CITY OF OAKLAND

Privacy Advisory Commission

December 6, 2018 5:00 PM
Oakland City Hall
Hearing Room 1
1 Frank H. Ogawa Plaza, 1st Floor
Meeting Agenda

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian M. Hofer, **District 4 Representative**: Lou Katz, **District 5 Representative**: Raymundo Jacquez III, **District 6 Representative**: Vacant, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Saied R. Karamooz, **Mayoral Representative**: Heather Patterson*

Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.

1. 5:00pm: Call to Order, determination of quorum

2. 5:05pm: Review and approval of November 26 special meeting minutes

3. 5:10pm: Open Forum

4. 5:15pm: Surveillance Equipment Ordinance – DOT – Unmanned Aerial Vehicle Anticipated Impact Report and draft Use Policy – review and take possible action

5. 5:35pm: Surveillance Equipment Ordinance – OFD – Discuss with staff existing equipment capabilities, report and policy drafting sequence

6. 5:50pm: Federal Task Force Transparency Ordinance – Discuss with OPD annual reporting metrics

7. 6:20pm: Surveillance Equipment Ordinance – OPD – Body Worn Camera Anticipated Impact Report and draft Use Policy – review and take possible action

8. 7:00pm: Adjournment

CITY OF OAKLAND

Privacy Advisory Commission

November 26, 2018 5:00 PM
Oakland City Hall
Hearing Room 2
1 Frank H. Ogawa Plaza, 1st Floor
Special Meeting Agenda

***Commission Members**: **District 1 Representative**: Reem Suleiman, **District 2 Representative**: Chloe Brown, **District 3 Representative**: Brian M. Hofer, **District 4 Representative**: Lou Katz, **District 5 Representative**: Raymundo Jacquez III, **District 6 Representative**: Vacant, **District 7 Representative**: Robert Oliver, **Council At-Large Representative**: Saied R. Karamooz, **Mayoral Representative**: Heather Patterson*

Each person wishing to speak on items must fill out a speaker's card. Persons addressing the Privacy Advisory Commission shall state their names and the organization they are representing, if any.

1. 5:00pm: Call to Order, determination of quorum

Quorum was met with the following members in attendance: Hofer, Suleiman, Katz, Jacquez, Oliver, and Karamooz.

2. 5:05pm: Review and approval of November meeting minutes

The November 1st Meeting Minutes were approved unanimously.

3. 5:10pm: Open Forum

There were no Open Forum Speakers.

4. 5:15pm: Surveillance Equipment Ordinance – Unapproved Use of UAV by OPD during exigent circumstances – presentation of revised staff report and take possible action

OPD shared the updated report that included questions the PAC had asked at the October 4th meeting and the PAC voted to recommend the report be forwarded to the City Council.

5. 5:25pm: Review and take possible action on a Federal Task Force MOU with the U.S. Marshals Service (USMS)

The PAC reviewed the Resolution and the actual draft MOU and made three recommendations:

   a. *That the second to last resolved in the resolution be changed to limit the City Administrator's authority to negotiate any changes to the MOU, its schedule, extensions, etc. this is because the Charter requires that the City Council approves all MOUs and therefore, giving the City Administrator authority to make changes, without returning to Council, would be a violation. The new language ensures that the final MOU is what the City Council approves, keeping the authority with the Council.*

b. *That the resolution language refer to the actual MOU (as an exhibit) so that there is no confusion that the Council is adopting an MOU versus granting the City Administrator to do so.*
c. *The PAC recommends that the City Council insert the same language it recommended for the DEA MOU that holds the Federal Members of the Task Force to the higher standards that OPD Officer's must abide by. Below are the recommended additions:*

The Oakland Police Department's Task Force Officer will not participate in any enforcement action relating to the cultivation, sale, possession, or use of marijuana unless such action violates California law and/or City of Oakland ordinance(s).

The DEA Special Agents assigned to the Task Force Group (Oakland) agree to adhere to the following state or local laws, policies, or procedures, when performing as part of the Task Force Group (Oakland), unless existing DEA policies or procedures are more restrictive:

- *SB 54 – California Values Act (Cal. Gov. Code §7284 et seq.)*
- *SB 31 – California Religious Freedom Act (Cal. Gov. Code §8310.3 et seq.)*
- *Oakland Sanctuary City Ordinance (code pending)*
- *Oakland Police Departmental General Order M-17, Section V "Professional Standards"*
- *Oakland Police Departmental General Order M-19, Sections III and VIII (A, C)*

Staff indicated that they would take these recommendations into account in the supplemental report but also noted that the federal agencies have all stated they would NOT enter into the agreement with the more restrictive language.

6. 5:35pm: Review and take possible action on a Federal Task Force MOU with the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF)

The same conversation and recommendations that were made on the above item were also made on this item.

7. 5:45pm: Surveillance Equipment Ordinance – Cell Site Simulator draft Use Policy – review and take possible action on revised staff policy.

Approved with the motion that OPD return to the PAC with a determination as to whether the CAL ECPA applies to the use of this technology.

8. Adjournment: the meeting adjourned at 6:15.

Anticipated Impact Report for Unmanned Aerial Vehicles (UAV)/Drones

1. Information Describing the Unmanned Aerial Vehicles and How It Works

An Unmanned Aerial Vehicle (UAV) is an aircraft that is intended to navigate in the air without an on-board pilot. UAVs are alternatively called Remotely Piloted Aircrafts (RPA), Remotely Operated Vehicles (ROV), or Drones. UAVs are part of Unmanned Aircraft Systems (UAS) that include the necessary equipment, network, and personnel to control UAVs.

Sample Images of a street improvement project that would be captured with a UAV:

UAVs may be equipped with Cameras and/or Mapping Software:

Cameras

- UAVs may be equipped with regular RGB (visible light) cameras for digitally capturing still images and video footage.
- Depending on the need and capacity, UAV cameras may also use thermographic camera technology to sense infrared radiation for capturing still 3-D image and/or video 3-D footage. Thermal imaging cameras detect infrared radiation, typically emitted from a heat source (thermal radiation), to create a "picture" assembled for video output.

Thermal imaging cameras detect the heat given off by an object or person. A person, warmer than the surrounding air, appears "white" while the cooler surrounding air or buildings will appear in varying shades of gray. The "white" images do not always show a clear silhouette and, as such, are subject to the observer's interpretation.

Sample UAV Regular RGB (Visible Light) Image of Earthquake Rescue (Beichuan, China)

Sample Thermal Image to Identify People in the Dark (San Diego)


11-NOV-2007 San Diego Police
01:04:47
FLIR
RATE
011
297
PCORR

Mapping Software

In addition to cameras, UAVs may also be equipped with a mapping system that link images from compatible camera(s) with a Ground Control Point (GCP) taken from a Global Positioning System (GPS) or Real Time Kinematic (RTK) coordinate. Mapping may be used to capture essential identifying, topographical, or functional information regarding a transportation or natural disaster site.

Information that may be available from the use of mapping software includes:

- Site identifiers (e.g., addresses, business names, parcel numbers);
- Topographical information (e.g., terrain area, elevation, land contour lines and boundaries, water drainage areas, soil erosion, areas with water leaks or poor insulation coverage); and
- Functional information (e.g., 3D models of construction sites, stockpiles of raw materials, health of agricultural plots, etc.).

2. Proposed Purpose

UAVs/drones with cameras and/or mapping systems will be used by the Department of Transportation (DOT) for two primary purposes:

1) For DOT project documentation to capture before and after impacts of transportation improvement projects in the public right of way; and

2) For emergency response to rapidly assess roadway and infrastructure conditions without endangering city staff on public and private properties following a natural disaster (e.g., mudslide, flood, earthquake, fire, sinkhole, etc.).

When UAVs are deployed by the Department of Transportation for use in these situations, they will be guided by a pilot in command (PIC) who has an FAA Remote Pilot Certificate. The PIC will be accompanied by one or more Visual Observers (VO) who are trained to view live footage.

Any cameras or mapping systems will be activated only when in the relevant area, such as:

- **DOT Transportation Project Areas**
  Once the UAV enters a DOT project area, the PIC and VO will be permitted to take still images, record video footage, and/or map public rights-of-way from specific angles that capture the local of proposed or completed transportation improvement projects. The purpose of this information is to communicate Department of Transportation work to the public.

- **Emergency Response Sites**
  Once the UAV enters the emergency response areas, the PIC and VO will be permitted to take still images, record video footage, and/or map natural disasters in order to assess conditions that may endanger public safety. The purpose of this

information is to allow Department of Transportation staff to quickly and safely respond to natural disasters.

3. Locations Where UAVs May Be Deployed

Federal guidelines state that UAVs may fly no higher than 400 feet and remain below any surrounding obstacles when possible. They must remain thoroughly clear of and not interfere with manned aircraft operations and must avoid other aircraft and obstacles at all times.

UAVs may be deployed by DOT to observe and document only:

1. DOT transportation improvement projects; and
2. Sites of natural disaster for which the DOT needs to assess conditions that may endanger public safety.

4. Potential Impact on Civil Liberties & Privacy

The Department of Transportation recognizes that all people have an inalienable right to privacy and is committed to protecting and safeguarding this right. The DOT also recognizes that the UAV could raise concerns regarding real and/or perceived threats to civil liberties and privacy.

Specifically, the Department recognizes the following actual or potential public concerns:

a) Capturing the identity or recording the activity of persons

The public may be concerned that UAVs/Drones will capture personally identifiable information (PII) without notice or consent, or that UAVs/Drones will enable individuals' behaviors to be revealed to and/or monitored by DOT or other government agencies, their partners or affiliates, and/or the public. To these points, it should be noted that UAV cameras and integrated mapping system will be deployed for infrastructure documentation and public safety purposes. They will not be deployed to establish the identity or monitor the behavior of individuals or groups of individuals. Finally, these devises will not be used by law enforcement. UAV photographs and video recordings are similar to existing project photographs and emergency response photographs presently taken by Department of Transportation staff.

b) Targeted high-powered surveillance or voyeurism

Two concerns stem from potential surveillance and voyeurism practices enabled by UAVs.

- First, the public may be concerned about UAV and other surveillance technologies using powerful cameras for discriminatory targeting or other purposes. To this end, it should be noted that the RGB and infrared cameras available on commercially-available drones, which the DOT would acquire, cannot see through exterior walls, roofs, cars, clothing, or any object that would normally block a view observable by the naked eye. They also cannot see through glass because glass has its own thermal profile. Further, unlike night vision cameras that have the ability to see in low light conditions, infrared cameras can only detect an abnormal heat source which would appear

"white" while the cooler surrounding air or buildings will appear in varying shades of gray. The "white" images do not always show a clear silhouette and, as such, are subject to the observer's interpretation.

- Second, the public may be concerned about UAVs enabling voyeurism. Concerns over voyeurism often stem from UAV operators who work alone, since it provides the most opportunity for abuse. To this end, it should be noted that UAV Visual Observer (VO) cannot operate the integrated mapping system without the UAV Pilot in Command (PIC) present, since the system can only be operated while the UAV is in flight. Second, while the UAV Visual Observer (VO) may potentially see members of the public who are incidentally present at the site of the transportation project or natural disaster, the observer would only be able to view the image for a brief period through the UAV monitor since the focus would remain on the transportation project or disaster site being assessed.

c) **Data Use and Retention, Accountability and Auditing.** Finally, potential privacy and civil liberties concerns may arise from uncertainties regarding UAV/Drone data access, use, distribution, storage, security, and the accountability of handlers and owners of that data.

5. Mitigations

To be directly responsive to potential or feared impacts enumerated in Section 4 of this Anticipated Impact Report, DOT will take the following actions to protect the Privacy, and Civil Rights and Civil Liberties interests of the public:

a) Capturing the identity or recording the activity of persons.
To further assuage public concerns about identity capturing and/or activity monitoring identified in Section 4, the following protective measures will be taken by DOD or those acting on its behalf:

1. DOT will <u>not</u> capture still or video footage of persons in areas where there is an expectation of privacy without the individual's permission, unless responding to a natural disaster.

2. Excepting deployments for natural disaster impact assessments or for project monitoring in areas where there is no reasonable expectation of privacy, as in a public transit area, DOT will provide <u>advance and ongoing notice</u> to the public regarding where, when, and for how long UAVs will be authorized to operate. Notice will be posted conspicuously onsite 72 hours prior to the first anticipated usage and including a project date range.

3. Where PII, such as faces, license plates, and house numbers, is captured in camera or video footage that is retained by DOT that data will be <u>obfuscated</u> through technical means, such as blurring, pixilation, blocking, or redaction of hard copies, such that it is no longer identifiable or reasonably re-identifiable.

4. The DOT will keep the public informed about planned and actual DOT UAV usage, as well as changes that would significantly affect privacy, civil rights, or civil liberties.

b) Targeted high-powered surveillance or voyeurism

To further assuage concerns regarding high-powered surveillance or voyeurism raised in Section 4, DOT will take the following steps:

5. DOT will not supplement existing commercially-available UAV technology with technologies that enable the detection of persons or objects through walls, roofs, cars, clothing, or other objects that would normally block a view observable by a standard RGB camera or the naked eye.

6. All recordings made by the UAV VO will be subject to review by the Department of Transportation.

c) **Data Use, Retention, Distribution, and Accountability and Auditing.**
Finally, to assuage potential privacy and civil liberties arising from uncertainties regarding UAV/Drone data access, use, storage, security, and the accountability of handlers and owners of that data, the following mitigating steps will be taken:

7. DOT will collect information using UAVs, or use UAV-collected information, only to the extent that such collection or use is consistent with and relevant to an authorized purpose and DOT privacy and use policy.

8. PII collected by DOT with UAVs that cannot be technically obfuscated will be used solely for the purpose(s) specified in the notice. PII will be retained for no longer than 730 days unless retention of the information is determined to be necessary to an authorized mission, is maintained in a system of records covered by the Privacy Act or is required to be retained for longer period by any other applicable law or regulation.

9. Video footage or photographs may potentially be shared with the following: a)The public to increase awareness and understanding of transportation improvement projects and natural disasters; b)Data on natural disasters may be shared with relevant utility companies (e.g. PG&E) and partner agencies (e.g. EBMUD, Caltrans). Outside of these planned distributions, DOT will take steps to ensure that systems and data will not be disseminated outside of DOT unless dissemination is required by law, or fulfills and authorized purpose and complies with the DOD's UAV use purposes.

10. DOT will make available to the public, in an Annual Surveillance Report pursuant to Chapter 9.64 of the Oakland Municipal Code, a description of how the technology was used, including the type and quantity of data gathered or analyzed by the technology; whether and how often data acquired through the technology

was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standards the information was disclosed, and the justification for the disclosure(s); and other information required per Section 9.64.010 of that Ordinance.

6. Data Types and Sources

Data Sources	Data Types	Information
RGB and IR Cameras	• Regular (visible light) RGB still images • Regular (visible light) RGB video images • Thermal (thermographic/infrared) 3-D still images • Thermal (thermographic/infrared) 3-D video images	• Images and videos of streets, crosswalks, medians, sidewalks, curb cuts, and other transportation infrastructure • Images and videos of incidentally-captured persons, vehicles, and dwellings, and commercial buildings • Images and videos of natural disaster sites
Mapping Software	• Linked images from compatible camera(s) with a Ground Control Point (GCP) taken from a Global Positioning System (GPS) or Real Time Kinematic (RTK) coordinate	• Site identifiers (e.g., addresses, business names, parcel numbers); • Topographical information (e.g., terrain area, elevation, land contour lines and boundaries, water drainage areas, soil erosion, areas with water leaks or poor insulation coverage); and • Functional information (e.g., 3D models of construction sites, stockpiles of raw materials, health of agricultural plots, etc.).

7. Data Security

DOT will protect all acquired and stored data through appropriate security safeguards against risks such as loss, unauthorized access or use, destruction, modification, or unintended or inappropriate disclosure.

8. Fiscal Cost

The Department of Transportation will acquire UAV equipment from KTOP TV-10, the City of Oakland's own TV station.

Potential Sources of Funding
The UAV will be fully funded with grants from UASI (Urban Areas Security Initiative) and SHSGP (State Homeland Security Grant Program).

9. Third Party Dependence

Data will be collected, processed, and stored by a City Staff who will share images and video footage exclusively with the relevant Department of Transportation staff. All data collected by DOT will be owned by the City of Oakland, which will be accountable for ensuring that staff adheres to all data use and handling principles, provides appropriate data handling training to all its employees and contractors, and is audited regularly to demonstrate compliance with these principles and all applicable privacy protection requirements.

10. Alternatives

Project photography: an alternative that the Department of Transportation has employed is the use of electrical services "bucket" trucks, typically used to service traffic signals. This effort has proved an unsustainable use of staff time: rather than servicing broken signals and lights, electricians are deployed to project locations to take photographs. Capacity to complete this work has been limited.

Emergency response to natural disasters: presently, Department of Transportation staff take photographs from ground level to capture impacts of natural disasters, and in certain circumstances, staff can't fully assess the scene of a natural disaster if conditions are unsafe to enter. Further, staff might enter an area believed to be safe from visual inspection, but may realize upon entry that there are hazards beyond their initial viewpoint that may endanger their safety.

11. Track Record

[[INSERT CITY MATERIAL HERE, PULLING FROM http://www.cacities.org/Policy-Advocacy/Hot-Issues/Drones and other sources]] As of March 2018, a minority of state DOTs report deploying drones on a daily basis for purposes as varied as visually documenting highway construction projects, surveying, public education and outreach, bridge inspection, and emergency response.

OAKLAND DEPARTMENT OF TRANSPORTATION

[Proposed] Use Policy for Unmanned Aerial Vehicles (UAV)/Drones

1. Purpose

The unmanned aerial vehicles (UAV)/drones shall be used by City staff for two purposes: 1) for project photography purposes to capture before and after impacts of transportation improvement projects in the public right of way, and 2) to rapidly assess roadway and infrastructure conditions without endangering city staff on public and private properties following a natural disaster (mudslide, flood, earthquake, fire, sinkhole, etc.).

2. Authorized Use

- Project photography (before and after images of street improvement projects)
- Assessment of conditions following a natural disaster
- All other uses not referenced above shall be prohibited.

3. Data Collection

The following data may be obtained through UAVs/Drones:

Camera

- Regular still images
- Regular video images
- Thermal still and video images
- 3D video images

The system's camera will be activated only when the UAV is operating in the project area to be photographed, or in an area where there is a reasonable suspicion that a natural disaster may have caused unsafe conditions.

Any data obtained through the UAVs/drones must be used and handled pursuant to this policy.

4. Data Access

- Access to live mapping information and video image is limited to the pilots in command (PIC) and visual observers.
- Video footage/still images may be downloaded and viewed by relevant city staff.
- Video footage/still images may be released publicly in accordance with the Department's existing image sharing practices.

5. Data Protection

The City of Oakland will operate UAVs/drones with specific project locations/emergency response locations identified. Where personally identifiable information (PII), such as faces, license plates, and house numbers, is captured in camera or video footage retained by DOT or vendors will be obfuscated through technical means.

Access to live data is limited to the following :

- Pilots in command (PIC)
- Visual observers

Copies of video or still images shall be released to the project manager for project photography of street improvement projects, City staff, assigned to respond to emergencies in the event of a natural disaster.

6. Data Retention

Similar to existing project photographs and video footage/still images related to natural disasters, data may be retained by the Department of Transportation in perpetuity and shared publicly to increase awareness and understanding of the purpose and impacts of street design improvements and/or to notify the public of the severity of natural disasters. In cases where personally identifiable information (PII) is captured, data will be retained for no longer than 730 days unless retention of the information is determined to be necessary to an authorized mission, in maintained in a system of records covered by the Privacy Act or is required to be retained for longer period by any other applicable law or regulation.

7. Public Access

The public may access photographs and videos that are not publicly shared by request.

8. Third-Party Data-Sharing

Video footage or photographs may potentially be shared with the following:

- The public to increase awareness and understanding of transportation improvement projects and natural disasters
- Data on natural disasters may be shared with relevant utility companies (e.g. PG&E) and partner agencies (e.g. EBMUD, Caltrans)
- Investigating Officer
- In response to a court order

9. Training

Training for operating the UAVs/drones will be provided and will be limited to staff assigned as PIC and Visual Observers. City staff shall be trained in UAV safety and privacy procedures.

10. Auditing and Oversight

The PIC shall complete and submit a preflight checklist and risk assessment each time the UAV/drone flies. City staff shall ensure that these operations are met.

11. Maintenance

City staff will be required to maintain the integrity of the data captured and the safety of the UAV.

OAKLAND POLICE DEPARTMENT

Surveillance Impact Use Report
Body Worn Camera

1. Information Describing the Cell Site Simulator and How It Works

The Body Worn Camera (BWC) is a durable video camera meant to attach to a police officer's uniform. The BWC has an "on" and "off" switch 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.

The Portable Video Management System (PVMS) is a computer server and/or internet cloud-based video archival, storage, and playback system.

2. Proposed Purpose

The authorized and required purposes for the PVMS including the BWC and for collecting information using that technology to:

a. Citizen contacts to confirm or dispel a suspicion that the citizen may be involved, as a suspect, in criminal activity;

b. Detentions and Arrests; Assessment or evaluation for a psychiatric detention;

c. Involved personnel during a vehicle pursuit;

d. Serving a search or arrest warrant;

e. Crowd control operations

f. Conducting any of the following searches of a person and/or property;

- Incident to arrest;
- Cursory* (i.e., patdown or limited weapons search);

Commented [SB3]: Added here

- Probable Cause; Probation/Parole; Consent; or Inventory[1]
- Transporting any detained or arrested citizen (excluding prisoner wagon transports); or
- Upon the order of a higher-ranking member.

OPD BWC policy dictates that personnel shall de-activate their BWCs during the following situations:

a. Their involvement in the citizen contact, arrest or detention has concluded or becomes a hospital guard.

b. They receive an order from a higher-ranking member;

c. They are discussing administrative, tactical or law enforcement sensitive information away from the citizen;

d. 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.);

e. The search requiring activation has concluded, and the officer believes they will have no further interaction with the person;

f. The officer reasonably believe the recording at a hospital may compromise patient confidentiality;

g. A pursuit has been terminated;

h. The officer is interviewing an 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; or

i. The officer is meeting with an undercover officer. At the conclusion of the meeting, the BWC shall be re-activated until no longer required by policy;

j. Taking a statement from a victim or witness in lieu of taking a written statement (shall not be used to record statements from child abuse or sexual assault victims); Personnel shall advise or obtain consent from victims or witnesses when taking a BWC recorded statement;

k. Officers, when not prohibited from or required to activate their BWC, may use their own discretion when deciding to activate and de-activate the BWC.

Commented [TB4]: Why is this highlighted?

3. Locations Where, and Situations in which BWCs may be deployed or utilized.

Officers may use BWCs anywhere where officers have jurisdiction to operate as sworn officers. Officers shall not use BWCs during certain proscribed

[1] "Inventory" is not technically a search, but is the process by which an officer records the contents of a vehicle that has been impounded or similar.

situations described above in Section 2.

4. Mitigations

Commented [SB5]: Maybe leave for PAC discussion?

Commented [TB6R5]: Agreed. We may also want to list prohibited uses here?

5. Data Types and Sources

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."

6. Data Security

The PVMS 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 moved to separate folders where they cannot be deleted. OPD employs an "on-premises" server back-up system to maintain all BWC video files. The cloud-based archive system has built-in redundancy with multiple servers to ensure the data integrity.

OPD's BWC policy helps to ensure data security through numerous protocols:

All BWC files are the property of the Oakland Police Department.

Formatted: Font: (Default) Arial, Complex Script Font: Arial

a. Unauthorized use, duplication, editing, and/or distribution of BWC files is prohibited;
b. Personnel shall not delete any BWC file, except as specified in policy;
c. Personnel shall not remove, dismantle or tamper with any hardware/software component or part of the BWC;
d. Personnel are prohibited from wearing or using personally owned video recording devices in place of or in conjunction with an assigned BWC;
e. The Project Resource Management Unit is designated as the Custodian of Record for all BWC data files;
f. Personnel shall not intentionally use the BWC recording functions to

record any personal conversation of, or between another member/employee without the recorded member/employee's knowledge; and

g. Personnel 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.

7. Third Party Dependence

The Oakland Police Department uses a private vendor BWCs and is reliant upon the private vendor for BWC maintenance. The contract with the vendor allows for OPD to begin using the PVMS for video file back-up, search, and storage and security.

8. Alternatives Considered

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.

PRDR 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 and/or not utilizing BWCs. 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.

9. Track Record of Other Entities

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.

DEPARTMENTAL GENERAL ORDER

I-15: BODY WORN CAMERA PROGRAM

Effective Date: XX Jul 19
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 personnel 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.

Commented [TB1]: 9.64.010 7 A Purpose: The specific purpose that the surveillance technology is intended to advance.

A. Description of the Technology

The BWC system consists of two fundamental components: 1) the BWC itself, and 2) the video management system.

A – 1. How the BWC Works

The BWC is a durable video camera meant to attach to a member's uniform. The BWC has an "on" and "off" switch to allow personnel to record only during authorized and required uses as described above. The on/off switch also opens and closes the lens cover so as to protect the lens when not in use. The BWC contains a solid-state computer storage unit capable of storing digital video files. The BWC records video footage directly onto the solid-state internal storage unit when in recording "on" function.

A – 2. How the Video Management System Works

The video management system is a computer and/or internet cloud-based video archival, storage, and playback system.

B. BWC Use

All personnel 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 personnel, as determined by the COP, may also be assigned a BWC.

Commented [TB2]: 9.64.010 7 D. Data Access: The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information.

B – 1. General Guidelines

1. All personnel 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. Unauthorized use, duplication, editing, and/or distribution of BWC files is prohibited.

4. Personnel shall not delete any BWC file, except as specified in this policy.

5. Personnel shall not remove, dismantle or tamper with any hardware/software component or part of the BWC.

6. Personnel are prohibited from wearing or using personally owned video recording devices in place of or in conjunction with an assigned BWC.

7. The Project Resource Management Unit is designated as the Custodian of Record for all BWC data files.

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

9. Personnel 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 - 2. BWC Training

Training requirements for members issued BWCs include completion of training by the manufacturer of the technology or appropriate subject matter experts as designated by the Oakland Police Department. Such training shall include Federal and state law; applicable policy and memoranda of understanding; and functionality of equipment. Training updates are required when the technology and/or associated use changes.

Commented [TB3]: 9.64.010 7 I Training: The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology.

B – 3. BWC Operability and Maintenance

Members shall not utilize or wear a BWC unless it is properly functioning. If at any time, after deploying to the field, a BWC malfunctions or becomes inoperable it shall be replaced as soon as practical.

1. Function Check

   Members assigned or checking out a BWC shall test the equipment prior to every shift. Once activated, the indicator light of a fully functioning BWC should change from solid green to blinking green. If this does not occur, the BWC is not fully functional and a backup camera shall be checked out prior to deploying in the field.

   a. Members shall report all malfunctioning or inoperable BWC issues to a supervisor as soon as practical. Additionally, any unresolved BWC equipment malfunctions/problems shall be reported to the Project Administrator for camera replacement or

repair.

b. Absent exigent circumstances, members shall check out a backup camera prior to deploying in the field and utilize it as required until such time as their assigned camera is operational or a new camera is assigned.

2. Battery Maintenance

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

b. Personnel assigned to maintain and issue backup BWCs shall ensure the batteries are fully charged before issuing.

3. Data Upload

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

4. Replacement Procedures

a. Personnel shall report any recognized problems with the BWC as well as a lost, stolen or damaged BWC to their immediate supervisor as soon as practical. Upon notification, the supervisor shall facilitate the replacement of the BWC as soon as practical.

b. Supervisors shall document a lost, stolen or damaged BWC as specified in DGO N-5, Lost, Stolen, Damaged City Property, unless the BWC stops functioning properly for no apparent reason and the supervisor does not observe any sign of damage.

B – 3. BWC Placement

Video files can only be generated when BWCs are activated by OPD officers. The position of the BWC when activated by OPD members may impact the clarity and sound of video files, thus limiting the type of image and sound collected.

1. 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.

2. 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 – 4. BWC Use Documentation

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

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

Personnel are required to document and explain in one of the reports specified above any delayed or non-activation of their BWC when BWC activation was required.

C. BWC Data Collection and File Information

C – 1. Data Collected

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.

Commented [TB4]: 9.64.010 7 C Data Collection: The information that can be collected by the surveillance technology. Where applicable, list any data sources the technology will rely upon, including "open source" data.

C – 2. BWC Required File Information

To ensure accountability for the proper identification, tracking and chain of custody for all original BWC video files stored on the Department server and external copies of the BWC video files, all personnel shall follow the protocols below.

1. Members shall enter in VERIPATROL the RD # associated with each video file. If no RD # is created for the video, the full CAD incident number shall be entered. Members shall add this data to the file by using the "Add Details" button in the VERIPATROL software program:
    a. Category column- Select the appropriate category from the drop-down menu; and
    b. Case # column- Enter the report number if one exists, or if none exists, the full 15-digit incident number (i.e. LOP141002001196); or

c. If a BWC video file was created and does not have an associated RD or incident number, the member shall enter "NONE" in the comment column. This task should be completed by logging into VERIPATOL Mobile in the patrol vehicle where viewing and annotation can be completed daily throughout the member's shift.

2. Members are authorized to view their video in order to properly identify the data file unless otherwise prohibited by policy.

3. Entering the information specified in Section 1, above, shall be completed daily. Should conditions exist that prohibit completion during the member's shift, it shall be completed minimally by the end of the member's next regularly scheduled work day.

During incidents that require a large-scale activation of the Department's members, (i.e. protest, natural disaster, etc.), the incident commander may approve delayed information entry, except in cases that require an investigative callout (e.g. Level 1 UOF, ICD, VPRD, criminal investigation of a member or employee.) The Incident Commander shall document their orders in the After-Action Report.

D. Activation and Deactivation

D – 1. Required Activation

Members shall activate their BWCs prior to any of the below:

1. Citizen contacts to confirm or dispel a suspicion that the citizen may be involved, as a suspect, in criminal activity;

2. Detentions and Arrests;

3. Assessment or evaluation for a psychiatric detention (5150 W&I);

4. Involved personnel, as defined by DGO J-04, PURSUIT DRIVING, during a vehicle pursuit;

5. Serving a search or arrest warrant;

6. Conducting any of the following searches of a person and/or property:

   a. Incident to arrest;

   b. Cursory* (i.e., patdown or limited weapons search);

   * Refer to Training Bulletin (TB) I-O.02, The Legal Aspects of Searching Persons

c. Probable Cause;
d. Probation/Parole;
e. Consent; or
f. Inventory

7. Transporting any detained or arrested citizen (excluding prisoner wagon transports).

Commented [TB5]: 9.64.010 7 B Authorized Use: The specific uses that are authorized, and the rules and processes required prior to such use.

D – 2. BWC Activation Not Required

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

1. Members taking a report when the information available to them indicates the suspect is not on the scene;

2. During a preliminary investigation with a child abuse victim or a victim of a sexual assault;

3. Members meeting with any Confidential Informant, as defined in DGO O-04, Informants; or

4. 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.

D – 4. Deactivation of the BWC

Members shall not de-activate their BWC, when it was activated as required by this policy, until one of the following occurs:

1. Their involvement in the citizen contact, arrest or detention has concluded or becomes a hospital guard (see part II, C, 4 above);

2. They receive an order from a higher ranking member;

3. They are discussing administrative, tactical or law enforcement sensitive information away from the citizen;

4. 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.);

5. The searches requiring activation as enumerated in Part II, A have concluded, and the member believes they will have no further interaction

with the person;

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 actions, as specified in DGO J-04, or notifies Communications they are in-service;

8. They are interviewing an 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; or

9. They are meeting with an undercover officer. At the conclusion of the meeting, the BWC shall be re-activated until no longer required by policy.

10. They are ordered to deactivate by a higher-ranking member.

After a member de-activates a BWC, it is the member's responsibility to ensure the BWC is reactivated should the circumstances require it.

D – 5. Recording Statements with the BWC

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

1. Personnel shall advise or obtain consent from victims or witnesses when taking a BWC recorded statement.

2. BWC statements shall be recorded as an individual separate file, barring exigent circumstances. Therefore, during a required activation, where none of the de-activation criteria have been met, members may temporarily de-activate their BWC to record individual separate statements.

3. Personnel shall follow the steps below when de-activating their BWC for statement taking:

   a. Prepare to immediately take the statement;

   b. Deactivate the BWC then immediately reactivate the BWC and begin taking the statement; and

   c. Upon completion of the statement, de-activate the BWC then immediately re-activate the BWC, if continued recording is required.

   Members shall repeat the above steps when de- activating/activating their

BWC to take multiple statements.

e. Personnel whose BWC is not already activated shall activate it before and deactivate it after each statement is taken to create a separate individual file.

Refer to Report Writing Manual (RWM) S-01, STATEMENTS.

D – 6. Discretionary Activation and De-Activation

Members, when not prohibited from or required to activate their BWC, may use their own discretion when deciding to activate and de-activate the BWC.

E. Viewing, Copying, and Deletion of BWC Video

E – 1. Viewing BWC Video

Authorized 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.

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.

When personnel are authorized to view a BWC file by this policy, the video file shall be reviewed on a Department computer by logging onto the VERIPATROL system.

1. Level 1 Use of Force, Level 1Pursuit or In-Custody Death

In the event of a Level 1 use of force, Level 1 pursuit or an in- custody death, 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.

Commented [TB6]: 9.64.010 7 D. Data Access: The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information.

Commented [TB7]: 9.64.010 7 D. Data Access: The category of individuals who can access or use the collected information, and the rules and processes required prior to access or use of the information.

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 the member has been interviewed by the appropriate investigator, the investigator will 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.

2. Investigation of a Member

a. Criminal Investigation of 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.

b. 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. Requesting Review of Audio/Video Recordings

1) Subject or witness personnel wanting to view any of the audio/video recordings related to the incident shall make a request to do so, in writing or via email, to the CID or IAD Commander, as appropriate.

2) The CID or IAD Commander receiving the above request shall notify the member, in writing or via email, of the approval or denial to view the recordings.

3) The CID or IAD Commander shall document the approval or denial in the case file notes/log or include a copy of the approval or denial correspondence in the case file.

4) Approval to view the audio/video recordings may be made by the CID or IAD Commander as long as he/she has determined that

allowing the recordings to be viewed will not be detrimental to the investigation.

3. Investigatory Review

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 or internal investigations shall:

a. Advise the Project Administrator or a System Administrator to restrict public disclosure of the BWC file in criminal or internal investigations, as necessary;

b. Review the file to determine whether the BWC file is of evidentiary value and process it in accordance with established protocols; and

c. Notify the System Administrator to remove the access restriction when the criminal/internal investigation is closed.

4. Supervisor and Commander Review

a. 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.

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

1) Conduct a random review of at least one BWC recording for each of their subordinates on a monthly basis. Sergeants shall ensure that each selected recording:

a) Is viewed in its entirety; and
b) Has a minimum length of ten (10) minutes.

2) Conduct a review of all BWC recordings of subordinate arrests/ incidents involving:

a) 69 PC (Resist an Officer);
b) 148 PC (Resist, Delay, or Obstruct an Officer); and
c) 243(b) or (c) (Battery on an Peace/Police Officer).

For the above arrests/incidents, sergeants shall view BWC recordings from beginning of the incident to the arrest.

3) When approving or investigating a UOF or vehicle pursuit, conduct a review of BWC recordings for all subordinates who are a witness to or involved in the UOF or vehicle pursuit.

b. Supervisor review of subordinate BWC recordings shall include an assessment of:

1) Officer performance and training needs;

2) Policy compliance; and

3) Consistency between written reports and video files.

d. When a member does not activate or de-activate their BWC as required, supervisors and commanders shall determine if the delayed or non-activation was reasonable, based upon the circumstances.

1) If the supervisor determines that the delay or non-activation was reasonable, the supervisor shall document the justification in the UOF report.

a) If no UOF report is generated, this shall be documented in an SNF for the officer.
b) The supervisor's commander shall be advised and their name noted in the SNF.

f. 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.

5. Use of BWC Files for Training Purposes

a. 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, and the Department as a whole. A recommendation to utilize a BWC file for such purpose may come from any source.

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

c. 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.

6. Other Review

   OIG staff (when conducting audits), supervisors, commanders, active FTOs and the FTO Coordinator are authorized to view BWC files to investigate allegations of misconduct or evaluate the performance of members, unless otherwise prohibited by policy.

E – 2. Copying BWC Files

1. Departmental Requests for Copies of BWC Files

   a. Personnel requiring a copy of BWC audio/video file(s) for court shall contact their first line supervisor. If the first line supervisor is unavailable, personnel shall contact any System Administrator.

   b. In non-patrol assignments, requests for BWC audio/video file(s) shall be forwarded to the designated System Administrator.

   d. Any BWC copies not entered into evidence shall be returned to the first line supervisor or a System Administrator for destruction.

2. Non-Departmental Requests for Copies of BWC Files

   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.

3. Copying BWC Recordings for Court

   a. CID and other investigative personnel taking a case to the District Attorney for charging are responsible for obtaining copies of all applicable BWC files for presentation to the DA.

   b. 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.

   b. 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

Commented [TB8]: 9.64.010 7 H. Third Party Data Sharing: If and how other City departments, bureaus, divisions, or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information.

Commented [TB9]: 9.64.010 7 G Public Access: How collected information can be accessed or used by members of the public, including criminal defendants.

Commented [TB10]: 9.64.010 7 G Public Access: How collected information can be accessed or used by members of the public, including criminal defendants.

each video file.

e. The documentation of the chain of custody and responsibility to secure the copy shall transfer to the person receiving the copy until:

1) The copy is received by non-Department personnel (e.g. District Attorney, City Attorney, Court Clerk, etc.);

2) The copy is admitted in to evidence; or

3) The copy is returned to a system administrator for destruction.

4. Copying BWC Recordings for Reasons other than Court

a. 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.

b. 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.

c. All personnel are prohibited from:

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.

E – 3. Deleting BWC Files

In the event of an unintended or inappropriate activation of the BWC and 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 immediate supervisor with sufficient information to locate the BWC file.

Approved requests shall be submitted to the Project Administrator at_

BWC@oaklandca.gov.

F. Data Retention

BWC files shall be retained for a period of three years unless it is required for:

1. A criminal investigation;
2. An administrative investigation;
3. Research;
4. Civil litigation;
5. Training; and/or
6. Other Departmental need.

G. Administrative Responsibilities

G – 1. Project Administrator

The Project Administrator is designated by the Chief of Police and has oversight responsibilities to include, but 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 industry-standard safeguards that protect information from unauthorized access, including encryption and access control mechanisms.

   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 moved to separate folders where they cannot be deleted. OPD employs an "on-premises" server back-up system to maintain all BWC video files. The cloud-based archive system has built-in redundancy with multiple servers to ensure data integrity.

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

7. Establish policy and procedures for the replacement of non-functioning BWCs and the check-out of spare BWCs.

Commented [TB11]: 9.64.010 7 F Data Retention: The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period.

Commented [TB12]: 9.64.010 7 E Data Protection: The safeguards that protect information from unauthorized access, including encryption and access control mechanisms.

9.64.010 K Maintenance: The mechanisms and procedures to ensure that the security and integrity of the surveillance technology and collected information will be maintained.

8. The BWC Program Administrator shall provide the Chief of Police, Privacy Advisory Commission, and Public Safety Committee with an annual report that contains all of the following for the previous 12-month period:

   a. The total number of videos recorded;
   b. The average number of videos recorded per user;
   c. The average length of videos;
   d. The total number of videos deleted;
   e. Total amount of BWC video recorded by OPD personnel as measured in hours of recordings and terabytes of file storage.
   f. Total costs for maintenance, licensing and training, if any.
   g. The results of any internal audits and if any corrective action was taken, subject to laws governing confidentiality of employment actions and personnel rules.
   h. The effectiveness of the technology in assisting in investigations based on data collected.

Commented [TB13]: 9.64.010 7 J Auditing and Oversight: The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal recordkeeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy.

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 Patrol Division 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. User training;
   c. Ensure the return of damaged equipment to the Project Administrator;
   d. Make 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; and
   f. Approve/disapprove requests for deleting accidental recordings.

4. 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.

By Order of

Anne E. Kirkpatrick
Chief of Police

Date Signed: