activated. This means accidental button activation could start or stop videos unintentionally, or change video modes, audio modes, etc.

In conclusion, it is recommended that the devices only have on/off or start/stop controls. This keeps the officer from focusing on multiple features and device aspects, and reserves their attention to simply deciding to record or stop recording. Fewer buttons and controls make accidental feature changes less likely. Positioning of the controls should be away from the body side of the device to minimize accidental button activations. The type and sensitivity of the controls should also be selected to minimize accidental activations.

### *LED Indicators*

It is important for the field officer to know when the devices are active, recording, or not active and recording. This generally requires an indicator LED for the status. Without an indicator LED, officers may believe the unit is activated or recording based on switch position or other physical features. Physical features though do not account for depleted charges and electronic malfunctions.

LED indicators can also be used to make citizens aware of the recording in progress. This may serve to affect citizen behavior in a positive manner. At the same time, LED indicators should not be so bright or observable as to give away police officer positions in adversarial encounters.

In conclusion, LED indicators are required for reliable device use, but must meet appropriate thresholds of visibility to avoid being a safety issue.

### *Audible Indicators*

Audible indicators have the advantage of alerting the officer to the device status without the officer having to look at the device. The disadvantage of audible indicators is they may give away police officer positions in adversarial situations. Continuous or repeated audible indicators while recording also may serve as a distraction while engaged in dialog with citizens.

Some devices offer audible indicators as an agency configurable feature. This means the agency could decide to set these to active or inactive, and could change them after initial implementation.

In conclusion, audible indicators have more significant limitations than LED indicators. LED indicators are generally preferred, but agency configurable audible indicators would provide the most flexible option.

### *On Device Video Display*

Some devices include playback displays and controls on the device itself. This allows the officers to review the recordings in the field without a separate computer, tablet, or other smart device.

Adding displays to the devices create an additional potential point of failure as displays are more susceptible to physical damage. Displays also have the potential to expose recorded video to any person who may come into possession of the device, making the recorded video less secure in the event of a lost or stolen device. Displays are features that affect the form factor of the device, as well as deplete the device battery life.

In conclusion, on device displays do not provide benefits that outweigh their associated concerns and limitations.

### *Passive/External Recording Triggers*

Currently available market devices generally require the officer wearing the camera to manually start and stop the recording feature. There are some devices that offer limited integration with in-car video systems to passively trigger recording activation. There are also device providers who report to be actively working on features to passively trigger recording, such as Electrical weapon deployments, computer-aided dispatch (CAD) unit status, and others.

Baltimore County does not currently utilize in-car video systems, and as such these are currently out of scope for this research project. The limited availability in the current market would make this feature difficult to obtain and implement. It would also create dependencies for interfaces to other devices and systems, complicating implementation and ongoing support. Additionally, without a full time wide area wireless connection, the passive triggers would not function outside of the personal area network range of a patrol vehicle, especially for officers who work in non-patrol functions.

In considering the limitations of passive recording triggers, even with these features it is likely the police officers will have times when they need to manually activate the cameras. If the officers have to be consciously aware of when the devices are automatically activated and when they require manual activation, this requires more of their attention than establishing a behavioral pattern where they always know to activate the recording.

In conclusion, the limited availability and application of passive recording triggers make this an unnecessary and unreliable feature at this time.

### *Pre-Event Recording Buffer*

Many devices offer a pre-event recording buffer. This means that the device operates in a standby mode where recording is continuously occurring, but only a short period of rolling video and audio is retained until the user activates the recording feature. The result is that when an officer activates the recording process, the buffered period (usually 30 seconds) prior to activating the recording is captured and retained as part of that recording.

This feature is designed to allow officers to capture pre-event activity in circumstances where they did not expect activity to require recording in advance, or when situations escalate or deteriorate quickly without notice. It also allows the officer to address spontaneous threats and incidents with a safety response first, followed by recording activation, without missing part of the incident. Officers should not be expected to first focus on recording activation and secondarily on safety measures.

The disadvantages of pre-event recording buffers is that they may capture unintended segments of audio and video that are unrelated to the event for which the device was activated. These could include personal conversations, privileged conversations, and private areas such as restrooms and locker rooms. This also may cause officers to try to estimate the buffer time so that they end up waiting 30 seconds prior to activation to avoid unintended recordings. This again takes a lot of the officer's focus away from handling the situation, and places too much on device operation.

Some devices offer pre-event recording buffers as an agency configurable feature. This means the agency could decide to set these to active or inactive, and could change them after initial implementation. These selections could be affected by user feedback, but could also be affected by unforeseen future legislative changes.

In conclusion, agency configurable pre-event recording buffer (including deactivation) is the recommended feature to satisfy current and future operational and legal requirements.

### Device Managed Metadata

Most market devices offer some level of device managed metadata. This means the files are embedded with data about the recordings such as the date, time, location, and owner. This data is useful in review of recordings, and adds additional safeguards to the integrity of the files.

### *Date/Time Stamp*

One essential element of recording with body-worn cameras is the ability to track the date and time of the recording. All devices currently available in this market include the ability to embed the date and time stamp in the recorded file, making this an industry standard item.

Another essential element of the date/time stamp feature is a mechanism to asynchronously maintain the accuracy of the device's internal clock. This can be done by having the file extraction software also update the device's internal clock against single coordinated universal time server. This would minimize discrepancies from device and desktop computer variances.

In conclusion, the device must support date/time stamp embedding and date/time synchronization with a coordinated universal time server.

### *Global Positioning System (GPS) Coordinates Stamp*

Some devices offer features to embed GPS coordinates in the recording files, thus capturing the location of the device at the time the recordings are captured. This feature generally relies on the reception of signals from orbiting satellites, and can vary in accuracy by device.

The advantage to tracking GPS coordinates in the video is the passive preservation of the location data at the time of the recording, providing additionally preserved information about their location of origin.

Limitations of GPS features are the location data may be affected by indoor conditions, or other items that would interfere with location calculation. Embedded GPS receivers also have a considerable draw on battery power from the device negatively impacting operating time. External GPS receivers linked to body-worn cameras require the user to charge, carry, and account for an additional device.

Whereas date/time stamps are critical metadata because recorded images and video do not regularly capture indicators of the event time, location data is different. Video recording captures visual information about an event that frequently can be used to identify or verify the source location of that recording.

In conclusion, GPS coordinate stamping of recorded files is preferred if it does not negatively impact other areas of specification, such as operating life. GPS coordinate stamping is not required based on the limited benefits it provides.

### *User Assignment*

Many devices are managed through a computer system that requires the device to be assigned to an individual police officer for use. This allows the device to embed the

officer's identity (usually a name or department identification number) in the recorded files.

Since the point of view captured by the camera does not generally capture the user's face or image, it is important for the identity of the police officer to be preserved with the video. Managing this assignment of identification through system administration also provides an additional safeguard for the integrity of the video and related data.

In conclusion, administrative tracking of device user assignment is a required feature.

### Video and Audio Specifications

Currently available devices in the body-worn camera market offer a wide variety of video and audio specifications. Each of these has independent and interdependent impacts on the successful implementation of a particular solution.

#### *Field of View*

One of the most important specifications for any body-worn camera is the field of view, or viewing angle of the camera. Current market devices range from 60 degrees to 180 degrees. Approximately 120 degrees is generally the most common, but other factors significantly impact the recommendation in this area.

Although the human eye is capable of almost 180 degrees of horizontal viewing and about 120 degrees of vertical viewing, the mind is not capable of focusing on all of that viewing area simultaneously. So one consideration in this area is that wide fields of view may capture many things that a police officer was unable to perceive at the time of the recording, and that could be misleading to another person reviewing that video at a later time. Another consideration particular to torso-mounted devices is that since the devices do not change position with turns of the head, narrow fields of view may not capture the actual areas of focus of the police officer's attention.

In conclusion, to most closely approximate the perspective of the police officer, point-of-view systems should have a narrower field of view. Torso-mounted devices would require a larger field of view to compensate for non-responsiveness to head movement.

#### *Resolution*

Current market devices offer a range of resolution settings from 320X240 to 1920X1080p. Many devices offer configurable settings to change the recorded video resolutions within those ranges. Higher resolution specifications will result in better image quality. At the same time, higher resolution also results in large file sizes, which directly affect data storage and management needs and cost.

In reviews by other police departments, as well as some experimentation by our own personnel, the minimum resolution of 640X480 appears to be sufficient for capturing a

close approximation to the officer's perspective. This also uses the minimal amount of storage requirements, directly impacting over all storage and management effort and cost.

### *Recording Speed*

Current market devices offer a range of video frame rates from 15 frames per second to 60 frames per second. As with resolution settings, higher frame rates result in higher file sizes and increased storage and management needs.

While the perceivable frame rate of the human eye varies among individuals, it is generally accepted that about 24 frames per second produces a smooth moving image for the human eye. A good point of reference would be movie and television videos that generally range from 24 to 30 frames per second.

Although higher frame rates may provide the ability to extract higher quality still images from the video, this would be inconsistent with the goal of sharing the police officer's perspective since the officer is not likely to be able to perceive the still images in the real time environment.

In conclusion, a rate of 30 frames per second is recommended to capture fluidly moving video and minimize storage and management effort and cost.

### *Lux Rating*

The Lux rating is the minimum amount of light that is required to produce an acceptable video image. One lux is equal to one lumen per square meter. Current market devices range from 1.5 lux to 0.03 lux, although not all devices publish this specification. This does not include infrared vision or other types of night vision recording.

It is generally accepted that the human eye can perceive vision with a minimum lux of between 0.5 and 1. This means devices with minimum lux ratings over 1 would not capture as much as the officer is likely to perceive in low light settings. It also means that devices with minimum lux ratings below 0.5 would capture more than the officer is likely to perceive in low light settings.

In conclusion, the recommended lux rating is in the area of 1 to 0.5 in order to most closely approximate the perception of the police officer.

### *Microphone Specifications*

Microphone and audio recording specifications for current market devices are generally less available than other specifications. Microphones should capture audio in various settings that is consistent with the general range of hearing of the human ear. It is not desirable to either capture less than what the officer could reasonably hear, nor more

than the officer could reasonably hear. Considerations should also be made for wind shielding, and other available environmental control features.

In conclusion, the device microphone should capture audio consistent with the range of normal human hearing, and with minimal degradation due to environmental factors. Activation and deactivation of the microphone should be a feature that is configurable by the administrator.

### *Observational Enhancements*

Optical enhancements, such as night vision, improve the recorded video to capture a perspective that is clearly beyond the ability of the police officer to perceive with natural senses. Likewise, extended range microphones may also capture audio information that would have been beyond the normal hearing abilities of the human ear. While these may capture more detailed evidence for use in case investigation and prosecution, both would likely be very misleading as to what the officer was able to perceive at the time of the police action.

There are also potential legal and privacy limitations on the use of enhanced observation abilities. There could be significant Fourth Amendment issues with a system that is capable of enhanced recording beyond the observations of the police officer. Although images recorded by or during the use of a flashlight would not fall under a higher level of scrutiny, the use of other types of enhanced visual devices may be considered a Fourth Amendment violation, particularly when such a recording occurs within a constitutionally-protected area. The courts have not addressed the use of enhanced visual devices. Additional information will likely be included in the “Legal Implications” section of the larger workgroup’s document.

In conclusion, optical and auditory enhancements are not recommended as they are inconsistent with the goal of closely approximating the police officer’s perspective, and may be incongruent with established law. Devices must be without these features, or allow the agency administrator to disable them.

### *File Formats*

There are a wide variety of video and audio file formats in today’s digital age. While some file formats are proprietary, several devices utilize non-proprietary file formats.

Non-proprietary file formats allow the captured videos to be reproduced without the need of special media players, codecs, or plug-ins. An example of a commonly available non-proprietary file format is MPEG-4.

In conclusion, a non-proprietary file format is required to ensure compatibility with existing systems, and reducibility for prosecution, defense, and public disclosure.

### *Administrator Configuration Options*

As indicated in the preceding sections, it is generally preferable for the device or system administrator to be able to manage the selection of device settings. Configurable devices allow for flexibility in the event of changes in laws or operational needs.

Restricting the configuration changes to an administrator helps to ensure settings are controlled agency wide, and reduce the risk of intentional or inadvertent reconfigurations by field users.

It is also preferable that administrator configurations can be managed both remotely and globally. In other words, the administrator should not generally be required to handle the device for configuration management, and the administrator should be able to establish agency wide settings rather than having to make all changes at the individual device level.

In conclusion, the system software should allow the administrator to manage field devices remotely and globally for all agency configurable features.

### Device Operating Duration and Capacity

Police officers typically work a tour-of-duty consisting of eight hours. Overtime assignments are also common for operational needs.

The amount of tour-of-duty time that is captured or video and audio recorded will be dependent on policy decisions regarding use. For evaluation purposes, we have identified three tiers of recording estimates for a tour-of-duty:

- MINIMUM would be for recording only enforcement and use of force activities. We estimate that a typical tour-of-duty would produce two hours of video with this standard.
- MEDIUM would be for recording enforcement activities and calls for service of criminal, suspicious, or adversarial nature. We estimate that a typical tour-of-duty would produce four hours of video with this standard.
- MAXIMUM would be for recording the entire tour-of-duty without interruption. We estimate that a typical tour-of-duty would produce eight hours of video with this standard.

### *Recording Life*

For MINIMUM recording use, the device would need to have a recording life of four hours in order to accommodate tours of duty that exceed the estimated average two hours of recording.

For MEDIUM recording use, the device would need to have a recording life of eight hours in order to accommodate tours of duty that exceed the estimated average four hours of recording.

For MAXIMUM recording use, the device would need to have a recording life of 12 hours in order to accommodate tours of duty that are extended for operational necessity beyond the standard eight hour scheduled tour.

There is a risk in implementing a device with a capacity less than 12 hours in both the MEDIUM and MAXIMUM scenarios. Police officers do not frequently handle incidents with a continuous duration of eight to 12 hours. However when they do, these situations are typically subject to higher level risk, priority, attention, and scrutiny making complete video recordings especially important.

In conclusion, the recording life estimates should support the MAXIMUM recording period of 12 hours as estimated in this section to support both typical and extended incidents.

### *Storage Capacity*

The storage capacity of currently available devices generally ranges from 8GB to 32GB. The storage capacity requirements are tied closely to the recording life and the video specifications including resolution and frame rate.

In conclusion, the storage capacity should minimally support the full recording life desired when using the 640X480 resolution and 30 frames per second rate. Ideally the storage capacity should support the full recording life desired when using a 1280X720 resolution and 60 frames per second rate in the event that pilot use and operational results indicate higher video quality is required.

### *Overwrite Protection*

Recognizing that all devices have a limited storage capacity that can be exhausted, it is important for the device not to overwrite recorded video in a continuous loop prior to extracting it from the device for tagging and transfer to system storage. Allowing new videos to record over old videos prior to extraction creates a potential for loss of recordings. Ideally, the device would provide a visual warning to the police officer that the device has reached capacity.

In conclusion, the device should prevent overwriting of recordings until they have been extracted from the device.

### *Removable/Expandable Storage*

As indicated in other sections, there is a heavy focus on simplicity of use for the field officer as well as the need for safeguards of the integrity of recordings. Devices that

utilize removable storage for primary storage, or allow expansion through removable storage do not support these two concepts. Devices with permanently installed storage are typically simpler to operate since this is a non-issue for the focus of the user, and they provide one less potential point of failure. More importantly the permanently installed storage is less susceptible to loss, damage, or tampering, thus better ensuring the integrity of the recordings.

In conclusion, devices should not utilize removable storage media.

### *Battery Life*

Many devices currently available have recording life periods and capacity that exceed the battery life. This means that the device can handle extended recording operations, but would require charging within the use cycle prior to reaching capacity. This is not realistic for police field operations, and causes the police officer to spend additional time and attention to the battery charge level during the tour-of-duty.

In conclusion, regardless of the intended recording time per tour-of-duty, the operating duration of these devices must be able to handle at least an eight hour tour-of-duty between charging cycles.

### *Removable Battery*

Only about one quarter of the devices available in the current market indicate that they have removable batteries. This would allow the devices to swap batteries during operational use and avoid taking the units out of service for charging.

Although this may be beneficial generally, it requires the agency to invest in additional batteries for every camera device in order to leverage it operationally. Additionally the benefits must be weighed against charging cycle time, download cycle time, battery life, recording life, and operational needs. Should the selected device have sufficient battery life and recording life to operate for an entire tour-of-duty, and have a download period that requires more than a few minutes to transfer from the device, then the swappable nature of removable batteries would have little to no significant benefit.

In conclusion, removable batteries have limited benefits and require additional investment and do not likely provide enough benefit to be recommended accessories.

### *Charging Cycle*

The charging cycle refers to the amount of time the device battery must be allowed to charge between uses. The current operational schedule of the police department has personnel generally off duty for 16 hours between shifts, however biweekly schedule rotations and operationally required overtime regularly reduce that time between tours to eight hours.

Generally, currently available devices are designed to be assigned to individual officers rather than shared between shifts of officers. Some of these design constraints include managing device assignment tracking, security measures, stored video management, download time, and charging time.

Currently available devices have a range of charging cycles from two hours to six hours, with four hours being the most typical. A four hour charging cycle would ensure the smallest of operational downtime is required for charging periods.

In conclusion, the charging cycle should not exceed a period of four hours to allow the most reasonable and efficient management of device downtime.

### Device Data Security

From the time the video is recorded to the time it is extracted, the stored video must be secured to avoid intentional and unintentional loss, damage, or interception. In fact many devices continue to store recorded video after extraction until the storage space is needed for additional recordings. This means that the security of the data on the device must be adequately protected.

### *Device Physical Tamper Resistance*

There are two areas of consideration when evaluating the tamper resistance features of body-worn cameras.

First there is a large emphasis in police body-worn camera programs to ensure transparency of government for the public. A device with features to limit tampering with the video and audio content provides a reasonable safeguard to uphold the public trust in this area when it comes to the officers operating the devices.

Second there is a risk of theft or loss of these portable devices as police officers engage the public in the field. A device with features to limit tampering with the video and audio content provides a reasonable safeguard to prevent criminal actors from accessing evidence and other private citizen information from police activities.

Tamper resistance features can include units that are sealed and have no removable parts (other than removable batteries). Storage media such as SD cards are easily manipulated if readily removed from these devices. Proprietary connection cables can also provide a level of tamper resistance, but these are not common in the current market.

In conclusion, tamper resistance features must be sufficient to uphold the public trust regarding both police transparency and criminal interception.

### *Device Data at Rest Security*

Because there is a limited risk of loss of any portable device, there is a requirement that video and data stored on the device be encrypted to prevent interception. The Data at Rest standards for the “Storage” section of this document apply equally to the storage of data on the recording device itself. This will prevent someone from accessing the video and data on a lost or stolen device in the event the police are unable to locate it.

In conclusion, Data at Rest standards for long term storage should also be required for on device storage.

### Device Data Interface

Once the device has recorded video and audio in the field, there must be a mechanism for extracting it from the device and transferring it into a digital file management system. Current market devices widely support wired interfaces for this transfer. Other options can include Bluetooth or WiFi transfers.

#### *Wired Interfaces*

At the computer end of the wire, the connection could also be proprietary or non-proprietary. The need to be able to readily interface these devices with existing government computers and systems requires this to be a non-proprietary connection, specifically a USB standard. A proprietary connection on this end would require investment in computer components for each workstation likely to be required for video transfer.

At the device end of the wire, the connection could be proprietary or non-proprietary. A proprietary connection provides an additional safeguard against tampering or interception of recorded videos, since the connecting cable is likely not widely available outside of the market. It should be noted that most current market devices however do not use a proprietary connection.

In conclusion, a non-proprietary (USB standard) connection is required for the computer end of the wire transfer cable. A proprietary connector is preferred for the device end of the cable, but not required.

#### *Wireless Interfaces (WLAN, WWAN, WPAN)*

Wireless interfaces can include Bluetooth, WiFi, and other standards. Many current market devices offer wireless connectivity, however they vary on the application of these connections. While some allow wireless interface for reviewing and tagging of recording files, others may offer wireless transfer of recording files.

The potential for wireless interfaces to passively manage video uploads to system servers is certainly desirable. This is however an emerging area for body-worn cameras and it is difficult to anticipate future application of this feature among developers.

In conclusion, wireless interfaces require in depth review specific to selected devices and systems.

### *Voice Radio Interface*

Some devices offer a physical connection to public safety voice radios. The idea generally is to replace the lapel microphone on the radio with the body-worn camera that can serve as the lapel microphone.

This is a limited offering which creates an additional level of integration dependencies as well as an additional potential point of failure. Specifically this may create limitations of body-worn camera selection or voice radio selection for compatible hardware while each technology evolves independently.

Police officers also commonly attach lapel microphones in a loose fashion to their shoulder epaulettes. This is meant for ease of use as they turn the microphone to speak into it. The loose attachment may cause the camera to be unstable, and the turning of the microphone may cause problems with positioning of the camera lens as well.

In conclusion, interface to voice radios is not recommended.

### Extraction, Reviewing, Classification, and Transfer

Although capturing video on the device should be as passive as starting and stopping the recording, the extraction, classification, and transfer of video following capture is largely a manual process for the police officer. Minimizing the time, attention, and effort required for these workflow steps requires consideration of several specifications.

### *Supported Interface Devices and Operating Systems*

The current standard and most widely deployed computer operating system for Baltimore County is Windows 7. This includes desktop computers, laptop computers, and in vehicle computers regularly used by police.

Baltimore County is expanding deployment and use of both Android and iOS platforms for tablets, phones, and smart devices. This coincides with the proliferation of these systems and devices in society.

In conclusion, body-worn camera devices must support interface with Windows 7 for current implementation within Baltimore County. Devices should support interface with Android and iOS devices for future implementation with mobile devices.

### *File Management Client*

The vast majority of body-worn camera devices come with a proprietary thick client application for managing their stored recordings. This client application allows officer to access the files on the device, review the videos, tag/categorize the videos, and transfer them to the digital file management system.

This application is typically proprietary in that it only works with a specific brand or make of device. Since devices typically store videos at rest with encryption, the proprietary client is almost always required for access.

Any device that would allow non-proprietary file transfer, such as those native to computer operating systems, would not provide the security required to minimize interception, duplication, deletion, and altering.

In conclusion, the solution must provide a proprietary client application for securely managed extraction, review, categorizing, and upload of recorded videos.

### *File Extraction, Review, Classification, and Transfer Process*

There are two main workflow processes for officers to get the video from the device to the digital file management system with the appropriate classifications.

The first and most common method is to connect the device to a computer using a proprietary client application to extract the files from the device, then review the videos, tag/categorize them, and finally transfer them to the digital file system. In solutions where manual transfer and tagging is required, this is the preferred workflow process. It allows the officer to do all of the required user interactions prior to the data being uploaded to the larger system. Therefore the officer does not have to wait for the file transfer process to complete with the system server, which may be considerable time depending on file size and bandwidth availability. This method also prevents other users of the system from viewing the video until it is properly classified by the originating officer.

The second method is to upload the video from the device to the digital file system and then have the videos reviewed and classified. In this method, the officer must wait for the upload process to be completed before the videos can be reviewed and classified. This may result in considerable wait time for the end user depending on file size and bandwidth requirements. This method would work better if there was a passive upload of the data from the device as the officer worked throughout the day, but would still be problematic for end of shift incidents. Passive upload throughout the day is also not a widely available feature.

In conclusion, the system must allow the officer to extract, review, tag/categorize, and upload the video files in that workflow order.

### *Bandwidth Requirements*

Police officers currently work in a flexible mobile environment. They are provided with radios, computers, and wireless network service in their police car. This provides ready access to Department systems, and reduces their dependency on spending time inside a police facility. Less time in a police facility means more time spent in the community they serve.

Video file transfer commonly comes with highly demanding bandwidth requirements in order to manage and transfer it effectively. Mobile wireless service typically only provides 4G-LTE bandwidth availability in the field. This is significantly more limited bandwidth than WiFi and traditional wired networks in government facilities.

The ability for officer to tag and upload video recordings from the field would be advantageous for both timeliness of delivery and minimizing operational downtime associated with returning to the police facilities to transfer the files.

In conclusion, consideration should be given for file uploads over secure WWLAN if reasonable performance is obtainable.

### *Device Video Extraction Time*

The time spent extracting videos from body-worn cameras is time the police officer is spending on administrative tasks, depleting available operational and patrol time. For this reason, it is essential that the time required to extract videos from the device to a computer is as minimal as possible. Extraction time must be a small fraction of the actual video play time. Hours of video should be transferred in minutes.

Requirements for this specification would need to be evaluated in a pilot group due to other technical considerations, such as existing County computers, that affect this performance.

### *Device Video Upload Time*

The time spent uploading body-worn camera videos from computers to the digital file system should also be minimized. Although this can conceivably be completed during non-operational time if preceded by reviewing and tagging, it does make the device unavailable for field use capturing additional video. For this reason, the time required to upload videos from a computer to the server should be as minimal as possible. The need for this performance is decreased if the transfer occurs as an unattended action, but is still important to device availability as stated above. Upload time should be a fraction of the actual video play time.

Requirements for this specification would need to be evaluated in a pilot group due to other technical considerations, such as existing County network connectivity, that affect this performance.

## Categorizing/Tagging Video Files

Both the type and quantity of recorded videos are expected to be vast for any body-worn camera system. Categorizing, also called tagging, videos with valuable searchable metadata is essential to searching, correlating, retaining, purging, and otherwise managing this vast collection.

### *Passive Tags*

Passive tags are largely those tags established by the body-worn camera device at the time of capture, and the proprietary application at the time of transfer/upload. These can include the device identity, capture date/time, upload date/time, GPS coordinates, assigned officer identity, uploading officer identity, and more.

The capture and transfer of all available passive tags is required.

### *Selectable Tags*

Selectable tags offer the end user the ability to apply preset categories to their videos. The method of tagging videos typically involves checkbox type selections for the officer. The categories are established in the system by the agency, and commonly reference videos as evidence or non evidence, incident type, enforcement related, and more. Systems generally allow officers to apply multiple tags to videos so they can be correlated to multiple categories.

The ability for the officer to assign multiple agency developed tags is a requirement.

### *Free Form Entry Tags*

Free form entry tags allow the officers to type in identifying video data. A common example of this is the call for service incident number, commonly referred to in Baltimore County as the Central Complaint number (CC#). Tracking the incident number allows for easy correlation between recorded videos, the computer-aided dispatch system, and the records management system.

The ability to assign the call for service incident number to each video is a requirement.

### *Manual versus Automatic Tagging*

There are system providers who currently offer or are developing automated methods for tagging and categorizing body-worn camera video. These systems generally rely on correlating call for service dispatch data elements with video device data elements. For example, a video from a body-worn camera assigned to Officer Smith 1234, working patrol unit 626, at 1705hrs on 01/01/2015 would be related to a call for service dispatched to patrol unit 626 at 1700hrs on 01/02/2015. Then the other call for service

information, such as the event type, the disposition, the situation found, the event duration, etc., could be used for categorization.

Automated tagging of videos offers a passive way to accomplish the task, but it also has many limitations. First, it can only approximate video correlations through matching logic, and instances where calls for service data does not match would not be captured. Examples include calls for service initiated in the computer-aided dispatch (CAD) system after the conclusion of an event, or calls generated while the CAD system is unavailable. Second, it does not account for videos captured without a corresponding call for service record. Third, it does not link videos from follow up activities to calls for service when they occur hours, days, or weeks later. Fourth, it does not account for police units that do not regularly make use of the CAD system for their daily activities, such as detectives, support operations, and other specialized positions.

In conclusion, automated categorizing/tagging of body-worn camera video may be preferred as the technology matures, but is not recommended in the current state.

### System Administration

The acquisition, deployment, and management of body-worn camera devices require a significant amount of effort and investment into the supporting infrastructure. Captured video must be indexed, stored, secured, backed up, and reproduced.

### *Video/Audio File Storage Capacity*

Estimates and recommendations related to video/audio file storage are largely dependent on operational deployment assumptions.

The first assumption to be established is the standard for video specifications. This report uses the following assumptions for the camera specifications: Video format will be MPEG4, at Standard Level resolution, with a 30 frame per second recording speed.

Another assumption that must be established is the total predicted amount of video capture. This is based largely on the number of officers deploying the cameras, and the work schedules of those officers. For the purposes of this report, it was assumed that deployment would largely consist of patrol and traffic personnel, excluding detectives, school resource officers, and other specialized assignments. This places our estimate at 1,200 Officers who would be individually equipped with body-worn cameras. Police officers typically work about 20 days per month, and a tour-of-duty consisting of eight hours per work day.

The amount of tour-of-duty time captured on video and audio recording will be dependent on policy decisions regarding use. For evaluation purposes we have identified three tiers of recording estimates for a tour-of-duty:

- MINIMUM would be for recording only enforcement and use of force activities, roughly two hours per tour-of-duty.
- MEDIUM would be for recording enforcement activities and calls for service of criminal suspicious or adversarial nature, roughly four hours per tour-of-duty.
- MAXIMUM would be for recording the entire tour-of-duty without interruption, or eight hours per tour-of-duty.

Storage space for video and audio data is typically measured in Gigabytes (GB) which equates to roughly 0.75 hours of data using the selected standard for video recording as stated above. This results in the following per officer video capture estimates:

- MINIMUM requires 1.5 GB per tour, 30 GB per month, 360 GB per year
- MEDIUM requires 3 GB per tour, 60 GB per month, 720 GB per year
- MAXIMUM requires 6 GB per tour, 120 GB per month, 1,440 GB per year

The final assumption for determining raw storage requirements is the retention period for the captured files. The Legal Section representative has recommended a standard file retention of 42 months, absent evidentiary requirements. Evidentiary requirements are more complex than what can be addressed in this section, but will have significant impact in increasing storage requirements by virtue of their longer retention periods.

Total storage estimates are driven by the video capture rate, aggregated monthly until retention periods expire. For each of the monthly capture thresholds, we have multiplied the average capture total against the number of officers, and then compounded them monthly for the total aggregate storage requirements.

\*NOTE: Although raw aggregation would end six months into year four, the retention of files classified as evidence for criminal or civil actions would offset this savings in an unknown amount.

YEAR 1	Month 1 per Officer		Month 1 Department			Month 12 per Officer		Month 12 Department		
	GB	TB	GB	TB	PB	GB	TB	GB	TB	PB
MINIMUM	30.00	0.03	36,000.00	35.16	0.03	360.00	0.35	432,000.00	421.88	0.41
MEDIUM	60.00	0.06	72,000.00	70.31	0.07	720.00	0.70	864,000.00	843.75	0.82
MAXIMUM	120.00	0.12	144,000.00	140.63	0.14	1,440.00	1.41	1,728,000.00	1,687.50	1.65
YEAR 2	Month 1 per Officer		Month 1 Department			Month 12 per Officer		Month 12 Department		
	GB	TB	GB	TB	PB	GB	TB	GB	TB	PB
MINIMUM	390.00	0.38	468,000.00	457.03	0.45	720.00	0.70	864,000.00	843.75	0.82
MEDIUM	780.00	0.76	936,000.00	914.06	0.89	1,440.00	1.41	1,728,000.00	1,687.50	1.65
MAXIMUM	1,560.00	1.52	1,872,000.00	1,828.13	1.79	2,880.00	2.81	3,456,000.00	3,375.00	3.30
YEAR 3	Month 1 per Officer		Month 1 Department			Month 12 per Officer		Month 12 Department		
	GB	TB	GB	TB	PB	GB	TB	GB	TB	PB
MINIMUM	750.00	0.73	900,000.00	878.91	0.86	1,080.00	1.05	1,296,000.00	1,265.63	1.24
MEDIUM	1,500.00	1.46	1,800,000.00	1,757.81	1.72	2,160.00	2.11	2,592,000.00	2,531.25	2.47
MAXIMUM	3,000.00	2.93	3,600,000.00	3,515.63	3.43	4,320.00	4.22	5,184,000.00	5,062.50	4.94
YEAR 4*	Month 1 per Officer		Month 1 Department			Month 12 per Officer		Month 12 Department		
	GB	TB	GB	TB	PB	GB	TB	GB	TB	PB
MINIMUM	1,110.00	1.08	1,332,000.00	1,300.78	1.27	1,440.00	1.41	1,728,000.00	1,687.50	1.65
MEDIUM	2,220.00	2.17	2,664,000.00	2,601.56	2.54	2,880.00	2.81	3,456,000.00	3,375.00	3.30
MAXIMUM	4,440.00	4.34	5,328,000.00	5,203.13	5.08	5,760.00	5.63	6,912,000.00	6,750.00	6.59

### *On Premise System vs. Cloud Hosted System*

An *on premise system* is one that is built, housed, maintained, and supported by Baltimore County information technology staff. There are many items to consider in the total cost of ownership for on premise systems and storage.

Using the maximum recording option of eight hours of video per officer per shift will require 2 to 3 Petabytes of storage, not including storage for backup. This puts cost estimates for on premise storage at more than \$2,000,000 annually when the infrastructure equipment is refreshed every five years. Maintenance for storage will cost between \$300,000 and \$400,000 in annual operating expense. A full time engineer would be required just to manage this amount of storage and backup. Additional unseen costs also need to be evaluated for on premise systems, such as electrical, environmental, security, and facility space for the data and data center.

An on premise solution would require the County to develop or purchase an off the shelf content management system robust enough to index, store, secure, and manage the files with proper audit tracking from capture to purging. It would take thousands of hours to develop and or configure such a system, and will take at least one full time employee to manage implementation.

Beyond the storage and management requirements, the County will need to invest in a redaction tool that can track and layer redactions without affecting the original “gold copy” of the video. Implementing separate storage, content management and redaction systems can raise significant logistical and integrity concerns for maintaining proper chain of custody.

A *cloud hosted system* is one that is built, housed, maintained, and supported by a third party service provider contracted by the Baltimore County Office of Information Technology. Many of the items to consider in the total cost of ownership for cloud hosted systems are implicitly handled as part of the provided service.

Hosted solutions offer redundant data centers for proven uptime greater than on premise solutions. The cost of hardware is avoided since the host is responsible for hardware costs and maintenance. Security levels are typically greater than most municipalities can afford to match; for example Evidence.com spends over \$1 million per year on security alone. Total cost of ownership is typically lower since there are no added costs from additional staffing, electrical service, environmental controls, and facility space.

Baltimore County already maintains the bandwidth capacities required to support a hosted solution. Additional investment in this area would not be anticipated.

Hosted solutions offer mature content management systems with robust role based security and auditing capabilities. Hosted solutions also commonly offer robust redaction tools as part of a total solution that simultaneously preserve the original “gold

copy” of the video while fulfilling redaction needs. These content management, user management, security, and redaction features are included in the service fee, making the hosted solution fiscally comprehensive.

In summary, the recommendation would be to pursue a hosted cloud based solution to manage fiscal constraints and simultaneously leverage advanced management of content, users, security, and redaction features.

### *Enterprise Solution*

This document addresses many specifications from devices to storage, and redaction to reproduction. Although each specification recommendation carries a different weight and impact on such a project, it is important to recognize the value in establishing a single enterprise solution for implementation of a body-worn camera program.

Body-worn camera programs can be established using multiple components or using a single enterprise, or end to end, vendor solution. In the multiple component based approach, the County could identify a device to be provided by one vendor, a file management solution from a second vendor, and a redaction and reproduction tool from yet a third vendor. In an enterprise approach, a single vendor offering is implemented to cover the entire program from point of capture through reproduction or purging.

Although a multiple component approach may support the direct satisfaction of many individual requirements, an enterprise solution is significantly more advantageous for the County. Component based approaches create multiple potential points of failure that are often difficult to troubleshoot, and require significant coordination resources between multiple vendors. End users and County support staff are required to learn multiple systems and multiple interfaces. This approach also requires chain of custody and audit trails through multiple systems that are difficult to coordinate and manage in a cohesive fashion.

An enterprise, or end to end, solution eliminates the complications of transferring data between systems. It eliminates requirements for establishing chain of custody through disparate systems. It eliminates coordination of multiple vendor support operations, and places the responsibility on one entity for a comprehensive service and support plan. An enterprise solution streamlines overall effort for both end users and County support staff.

In conclusion, an enterprise solution is highly recommended for this program.

### *Scalability*

As indicated in the storage requirements chart, the amount of required storage will grow drastically over the first four years, simply through collection and retention established for a consistent number of users. Expansion to other officers such as school resource officers, special operations, and investigators would dramatically impact the amount of

data storage requirements. Operational needs and legislative mandates may also affect the amount of data storage, including the possibility of reduction in storage needs.

In conclusion, a solution should be designed for ready scalability as this program changes over time.

### *Redundant Storage and Availability*

The storage estimates captured in the chart above refer only to the raw capture and storage estimates without accounting for redundant storage. Best practices would dictate that if the data is important enough to store, then it is important enough to backup. The dependency the County would develop for this data requires it to be protected from loss through hardware failure, network availability, and other issues.

In conclusion, the storage solution should include provisions for redundant storage to protect against loss, corruption, or unavailability.

### *Retention & Purging*

The Legal Section representative has recommended standard file retention of 42 months, absent evidentiary requirements. This program would collect vast amounts of video that will not be identified as having evidentiary value. This volume of video would be impossible to review for purging determinations, and purging will have to rely on the original classification of the originating police officer. The enormous quantity of video will require the automatic purging of videos not classified as evidentiary.

There will undoubtedly be video/audio files where longer retention periods will be required. Such files will have to be tagged as evidence or other with special categories for longer retention. Given the complexity of evidentiary retention standards, it is unlikely that automatic purging of such files can be established. Digital evidentiary retention will have to be managed in the same fashion as traditional evidence is managed, through coordination of the evidence custodian and the investigating officer.

In conclusion, the system must provide automatic purging for non-evidentiary videos, and allow for indefinite retention of evidentiary videos.

### *Expungement*

The Legal Section representative would be required to determine the impact and proper procedures for automatic and court ordered expungement relating to body-worn camera video and audio files.

Expungement technical specifications and feature requirements would need to be established as they relate to the legal and procedural requirements that are yet to be determined.

### *System Reports*

Management of data use, storage, security, and retention will require statistical reports about the stored videos. Standard user reports will be required for all metrics available in the video metadata, including all tags as well as the properties of the video files such as date, time, and duration.

Audit history reports would be required for individual file tracking (chain of custody), user activity (user accountability), and overall system metrics.

In conclusion, the system should include a feature to produce reports on all aspects of available data.

### *Other Digital Evidence*

Body-worn camera video recordings are not the only digital video that comes into possession of police departments. Existing work processes require police departments to capture, store, redact, and reproduce video evidence from multiple sources. Additional types of digital evidence include audio recordings, still images, and many other types.

Although digital evidence from other sources is not explicitly within the scope of a body-worn camera project, significant consideration should be given to the value of leveraging an enterprise management system for additional purposes. Most enterprise systems can also accommodate other digital evidence, increasing the value of the service provided as a one stop digital evidence shop for investigators and prosecutors.

In conclusion, leveraging an enterprise solution for additional purposes should be explored to increase the return on investment in such a system.

### System Security

Law enforcement activities are generally considered sensitive by the public, and are required to be secured appropriately. Proper security measures are required to ensure public trust in the integrity and privacy of the captured video.

### *Network Standards*

The solution provider should filter all transactions to only allow internet protocol addresses authorized by Baltimore County. This should be configurable by Baltimore County for future operational needs.

The solution should be able to work within the robust private network established by Baltimore County including the use of a proxy server for internet traffic, and without conflicting existing firewalls and other security measures.

### *Security Standards*

The storage solution provider must meet or exceed all CJIS security standards necessary to store law enforcement data.

Data encryption during transfer must meet SSL RSA 2048-bit key, 256- or 128-bit ciphers (depending on client browser).

Data encryption during rest (storage) must meet 256-bit Advanced Encryption Standard (AES-256)

### *Hashed File Verification*

A hash value is a unique hexadecimal value associated with a file. A hash value is a digital fingerprint of sorts, as it provides a unique identifier that can be used to identify and authenticate a file. Digital data of potential evidentiary value is hashed to show that the files have not changed from the time they were obtained to the time they are presented in court. The hash value therefore is an essential element in the establishment and maintenance of chain of custody records in compliance with law enforcement and judicial standards.

Storage solutions being considered by the County for the storage of video extracted from body-worn cameras should have a hash authentication feature. The video uploaded is considered the “gold copy” which should remain pristine and unedited, which is documented by way of an audit trail. Edits and redactions should be performed on a copy or an overlay layer that can be tracked in a second audit trail distinctly separate from that of the “gold copy.”

In conclusion, a storage solution must support preservation of hash values.

### *Role Based Permission Groups*

The size and nature of a body-worn camera program would require decentralized management of many aspects. A variety of stakeholders including officers, detectives, internal investigators, commanders, evidence technicians, legal personnel, media personnel, Training Section personnel, and technical support staff will all require different roles in the system. A segregation of these roles should be managed through role based permission groups in the system. This maintains the integrity of processes by minimizing opportunity for a user in one area to intentionally or unintentionally affect another area.

Role based permission groups are a requirement for managing any solution.

### *User Authentication*

Baltimore County utilizes Active Directory for single sign-on user authentication wherever possible. This streamlines user management, provides consolidated user security, and is generally well received by members who do not want to maintain more sets of system credentials than are necessary.

A solution that integrates user authentication with Baltimore County's Active Directory would be preferred.

### *Self-Password Reset*

In the event that a solution does not provide integration with our Active Directory services, a secure self-service password reset feature is essential in reducing burden on the OIT Help Desk when members forget their credentials.

This feature is preferred in the absence of the single sign-on feature.

### *System Audit History*

The system must provide an audit history of all activity associated with an individual video. This would allow an administrator to review the capture, tagging, upload, viewing, redacting, reproducing, and purging activities for any individual video recording in support of chain of custody standards. This is an essential element of established chain of custody standards.

Similarly, audit reports for user activity in the system (not single file centric) would be required for user accountability. Reports would be required to track system access, file viewing, file editing, and all other actions.

### Dissemination

The purpose of body-worn cameras is not simply to collect video, but rather to collect video and make it useful to police, prosecutors, defense attorneys, courts, and the public. Collected videos will need to be reproduced, or otherwise made available for many purposes and many audiences.

### *Direct System Access*

The most frequent method for reviewing video will be through direct system access according to the established role based security. Personnel from many assignments internal to the police department will require direct access to the video/audio files for their operational needs. This includes searching for files as well as reviewing them within the system.

In conclusion, the system must support searching, retrieving, and playback of video and audio files through the native user interface.

### *System Access Sharing*

Some available systems allow reviewing of videos or redacted videos by people external to the agency through a hypertext transfer protocol link embedded in an email message. Issuing permission to this link would be a feature managed through role based permission groups.

Video link sharing features typically have many configuration options to be established either by the administrator or by the user publishing the link. These include whether the video link has an expiration date, a limited number of views, credential requirements, and more. While controls on the reproduction of these videos may be limited, it is important to remember that videos produced and disseminated by disc are very easily reproduced by intended recipients or unintended intercepting parties.

System access sharing is an alternative to reproducing video on optical media such as CD and Blu-ray. The benefits include cost savings of the discs themselves, cost savings of shipping, reduced logistical management, and immediate delivery to the intended recipient.

System access sharing may be useful for sharing video with attorneys, courts, and even the media.

### *Transferable Media*

There will always be a need to reproduce video and audio files on physical transfer media such as optical discs and USB storage drives.

The system must support transfer of files to transferable physical media.

### *File Format*

Dissemination of video and audio must produce the files in a non-proprietary file format to ensure playback compatibility for the intended recipient.

### *Video and Audio Redaction*

There are many established laws and legal standards that affect reproduction and dissemination policy and procedures. Several will require the redaction of visual and audible elements of body-worn camera video.

The first point of consideration in the area of redaction is to include the redaction tools as part of the enterprise solution rather than as an external process or system. External redaction processes require files to be exported and stored separately. The exported

file then is subject to a disparate audit and chain of custody record, if the redaction suite offers any tracking at all. The exported file also creates extra storage requirements as it must be stored separately from the system files, and of course backed up to ensure preservation. Lastly, redacted files stored separately may be difficult to track, and could result in multiple redaction efforts when multiple dissemination requests are fulfilled for the same files.

Including the redaction tools within the enterprise solution create a one stop shop for the system user. The video original uploaded is considered the “gold copy” which should remain pristine and unedited, which is documented by way of an audit trail. Edits and redactions can then be performed as an overlay that can be tracked through an independent audit trail. This allows tracking that is distinctly separate from that of the “gold copy.” Logistical and storage issues are minimized.

The level of effort for redaction of video and audio files with capture specifications recommended in this document is estimated at a ratio of 30 to 1 redaction effort time to video playback time. This is a statistic reported by other agencies including Sarasota, Florida, and has been confirmed with basic evaluation by our own technical staff. This tremendous level of effort, multiplied by the anticipated demand for reproduction and dissemination, make a robust integrated redaction tool a high level requirement for this program.

### User Support

Body-worn camera devices and enterprise solutions are more than a onetime vendor purchase. These programs require ongoing support by manufacturers and service providers to ensure desired program performance.

### *Warranty*

All acquisitions of hardware should include comprehensive warranty coverage for a period no less than one year and ideally for three years or the estimated life cycle of the warranted items.

### *Service Agreement*

A service agreement should be implemented to cover all technical and support labor needs for the entire life cycle of the hardware and software.

The service agreement should include 24 X 7 remote support through telephone, email, and web presence. Cross shipping of hardware should also be included.

### *Device Life Cycle Refresh*

All electronic devices have estimated life cycles. Based on the available life cycle refresh plans available from current market providers, a minimum life cycle period recommendation is three years.

The agency should plan for device refresh or replacement according to the manufacturer's specifications. If possible, this should be managed as part of a service agreement with the device provider.

### *Field Technician Certifications*

All agency configurable device features should be able to be managed by either the agency system administrator or an agency field technician. Ideally these would be managed through a device management portal in an enterprise solution.

Any components of body-worn camera devices that are typically susceptible to damage or failure should be capable of being supported by agency staffed field technicians. This includes interchanging of parts such as cables, batteries, and mounting accessories.

The vendor should provide the training necessary for agency field technicians to complete these tasks and provide this level of service to the end users.

### Technology Fiscal Investment

There are many fiscal considerations in a body-worn camera program. This section addresses only those directly related to hardware and software.

Earlier in this document recommendations have been provided that an enterprise solution would be best. Enterprise solutions typically provide package pricing for all aspects from device acquisition to device refresh, from warranties to user support, and from raw storage to enhanced management tools. Fiscal evaluations from any single section in this document should be considered both independently and within the context of an enterprise solution.

### *Device Investment*

Prices for current market body-worn cameras range generally from \$400 per unit to \$1,000 per unit. This is a substantially wide range of pricing, but is directly related to the individual device specifications desired by an agency. On the assumption of equipping 1,200 personnel with body-worn cameras, a device only investment would range from \$480,000 to \$1,200,000.

Pricing for devices can also be affected through negotiation of available enterprise agreements.

## *Cost of Cloud Storage*

This report compares the cost of cloud based storage of two major vendors in the body-worn camera marketplace; Evidence.com and VieVu. Both companies represent a large portion of the current market share, and offer several cloud storage plans based on data usage. The comparison will consider the cost, essential features, product support, warranty and service agreements of both vendors for demonstrative purposes. Also of note, this section refers to the costs on an individual user basis, but detailed vendor negotiation may result in a cost savings by allowing the use of pooled storage among all users.

Evidence.com is the storage management component of TASER International. TASER markets and sells the Axon Body and Axon Flex cameras. Evidence.com offers four storage plans with various feature sets and storage limitations and identifies them as Basic, Standard, Pro, and Ultimate. They range in monthly per user storage size limits of 5GB, 10GB, 15GB, and 20GB respectively. All plans allow the user to purchase additional storage above the monthly maximum at the cost of \$0.125 per GB. The Ultimate plan allows the purchase of unlimited Axon Body and Axon Flex data storage for an additional \$24 per month. Only the Pro and Ultimate plans offer a proprietary redaction tool, which the County requires. In addition, the Ultimate plan provides an equipment refresh/upgrade of the body-worn camera every 2.5 years. All Evidence.com plans include business hours support by telephone and email. A Professional Services package is available that includes additional on-site support. No pricing information is available on that package at this time.

Using the identified storage requirements for the three scenarios presented, the monthly cost for the County to use Evidence.com cloud storage would be as follows:

- *Pro Plan* - Base cost \$39/month, 15 GB maximum plus \$0.125 for each additional 1 GB/month, no equipment refresh
  - >For MINIMUM recording, 30 GB of storage space per month for each officer would cost \$40.88 per month. This equates to \$588,600 to equip 1,200 officers in Year 1
  - >For MEDIUM recording, 60 GB of storage space per month for each officer would cost \$44.63 per month. This equates to \$642,600 to equip 1,200 officers in Year 1
  - >For MAXIMUM recording, 120 GB of storage space per month for each officer would cost \$52.13 per month. This equates to \$750,600 to equip 1,200 officers in Year 1

Based on the aggregate storage criteria determined by the departmental retention policies previously stated, the cost to equip the Department in the Evidence.com Pro Plan for that same period is as follows:

Evidence.com - Pro Plan								
Year 1	Month 1 per Officer		Month 1 Department		Month 12 per Officer		Month 12 Department	
	GB	Cost	GB	Cost	GB	Cost	GB	Cost
MINIMUM	30	\$40.88	36,000.00	\$49,050.00	360.00	\$490.50	432,000	\$588,600.00
MEDIUM	60	\$44.63	72,000.00	\$53,550.00	720.00	\$535.50	864,000	\$642,600.00
MAXIMUM	120	\$52.13	144,000.00	\$62,550.00	1,440.00	\$625.50	1,728,000	\$750,600.00
Year 2	Month 1 per Officer		Month 1 Department		Month 12 per Officer		Month 12 Department	
	GB	Cost	GB	Cost	GB	Cost	GB	Cost
MINIMUM	390	\$85.88	468,000.00	\$103,050.00	720.00	\$1,030.50	864,000	\$1,236,600.00
MEDIUM	780	\$134.63	936,000.00	\$161,550.00	1,440.00	\$1,615.50	1,728,000	\$1,938,600.00
MAXIMUM	1560	\$232.13	1,872,000.00	\$278,550.00	2,880.00	\$2,785.50	3,456,000	\$3,342,600.00
Year 3	Month 1 per Officer		Month 1 Department		Month 12 per Officer		Month 12 Department	
	GB	Cost	GB	Cost	GB	Cost	GB	Cost
MINIMUM	750	\$130.88	900,000.00	\$157,050.00	1,080.00	\$1,570.50	1,296,000	\$1,884,600.00
MEDIUM	1500	\$224.63	1,800,000.00	\$269,550.00	2,160.00	\$2,695.50	2,592,000	\$3,234,600.00
MAXIMUM	3000	\$412.13	3,600,000.00	\$494,550.00	4,320.00	\$4,945.50	5,184,000	\$5,934,600.00
Year 4	Month 1 per Officer		Month 1 Department		Month 12 per Officer		Month 12 Department	
	GB	Cost	GB	Cost	GB	Cost	GB	Cost
MINIMUM	1110	\$175.88	1,332,000.00	\$211,050.00	1,440.00	\$2,110.50	1,728,000	\$2,532,600.00
MEDIUM	2220	\$314.63	2,664,000.00	\$377,550.00	2,880.00	\$3,775.50	3,456,000	\$4,530,600.00
MAXIMUM	4440	\$592.13	5,328,000.00	\$710,550.00	5,760.00	\$7,105.50	6,912,000	\$8,526,600.00

- *Ultimate Plan 1* - Base cost \$55/month, 20 GB maximum plus \$0.125 for each additional 1 GB/month, equipment refresh every 2.5 years

>For MINIMUM recording, 30 GB of storage space per month for each officer would cost \$56.25 per month. This equates to \$810,000 to equip 1,200 officers in Year 1.

>For MEDIUM recording, 60 GB of storage space per month for each officer would cost \$60.00 per month. This equates to \$864,000 to equip 1,200 officers in Year 1.

>For MAXIMUM recording, 120 GB of storage space per month for each officer would cost \$67.50 per month. This equates to \$972,000 to equip 1,200 officers in Year 1.

Based on the aggregate storage criteria determined by the departmental retention policies previously stated, the cost to equip the Department in the Evidence.com Ultimate Plan 1 for that same period is as follows:

Evidence.com - Ultimate Plan 1								
Year 1	Month 1 per Officer		Month 1 Department		Month 12 per Officer		Month 12 Department	
	GB	Cost	GB	Cost	GB	Cost	GB	Cost
MINIMUM	30	\$56.25	36,000.00	\$67,500.00	360.00	\$675.00	432,000	\$810,000.00
MEDIUM	60	\$60.00	72,000.00	\$72,000.00	720.00	\$720.00	864,000	\$864,000.00
MAXIMUM	120	\$67.50	144,000.00	\$81,000.00	1,440.00	\$810.00	1,728,000	\$972,000.00
Year 2	Month 1 per Officer		Month 1 Department		Month 12 per Officer		Month 12 Department	
	GB	Cost	GB	Cost	GB	Cost	GB	Cost
MINIMUM	390	\$101.25	468,000.00	\$121,500.00	720.00	\$1,215.00	864,000	\$1,458,000.00
MEDIUM	780	\$150.00	936,000.00	\$180,000.00	1,440.00	\$1,800.00	1,728,000	\$2,160,000.00
MAXIMUM	1560	\$247.50	1,872,000.00	\$297,000.00	2,880.00	\$2,970.00	3,456,000	\$3,564,000.00
Year 3	Month 1 per Officer		Month 1 Department		Month 12 per Officer		Month 12 Department	
	GB	Cost	GB	Cost	GB	Cost	GB	Cost
MINIMUM	750	\$146.25	900,000.00	\$175,500.00	1,080.00	\$1,755.00	1,296,000	\$2,106,000.00
MEDIUM	1500	\$240.00	1,800,000.00	\$288,000.00	2,160.00	\$2,880.00	2,592,000	\$3,456,000.00
MAXIMUM	3000	\$427.50	3,600,000.00	\$513,000.00	4,320.00	\$5,130.00	5,184,000	\$6,156,000.00
Year 4	Month 1 per Officer		Month 1 Department		Month 12 per Officer		Month 12 Department	
	GB	Cost	GB	Cost	GB	Cost	GB	Cost
MINIMUM	1110	\$191.25	1,332,000.00	\$229,500.00	1,440.00	\$2,295.00	1,728,000	\$2,754,000.00
MEDIUM	2220	\$330.00	2,664,000.00	\$396,000.00	2,880.00	\$3,960.00	3,456,000	\$4,752,000.00
MAXIMUM	4440	\$607.50	5,328,000.00	\$729,000.00	5,760.00	\$7,290.00	6,912,000	\$8,748,000.00

- Ultimate Plan 2 - Base Cost \$55/month plus \$24/month for unlimited storage capacity add on, equipment refresh every 2.5 years**  
 >For all three levels of usage, and based on the aggregate storage criteria determined by the departmental retention policies previously stated, the monthly cost for unlimited storage space for each officer would cost \$79 per month. This equates to \$1,137,600 annually to equip 1,200 officers in Years 1 through 4, regardless of the amount of Axon camera data stored.

Year 1	Month 1 per Officer		Month 1 Department		Month 12 per Officer		Month 12 Department	
	GB	Cost	GB	Cost	GB	Cost	GB	Cost
MINIMUM	30	\$79.00	36,000.00	\$94,800.00	360.00	\$948.00	432,000	\$1,137,600.00
MEDIUM	60	\$79.00	72,000.00	\$94,800.00	720.00	\$948.00	864,000	\$1,137,600.00
MAXIMUM	120	\$79.00	144,000.00	\$94,800.00	1,440.00	\$948.00	1,728,000	\$1,137,600.00
Year 2	Month 1 per Officer		Month 1 Department		Month 12 per Officer		Month 12 Department	
	GB	Cost	GB	Cost	GB	Cost	GB	Cost
MINIMUM	390	\$79.00	468,000.00	\$94,800.00	720.00	\$948.00	864,000	\$1,137,600.00
MEDIUM	780	\$79.00	936,000.00	\$94,800.00	1,440.00	\$948.00	1,728,000	\$1,137,600.00
MAXIMUM	1560	\$79.00	1,872,000.00	\$94,800.00	2,880.00	\$948.00	3,456,000	\$1,137,600.00
Year 3	Month 1 per Officer		Month 1 Department		Month 12 per Officer		Month 12 Department	
	GB	Cost	GB	Cost	GB	Cost	GB	Cost
MINIMUM	750	\$79.00	900,000.00	\$94,800.00	1,080.00	\$948.00	1,296,000	\$1,137,600.00
MEDIUM	1500	\$79.00	1,800,000.00	\$94,800.00	2,160.00	\$948.00	2,592,000	\$1,137,600.00
MAXIMUM	3000	\$79.00	3,600,000.00	\$94,800.00	4,320.00	\$948.00	5,184,000	\$1,137,600.00
Year 4	Month 1 per Officer		Month 1 Department		Month 12 per Officer		Month 12 Department	
	GB	Cost	GB	Cost	GB	Cost	GB	Cost
MINIMUM	1110	\$79.00	1,332,000.00	\$94,800.00	1,440.00	\$948.00	1,728,000	\$1,137,600.00
MEDIUM	2220	\$79.00	2,664,000.00	\$94,800.00	2,880.00	\$948.00	3,456,000	\$1,137,600.00
MAXIMUM	4440	\$79.00	5,328,000.00	\$94,800.00	5,760.00	\$948.00	6,912,000	\$1,137,600.00

VieVu markets and sells the LE3 body-worn camera and offers a single storage plan for use with its camera called the VieVu Solution. This plan provides 60GB of cloud based data storage. Additional storage is available for purchase for \$0.125 per GB. The VieVu Solution includes the LE3 camera with a three year warranty and 24 x 7 technical support. There is no option for equipment refresh, but camera upgrades are included at no additional cost.

Using the identified storage requirements for the three scenarios presented the monthly cost for the County to use VieVu cloud storage would be as follows:

- VieVu Solution Plan* - \$199 one time upfront cost, \$55/month, 60 GB maximum plus \$0.125 for each additional 1GB/month

  - >For MINIMUM recording, 30 GB of storage space per month would cost \$55.00 per month plus a onetime cost of \$199 for each officer. This equates to \$1,030,800 to equip 1,200 officers in Year 1.
  - >For MEDIUM recording, 60 GB of storage space per month would cost \$55.00 per month plus a onetime cost of \$199 for each officer. This equates to \$1,030,800 annually to equip 1,200 officers in Year 1.
  - >For MAXIMUM recording, 120 GB of storage space per month would cost \$62.50 per month plus a onetime cost of \$199 for each officer. This equates to \$1,138,800 annually to equip 1,200 officers in Year 1.

Based on the aggregate storage criteria determined by the departmental retention policies previously stated, the cost to equip the Department in the VieVu Solution Plan for that same period is as follows:

VieVu - Solution Plan								
Year 1	Month 1 per Officer		Month 1 Department		Month 12 per Officer		Month 12 Department	
	GB	Cost	GB	Cost	GB	Cost	GB	Cost
MINIMUM	30	\$254.00	36,000.00	\$66,199.00	360.00	\$859.00	432,000	\$1,030,800.00
MEDIUM	60	\$254.00	72,000.00	\$66,199.00	720.00	\$859.00	864,000	\$1,030,800.00
MAXIMUM	120	\$261.50	144,000.00	\$75,199.00	1,440.00	\$949.00	1,728,000	\$1,138,800.00
Year 2	Month 1 per Officer		Month 1 Department		Month 12 per Officer		Month 12 Department	
	GB	Cost	GB	Cost	GB	Cost	GB	Cost
MINIMUM	390	\$96.25	468,000.00	\$115,500.00	720.00	\$1,155.00	864,000	\$1,386,000.00
MEDIUM	780	\$145.00	936,000.00	\$174,000.00	1,440.00	\$1,740.00	1,728,000	\$2,088,000.00
MAXIMUM	1560	\$242.50	1,872,000.00	\$291,000.00	2,880.00	\$2,910.00	3,456,000	\$3,492,000.00
Year 3	Month 1 per Officer		Month 1 Department		Month 12 per Officer		Month 12 Department	
	GB	Cost	GB	Cost	GB	Cost	GB	Cost
MINIMUM	750	\$141.25	900,000.00	\$169,500.00	1,080.00	\$1,695.00	1,296,000	\$2,034,000.00
MEDIUM	1500	\$235.00	1,800,000.00	\$282,000.00	2,160.00	\$2,820.00	2,592,000	\$3,384,000.00
MAXIMUM	3000	\$422.50	3,600,000.00	\$507,000.00	4,320.00	\$5,070.00	5,184,000	\$6,084,000.00
Year 4	Month 1 per Officer		Month 1 Department		Month 12 per Officer		Month 12 Department	
	GB	Cost	GB	Cost	GB	Cost	GB	Cost
MINIMUM	1110	\$186.25	1,332,000.00	\$223,500.00	1,440.00	\$2,235.00	1,728,000	\$2,682,000.00
MEDIUM	2220	\$325.00	2,664,000.00	\$390,000.00	2,880.00	\$3,900.00	3,456,000	\$4,680,000.00
MAXIMUM	4440	\$602.50	5,328,000.00	\$723,000.00	5,760.00	\$7,230.00	6,912,000	\$8,676,000.00

It is important to note that these illustrations are created with currently available pricing from indicated providers. These are subject to negotiation and changes over time.

## Acknowledgements

Such an undertaking with significant time constraints can only occur when an exceptional group of people come together for a singular cause. Every member of this workgroup dedicated considerable time and effort toward research, discussion, and determination for virtually every aspect of the project.

Success with regard to such a complex issue and task at hand is directly correlated to proper planning and research. Our team included three outstanding individuals whose efforts helped to drive the workgroup: Sergeant Vincent Luther, Officer Michael Koffenberger, and Officer Lauren Pomales. They gave us up-to-the minute information on an issue that is in its infancy and still developing.

In reporting on our discussions and findings, everyone pitched in. With regard to a couple of key areas, we had to rely on workgroup members who had unique expertise. Media and Communications Section Director Elise Armacost not only developed our awareness guidelines but was a huge help in editing our report, thanks to her tremendous communications skills. Legal Section Director Vickie Wash has an outstanding knowledge of consent and privacy issues, and not only educated our workgroup but others in County leadership, then had to document these complex implications.

Finally, our technology subgroup included Captain Joseph Conger, Chief Technology Officer Robert O'Connor, Forensic Services Supervisor Christopher Kollmann, and Information Technology Project Manager Chip Hiebler. This team had the unenviable task of developing recommendations not only for the actual BWC equipment but for storage solutions, and did a tremendous job of reporting their findings.

My deepest thanks go to every member of the workgroup for their stellar efforts.

Major Mark J. Warren, Workgroup Chair