POLICE 1

HOW TO BUY

BODY-WORN CAMERAS

Key steps for product selection, purchasing and implementation

Introduction

Never in the history of law enforcement has the American public so vehemently demanded police adopt a technology or device as they have for body-worn cameras (BWCs). Citizens see the technology as ensuring greater visibility into their police force – especially in the case of use-of-force incidents.

There are agency benefits as well. Deployment of BWCs by law enforcement professionals – patrol, corrections, SWAT and other tactical responders – offers significant advantages in keeping officers safe, enabling situational awareness and providing evidence for trial. Agencies already using BWCs report that they help reduce citizen complaints, lower instances of resistance and use of force, improve police-community interaction and enrich public safety.

While the value and utility of BWCs are understood at a fundamental level, there are factors police departments need to weigh and steps to take in order to have a long-standing and successful BWC program.

This Police1 guide – whether you are leading a body camera purchase for the first time or are looking to upgrade your current system – is a starting point for the several months or more procurement process.

Nancy Perry, Police1 Editor-in-Chief

Contents

REMINDER: Every department is subject to local or state purchasing rules. Make sure to understand and follow the procurement process for your department and take advantage of services provided by your city or county purchasing department.

KEY CONSIDERATIONS BEFORE PURCHASING BODY-WORN CAMERAS

Agencies considering the implementation of BWCs can benefit from their use in many areas, but only if the program is implemented correctly. Agencies that have not yet implemented a body-worn camera initiative must undertake such a project with purpose and intent – it is imperative to consider all the possible factors at stake.

There is a plethora of documented research and publications about BWC adoption, implications for use (e.g. officer safety, privacy, transparency, use-of-force) and efficacy. The guidelines presented in this document provide key steps for product selection, purchasing and implementation.

From budgeting, needs assessments and data management considerations, to legal and privacy issues, there are several items police departments will need to discuss and research prior to BWC procurement.

Further, agencies need to decide whether they should select a stand-alone body-worn camera or a camera that is part of a smartphone or other multi-purpose device.

Following are seven things to consider during the body-worn camera procurement process:

Due diligence

There are several BWC product providers that police departments can choose from, but before signing a contract with any BWC provider, it is critical for departments to do their due diligence prior to procurement to ensure the product they buy will perform the way the department needs it to.

Part of the due diligence process for BWC procurement includes, at a minimum, learning from other agencies that deployed the current version of the solution, conducting a needs assessment, documenting those needs, identifying and documenting agency business requirements, examining FBI CJIS requirements, and reviewing state and federal legislative requirements.

For some BWC procurements (depending on agency size and procurement regulations), this process also typically includes:

- Issuing a request for information or request for qualifications;
- Inviting BWC providers for in-person demonstrations;
- Developing and releasing a request for proposal;
- Inviting a smaller group of vendors back for additional demonstrations and questions;
- Reviewing RFP responses;
- Selecting a BWC vendor;
- Finalizing contract negotiations;
- Issuing an award;
- Developing test scenarios;
- System testing;
- Allowing time for break/fix cycles;
- Developing and administering policies;
- Implementing the BWCs to officers;
- Delivering training;
- Administering and maintaining the BWC program.

Budgeting

Discussing and documenting the basic functional requirements and use cases for BWCs will ensure a police department selects the right vendor for its BWC program. Procurement officers must be knowledgeable about what is being purchased, and they need to perform the necessary research and evaluation before acquiring.

Specific line items to review include:

- Acquisition;
- Installation (software, hardware and possible server);
- Any energy and energy dependence cost;
- Data storage
  - Cloud services
  - Cloud disaster recovery plan (services);
- Software licenses;
- Labor/operations (e.g., FOIA, discovery)
  - Time officers spend reviewing videos/data
  - Time officers spend tagging and uploading video evidence
  - Time for detectives to review and include videos with case filings for the DA's office;
- Equipment
  - Replacement hardware (BWCs can break)
  - Accessories (e.g., batteries, mounting hardware);
- Training;
- Maintenance;
- Service fees;
- Third-party integration fees (e.g., FirstNet, investigation software, evidence management software).

Just like a patrol vehicle or body armor, BWCs have a life expectancy – they need to be properly cared for, stored and maintained, and there needs to be a line item for replacements. It is important to identify a funding source in advance and allow for adequate time to implement.

BWC functionality

The user interface is the indexing and viewing software officers use to review videos. If the software is difficult to use, officers will struggle every time a video needs to be viewed. Features to look for include:

- **Search options:** How many parameters can be used to locate relevant video clips? These might include an officer's name, ID number, day, time, geo-coordinates, incident or case number, type of incident and clip length.
- **Security features:** There needs to be several levels of security, each with rights that expand with the level. The basic level might give only the ability to see clips that user had made. A sergeant could have access to clips made by anyone in his squad. Only upper levels of security would permit the user to copy the video to external media.
- **Chain of evidence:** Security should track every action by every user, so any change or copying can be tied to the person who did it.
- **Thumbnail indexing:** Many video management packages create a thumbnail, or small still frame, from the video every few seconds. This allows for quick review when you want to get to the portion of the video where the action takes place.
- **Viewing options:** By default, videos usually play in a small viewing window, with the perimeter surrounded by metadata. There should be an option to view the video full screen.
- **Redaction capabilities:** Before a video is released to an outside entity, you'll often want to redact information such as license plate numbers and faces of uninvolved witnesses. Manually redacting this information, usually by blurring the details, is a time-consuming process. Some vendors offer auto-redaction features that will follow any object you designate and redact it throughout the entire video.
- **Selective overlays:** Most viewing software allows the user to overlay text on the screen that provides time and date, officer's name, speed, whether emergency lights are on and other data elements. Make sure there is an option to include or remove all that information with every video.

Cloud service providers (BWC data storage/management)

There are several cloud service providers (CSPs) available in today's market. Selecting the most commonly known CSP is not always the best choice for an agency's business and operational needs. Below are selected authoritative resources* that public safety agencies need to review and become familiar with before selecting a cloud service provider.

- The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology;
- Evaluation of Cloud Computing Services Based on NIST SP 800-145 (NIST SP 500-322);
- NIST Cloud Computing Reference Architecture (SP 500-292);
- FBI CJIS: Recommendations for Implementation of Cloud Computing Solutions;
- HHS: Guidance on HIPAA & Cloud Computing.

Police departments need to develop a cloud disaster recovery (cloud DR) plan. When systems go down, officers are unable to access information they're dependent on. It is critical to have a cloud DR strategy in place for continuity of operations and to include it in the agency's operating budget. The cloud DR plan needs to include input from end-users, agency executives and IT. To get started, agencies need to perform at a minimum, a business impact analysis, a risk assessment and a risk management strategy, then test the cloud DR configuration.

** This is not a comprehensive list.*

Privacy policies

There are several legal issues around privacy that an agency seeking to implement a policy for officer use of BWCs must consider:

- **Federal privacy legislation:** Policies will need to address police wearing the cameras into private areas, especially homes.
- **State privacy legislation:** Each state varies in their statutes regarding the recording of conversations. Some states have two-party consent rules. Determine your state's privacy, eavesdropping and electronic monitoring statutes, and case law about police use of such techniques before using body cameras.
- **Fourth Amendment privacy against government intrusion:** In *Lopez v. U.S (1963),* the U.S. Supreme Court extended the "plain view" doctrine to recording, holding that officers may generally record what they can lawfully see or hear without violating the Fourth Amendment. But what if the camera captures something the officer did not see or hear? Would this be more akin to thermal imaging from a public vantage point, which the Supreme Court held in *Kyllo v. U.S. (2001)* required a warrant? Something may be seen or heard only by reviewing the tape repeatedly, or in slow motion, or stop frame, or digitally enhancing it? Are these actions a separate search requiring a warrant? These are just some of the considerations for agencies as they develop BWC privacy policies.
- **Privacy:** Officers need to have OFF/ON discretion. This needs to be specifically spelled out in policies with consequences for non-compliance. That implicates disciplinary actions and their attendant officer rights.

Public records

Every state has an open public records law. Most define a public record broadly enough to encompass BWC video. This makes the video subject to an open records or Freedom of Information (FOI) request. But most of these laws were written well before

BWCs and their attendant privacy implications existed.

It is imperative a police department understand its state's public records law, and any existing exemptions, before implementing BWCs.

The Federal Freedom of Information Act (FOIA) broadly exempts from disclosure "records or information compiled for law enforcement purposes" if their production:

a. Could reasonably be expected to interfere with enforcement proceedings;
b. Would deprive a person of a right to a fair trial or an impartial adjudication;
c. Could reasonably be expected to constitute an unwarranted invasion of privacy;
d. Could reasonably be expected to disclose the identity of a confidential source which furnished information on a confidential basis;
e. Would disclose techniques for law enforcement investigations or prosecutions that could reasonably be expected to risk circumvention of the law;
f. Could reasonably be expected to endanger the life or physical safety of anyone.

An agency must demonstrate that disclosure "would" cause the harm in only B and E – Congress lessened the standard to "could" in the other subsections. State and local public records and FOIA requests vary.

The resources needed to address not just production but storage, retention, review, retrieval and redaction under public records laws can be huge. Take a department with 25 officers running body cameras 32 out of every 40 hours, 46 weeks a year. That's 36,800 hours of video potentially subject to public records disclosure requests. There is also the discovery obligations owed to criminal defendants. Do we really want to be addressing these legal requirements after the cameras are rolling?

One solution may be to modify the public records and FOIA legislation that was enacted without body cameras in mind – before providing the devices to officers and agencies.

Video as evidence

BWC video can become evidence in court. Proper chain of custody must be maintained. There must be technical controls to protect against tampering, destruction and unauthorized access. If a third-party cloud service is used for storage, encryption may need to be "end-to-end." This is a system where the only people who can view the information are the people communicating. No one else can access the cryptographic keys needed to decrypt the information – not even a company that runs the messaging service.

To authenticate the video, the date, time and location of recording must be documented. A witness must verify the contents and relevant identities of those recorded and provide assurance it hasn't been edited or over-dubbed.

Prosecutors and attorneys representing officers/agencies in civil lawsuits may need expert witnesses who can explain the operational aspects of the camera regarding circumstances like those above.

If video footage becomes trial evidence, it will need to be retained if other evidence subject to an appeal and a possible retrial.

There is related precedent for excluding evidence that could have been captured on a BWC. In the case of custodial interviews, some states have gone beyond a rebuttable presumption and determined that such evidence is inadmissible if not recorded, absent a specified exception.

Finally, it is the police's and prosecution's duties under the Supreme Court cases of *Giglio* and *Brady* to turn over evidence to the defense that might be used to impeach the credibility of a prosecution witness, including police officers. This includes body camera evidence.

TOP IMPLEMENTATION CONSIDERATIONS FOR BODY-WORN CAMERAS

Whether your department is testing BWCs, sourcing funding for them, has had them for years or is still skeptical about the technology, there are many things an agency must consider. Police departments need to do extensive evaluation of various BWC systems and research best practices and policies prior to implementation.

Reach out to adjacent agencies to compare policy-related issues like BWC incident recording (officer discretion) or investigation during combined agency operations. Invite BWC product providers in to demonstrate the technology's capabilities. Make sure the capabilities and functionality are in alignment with the documented department's needs and requirements.

Here are five body-worn camera implementation considerations before you buy:

Policy development

There are several areas of BWC operation where absolutes are difficult to determine and opinions vary, even among the experts. Some of these, such as discretionary recording, incident review, recording advisory and citizens "opting out" have a degree of potential controversy and potential legislative requirement so you will need to do your due diligence before finalizing your policy.

Seek input from your stakeholders and set clear expectation in your policy. Many agencies modify their policy after real-world experiences dictate a need for change. Following are some considerations BWC policies should address:

1. Should officers be required to record every contact, or will they be permitted a degree of discretion?
2. When and under what situations will cameras be utilized?
3. Will notification of recording be required?
4. Should officers be required to advise persons being contacted that they are being recorded?
5. Should citizens have the right to prevent an officer's recording?
6. What are the primary and permitted uses of the video?
7. Should officers be permitted to review the recording of an incident before writing a report or giving a statement?
8. Who will have access to the video and how long will it be retained?
9. How will the security of the data be assured?

Notifying the public

Prior to the roll out, fully explain the system to the community, elected officials, the District Attorney and your officers. Partners in policy development should include such groups as the city attorney, local district attorney, police association, staff members and end users.

Remind citizens and officers that cameras are not indestructible, and that in the fray of an encounter that turns violent, the video recording may be compromised by mechanical or other failure. This is something that needs to be communicated to the public before a problem begins, not after.

The public, juries in particular, will need to be regularly reminded that officers' actions are judged based on the objectively reasonable standard as set forth in Graham v. Connor. That case decision stated that Court cautioned 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." As body-worn camera footage is made available and viewed in court, consideration for what the officer was seeing, hearing, and experiencing at the time of the event is what's important, not what the camera recorded. The camera simply cannot record the totality of the circumstances.

Training and deployment

Very few agencies try a single, department-wide roll out and for good reason: there are a lot of moving parts to a BWC program and it makes sense to start small, address issues as they come up, and expand the effort as lessons are learned and problems are resolved. The most effective approach is to start with a small pilot group of field officers.

Once operational basics are ironed out, expand the program to a specific unit or group for a period of 60-90 days. Not only will this make your training more manageable, this will facilitate resolution of issues related to infrastructure like network storage or bandwidth limitations.

At a minimum, training should consist of an in-depth review of policy, as well as equipment familiarization to include operational parameters and limitations. For instance, if your BWC units have an expected record time of six hours due to battery life, then you need officers to be aware of this so they can plan or monitor accordingly. Another important training consideration is the method and restrictions on accessing the recording and the method of storage or transfer. This will be unique to your system and your agency setup and should be outlined clearly in your policy.

It will take time for officers to have the mental awareness and primed thought process to initiate recording. Be prepared for those times when a recording was not obtained but the public expectation is that it should have been in operation. Encourage your officers to think ahead and consider activating the record function before an encounter begins or before arrival at a call.

Many agencies allow a period of time where there is no discipline for failing to use the BWC. This can be a good way to mitigate negative sentiment and let officers develop the thought processes that will make the use of BWC part of their routine.

Data access

Determining who has access to video evidence – and under what circumstances – is complex. In terms of public and media requests for BWC video, state and local laws may dictate a specific procedure. Accordingly, agencies should work collaboratively with their legal counsel.

Access considerations go well beyond public or media requests. What about using video for training purposes or performance review? Video can prove invaluable in building skills, especially during initial field training. However, if BWC video is used as an ongoing performance evaluation tool, labor representatives will likely express concern that the nature of police work is such that close monitoring of a targeted individual could result in unwarranted discipline.

Officers who feel like they're continually being subjected to critical review often claim a higher level of device malfunction or experience increased operator error. Open and candid dialogue accompanied by clear expectations and intent will go a long way to ensuring a successful program.

Given the ease of posting videos to the Internet, agencies should specifically prohibit personnel from accessing videos for their own use and from sharing, selling, distributing, or posting videos online. This is a situation where a single incident could result in loss of public trust and possibly compromise an investigation. Policy should clearly state the prohibition and the certainty of sanction.

Data retention

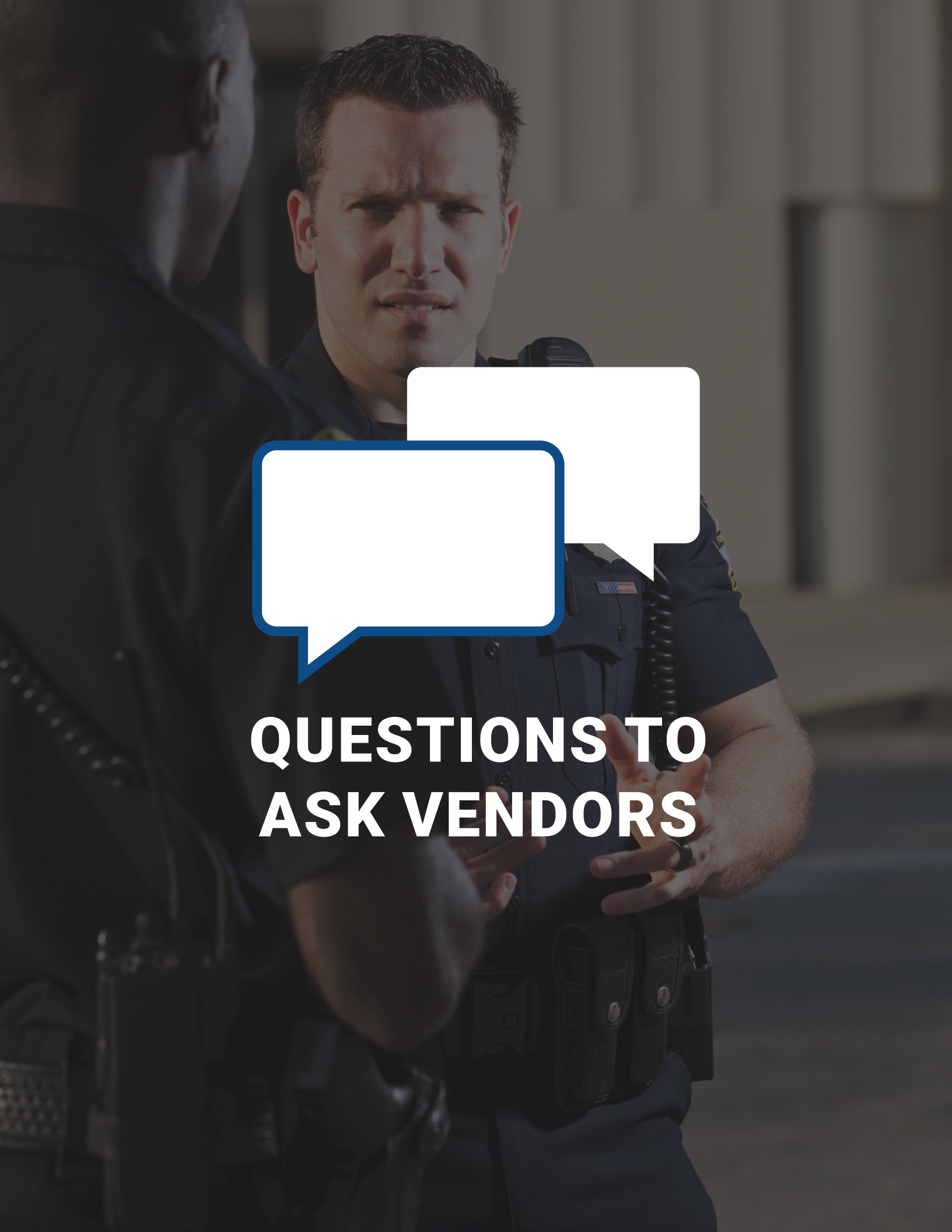
The process to retain BWC data requires a combination of due diligence, planning and strategic consideration. Police departments need to determine if there are existing laws, regulations or ordinances that may govern or mandate a minimum retention period for digital media evidence. Even the word “evidence” is a key consideration. Keep in mind that there is likely a difference between retaining BWC recordings that are evidence in a criminal investigation and BWC recordings of a pedestrian stop where no arrest has been made. These are the types of distinctions that need to be discussed, decisions made and clear direction given to those responsible for retaining the files.

If using in-house storage, you’ll need to provision accordingly and provide for adequate backup. Video takes a lot of space. It goes without saying that the longer you keep it, the more storage you will need.

If you have an existing in-car video system, do not assume you can simply double your storage needs. Most departments find that BWCs result in a much greater volume of recorded data.

Think strategically when you make decisions regarding retention. How best can your system meet the needs of your agency in terms of evidence, public interaction and training? And what will be the corresponding staffing impacts or benefits?

For instance, if you establish in your policy that video of an evidentiary nature is not to be released and kept for the life of the case while other non-evidentiary video is to be deleted after 30 or 60 days, you will be dealing with fewer requests for public or media disclosure. Don’t forget, it’s important that your retention schema complies with any legislatively imposed requirements. Set a reasonable and appropriate retention period based on legal requirements in your jurisdiction, operational and investigative needs, data storage capabilities along with related costs and a reasonable balance of the previous areas considering community expectations.



QUESTIONS TO ASK VENDORS

In order to make the most well-informed purchasing decisions, command staff must understand how the different cameras operate, what options are out there and how they plan to use the technology.

A vendor's website, see our directory in this guide, is a great place to start your research and narrow your choices. Review the technical specifications and testimonials from satisfied clients. Visit BWC companies at tradeshows and ask specific questions.

As the procurement process advances, ask your top vendor choices to visit your department. An in-person visit is an opportunity to involve other decision-makers and to get more questions answered.

For agencies that adopted BWCs and are looking to either upgrade to a new model from the same vendor or a contract with a different vendor, the questions below will help guide the decision. It is important to make this decision based on the agency's unique business requirements and needs. Similar to upgrading to a new CAD or RMS, several discussions need to take place regarding the migration and preservation of the agency's existing data into a new solution.

Here are some suggested questions to ask body-worn camera vendors during the purchasing process:

- What is the process for customer support?
- Who will be your primary point of contact after procurement? When can you meet them?
- What is the BWC performance (video and audio) like during rain? Snow? High winds? Night-time?
- What is the length of time for pre-event recording? Does pre-event recording include audio?
- What is the battery runtime?
- How long is the recording time?
- What is the low-light capability?
- Is there an LCD display?
- What is the lux rating (the minimum amount of light that produces an acceptable image during normal camera operation, not taking into account any night mode feature)?
- How frequently will we need to upgrade devices, batteries, chargers, etc.?
- How much are replacement parts that are not covered by warranty?
- What are the BWC mounting options (e.g. hat, collar, glasses, shoulder, body)?
- How much is data storage and management?
- What is the disaster recovery plan for the data? Is that included in the price of the data storage and management?
- How is data retrieved?

- Is your cloud service FBI CJIS compliant?
- What is the camera resolution?
- What is the field (point) of view (the surrounding area that the camera can monitor)?
- What is the frame rate (or recording speed)?
- What is the process for redacting any data? Is the process automated or semi-automated? Or will we need a technician to manually redact data?
- Does the BWC have a GPS coordinate feature?
- What is the warranty?
- Does your company offer a buyback program for used equipment as part of a replacement or upgrade?
- Explain how this BWC solution will be able to integrate with FirstNet. What is the cost?
- Explain how this BWC solution can integrate with the department's existing investigation software. What is the cost?
- Explain how this BWC solution can integrate with the department's evidence management software. What is the cost?
- Our agency previously deployed BWCs, what specific steps do we need to take to migrate to a new BWC model or solution?
    1. How will the data be migrated to the new software solution?
    2. How long will it take?
    3. How much will it cost?
    4. Should we maintain two databases?

Your department is sure to have other important questions. Tell the vendor which questions you'd like answered in writing and then forward those responses to the people involved in the procurement process.

BODY-WORN CAMERAS
COMPANY DIRECTORY

10-8 VIDEO
DIGITAL EVIDENCE SOLUTIONS

LENSLOCK

AXON

MOTOROLA SOLUTIONS

BODYWORN™

PATROLEYES®

Digital·Ally®

reveal

Getac
Video Solutions

SAFE FLEET
Driving Safety Forward™

FRONTLINE
PUBLIC SAFETY SOLUTIONS

WOLFCOM

KUSTOM SIGNALS, INC.®

VERITONE®


POLICE1
Police1 has the latest law enforcement news, expert how-to articles, industry analysis and police product updates.
POLICE1 BODY WORN CAMERAS
police1.com/police-products/body-cameras
LEXIPOL