

21 SEP 17 PM 2:03

APPROVED AS TO FORM AND LEGALITY


CITY ATTORNEY'S OFFICE

OAKLAND CITY COUNCIL

RESOLUTION NO. 88824 C.M.S.

INTRODUCED BY COUNCILMEMBER [IF APPLICABLE]

**RESOLUTION APPROVING THE OAKLAND POLICE DEPARTMENT (OPD)
BODY-WORN CAMERA (BWC) SURVEILLANCE USE POLICY AND
SURVEILLANCE IMPACT REPORT**

WHEREAS, OPD first developed General Order (DGO) I:15 “BWC Program” to set forth Departmental policy and procedures for the BWC system; and

WHEREAS, OPD has adopted BWC technology because of its usefulness in capturing audio/video evidence and enhancing the Department’s ability to conduct criminal investigations, administrative investigations, and review of police procedures and tactics; and

WHEREAS, OPD requires that sworn officers utilize BWCs to document the actions during field operations, and seeks to balance the benefits provided by digital documentation with the privacy rights of individuals who may be recorded during the course of legal and procedurally just public interactions; and

WHEREAS, Oakland’s Surveillance Ordinance No.13489 C.M.S., adopted by the City Council on May 15, 2018 adds Chapter 9.64 to the Oakland Municipal Code (OMC) covering policy areas related to surveillance technology; and

WHEREAS, OMC 9.64.030(1)(C) C requires City Council approval for new and existing surveillance technology; and

WHEREAS, OMC Section 9.64.020(2) requires that prior to seeking City Council approval for existing city surveillance technology under Section 9.64.030, City staff shall submit a surveillance impact report (“Impact Report”) and surveillance use policy (“Use Policy”) to the Privacy Advisory Commission (PAC) for its review at a regularly noticed meeting; and

WHEREAS, OPD staff presented DGO I:15 BWC Program Use Policy and BWC Impact Report to the PAC at their September 2, 2021 meeting; and

WHEREAS, the Use Policy covers several relevant areas required by the Surveillance Ordinance, including the following areas: Technology Description, Authorized Use, Use Restrictions, Data Access, Data Collection and Retention, and Security, Monitoring and Reporting, and System Training; and

WHEREAS, the Impact Report covers the following areas as required by the Surveillance Ordinance: Information describing the system and how it works, Purpose of the technology, Locations where, and situations in which the technology may be used (along with area crime data), Privacy Impact of the technology, Mitigations to prevent privacy impacts, Data Types and Sources, Data Security, Costs, Third Party Dependence, Alternatives Considered, and Track Record of Other Entities; and

WHEREAS, at the September 2, 2021 PAC meeting, after another robust discussion between PAC commissioners and OPD staff, the PAC voted unanimously to recommend that the City Council approve OPD's DGO I-15 BWC Use Policy and BWC Impact Report, with the following amendments: record when requesting that a person consent to a search, change the default 30 second silent buffer where BWCs are continuously recording to a 2-minute buffer, and with audio recording during the buffer (current default is no audio during continuous buffer), add required verbal consent to use BWC when officers take a statement from members of the public, and clarify in the "Training Section" of the Use Policy that training, "for those who are assigned a BWC, and training regarding the process for uploading and downloading BWC data," will be for the BWC Use Policy in particular; therefore be it

RESOLVED: That City Council does hereby approve the OPD BWC Impact Report as provided in *Attachment A* to the report accompanying this resolution; and be it

FURTHER RESOLVED: That City Council does hereby accept but not adopt the OPD DGO I:15 BWC Use Policy as provided in *Attachment B* to the report accompanying this resolution; and be it

FURTHER RESOLVED: That pursuant to OMC Section 9.64.030(2)(B), for the reasons provided herein and in the agenda report and surveillance impact report accompanying this resolution, the City Council finds that the benefits to the community of the surveillance technology outweigh the costs (cost benefit determination), that the proposal will safeguard civil liberties and civil rights, and that, no alternative with a lesser economic cost or impact on civil rights or civil liberties would be as effective; and so authorizes the City Administrator or designee's acquisition and use of BWCs.

IN COUNCIL, OAKLAND, CALIFORNIA, SEP 21 2021

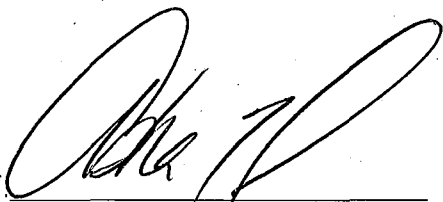
PASSED BY THE FOLLOWING VOTE:

AYES - FIFE, GALLO, KALB, KAPLAN, REID, TAYLOR, THAO AND PRESIDENT FORTUNATO BAS - 8

NOES - 0

ABSENT - 0

ABSTENTION - 0

ATTEST 

ASHA REED
City Clerk and Clerk of the Council
of the City of Oakland, California

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 holsters¹ that can activate BWCs when firearms are unholstered, even if an officer does not activate his/her BWC; this technology is useful in 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 Video²," 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 Monitor³ 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*

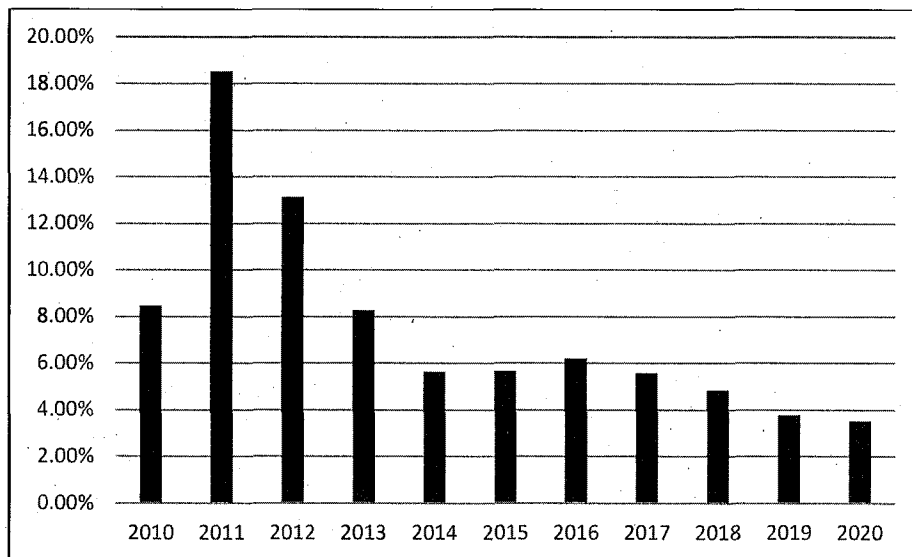
BWCs are used nationwide to increase public trust, transparency, and accountability for law enforcement. The use of BWCs allows OPD officers to document interactions with the public as officers conduct all manner of policing operations. They allow officers to record all activity occurring during police 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 officer
- 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 their 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 management 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 Administration⁵ 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 Scorecard⁶ 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 1-15), 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.bwccscorecard.org/>



I-15: BODY WORN CAMERA PROGRAM

Effective Date: XX MMM YY

Coordinator: Information Technology Unit

OPD strives to use technology that promotes accountability and transparency. OPD uses a Body Worn Camera (BWC) system to document the actions of sworn members during field operations. OPD seeks to balance the benefits provided by digital documentation with the privacy rights of individuals who may be recorded during the course of legal and procedurally just public interactions.

The intent of this policy is to set forth Departmental policy and procedures for the BWC system. OPD has adopted BWC technology because of its usefulness in capturing audio/video evidence and enhancing the Department's ability to conduct criminal investigations, administrative investigations, and review of police procedures and tactics.

A. GENERAL PROVISIONS

A - 1. Assignment of BWCs

All members in an assignment with primarily field-based responsibilities, as determined by the Chief of Police (COP), shall be assigned a BWC for the duration of the assignment. Other members, as determined by the COP, may also be assigned a BWC.

A - 2. General Provisions

The following provisions apply to the BWC program at all times:

1. All members assigned a BWC shall carry and use the BWC in accordance with the provisions of this order.
2. All BWC files are the property of the Oakland Police Department.
3. The OPD Information Technology Unit is designated as the Custodian of Record for all BWC data files.

A - 3. Specific Prohibitions

Members shall follow the expressed prohibitions regarding the BWC system:

1. Unauthorized use, duplication, editing, and/or distribution of BWC files is prohibited.
2. Members shall not delete any BWC file, except as specified in this policy.
3. Members shall not remove, dismantle or tamper with any hardware/software component or part of the BWC.
4. Members are prohibited from wearing or using personally owned video recording devices in place of or in conjunction with an assigned BWC.

5. 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.
6. 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.

B. USE OF BWC BY ASSIGNED USERS

B - 1. BWC Placement

The position of the BWC when activated by OPD members may impact the clarity and sound of video files and could limit the quality of video and audio collected. Members shall position and securely attach the BWC to 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.

B - 2. Function Check and Standby Mode Prior to Shift

Members utilizing a BWC shall test the equipment and place the BWC in stand-by mode so that the camera's buffer function is activated prior to every shift.

If a member's camera is not functional, or breaks during the shift, members shall – absent exigent circumstances – turn in the non-functional camera, notify their supervisor, and be assigned a new camera by a supervisor or authorized user as soon as possible.

B - 3. Battery Maintenance

Members shall ensure their BWC battery is fully charged at the beginning of their shift.

B - 4. Required Activation

Activation is turning the audio and visual recording of the BWC on. Activation saves a 12030 second audio and video-only clip (~~no audio~~) of what the camera captured prior to activation.

Members assigned a BWC shall activate it prior to participating in any of the following circumstances:

1. Contacts with a person to confirm or dispel a suspicion that the person may be involved in criminal activity as a suspect
2. Detentions and arrests

3. Assessment or evaluation for a psychiatric detention pursuant to Welfare and Institutions Code § 5150
4. Engaging in or trailing a vehicle pursuit as defined in DGO J-04, *Pursuit Driving*
5. Serving a search or arrest warrant
6. Conducting any search of a person or property
7. Transporting any detained or arrested person (members working as the prisoner wagon transport officer may deactivate their BWC during transport if they are transporting persons in the separate prisoner wagon compartment).
8. Incidents where a department member is involved in a vehicle collision while utilizing a department vehicle, the member is wearing a BWC, and it is practical and safe to do so.
- 8.9. Requesting that a person consent to a search.

B - 5. Deactivation of the BWC

Once activated pursuant to B-4, members shall not deactivate their BWC until one of the following occurs:

1. Their involvement in the contact, detention, search, or arrest has concluded
2. The contact, detention, or arrest becomes a hospital guard
3. They receive an order from a higher-ranking member
4. They are discussing administrative, tactical, or law enforcement sensitive information away from non-law enforcement personnel
5. They are at a location where they are not likely to have interaction or a chance encounter with the suspect (e.g. outer perimeter post, traffic control post, etc.)
6. They reasonably believe the recording at a hospital may compromise patient confidentiality
7. A pursuit has been terminated and the member performs the required terminating action as specified in DGO J-04 or notifies the Communications Division that they are back in service (909)
8. They are interviewing a prospective informant for the purpose of gathering intelligence. At the conclusion of the interview, the BWC shall be re-activated until no longer required by policy
9. They are meeting with an undercover officer. At the conclusion of the interview, the BWC shall be re-activated until no longer required by policy.

If circumstances arise requiring re-activation members shall re-activate pursuant to B-4, above.

B - 6. When BWC Activation is Not Required

BWC activation is not required under any of the following circumstances:

1. Members taking a report when available information indicates the suspect is not on scene
2. During any meetings with a Confidential Informant as defined in DGO O-04, *Informants*
3. Members on a guard assignment at a police, medical, psychiatric, jail, or detention facility. Members shall assess the circumstances (e.g. suspect's demeanor/actions, spontaneous statements, etc.) of each guard assignment, on a continuing basis, to determine whether to discretionarily activate or de-activate their BWC.

B - 7. Recording Statements with BWC

Members are authorized to use the BWC to record statements in lieu of a written statement. BWC statements shall not be used to record statements from child abuse or sexual assault victims.

Members taking BWC statements shall follow the BWC statement guide set forth in Report Writing Manual S-01.

Members shall request verbal consent to record statements with BWCs, and record the verbal request.

B - 8. BWC Use Documentation

Members are required to document all activations of their BWC, except for tests or accidental recordings. Documentation shall be made in at least one of the following reports, as appropriate:

1. Crime Report
2. Consolidated Arrest Report or Juvenile Record
3. Field Interview Report
4. CAD notes, or
5. Use of Force Report.

Delayed or non-activations of the BWC, when activation was required by policy, shall be documented in the appropriate report and reported to the member's supervisor.

B - 9. Data Upload

Members shall upload BWC data files (videos) at the end of and, if needed, during their shift to ensure storage capacity is not exceeded.

B - 10. Annotation of BWC Files

All members shall annotate BWC data files (videos) daily, or, if not feasible, by the end of the member's next regularly scheduled workday. The following information shall be annotated on every BWC data file:

1. Report number associated with the incident recorded; or
2. Incident number (if there is no report number associated with the incident being recorded)
3. The type of incident (e.g., car stop, use of force, arrest, etc.) using the appropriate drop-down or select field.

If neither report number nor incident number exists, members shall write a brief description of the incident in the "comments" field.

Members are authorized to view their video in order to identify the file for annotation unless otherwise prohibited by policy.

During incidents that require exceptional resources or large-scale activation of Department members (e.g. natural disaster), the incident commander may approve delayed annotation of BWC files except in cases that require an investigative call-out. The incident commander shall document any such orders in the appropriate after-action report.

B - 11. Discretionary Activation and De-Activation

Members may use their own discretion when deciding to activate or deactivate their BWC when not required to activate or prohibited from activation as described above.

C. VIEWING OF BWC FILES

C - 1. User Review of Their Own BWC Files

Members are authorized to review their own BWC recordings to properly identify the data files, refresh their memory regarding an incident, or any other work-related purpose, unless otherwise prohibited by policy.

Personnel viewing any video file shall document the reason for access in the "Comments" field of each video file viewed. The entry shall be made either prior to viewing the video or immediately after viewing the video.

C - 2. When Members are Prohibited from Reviewing BWC Files

1. Members designated as involved in a Level 1 Investigation.
Members who are involved in a Level 1 Investigation, as determined by the BOI Deputy Chief or designee, are prohibited from reviewing their

BWC files until the Level 1 investigator allows the review pursuant to section D-7.

2. Criminal Investigation of a Member.

Personnel who are the subject of a criminal investigation may not view any audio/video recordings related to the incident except upon approval, as specified below, by the CID or IAD Commander.

3. Administrative Investigation of a Member.

Personnel having received notification (Complaint Notification Report [CNR]) from the IAD and who are considered to be a subject or witness officer, may not view any audio/video recordings related to the incident except upon approval, as specified below, by the IAD Commander.

C - 3. Supervisor and Command Viewing of Subordinate BWC Files

Supervisors and commanders are authorized to review their own BWC video files, all video files of their subordinates and, as necessary to complete required duties, any associated video files of non-subordinate members, unless otherwise prohibited by policy.

C - 4. Review of BWC Files by Criminal Investigation Personnel

Personnel assigned to CID or other investigatory units are authorized to view any BWC video file associated to their active investigations, unless otherwise prohibited by policy.

Investigators conducting criminal investigations shall:

1. Advise the Project Administrator (see **G-1**) or a System Administrator (see **G-2**) to restrict public disclosure of the BWC file in criminal investigations, as necessary;
2. Review the file to determine whether the BWC file is of evidentiary value and process it in accordance with established protocols; and
3. Notify the System Administrator to remove the access restriction when the criminal investigation is closed.

C - 5. Use of BWC Files for Training

Training staff is authorized to view BWC files regarding incidents which may serve as learning or teaching tool. A BWC file may be utilized as a training tool for individuals, specific units, or the Department as a whole. A recommendation to utilize a BWC file for such purpose may come from any source.

A person recommending utilizing a BWC file for training purposes shall submit the recommendation through the chain-of-command to the Training Section Commander.

The Training Section Commander shall review the recommendation and determine how best to utilize the BWC file considering the identity of the person(s) involved, sensitivity of the incident, and the benefit of utilizing the file versus other means.

D. ACCOUNTABILITY AND INTERNAL INVESTIGATION REVIEWS

D - 1. Review Considerations for all Supervisor or Commander Reviews of BWC

As set forth in section D of this policy, supervisors and commanders have the ability to review their subordinates BWC recordings during the course of normal supervision, and have the obligation to review certain recordings pertaining to specific events. In addition to required assessments during other reviews, all BWC recording reviews by supervisors and commanders shall follow these guidelines:

1. Supervisor and command review of subordinate BWC recordings shall include an assessment of:
 - a. Officer performance and training needs;
 - b. Policy Compliance, including compliance with the provisions of this policy; and
 - c. Consistency between written reports and video files.
2. When a member does not activate or de-activate their BWC as required by policy, supervisors and commanders shall determine if the delayed or non-activation was reasonable, based upon the circumstances.

If the supervisor or commander determines that the delay or non-activation was reasonable, they shall document the justification in the appropriate report. If no report is generated, this shall be documented in an SNF for the officer. The supervisor's commander shall be advised, and their name noted in the SNF.
3. Supervisors, commanders, and managers who discover Class II misconduct during the review of BWC video, that does not indicate a pattern of misconduct, may address the Class II misconduct through non-disciplinary corrective action. Supervisors shall, at a minimum, document any Class II violation of this policy in an SNF for the officer.

D - 2. Supervisor Random Accountability Review

In addition to other required video recording reviews, all supervisors shall conduct a random review of at least one BWC recording for each of their

subordinates on a monthly basis. Supervisors shall ensure that each selected recording has a minimum length of ten (10) minutes.

D - 3. Supervisor Specified Incident Review

In addition to other required video recording reviews, all supervisors shall:

1. Conduct a review of relevant BWC recordings of the arresting officer(s) involving:
 - a. 69 PC (Resist an Officer)
 - b. 148 PC (Resist, Delay, or Obstruct and Officer); and
 - c. 243(b) or (c) PC (Battery on a Peace/Police Officer)

For the above arrests/incidents, supervisors shall at minimum review the BWC recordings of the arresting officer(s), starting from the officer(s) initial interaction with the subject of the arrest.

During incidents involving multiple officers, and absent a reported Use of Force, supervisors are *not* required to view all of the involved officer's BWC recordings where doing so would be redundant.

D - 4. Force Investigation Review (Level 2-4 UOF)

When approving or investigating a Use of Force (UOF) categorized under Level 2 or Level 3, supervisors shall conduct a review of the pertinent section of BWC recordings for all members who are witnesses to or involved in the UOF.

When approving or investigating a UOF categorized under Level 4, supervisors shall conduct a review of the pertinent section of BWC recordings of the specific member(s) who used force, for the purpose of determining if the Use of Force was in compliance with department policy.

BWC related to a documented Level 4 Type 32 Use of Force may require different review than other force types; such review shall be delineated by Special Order, with the specific order referenced below.

D - 5. Vehicle Pursuit Investigation Review

When approving or investigating a Vehicle Pursuit, Supervisors shall conduct a review of the pertinent section of BWC recordings for all members who were involved in the pursuit as the primary or secondary unit (at any point during the pursuit). This review shall include the BWC recordings of members from the beginning their involvement in the pursuit, until the termination of their involvement in the pursuit.

For involved members who were riding together in the same vehicle during the pursuit, the approving or investigating supervisor may review only one member's BWC footage if the footage is redundant.

D - 6. Division-Level Investigation Review

When completing a division-level investigation, the assigned investigator shall at minimum review BWC footage that is pertinent to the investigation and which provides evidentiary value or assists in completing the investigation.

D - 7. Level 1 Investigation Review

In the event of a Level 1 investigation, all BWC recordings shall be uploaded to the server as soon as practical.

An involved or witness member's BWC shall be taken from them and secured by a supervisor, commander or appropriate investigator, as necessary. The recordings shall be uploaded by personnel designated by the CID investigator.

After the recordings are uploaded, the CID investigator or designee shall turn the BWC in to property until the CID and IAD Commander determine it may be released back to the member. The CID investigator shall ensure the chain of custody is documented in their report.

All personnel uploading secured BWCs shall document that fact in their report and the "Comment" field of each video file they uploaded.

Personnel uploading secured BWC video files shall not view the files unless authorized by the CID investigator.

No personnel involved in or a witness to the incident may view any audio/video recordings prior to being interviewed by the appropriate investigative unit and receiving command approval.

Once a member's report(s) has been submitted and approved and/or the member has been interviewed by the appropriate investigator, the investigator may show the member his/her audio/video. This will occur prior to the conclusion of the interview process.

Personnel will be given the opportunity to provide additional information to supplement their statement and may be asked additional questions by the investigators.

D - 8. Command Review

Following the investigation and approval of a Level 2 or Level 3 Use of Force by a supervisor, both the investigator's first level commander and the division commander shall conduct a review of the pertinent section of BWC recordings for all members who are witnesses to or involved in the UOF.

D - 9. Auditing and Other Review

OIG staff (when conducting audits), supervisors, commanders, active FTOs and the FTO Coordinator are authorized to view BWC files to assist with the conduct of audits and inspections (OIG) or evaluate the performance of members subordinate or trainee members, unless otherwise prohibited by policy.

E. COPYING OF BWC FILES

E - 1. Court and Judicial Proceeding BWC File Copies

Personnel requiring a copy of BWC audio/video file(s) for court (e.g. for Traffic court, or a proceeding in a different county) shall contact their first line supervisor or their designated System Administrator (for non-patrol assignments). If the first line supervisor is unavailable, personnel shall contact any System Administrator. Any BWC copies not entered into evidence shall be returned to the first line supervisor or a System Administrator for destruction.

CID and other investigative personnel taking a case to the District Attorney for charging are responsible for obtaining copies of, and/or using the File Management System's secure sharing capability to share, all applicable BWC files for presentation to the DA.

1. Prior to copying the BWC video file, members authorized to make copies shall document the reason for making the copy and the name of the person receiving the copy in the "Comments" field of each video file copied. If applicable, the name entry shall also include the person's rank and serial number.
2. The person receiving the copy shall maintain the copy in a secure location until it is needed for court or custody is transferred to another person. Additionally, they shall document, as soon as practical, the name and/or position of the person receiving the copy in the "Comments" field of each video file.
3. The documentation of the chain of custody and responsibility to secure the copy shall transfer to the person receiving the copy until:
 - a. The copy is received by non-Department personnel (e.g. District Attorney, City Attorney, Court Clerk, etc.);
 - b. The copy is admitted into evidence; or
 - c. The copy is returned to a system administrator for destruction.

E - 2. Public Records Requests for BWC File Copies

Public Records requests shall be accepted and processed, in accordance with the provisions of federal, state, local statutes and DGO M-09.1, Public Records Access, and forwarded to the Project Administrator.

Copies of BWC video files for release pursuant to a public records request, or as authorized by the Chief of Police or designee, shall be redacted as required by prevailing law and Department procedures prior to release.

E - 3. Copying BWC Recordings for Reasons other than Court

Members may make copies of BWC recordings to facilitate their review and accountability authorities and responsibilities, as set forth in Sections C and D of this order.

Prior to copying the BWC video file, members authorized to make copies shall document the reason for making the copy and the name of the person receiving the copy in the "Comments" field of each video file copied. If applicable, the name entry shall also include the person's rank and serial number.

Copies of BWC video files for internal use shall be maintained in the appropriate case file or a secure location. When the copy is no longer needed, it shall be returned to a system administrator for destruction. The system administrator shall make an entry in the "Comments" field of the video file that the copy was destroyed.

E - 4. Prohibited Copies and File Sharing

All personnel are prohibited from the following:

1. Making unauthorized copies of an original or copied BWC video file;
2. Giving or showing copies of BWC video files to anyone without a lawful right to know and need to know, unless authorized by the Chief of Police; and
3. Posting or having another person post a copied BWC video file on any social media site or public site, unless authorized by the Chief of Police or designee.

F. DELETION OF BWC FILES AND AUDIT LOGS

F - 1. Removal Requests for Accidental Recordings

In the event of an unintended or inappropriate activation of the BWC where the resulting recording is of no investigative or evidentiary value, the respective member may request that the BWC file be deleted by submitting an

email request to their first level commander with sufficient information to locate the BWC file. The first level commander shall approve or deny the request.

Approved requests shall be submitted to the Project Administrator at BWC@oaklandca.gov and the Project Administrator or designee will delete the accidental recordings.

F - 2. Data Retention and Scheduled Deletion of Files

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.

BWC files that are not flagged for retention for any of the above reasons will be deleted by the File Management System's data retention processes upon expiration of the set retention period, which are set and maintained by the Project Administrator or designee.

F - 3. Access and Deletion Logs

Audit logs of access, review, copying, and deletion of BWC files shall be retained permanently.

G. ADMINISTRATIVE INFORMATION

G - 1. Project Administrator

The Project Administrator is the commander over the Information Technology unit unless otherwise designated by the Chief of Police. The Project Administrator has oversight responsibilities that include, but are not limited to, the following:

1. Document and track malfunctions and equipment failures;
2. Policy and procedure review and evaluation;
3. Ensure BWC files are secured and retained for the appropriate time period. Such security shall include FBI Criminal Justice Information Services (CJIS) compliant safeguards that protect information from unauthorized access, including encryption and access control mechanisms.

4. Ensure BWC files are reviewed and released in accordance with federal, state, local statutes, and Departmental General Order M-9.1, Public Records Access;
5. Train the System Administrators to ensure consistency; and
6. Establish policy and procedures for the replacement of non-functioning BWCs and the check-out of spare BWCs.
7. The BWC Program Administrator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report that contains all components required by the Surveillance Technology Ordinance, as enshrined in Oakland Municipal Code 9.64.

G - 2. System Administrators

1. System Administrators shall be designated by the Bureau Commander for non-patrol assignments or the CID Commander for CID personnel.
2. All Sergeants of Police assigned to the Bureau of Field Operations are System Administrators.
3. System Administrator responsibilities shall include, but are not limited to, the following:
 - a. Ensure officers are assigned a fully functional BWC. Malfunctioning BWCs shall be replaced as soon as practical, in the manner specified by the Project Administrator;
 - b. Refresher training for members as needed;
 - c. Ensuring the return of damaged equipment to the Project Administrator;
 - d. Making copies of BWC files for court or other authorized activities;
 - e. Destruction of copied BWC files not admitted as evidence in court or no longer needed internally. System Administrators receiving a video file copy for destruction shall ensure the copy is destroyed and make an entry in the "Comments" field of the video file that the copy was destroyed.

G - 3. Training

The Training Section shall ensure that members receive department-approved training on this Use Policy as needed for those who are assigned a BWC, and training regarding the process for uploading and downloading BWC data.

G - 4. Description of the Technology BWCs

The BWC is a combination camera and microphone that collects audio and video in a digital format. The camera is worn on the user's body facing away from the user in order to get a first person view similar to what the user would see. The camera system is activated by either a user's touch or by other technological means and records audio / video for a time period as defined by the user. The user then uploads the captured audio / video to a secure storage facility where it can be reviewed as needed.

G - 5. Description of the Technology BWC File Management System

The BWC system employed by OPD features BWC docking stations and an internet web interface for controlling how files are uploaded and archived. The interface allows for Internet Protocol restriction features to control the locations where the system can be accessed. These restrictions limit BWC video file access to only authorized OPD personnel. Videos that are tagged for any reason as part of an investigation are not subject to the automatic deletion processes regardless of the retention schedule. Axon stores all BWC data in CJIS compliant cloud storage that utilizes redundancy and encryption to make sure evidence is not lost or compromised. The cloud-based server system has built-in redundancy with multiple servers to ensure data integrity and CJIS compliance.

By order of

LeRonne L. Armstrong
Chief of Police

Date Signed: _____