OAKLAND POLICE DEPARTMENT

Surveillance Impact Report: Body-Worn Cameras

A. **Description:** *Information describing Body Worn Cameras (BWC) and how they work, including product descriptions and manuals from manufacturers.*

The Body Worn Camera (BWC) is a durable video camera meant to attach to a police officer's uniform (see ***Attachment A for Axon Body 3 Camera User Manual***). The BWC has an "on" and "off" button to allow personnel to record only during authorized and required uses. OPD BWC policy dictates that officers are to wear the BWCs on the front of their uniform or uniform equipment, as the primary recording location, to facilitate recording. The BWC may be temporarily moved from the primary location to facilitate recording in furtherance of a police objective. Upon completion of the objective, the BWC shall be returned to the primary recording location as soon as practical.

The BWC records video footage directly onto the solid-state internal storage unit when in recording "on" function. The BWC contains a solid-state computer storage unit capable of storing digital video files.

Axon has developed firearm holsters[1] that can activate BWCs when firearms are unholstered, even if an officer does not activate his/her BWC; this technology is useful, as situations where an officer must access his/her firearm may not leave time to also activate a BWC. Similarly, Axon also now provides "Axon Signal Video[2]," which is a system that connects fleet vehicles with the BWCs. OPD can configure the system so that triggers such as a vehicle siren will activate the BWC – whether or not an officer manually activates their BWC. These systems help officers focus on critical events and ensure greater compliance with BWC activation policies.

The Independent Monitor[3] has identified on-time activations of BWCs as critical to complying with the Federal Negotiated Settlement Agreement (NSA)[4] related to use-of-force tasks.

The new Axon proposal also utilizes "Evidence.com," Axon's secure cloud-based video storage system. Evidence.com is fully compliant with the Criminal Justice Information Services (CJIS) security standard. The system manages all digital evidence in a single location, including a much more efficient video analysis and secure sharing system – which will save the OPD hundreds if not thousands of hours annually of staff time. Currently, staff need to download footage to a DVD for each case that is charged by a District Attorney(DA)'s Office (sometimes this current process requires overtime for urgent cases). Evidence.com allows OPD to share a

[1] https://www.axon.com/products/axon-signal-sidearm

[2] https://global.axon.com/products/signal-vehicle

[3] https://www.oaklandca.gov/resources/opd-independent-monitoring-team-imt-monthly-reports-2

[4] More information about the NSA can be found here: https://www.oaklandca.gov/resources/oakland-police-negotiated-settlement-agreement-nsa-reports. An NSA Status Update Report is scheduled to the September 14, 2021 Public Safety Committee

link to specific footage with the District Attorney and Public Defender, or private attorney for the case. This streamlined internet-based data sharing system will result in a significant staff-time savings, which will allow staff to focus on other important projects. Other highlights of Evidence.com include:

- Transitioning of OPDs 10+ years of existing BWC data to a new platform (OPD needs to maintain its current data and integrate with a new platform for seamless search across past and future audio/video data. OPD has approximately 500 terabytes of existing audio video data from its use of BWCs – on both on-premises servers as well as with VIEVU-cloud BWC data storage. The Axon contract will allow OPD to migrate all this data onto the Evidence.com platform to have a continuous storage of all data on one platform.
- New OPD BWC audio/video footage storage.
- 3rd party evidence – in the case where OPD needs to add other video sources to a case file (e.g., video from community members or video from a business' security cameras).
- Automated, advanced redaction and object tracking – this advanced feature is important for the efficiency of staff time, saving personnel from more manual processes.
- Integration and auto-tagging with OPD's computer-aided dispatch (CAD) and Records Management System (RMS) to ensure video is properly categorized and retained. Automated tagging of video to assist officers when they must annotate BWC video after events where the BWC video was created.
- Direct link connection to the Alameda County District Attorney's Office – makes evidence sharing for prosecution cases much more efficient, saving personnel time (Alameda County District Attorney's Office personnel share relevant BWC footage and other evidence with a defendant's counsel pursuant to law and their policy).

B. Purpose: *How OPD intends to use BWC Technology*

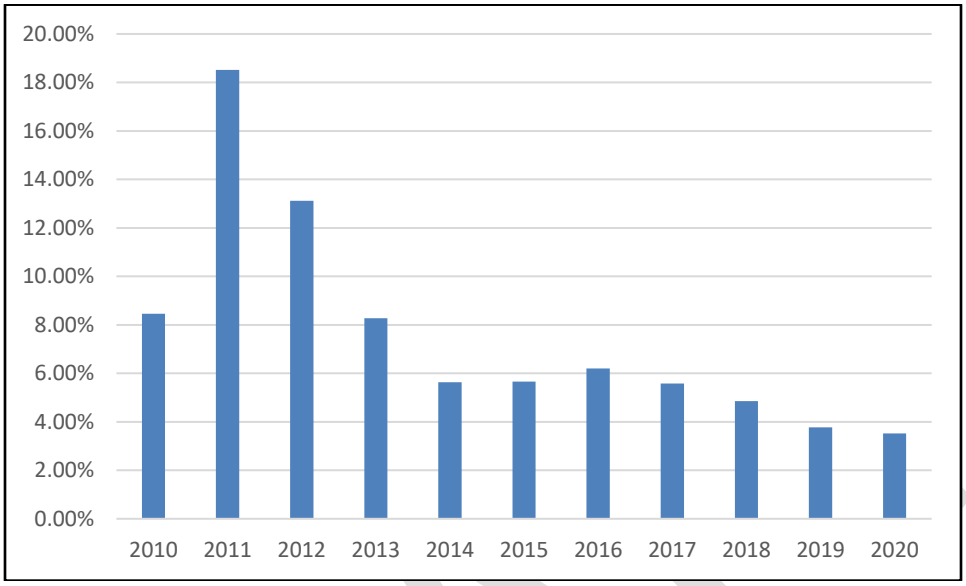
BWCs are used nationwide to increase public trust, transparency, and accountability for law enforcement. The use of BWCs allows OPD officers to document interactions with the public as officers conduct all manner of policing operations. They allow officers to record all activity occurring during police interactions so that a record of events is maintained by the Department. BWCs also create evidence that is useful in examining police conduct and policing protocols. BWC video is used as evidence in internal and criminal investigations. OPD continues to work with Stanford University in leading the country by using BWC video as a training tool, leading to groundbreaking research in police-community interactions.

BWCs offer the potential to increase accountability, reduce complaints, and increase trust between the police and the public. OPD has been a national leader in the evolution of BWC use among police agencies over the past ten plus years. The City of Oakland has garnered national attention for OPDs model program.

BWCs offer the potential for increased accountability and community trust through better transparency, corroborating of evidence, and training opportunities to advance professionalism among law enforcement personnel. The use of BWCs has also increased the percentage of community complaints with resolutions. ***Figure 1*** below

illustrates the decrease in "Not Sustained" findings in community complaints between 2010-2020.

Figure 1: "Not Sustained" Findings from OPD Community Complaints – 2010-2020



OPD's Internal Affairs Division (IAD) investigates all complaints received from the public. Complaints can relate to several categories of policing (e.g., observed conduct towards others, performance of duty, or officer demeanor or conduct). Following an investigation, the findings are as follows:

- Sustained: The investigation disclosed sufficient evidence to determine that the alleged conduct did occur and was in violation of law and/or Oakland Police Department rules, regulations, or policies.
- Exonerated: The investigation disclosed sufficient evidence to determine that the alleged conduct did occur, but was in accord with law and with all Oakland Police Department rules, regulations, or policies.
- Unfounded: The investigation disclosed sufficient evidence to determine that the alleged conduct did not occur. This finding also applies when individuals named in the complaint were not involved in the alleged act.
- Not Sustained: The investigation did not disclose sufficient evidence to determine whether or not the alleged conduct occurred.

C. Location: *The Locations and situations in which BWC Technology may be deployed or utilized.*

Officers may use BWCs anywhere where officers have jurisdiction to operate as sworn officers; however, there are specific prohibitions that preclude officers from using the cameras in certain situations. DGO I-15, part A.3 "Specific Prohibitions" explains that:

Members shall not intentionally use the BWC recording functions to record any personal conversation of, or between, another member without the recorded member's knowledge.

Members shall not intentionally use the BWC to record at Department facilities where a reasonable expectation of privacy exists (e.g., bathrooms, locker rooms, showers) unless there is a legal right to record and a Departmental requirement to record.

D. Privacy Impact: *How is the BWC Surveillance Use Policy Adequate in Protecting Civil Rights and Liberties and whether BWCs are used or deployed, intentionally or inadvertently, in a manner that is discriminatory, viewpoint-based, or biased via algorithm.*

BWC technology provides video and audio documentation of policing activity in addition to the recollection and oral and written statements of officers, victims, and witnesses. BWCs provide OPD with an important tool to promote personnel accountability as well as policing transparency. Many community members support BWC usage because of the common understanding that the accountability derived from BWC-use promotes high quality procedurally just policing.

OPD recognizes that the use of BWC technology can raise privacy concerns, especially regarding the retention of video files, the fact that an accountability tool also captures members of the public during their everyday lives, and the uses of the footage by the Department and City. For example, there is concern that the use of BWC technology can capture people at their most vulnerable (such as after having been a witness to a violent crime) or that it may capture intimate parts of their personal lives (such as when officers respond to a residence for a call of a domestic violence incident). People also may have concerns about being recorded while peacefully gathering to assemble and/or legally protest political activity.

OPD Department General Order (DGO) I-15: Body Worn Camera, as explained in the Mitigation (Section 5 below) details how authorized personnel may only use BWC technology during certain conditions. DGO 1-15 also describes how BWCs will not be used during certain conditions so as to support the privacy of individuals during certain conditions (e.g. taking testimony from sexual assault victims). Furthermore, OPD policy requires that officers annotate each video file at the end of their work shift, so officers must justify their activity in which a video file was generated. Additionally, a log file is created whenever authorized personnel log into the BWC PVMS. The “need to know” access requirement (in Section E.5 “Prohibited Actions”) for viewing files, the required video annotations, and the log files generated by viewing BWC files creates a multi-layered system to guard against the unauthorized access to video evidence.

E. Mitigations: *Specific, affirmative technical and procedural measures that will be implemented to safeguard the public from each of the impacts.*

OPD BWC policy provides several mitigations which limit the use of this audio and video technology. Firstly, OPD Department General Order (DGO) I-15: Body Worn Camera Program follows many of the recommendations set forth in California Penal Code 832.18, Best Practices on body-worn cameras worn by Peace Officers. Section A of the policy (“Purpose of the Technology”) also provides clarity and direction for when BWCs can or cannot be used, or for when officer discretion is allowed. For example, BWC usage is required per policy during detentions and arrests; policy requires that BWCs be deactivated during used to record statements from child abuse or sexual assault victims.

DGO I-15 explains that all BWC files are the property of the Oakland Police Department, and that the unauthorized use, duplication, editing, and/or distribution of BWC files is prohibited. Officers are assigned particular BWCs that each have serial numbers and upload video files that are automatically tagged to the assigned officer.

The OPD Information Technology Unit is designated as the Custodian of Record for all BWC data files. Officers cannot modify or delete video footage recorded from their BWCs, and once the BWCs are docked (at the end of a shift) the video is automatically uploaded to the video management system. Video footage is only accessible on a need-to-know basis per OPD policy. Personnel are not allowed to remove, dismantle or tamper with any hardware/software component or part of the BWC. OPD's BWC platform always requires double-layer authentication login (authorized personnel receive an email or text message code which must be entered as part of the login). Additionally, the BWC platform utilizes software that creates cryptographic files which would leave an evidence trail of any type of alteration of the video file.

OPD BWC Policy requires that all sergeants audit BWC videos involving certain arrests and incidents involving Use of Force, and they are required to assess performance and policy compliance during these reviews.

DGO I-15 D-1 articulates that members of OPD are not allowed to intentionally use the BWC recording functions to record any personal conversation of, or between another member without the recorded member's knowledge. This section also explains that personnel may not intentionally use the BWC to record at Department facilities where a reasonable expectation of privacy exists (e.g., bathrooms, locker rooms, showers) unless there is a legal right to record and a Departmental requirement to record. These rules serve to support the privacy of OPD members.

DGO I-15 Section H-2 explains that OPD will produce an annual report for the PAC and the Public Safety Committee. The annual report will provide numerous metrics related to the use of BWCs:

Protocols for the use of BWCs during certain interviews with victims and witnesses provides another policy mitigation to ensure public privacy. DGO 15 provides that officers shall not use BWCs during contact with victims and witnesses to possible sexual assault, domestic violence and/or child abuse.

OPD's BWC data retention policy, noted in DGO I.15.F.2 "Data Retention and Scheduled Deletion of Files" is as follows: "BWC files shall be retained for a period of two years unless it is required for:

1. A criminal investigation;
2. An administrative investigation;
3. Research;
4. Civil litigation;
5. Training; and/or
6. Review and possible release pursuant to Public Records Request

State law also provides mitigations in support of BWC and policing transparency. SB-1421 (Police Officer Release of Records), enacted in 2018, requires the public release of BWC data related to the following:

- A report, investigation or findings of an incident involving the discharge of a firearm at a person by a peace officer or a custodial office
- A report, investigation or findings of an incident in which the use of force by a peace officer or a custodial officer against a person results in death or great bodily injury.
- Records relating to an incident in which a sustained finding was made by any law enforcement agency or oversight agency that a peace officer or custodial officer engaged in sexual assault involving a member of the public; and
- Records relating to an incident in which a sustained finding was made by any law enforcement agency or oversight agency of dishonesty by a peace officer or custodial officer directly relating to the reporting, investigation, or prosecution of a crime, or directly relating to the reporting of, or investigation of misconduct by, another peace officer or custodial officer, including but not limited to, any sustained finding of perjury, false statements, filing false reports, destruction of evidence or falsifying or concealing of evidence.

This law also restricts BWC data redaction to the following limited cases:

- Personal information; and
- Information to preserve the anonymity of complainants and witnesses.

OPD mitigates against improper public release of video footage with protocols outlined in DGO 15; BWC files are reviewed and released in accordance with federal, state, local statutes, and Departmental General Order M-9.1 (PUBLIC RECORDS ACCESS. However, OPD will also comply with the newly enacted Assembly Bill 749 (signed by Governor Edmund G. Brown, Jr. on September 30, 2018). This new law mandates that audio and visual recordings of "critical incidents" resulting in either the discharge of a firearm by law enforcement or in death or great bodily injury to a person from the UOF by a police officer to be made publicly available under the Public Records Act within 45 days of the incident, with certain exceptions.

F. **Data Types and Sources*****:*** *A list of all types and sources of data to be collected, analyzed, or processed by the surveillance technology, including "open source" data, scores, reports, logic or algorithm used, and any additional information derived therefrom.*

BWC data is composed of recordings of live video and sound footage of incidents where personnel activate there BWCs. The audio/video recordings utilize standard data file formats (e.g., mp4).

BWCs record digital video files. BWC video may contain images and voice recordings of members of the public who have been stopped by officers during regular police operations; videos may also contain images and voice recordings of individuals such as witnesses, victims of crimes and/or individuals being asked to provide information to officers related to criminal activity or suspected criminal activity. Videos may also contain information and voice recordings related to any activity where OPD personnel are required to activate BWCs as described above in Section #2 "Proposed Purpose."

G. **Data Security:** *Information about the steps that will be taken to ensure that adequate*

security measures are used to safeguard the data collected or generated by the technology from unauthorized access or disclosure.

The current and planned future BWCs and cloud platform data mange met system allow for controls for how files are uploaded and archived. The current VIEVU system provides restriction controls that limit BWC video file access to only authorized OPD personnel. OPD historically used an "on-premises" server back-up system to maintain all BWC video files; OPD has since switched to a cloud-based system with VIEVU. OPD will switch to the Axon evidence.com cloud storage solution.

Evidence.com is a modern BWC data management platform. The system offers many data security protocols such as:

- **Authentication**
  - Customizable password length and complex password requirements
  - Customizable failed login limit and lockout duration
  - Enforced session timeout settings
  - Mandatory challenge questions when authenticating from new locations
  - Multi-factor authentication options for user login and prior to administrative actions (one time code via SMS or phone call-back)
  - Restrict access to defined IP ranges (limit access to approved office locations)
- **Authorization and Permissions**
  - Granular role-based permission management
  - Application permission management (for example, allow specific users to use the web-based interface, but not a mobile application)
  - Integration with directory services for streamlined and secure user management
- **Auditing and User Reporting and Management**
  - Detailed, tamper-proof administrator and user activity logging
  - Intuitive administration web portal to manage users, permissions and roles
- **Secure Sharing**
  - Intra-agency, inter-agency and external evidence sharing without data transfer, data duplication, physical media or email attachments
  - Detailed chain-of-custody logging when sharing
  - Revoke access to previously shared content
  - Prevent a recipient of shared content from downloading or re-sharing evidence
- **Encryption**
  - Data Encryption in Transit:
    - FIPS 140-2 validated: Axon Cryptographic Module (cert #2878)
    - TLS 1.2 implementation with 256 bit connection, RSA 2048 bit key, Perfect Forward Secrecy
  - Evidence Data Encryption at Rest:
    - CJIS Compliant, NSA Suite B 256 bit AES encryption

These policies help to ensure that OPD BWC video footage remains well secured on

BWCs and OPD and/or Axon servers; all video footage is the property of OPD and OPD does not share video footage with other organizations. Axon BWCs encrypt video data both within the BWC as well as in the cloud-based storage system for data security.

H. **Fiscal Cost:** *The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding.*

The table below outlines the annual combined cost for the BWCs as well as Axon electronic control weapons (ECW), and evidence.com storage system each year ($1,604,550) as well as the separate annual cost for the interview room cameras and integration with evidence.com ($33,955). A significant part of this contract is for the ECWs; however, Axon is offering the combined products as a package price. While staff cannot specifically disentangle only the BWC costs, especially as the evidence.com cloud storage system serves for both the BWC data needs as well as the ECW and interview room camera data storage needs, the package does include discounts that make obtaining both of these necessary technologies more affordable for the City.

Year	BWC, ECW, and Evidence.com
2022	$1,604,550
2023	$1,604,550
2024	$1,604,550
2025	$1,604,550
2026	$1,604,550
Total	**$8,022,750**

I. **Third Party Dependence:** *Whether use or maintenance of BWC technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis.*

OPD is reliant upon the BWC vendor for data storage and management. OPD currently uses VIEVU brand BWCs and is reliant upon the Axon-purchased VIEVU data cloud storage system, for BWC maintenance and data storage. Historically, police agencies could opt to store BWC data on standard computer servers. However, contemporary platforms provide video character tagging and search analysis tools that cannot be easily purchased and maintained as stand-alone products. Axon has increasingly become a leader in BWC and video evidence, as well as with their ECW system technology. Axon was a bidder in OPD's 2016 BWC Request for Proposal process. Previously, only Axon and VIEVU could provide the integrated BWC and integrated video evidence storage systems needed by large modern police agencies. In 2018, Axon purchased VIEVU from Safariland, its former corporate owner. Axon is now the global leader in BWC technology and currently the only company capable of providing an integrated BWC and easily searchable video evidence storage system (OPD already uses evidence.com for ECW taser use data management). Furthermore, evidence.com also provides data-secure procedures for data sharing with other agencies (e.g., the District Attorney's

Office) as described in Section A above. These technologies promise to provide much greater efficiency to OPD and free staff from many hours of manual data tagging, downloading, and data sharing tasks. Therefore, OPD is recommending a new contract for Axon for BWC, tasers, and the BWC / taser evidence.com data management system.

J. **Alternatives Considered:** *A summary of all alternative methods considered in-lieu of BWC, including the costs and benefits associated with each alternative and an explanation of the reasons why each alternative is inadequate*

OPD officers and investigators rely primarily on traditional policing techniques to gather evidence related to criminal investigations such as speaking to witnesses and suspects, gathering information from observations, and using standard data aggregation systems. These methods will continue to be employed as primary investigative tools that will be supplemented by use of BWCs to document police activity.

BWC technology provides video and audio documentation of policing activity in addition to the oral and written statements of officers, victims, and witnesses. Alternatives to the use of BWCs would be vehicle-based cameras, audio recording only, and/or not utilizing BWCs, among other possible policy and technology changes. Another alternative would be for officers to rely more upon their own memory and simply not have a recording of numerous types of police encounters. Staff does not recommend such an alternative as the oversight and accountability provided by BWC usage would be lost.

However, OPD sees the use of BWCs as an integral strategy to ensuring that officers use procedurally just strategies and to ensure compliance with how officers interact with members of the public. The video and audio files generated using BWCs provide an important record of police encounters which can be reviewed against statements made by officers and members of the public. OPD's BWC usage provides a layer of accountability and transparency for OPD as well as for all Oakland residents and visitors.

K. **Track Record of Other Entities:** *A summary of the experience (if any) other entities, especially government entities, have had with the proposed technology, including, if available, quantitative information about the effectiveness of the proposed technology in achieving its stated purpose in other jurisdictions, and any known adverse information about the technology (such as unanticipated costs, failures, or civil rights and civil liberties abuses).*

Scores of police agencies have now adopted BWCs as a tool to promote officer accountability. Many departments have developed their own usage policies which may include standards for required officer use, supervisory review, storage and data retention standards, and internal and public access.

A report for the U.S. Bureau of Justice Administration[5] cites a 2013 Rialto, CA study that showed that the use of BWCs led to a 59 percent decrease in UOF and an 87.5 percent decrease in citizen complaints. Likewise, the Mesa, AZ report noted in "Impact" Section above also points to large decreases in UOF and citizen complaints.

The 2017 Police Body Worn Cameras: A Policy Scorecard[6] provides an analysis of how scores of different police agencies have employed BWCs through the following metrics:

- Is the policy available for the public?
- Limits on officer discretion for when to record;
- Does the policy address personal privacy concerns?
- Are there prohibitions on officer pre-report viewing?
- Is there a specific data-retention policy?
- Policies for tampering with video footage;
- Is footage available to individuals filing complaints?; and
- Are there limits against biometric data analysis?

In 2017, the California Legislature passed AB 1516, which amended the Penal Code to establish "policies and procedures to address issues related to the downloading and storage data recorded by a body-worn camera worn by a peace officer." These were based on best practices, and the law (Penal Code 832.18) states that "When establishing policies and procedures for the implementation and operation of a body-worn camera system, law enforcement agencies, departments, or entities shall consider the following best practices regarding the downloading and storage of body-worn camera data".

During creation of the BWC Use Policy (proposed DGO I-15), OPD did consider each of the legislature's best practice recommendations.

[5] https://www.bja.gov/bwc/pdfs/14-005_Report_BODY_WORN_CAMERAS.pdf - pages 6-8
[6] https://www.bwcscorecard.org/