**STAFF REPORT**

**DATE:** July 10, 2018

**TO:** City Council

**FROM:** Darren Pytel, Police Chief

**SUBJECT:** Surveillance Technology – Covert Personal Recording Devices

---

**Recommendation**

Informational. The Police Department is submitting this informational staff report on consent calendar at least 30 days prior to asking the City Council to hold a public hearing to continue using covert personal recording devices. This informational staff report has been posted on the City website with the City Council agenda (26.07.030 (c) Davis Municipal Code (DMC)).

**Fiscal Impact**

There is no fiscal impact to this report. If Council provides direction, future actions could have fiscal impacts.

**Council Goal(s)**

Goal 7 - Ensure a Safe and Health Community. This item is not called out as a specific task.

**Background and Analysis**

A City department seeking approval to acquire/use surveillance technology as defined by 26.07.020 DMC shall submit to the City Council a Surveillance Impact Report and a proposed Surveillance Use Policy via an informational staff report on a regular City Council meeting consent calendar at least thirty (30) days prior to the public hearing required under 26.07.030 (a). The informational staff report shall be posted on the City website with the City Council agenda. This staff report is being is submitted to fulfill the notice requirements.

**Surveillance Impact Report**

Information describing the surveillance technology and how it works, including product descriptions from manufacturers;

**(a) Information on the proposed purpose(s) for the surveillance technology:**

Covert Personal Recording Devices come in various forms, including hidden microphones attached directly to an individual's body; items within an individual's possession designed to function as a recording device, such as clothing or eyeglasses; and/or items within an individual's immediate control that contain covert recording devices, such as a cell phone, coffee cup or various other common personal possessions. Covert recording devices are used by peace officers or individuals who are considered their agents while conducting a law enforcement investigation.

**(b) If applicable, the location(s) it may be deployed and crime statistics for any location(s);** Covert Personal Recording Devices are generally deployed with an individual, either on their person or nearby within their control.

**(c) An assessment identifying any potential impact on civil liberties and civil rights and discussing any plans to safeguard the rights of the public;** Covert Personal Recording Devices are used by law enforcement to surreptitiously record statements made by individuals who are suspected of criminal activity. California law allows law enforcement to record individuals without their knowledge if they are the focus of a criminal investigation.

**(d) The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding;**

Initial Purchase Cost
Range $1,000 to $6,000 depending on type of device (already purchased)

Personnel Costs
No extra costs

Ongoing Costs
None

Potential Sources of Funding
Regular police department operational budget

**(e) Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis;** Data gathered by some types of Covert Listening Devices are stored on a vendor's secured server. Users can access their accounts through password and generate reports, which can be obtained for a case investigation. Other devices record directly into a recording device possessed by investigators and are retained without third party storage.

**(f) A summary of the experience, if any, other governmental entities have had with the proposed technology, including information about the effectiveness, any known adverse information about the technology such as unanticipated costs, failures, civil rights or civil liberties abuses.**
Covert Personal Listening Devices are common law enforcement tools that are effective at gathering information during criminal investigations. These devices can be placed on an individual's body, placed in clothing worn by an individual, or placed in an object in possession of the individual. The device can either be deployed by a peace officer or an individual who is being directed by that officer in the course of a criminal investigation. The devices allow law enforcement to eavesdrop on the conversations of suspected law breakers. The technology these devices utilize is the same used by standard digital recording devices or video recording devices. What sets them apart is their covert nature. California law allows law enforcement to record individuals without their knowledge if they are the focus of a criminal investigation.

**Surveillance Use Policy**

Council must adopt a policy at a regularly scheduled City Council meeting for use of the surveillance technology that at a minimum specifies the following:

**(a) Purpose: The specific purpose(s) that the surveillance technology item is intended to advance.**

Improve public safety by providing an effective method of investigating criminal activity.

**Authorized Use: The uses that are authorized, and the rules and processes required prior to such use.**

Personal Covert Recording Devices will be used for undercover operations during criminal investigations. Covert Personal Recording Devices will be used or monitored by sworn peace officers. Use of the devices must be authorized by a supervisor or manager.

Equipment shall not be used in an unequal or discriminatory manner and shall not target protected individual characteristics including, but not limited to race, ethnicity, national origin, religion, disability, gender or sexual orientation.

Equipment shall not be used to harass, intimidate or discriminate against any individual or group.

**(b) Data Collection: The information that can be collected by the surveillance technology, including "open source" data.**

Covert Personal Recording Devices record voice conversations or video images. The data is not open source and is stored on a vendor secure server.

**(c) Data Access: The category of individual who can access or use the collected information, and the rules and processes required prior to access or use of the information.**

The information will be accessed by law enforcement officers during an investigation and court process. If the information is included as evidence in a criminal case, the information will be accessed by the prosecuting attorney and the defense attorney through the discovery process.

All downloaded media shall be stored in a secure area with access restricted to authorized persons. A recording needed as evidence shall be copied to a suitable medium and booked into evidence in accordance with established evidence procedures. All actions taken with respect to retention of media shall be appropriately documented.

**(d) Data Protection: The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms. Nothing in this subsection shall be construed to require the disclosure of information that could reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of the City.**

Information gathered by Covert Personal Recording Devices can be stored in one of two ways. Devices that are simply recording to a receiver that is controlled by the investigating

officer, is generally stored on the device and then downloaded onto a secure police evidence server. Devices that require vendor support generally keep information stored on the vendors secure servers.

All downloaded and retained media shall be treated in the same manner as other evidence. Media shall be accessed, maintained, stored and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements. Electronic trails, including encryption, digital masking of innocent or uninvolved individuals to preserve anonymity, authenticity certificates and date and time stamping, shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.

**(e) 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.**

The type of video surveillance technology employed and the manner in which recordings are used and stored will affect retention periods. The recordings should be stored and retained in accordance with the established records retention schedule and for a minimum of one year. If recordings are evidence in any claim filed or any pending litigation, they shall be preserved until pending litigation is resolved.

Any recordings needed as evidence in a criminal or civil proceeding shall be copied to a suitable medium and booked into evidence in accordance with current evidence procedures.

**(f) Public Access: How collected information can be accessed or used by members of the public, including criminal defendants.**

Members of the public do not have access to this information when it is gathered as part of a criminal investigation.

**(g) Third Party Data Sharing: If and how other City 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.**

Information gathered by Covert Personal Recording Devices may be shared with other law enforcement agencies who are involved in a joint investigation, or who are conducting their own investigations. Covert Personal Recording Devices can also be shared with various prosecutors' offices, including District Attorney's, State Attorney or United States Attorney. Data may also be shared with defense attorneys through the discovery process when they are evidence.

**(h) Training: The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology.**

All department members authorized to operate or video shall receive appropriate training. Training should include guidance on the use of cameras, interaction with dispatch and patrol operations and a review regarding relevant policies and procedures, including this policy.

Training should also address state and federal law related to the use of video surveillance equipment and privacy.

**(i) 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 record keeping 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.**

Covert Personal Recording Devices must be authorized by a police sergeant, Lieutenant or other sworn administrator. Use of these devices for criminal investigations is documented in police report. Devices are stored at the police department or other law enforcement facility while not in use. A member is subject to discipline for unauthorized use or misuse.

The Police Chief or the authorized designee will conduct an annual review of the public safety video surveillance system. The review should include an analysis of the cost, benefit and effectiveness of the system, including any public safety issues that were effectively addressed or any significant prosecutions that resulted, and any systemic operational or administrative issues that were identified, including those related to training, discipline or policy.

The results of each review shall be appropriately documented and maintained by the Police Chief or the authorized designee and other applicable advisory bodies. Any recommendations for training or policy should be promptly addressed.