Privacy Advisory Board Questions Received August 22, 2023

1. Please update Use Policy to include more information on encryption and security information (as discussed in PAB meeting).

   From PAB meeting: My understanding is that the camera uploads information to the Axon cloud only when put in its dock. What can someone do with physical access to the camera? (Such access is available to the officer using the camera. There is also a risk that a camera is recovered by an external party, and the question is what data they can get.)

   Officers can view recordings from their own body worn camera ("BWC") in the field. The footage can be viewed on a department smart phone which has the Axon application downloaded. The footage cannot be modified. It can only be viewed. The footage on the BWC is accessed via an application on the phone utilizing two factor authentication which meets all the standard information technology standards of the City of San Diego and the Police Department's information technology standards. The connection between the viewer and the body worn camera is achieved via a Bluetooth link which is encrypted at 256 bit. The viewer must have password access, via the application to view the footage.

   If a non-police officer / unauthorized user was to find a body worn camera in the field, the person would not be able to view the footage without Axon's proprietary viewer application which has password protection.

   The footage itself is encrypted on the device, providing an additional layer of security to prevent the footage from being viewed by an unauthorized user. There is a port on the base of the body worn camera which can be used to charge the device and download the camera when connected to a department charging dock in a secure police facility. The body cameras and the docking stations are both registered to the San Diego Police Department. The body worn camera videos cannot be uploaded using other agencies docks or vice versa. Given the encryption which exists on the device it is highly unlikely that an unauthorized user would be able to view the footage on the body worn camera. No such situation has happened in the 14 years the department has been using Axon body worn cameras.

   Can the holder of the camera download the data on it? Can they modify the data, or upload new data?

   The user / holder of the camera cannot download the data directly from the camera. The camera must be docked into a SDPD registered dock. The data is then uploaded to SDPD's Evidence.com account which only approved users have access too. Officers are not permitted to record the footage with another device. Doing so would be a violation of Department Procedure 1.49 AXON – Body Worn Cameras. Officers cannot modify the video they record. Every time the officer records a video on the BWC by activating the camera into event mode a new file is created. That video must be tagged with the appropriate meta data for later viewing, auditing, or use by the department. Even accidentally recorded videos must be accounted for. The camera will not "overwrite" previous videos.

   At the meeting the police said something about there being encryption on the camera itself, which was not stated in their documents. I am not sure how this works or how it would prevent access by a camera holder.

Privacy Advisory Board Questions Received August 22, 2023

Is it possible to get details like under what key is this encryption done, and where is the key stored? (If the key is on the camera, it can be directly accessed.)

Keys are managed by Axon Evidence. Camera storage cannot be directly accessed by the user.

The Use Policy has been updated to include, "Officers "Shall" comply with DP 1.49 as we are already bound to comply with Department Policies and Procedures." Also added into the Use Policy regarding security information is the following, "If a non-police officer / unauthorized user was to find a body worn camera in the field, the person would not be able to view the footage without Axon's proprietary viewer application which has password protection.

The footage itself is encrypted on the device, providing an additional layer of security to prevent the footage from being viewed by an unauthorized user. There is a port on the base of the body worn camera which can be used to charge the device and download the camera when connected to a department charging dock in a secure police facility. The body cameras and the docking stations are both registered to the San Diego Police Department. The body worn camera videos cannot be uploaded using other agencies docks or vice versa. Given the encryption which exists on the device it is highly unlikely that an unauthorized user would be able to view the footage on the body worn camera. No such situation has happened in the 14 years the department has been using Axon body worn cameras."

2. What is the relation between evidence.com and the Axon cloud? Are they the same? Is it Axon who manages evidence.com and uploads the data to it? Who hosts evidence.com?

   Axon Evidence runs on top of the Azure Government Cloud but the application stack, security, monitoring, etc, is all provided and maintained by Axon. This includes all compliance and certification. Axon does not rely solely on the underlying cloud infrastructure for monitoring and compliance. Along with the cloud infrastructure that Axon already have in place they use other tools including hardware and/or software systems to monitor and ensure rules and policies are in place.

   In any case, Axon will have full access to all the information, which is a concern. They could in principle run AI on the data and either use the results themselves or provide them to third parties. Are there any policies limiting this? Please document in the Use Policy.

   This is covered by the master services agreement. All data is owned by the customer and Axon is simply the custodian of that data. All administrator functions are monitored and managed per that policy and are compliant with CJIS and/or the appropriate policies and standards.

3. Similar to SSLs/ALPRs, is Axon using AWS with self-managed keys and the communications are SSL secured? Or is information on some proprietary Axon cloud?

Axon Evidence is hosted in the Microsoft Azure Government Cloud. All encryption keys are managed by Axon.

4. Explanation of how the Axon View app allows playback before storage. (It's unclear how this works technically if the information is not stored.)

   View simply operates as a viewer. It's the equivalent of a computer monitor connected to a PC. The video is not stored on the mobile device. To play video from an Axon camera, Axon View relies on the mobile device to pair with the Axon camera using Bluetooth technology. Viewing a paired Axon Camera's recorded video from Axon View does not store data on the mobile device. The mobile device can only view videos currently stored on the paired Axon camera. You cannot use Axon View or the mobile device to delete or alter original video files on the Axon camera.

5. Please update the use policy to describe details about sensitive locations and sensitive individuals, particularly in healthcare settings, in privacy spaces, and with minors and DV victims.

   The Office of the City Auditor conducted an extensive audit of the San Diego Police Department's BWC program. The audit was completed in July 2022. In response to the audit the Department has extensively re-written its body worn camera policy. Details pertaining to sensitive locations and individuals are addressed in the draft DP 1.49 Section V.N. and V.P.7. However, this draft policy has not been approved by the Office of the City Auditor. After the Office of the City Auditor has approved the draft policy, the policy must then be vetted through the Police Officers Association in the meet and confer process. The draft policy is currently with the Office of the City Auditor, awaiting final approval.

   The Department can state in the Body Worn Camera Use Policy that officers "shall" comply with DP 1.49 to ensure optimal compliance. Department policies are modified as needed to keep up with changes in best practices, vendors, and changes in the law. Having the Use Policy for BWCs reference the current DP 1.49 ensures officers are complying with the document and practices which have been approved by the Office of the City Auditor, the Department, and our Police Officers Association.

   It is important for the PAB to understand that all officers on the Department are bound to obey all Department policies and procedures. This directive is made clear as that <u>first</u> procedure of the Department's Administrative Procedures – Department Policy 1.01 DEPARTMENT POLICIES, PROCEDURES, ORDERS, COMMUNICATIONS AND CORRESPONDENCE (Revised 11/04/08). It states: Department directives (e.g., Legal Updates, Orders, Policies, Procedures and Training Bulletins) are written directives that convey the same authority. All members of the Department will be held responsible for abiding by the information contained in Legal Updates, Orders, Policies, Procedures and Training Bulletins. All members shall access Department directives via

the Resource Library on the LAN or Automated Field Reporting (AFR) systems in accordance with Department Procedure 1.01.

Department member compliance with procedures can be enforced with administrative sanctions. Thus, there is already a mechanism in place to ensure compliance. It is duplicative and unnecessary to memorialize specific items in a Use Policy. Having the Use Policy simply state officers "shall" comply with DP 1.49 will be adequate to ensure there is a "sanction" officers can face for failure to comply with DP 1.49.

6. Explanation of why all 1850 people need access to view videos

   Most police officers who work in a uniformed assignment (Patrol, K9 etc.) only have access to their own videos. This is to assist them with report writing and testifying in court. Only supervisors and investigators have access to other officers' videos. Investigators need access to assist in criminal investigations. Supervisors have access to other videos to investigate complaints.

7. Please update retention schedule in use policy to explain detective discretion, as discussed in PAB meeting.

   
   Category Retention Schedule 53123.xlsx

   The updated retention schedule has had no changes since last updated. Investigators do not have discretion on how long the files are retained. If an investigator places the files into a case in evidence.com to share with the City Attorney or District Attorney, those files no longer follow the retention schedule and are saved indefinitely.

8. Is there an (external to PD) Audits/Inspections Unit and can it be utilized to provide oversight?

   Yes. The Office of the City Auditor conducted an extensive audit of the San Diego Police Department's BWC program. The audit was completed in July 2022. The audit had four findings:

   1. Officers likely did not record many enforcement encounters, as required.
   2. In many cases, officers did not appear to record the entire incident, as required.
   3. Officers generally categorized videos correctly, but some changes would minimize the risk of deleting videos too soon.
   4. SDPD does not have a detailed policy on when it releases body camera video, creating confusion among the public and City Council.

   Given the auditor's findings, they recommended the following:

Privacy Advisory Board Questions Received August 22, 2023

1. The San Diego Police Department (SDPD) should amend its body camera procedure to require officers to turn on event mode to record body camera videos for all dispatched events and calls for service, including all incidents directed or self-initiated. SDPD should train all body camera users and supervisors on the new requirement. This recommendation would not impact SDPD's current procedure that requires officers to begin recording while driving to a call and prior to actual contact with a member of the public. Additionally, this recommendation should only impact calls for service and dispatched calls. Therefore, SDPD could keep its current procedure that allows officers to not record suspect interviews if the suspect declines to make a statement due to the body camera being activated and the SDPD procedure that prohibits recordings during contact with confidential informants.

   The Department responded: Agree. SDPD will add draft language to its existing BWC procedure from this recommendation and present it to the SDPOA in the meet and confer process. If agreement is reached, all Department members would be trained in accordance with the updated procedure. Target Implementation Date: July 2023

2. The San Diego Police Department (SDPD) should update the section in Procedure 1.49 related to supervisor reviews of officer videos to ensure supervisors confirm there is a body camera video for all dispatched events for each officer for days selected in the monthly review. SDPD should train all supervisors on the new requirement. This recommendation would not require supervisors to watch additional videos.

   The Department responded: Agree. SDPD will add draft language to its existing BWC procedure from this recommendation and present it to the SDPOA in the meet and confer process. If agreement is reached, all Department members would be trained in accordance with the updated procedure. Target Implementation Date: July 2023

3. The San Diego Police Department (SDPD) should clarify in Procedure 1.49 specifically when officers can stop recording an incident with their body camera. The procedure should clarify the definition of the conclusion of an incident and include examples. SDPD should communicate this procedural update in a department-wide training. (Priority 2)

   The Department responded: Agree. SDPD will add draft language to its existing BWC procedure from this recommendation and present it to the SDPOA in the meet and confer process. If agreement is reached, all Department members would be trained in accordance with the updated procedure. Target Implementation Date: July 2023

4. The San Diego Police Department (SDPD) should add to the sergeant reviews section of Procedure 1.49 to require that supervisor reviews include reviewing the end of body camera videos to confirm compliance with procedure. This recommendation would not require supervisors to review additional videos beyond the monthly review process already in place. SDPD should communicate this procedural update in a department-wide training.

> **The Department Responded: Agree.** SDPD will add draft language to its existing BWC procedure from this recommendation and present it to the SDPOA in the meet and confer process. If agreement is reached, all Department members would be trained in accordance with the updated procedure. Target Implementation Date: July 2023
>
> In response to the audit, the Department extensively re-wrote its body worn camera policy, D.P. 1.49. The draft policy was provided to the auditor in July of 2023. We are waiting for a final response from the Office of the City Auditor.

An audit program should, at minimum, include:

- There are clear documented policies and procedures to be followed.

Department Procedure 1.49 has been updated after an audit of the BWC program by the Office of the City Auditor.

- Person doing the audit/inspection is independent of the officer you are inspecting.

Body worn camera inspections are currently conducted by supervisors. They are also conducted by supervisors in the draft updated procedure (DP 1.49 (Section XII.A.)). Supervisors are independent of their employees by virtue of their rank. Supervisors need to be tasked with the conduct of their own employees as they are best suited to see behavior which is outside of the norm for the employee or identify trends in a particular officer's behavior. Having supervisors other than direct supervisors review their officers' footage would be disruptive to the functioning of the work units in the Department. There are other independent bodies which review BWC footage. Detectives are tasked with review of the BWC footage which is part of their investigative package submitted to the City or District Attorney's offices. They are tasked with a duty to report misconduct if they locate any. Internal Affairs will review body worn camera footage of the officers whenever they review the appropriateness of the officer's conduct during internal investigations. The Commission on Police Practices is an independent oversight body. They review the BWC footage which is part of their oversight of officer activities. The State Department of Justice is an independent oversight body.

- There is some planned and formal inspection scope/sample size of camera use or non-use. A sample size will then be able to infer the accuracy of the overall population.

A comprehensive inspection of the body worn camera program was conducted by the Office of the City Auditor. Their recommendations have guided a broad re-write of D.P. 1.49.

- Findings are not documented away as "one-offs" and explained away as not a problem. It must be extracted to the population and understood.

A comprehensive inspection of the body worn camera program was conducted by the Office of the City Auditor. Their recommendations have guided a broad re-write of D.P. 1.49. An update

to the BWC procedure addresses review of "accidental" recordings. (Section XI.A.8 requires review of "accidental" recordings).

- Findings are tracked and analyzed regularly for trends and "root cause" to be fixed.

A comprehensive inspection of the body worn camera program was conducted by the Office of the City Auditor. Their recommendations have guided a broad re-write of D.P. 1.49. Trends are already discussed Department wide. Internal Affairs routinely briefs the Chiefs on trends seen in the use of BWCs. These trends are discussed, when they are discovered, at the weekly Operations Meeting. Reminders are given to commanding officers to give appropriate guidance / reminders to officers about what is required under the BWC policy.

- Officers who have findings/exceptions from the policies are held accountable.

All officers are responsible to comply with Department Policies and Procedures. Failure to comply with DP 1.49 will result in discipline as written and as amended in the draft DP 1.49. There are escalating penalties associated with repeated non-compliance. This is in line with the Department's progressive discipline model.

9. Please provide an explanation of the buffer period and when and how a camera is then turned on from the buffer position.

   When the camera is on and not recording, it is in buffering mode. When an officer double taps the event button in the middle of the camera, the camera then starts recording video and audio. The camera will also record two minutes of video without audio prior to when the officer put the camera into event mode.

10. When are the OCA recommendations addressed?

    The OCA recommendations were addressed and sent back to the OCA on June 9, 2023, for a final review. The Department is awaiting a final response from the Office of the City Auditor.

11. Has OCA reviewed and agreed to changes/responses?

    The SDPD has tentative approval of the changes to DP 1.49 from the OCA. We are waiting for formal approval.

12. What agencies have subpoena-based access, under what conditions data will be shared, and to what extent?

    Only SDPD officers have access to our Evidence.com account. Other agencies can only view our files if they are shared with them by an SDPD officer. Files are shared with the City Attorney and District Attorney for criminal prosecutions. Files are shared by SDPD officers with other agencies to assist with criminal investigations. Any agency can request access to these videos for the purposes of a criminal investigation.

Privacy Advisory Board Questions Received August 22, 2023

13. Is there any AI run on stored BWC videos, and is there any plan to do so?

    No.

14. Under what conditions can an officer use discretion to turn the camera off?

    The rules governing when an officer can “turn off” their BWC are covered in DP 1.49 (V.J.8). These rules are expanded upon in draft DP 1.49 (V.I.K.a.1-5). We are waiting for approval of the draft policy from the Office of the City Auditor.

    Can an officer, on request, turn off their BWC and offer an off-the-record conversation?

    If, during a suspect interview, the suspect will not speak while being recorded, an officer or investigator could stop recording. This is contained in DP 1.49 and is also contained in the draft DP 1.49.