



FILED
OFFICE OF THE CITY CLERK
OAKLAND
2015 JUL -2 PM 12: 09

AGENDA REPORT

TO: Sabrina B. Landreth
CITY ADMINISTRATOR

FROM: Sean Whent

SUBJECT: Informational Report Re: Request of
100 Black Men of the Bay Area, Inc. –
Secure Storage of Digital Video

DATE: June 26, 2015

City Administrator
Approval

Date

COUNCIL DISTRICT: City-Wide

RECOMMENDATION

Staff recommends that the Public Safety Committee accept:

An Informational Report from the Oakland Police Department (OPD) in Response to the Rules Request from 100 Black Men of the Bay Area (Frank Tucker) Concerning the Sending of Law Enforcement Video, Dash Cams etc. to the Cloud in Real Time, to Avoid any Tampering of Evidence.

OUTCOME

This report will help facilitate discussion between the Oakland Police Department and the Public Safety Committee regarding a Rules request from 100 Black Men of the Bay Area (Frank Tucker) concerning the sending of law enforcement video, dash cams etc. to the cloud in real time, to avoid any tampering of evidence.

BACKGROUND / LEGISLATIVE HISTORY

At the April 16, 2015 Rules and Legislation Committee, the Committee approved for scheduling the 100 Black Men of the Bay Area Inc.'s (100 Black Men) request for a council report. The City Administrator assigned many of the 100 Black Men requests to the Oakland Police Department (OPD) for further response. This report is responsive to the sixth request, which is to "receive an informational report and possible action adopting legislation to send law enforcement video, dash cams etc. to the cloud in real time, to avoid any tampering of evidence."

Item: _____
Public Safety Committee
July 14, 2015

ANALYSIS

OPD has been using body-worn Portable Digital Recording Devices (PDRDs) since 2011. OPD was one of the first law enforcement agencies in California – and the United States – to equip officers with these devices. Use of PDRDs is an example of OPD leading the nation by bringing transparency to local law enforcement services. While the PDRD technology continues to improve, currently there are limitations which hinder OPD from taking the actions within this request.

The current body-worn Portable Digital Recording Device (PDRD) camera system does not allow for instant upload of video as it is recorded by officers. No video from body-worn cameras has ever been permanently lost. Video has been temporarily lost was during a system upgrade and all video was recovered. The battery life of the PDRD is generally no more than four or five hours. The battery cannot be swapped in and out of the unit for charging. The entire unit must be charged.

Video recordings resulting from body-worn cameras are uploaded by each Officer from the camera to a centralized secure video management server. OPD Department General Order (DGO) I-15.1 (Portable Video Management System, enacted 2014) V D states officers shall upload PDRD data files on a regular basis to ensure storage capacity is not exceeded. DGO I-15.1 is provided in its entirety as *Attachment A*.

The video evidence is securely stored and catalogued with a digital signature process compliant with Federal Information Processing Standard (FIPS) 140-2 to verify the video has not been altered. The National Institute of Standards and Technology (NIST) issued the FIPS 140 Publication Series to coordinate the requirements and standards for cryptography modules that include both hardware and software components. Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module. If the camera is lost or stolen, the proprietary security software will prevent unauthorized access to video evidence by anyone other than authorized members of OPD. Any data on a lost or stolen camera cannot be recovered unless the camera is recovered. Once the data upload is completed, only authorized OPD users with proper permissions and privileges have access to the video files.

As the current body worn cameras come wear out and require replacement in the next few years, OPD will explore opportunities to replace the current system with a system that instantly uploads video feeds from officers to secure storage. At present, there are two barriers to such a system. The first is financial: the cost of instantly uploading video would require a cellular subscription at an approximate cost of thirty dollars per camera per month. Equipping all 720 sergeants and officers in OPD with this technology would cost \$21,600 per month or \$259,200 per year. This is only the cost of instantly uploading the video. Additional costs include the new body worn cameras themselves and any additional hardware and software necessary for the new system. It is hoped that the cost of such technology will decrease as OPD's current cameras wear out and require replacement.

The second barrier to instant upload from body-worn video cameras is that of certifying any offsite storage (cloud) system as compliant with the FBI's Criminal Justice Information Services (CJIS). Such compliance is necessary to ensure that OPD has access to critical national law enforcement data. At this time, OPD is unaware of any offsite storage system that is certified as being compliant with the standards of CJIS. Such certification is necessary to ensure access to CJIS databases by OPD.

While instant uploading of video from body-worn cameras to the cloud is not practical at this time, there are currently safeguards in place to ensure no unauthorized access to recordings. Included in these safeguards is an inability of field personnel to tamper with video. OPD will continue to explore instant video upload and offsite storage as the current devices are replaced.

PUBLIC OUTREACH/INTEREST

This is of public interest as it directly relates to safety within the Oakland community.

COORDINATION

The Information Technology Department and Office of the City Attorney was consulted in preparation of this report.

COST SUMMARY/IMPLICATIONS

There are no costs associated with this report.

The costs of upgrading to an instant-upload video system from PDRDs could exceed an additional \$259,200 per year in the future.

SUSTAINABLE OPPORTUNITIES

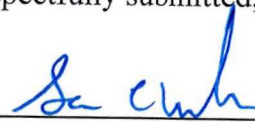
Economic: There are no economic opportunities identified in this report.

Environmental: No environmental opportunities have been identified.

Social Equity: This report provides valuable information to the Oakland community regarding social equity through transparent, fair, and impartial policing.

For questions regarding this report, please contact Police Services Manager Timothy Birch, Research and Planning, at (510) 238-6443.

Respectfully submitted,



Sean Whent
Chief of Police
Oakland Police Department

Prepared by:
Timothy Birch
Police Services Manager I
Research and Planning
Office of the Chief
Oakland Police Department

Attachment A: DGO I-15.1 Portable Video Management System



DEPARTMENTAL
GENERAL
ORDER

Effective Date
05 Mar 14

I-15.1

Evaluation Coordinator:
Research and Planning Division
Commander

Index as:

Portable Video Management
System

Evaluation Due Date:
05 Sep 14

Automatic Revision Cycle:
2 Years

PORTABLE VIDEO MANAGEMENT SYSTEM

The purpose of this order is to set forth Departmental policy and procedures for the Portable Video Management System (PVMS), which includes a Portable Digital Recording Device (PDRD), designed to record both audio and video of field activity.

Progressive police departments are increasingly utilizing a variety of audio/video technology to further the mission of their departments. The Oakland Police Department has adopted PDRD technology because of its flexibility to capture audio/video evidence and enhance the Department's ability to conduct criminal investigations, administrative investigations, and review police procedures and tactics.

I. POLICY

- A. Officers shall utilize the PDRD in accordance with the provisions of this order.
- B. Unauthorized use, duplication, editing, and/or distribution of PDRD files are prohibited.
- C. Personnel shall not delete any PDRD file except as specified in Part V, C (request for deletion of an accidental recording.)
- D. Personnel shall not remove, dismantle or tamper with any hardware/software component or part of the PDRD.
- E. Members are prohibited from wearing or using personally owned video recording devices in place of or in conjunction with their issued PDRD.
- F. The Project Resource Management Unit is designated as the Custodian of Record for all PDRD data files.

II. PDRD ACTIVATION AND DE-ACTIVATION

- A. Members, including cover officers, shall activate their PDRD under the following circumstances:
1. Citizen contacts (“consensual encounters”) to confirm or dispel a suspicion that the citizen may be involved in criminal activity as a suspect, victim or witness. This does not include victims of sexual assault;
 2. Detentions and Arrests;
 3. Assessment or evaluation for a psychiatric detention (5150 W&I);
 4. Involved personnel, as defined by DGO J-4, during a vehicle pursuit;
 5. Serving a search or arrest warrant;
 6. Conducting any of the following searches on one’s person and/or property:
 - a. Incident to arrest;
 - b. Cursory;
 - c. Probable Cause;
 - d. Probation/Parole;
 - e. Consent; or
 - f. Inventory
 7. Transporting any detained or arrested citizen (excluding prisoner wagon transports); or
 8. Upon the order of a higher ranking member

Members shall activate their PDRD prior to initiating the circumstances enumerated in Part II. A. 1-7, above.

- B. PDRD Activation is not required during the following circumstances:
1. Members taking a report or conducting a preliminary investigation who reasonably believe no criteria for a required activation are present;
 2. During a preliminary investigation with a victim of a sexual assault;
 3. Members meeting with any Confidential Informant, as defined in DGO O-4, INFORMANTS; or
 4. Members on a guard assignment at a Police, Medical, Psychiatric, Jail or Detention facility. Members shall assess the circumstances of each guard assignment, on a continuing basis, to determine whether to discretionarily activate or de-activate their PDRD.
- C. De-activation of the PDRD
1. Members shall not de-activate their PDRD when it was activated as required by this policy until:
 - a. Their involvement in the citizen contact or detention has concluded; or
 - b. They receive an order from a higher ranking member; or
 - c. They are discussing administrative, tactical or law enforcement sensitive information away from the citizen; or
 - 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.); or
 - e. The searches requiring activation as enumerated in Part II. A have concluded and the member believes he/she will have no further interaction with the person; or
 - f. They reasonably believe the recording at a hospital may compromise patient confidentiality; or
 - g. A pursuit has been terminated and the member performs the required actions as specified in DGO J-4, PURSUIT DRIVING or notifies Communications they are in-service; or

- h. They are interviewing an informant for the purpose of gathering intelligence. At the conclusion of the interview, the PDRD shall be re-activated until no longer required by policy.

After a member de-activates their PDRD, it is his/her responsibility to ensure they re-activate their PDRD should the circumstances require it.

- 2. When a member activates his/her PDRD, and such activation was not required by policy and the circumstances do not require continued recording, he/she may use his/her own discretion when deciding to de-activate the PDRD.
- D. Personnel shall not intentionally use the PDRD recording functions to record any personal conversation of, or between another member/employee without the recorded member/employee's knowledge.
 - E. Personnel are not required to advise or obtain consent from a person when:
 - 1. In a public place; or
 - 2. In a location where the member is lawfully present.
 - F. During crowd control, protest or mass arrest incidents members shall use their PDRD consistent with this policy unless otherwise directed by the Incident Commander. The Incident Commander shall document his/her orders in an appropriate report (e.g. Operations Plan or After Action Report) and provide the orders to all personnel.
 - G. Part II also applies to cover officers.

III. OFFICER, SUPERVISORY AND INVESTIGATORY REVIEW OF PDRD

- A. Level 1 Use of Force, Level 1 Pursuit or In-Custody Death
 - 1. In the event of a Level 1 use of force, Level 1 pursuit or an in-custody death, all PDRD recordings shall be uploaded to the server as soon as practical. No member may view any audio/video recordings prior to completing and submitting the appropriate report(s) and being interviewed by the appropriate investigative unit.
 - 2. 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. The member will be given the opportunity to provide additional information to supplement his/her statement and may be asked additional questions by the investigators.

B. Investigation of a Member

1. Criminal - Members who are the subject of a criminal investigation may only view their own audio/video recordings at the direction of the CID or IAD Commander.
2. Administrative – Members having received notification (Complaint Notification Report [CNR]) from the IAD and who are considered to be a subject or witness officer, may only view their own audio/video recordings at the direction of the IAD Commander or designee.

C. Investigators conducting criminal or internal investigations shall:

1. Advise the Project Administrator or a System Administrator to restrict public disclosure of the PDRD file in criminal or internal investigations, as necessary.
2. Review the file to determine whether the PDRD file is of evidentiary value and process it in accordance with established protocols.
3. Investigators shall notify the System Administrator to remove the access restriction when the criminal/internal investigation is closed.

D. Supervisor Review

1. Supervisors shall conduct a random review of the PDRD recordings of each of their subordinates on a monthly basis.
2. When a supervisor is approving or investigating a UOF or vehicle pursuit they shall review the PDRD recordings of members who are a witness to or involved in the use of force.
3. Supervisors review of subordinate PDRD recordings shall include an assessment of;
 - a. Officer performance and training needs;
 - b. Policy compliance; and
 - c. Consistency between written reports and video files.

- E. When a member does not activate or de-activate his/her PDRD as required, supervisors and commanders shall determine if the delayed or non-activation was reasonable, based upon the circumstances. If the supervisor determines that the delay or non-activation was reasonable they shall document their justification in the UOF report or, if no UOF report is generated, in the officer's SNF. 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 PDRD 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 the officer's SNF.
- G. OIG staff conducting audits, training staff, supervisors, commanders, active FTOs and the FTO Coordinator may view PDRD files to investigate allegations of misconduct or evaluate the performance of members.
- H. When a member is authorized to view a PDRD recording by this policy, the audio/video recording shall be reviewed at a Department desktop computer by logging onto the server. Personnel reviewing the video shall document the reason for access in the "Add Details" field, under the "Comments" section on the video file.

IV. RESPONSIBILITIES

- A. The Project Administrator is designated by the Chief of Police and has oversight responsibilities to include, but not limited to, the following:
 - 1. Document malfunctions and equipment failures;
 - 2. Policy and procedure review and evaluation;
 - 3. Ensure PDRD files are secured and retained for a minimum of five (5) years;
 - 4. Ensure PDRD files are reviewed and released in accordance with federal, state, local statutes, and Departmental General Order M-9.1, PUBLIC RECORDS ACCESS; and
 - 5. Train the System Administrators to ensure consistency across the bureaus.
- B. System Administrators shall be designated by the Bureau Commander for non-patrol assignments. All Sergeants of Police assigned to the Patrol Division are System Administrators.

System Administrator responsibilities shall include, but are not limited to, the following:

1. Ensure officers are assigned a fully functional PDRD. Malfunctioning PDRDs shall be replaced immediately;
2. User training;
3. Return damaged equipment to the Project Administrator;
4. Make copies of PDRD files for court or other authorized activities;
5. Destruction of copied PDRD files not admitted as evidence in court; and
6. Approve/disapprove requests for deleting accidental recordings

V. OPERATING THE PDRD

- A. Members assigned a PDRD shall test the equipment prior to every shift. Once activated, the indicator light of a fully functioning PDRD should change from solid green to blinking green. If that does not occur, immediately report the malfunction to a supervisor.
- B. Members shall position and securely attach the camera to the front of their uniform or uniform equipment, as the primary location, to facilitate recording. Members shall not wear a PDRD that is damaged or not functioning properly due to low battery charge, damage, malfunction or memory exceeding capacity and shall notify their supervisor.
- C. Subject to the recording requirements of Part II of this policy, the PDRD may be temporarily removed and placed or mounted in the police vehicle or other location, to facilitate recording a citizen.
- D. Members shall upload PDRD data files at the end of and, if needed, during their shift to ensure storage capacity is not exceeded.
- E. Members shall ensure the battery is fully charged and operating properly at the beginning of their shift.
- F. Members shall report unresolved equipment malfunctions/problems to a System Administrator for camera replacement. Members shall check out a backup camera, as soon as practical, and utilize it as required until such time as their original camera is operational.

- G. Members are required to document the activation of their PDRD. Members are required to provide an explanation for any delayed or non-activation of their PDRD when PDRD activation is required.

Documentation shall be provided in at least one of the following reports, as appropriate:

1. Citation or Notice to Appear;
2. Crime Report;
3. Consolidated Arrest Report, electronic or paper, or Juvenile Record;
4. Field Interview; or
5. CAD notes

VI. PDRD FILE REQUESTS

A. Departmental Requests

Personnel requiring a copy of PDRD 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.

1. In non-patrol assignments, requests for PDRD audio/video file(s) shall be forwarded to the designated System Administrator.
2. Any PDRD copies not entered into evidence shall be returned to the first line supervisor or a System Administrator for destruction.

B. Non-Departmental Requests.

Public Records requests shall be accepted and processed, in accordance with the provisions of federal, state, local statutes and DGO M-9.1, PUBLIC RECORDS ACCESS, and forwarded to the Project Administrator.

C. Request for deletion of an accidental recording.

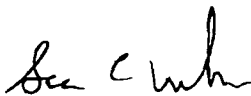
In the event of an accidental activation of the PDRD and the resulting recording is of no investigative or evidentiary value, the respective personnel may request that the PDRD file be deleted by submitting an email request to their immediate supervisor with sufficient information to locate the PDRD file. Approved requests shall be submitted to the Project Administrator at PDRD@oaklandnet.com.

- D. A PDRD file may be utilized as a training tool for individuals, specific units, and the Department as a whole. A recommendation to utilize a PDRD file for such purpose may come from any source.
1. A person recommending utilizing a PDRD file for training purposes shall submit the recommendation through the chain-of-command to the Training Section Commander.
 2. The Training Section Commander shall review the recommendation and determine how best to utilize the PDRD file considering the identity of the person(s) involved, sensitivity of the incident and the benefit of utilizing the file versus other means.

VII. REPLACEMENT PROCEDURES

- A. Personnel shall immediately report any recognized problems with the PDRD as well as a lost, stolen or damaged PDRD to their immediate supervisor. Upon notification, the supervisor shall facilitate the replacement of the PDRD as soon as practical.
- B. Supervisors shall document a lost, stolen or damaged PDRD as specified in DGO N-5, LOST, STOLEN, DAMAGED CITY PROPERTY, unless the PDRD stops functioning properly for no apparent reason and the supervisor does not observe any sign of damage.

By Order of



Sean Whent
Interim Chief of Police

Date Signed: 3-5-14