DATE: July 13, 2021

TO: Mayor and City Council

FROM: CIO/Director of Information Technology

SUBJECT: Informational Report on Data Transparency and Protection for Police Records

RECOMMENDATION

That Council accepts this informational report and provides further comments on data transparency and protection for police records this report.

SUMMARY

The City of Hayward protects both City and resident data in numerous ways, especially for its police records. The Police Department, Information Technology Department, and City Attorney's Office work in conjunction to protect resident and employee data in three primary areas: information technology data security; legal review of vendor contracts; and third-party data protection. This report will provide details surrounding these three focus areas.

BACKGROUND

Through the provision of police services and operations, records are generated and stored, which must be protected for data privacy. To achieve the goal of data protection and privacy, the systems that hold this data must adhere to strict public safety standards and protocols on data transit, storage, and retention. The Police Department, Information Technology Department, and the City Attorney's Office all play a role in the enforcement and implementation of security standards, protocols, and practices of this area of responsibility. The discussion section of this staff report provides an overview of data security, a summary of language that goes under legal review in vendor contracts, and an outline of third-party data protections, which protect City and resident data contained in police records.

DISCUSSION

Information Technology Data Security

Information technology data security goes beyond the software programs or hardware protections in place to protect data. It also encompasses standards and procedures that are required to be followed in order to store data. The Commission on Accreditation for Law Enforcement Agencies (CALEA) as well as the FBI Criminal Justice Information Services (CJIS) Division provide guidelines and requirements for data collection, use, protection, and sharing. The City also follows an established data retention schedule set forth by the City Clerk's office for information technology records. These three elements combine to ensure information technology data is housed, used, and disposed of securely.

CALEA Public Safety Policies

Established public safety policies for the collection, use, and sharing of data are in play to protect and outline the use of data. For example, the Hayward Police Department utilizes an internal process to compare and validate their policies against constantly updated professional standards from the CALEA. Hayward Police Department successfully completed its most recent reaccreditation in March 2021, which demonstrates their adherence to an established set of professional standards and includes an external, objective evaluation of departmental operations. CALEA accreditation is recognized internationally as the gold standard for law enforcement accrediatation. The accreditation process helps to ensure that law enforcement policies and procedures stay up to date as information and procedures evolve. Additional information on the Hayward Police Department's CALEA certification, including reports, is publicly available on the City's website[1].

CJIS Data Protection Elements

The Hayward Police Department must meet specific data security requirements of the FBI CJIS Division in order to maintain compliance to retain and utilize public safety technology records. The CJIS Security Policy provides a set of specific security requirements to protect and safeguard Criminal Justice Information (CJI) used by law enforcement. There are 13 Policy areas of the CJIS Security Policy that cover a range of requirements including security training, personnel and physical security, and data protection and integrity.

To strengthen the City's data security footprint, general best practices for secure access are applied when possible and available from the vendor community. A local example of this in action is the Police Department's use of Evidence.com for its body worn camera program. Axon has been certified by CJIS to store data in the cloud, which must follow the data security standards outlined by the CJIS Security Policy. Below is an example of how Axon adheres to the Core Cloud Requirements as defined by the CJIS Security Policy.

Examples of Core Cloud Requirements as defined by the CJIS Security Policy include:

a. Adhere to CJIS security policy 5.8 standards: Media Protection which covers media storage, access, transport, sanitation, and disposal.
b. Encryption of data at rest and in transit
c. Data Redundancy

[1] **HPD Policies and CALEA | City of Hayward - Official website (hayward-ca.gov)**

d. Limited and Controlled Access

Data Retention

Data record management and retention is a key element of Police Department data. Due to its importance in the organization, the Police Department employs a Records Manager, who serves as the primary data steward for police records. To further govern the City's documents of record, the City Clerk's office maintains a Data Retention Policy. These Departments work in collaboration to define, update, and adhere to the standards in this area. The City's current data retention policy is publicly available on the City's website.

Legal Review of Vendor Contracts

The City Attorney's Office, in conjunciton with the Information Technology Department, plays a critical role in establishing the guidelines for data protection and security with the vendors the City utilizes for services. Each contract is reviewed and negotiated, including key elements of data privacy and security.

Data Privacy, Ownership, and Audit Rights

Whenever the City contracts with an outside company for services, the City can negotiate the terms of a contract to a degree. For instance, in previous contracts with Axon, who provides the body worn camera devices for the Police Department, a "privacy" clause in the contract indicates that Axon cannot disclose agency content or information "except as compelled by a court or administrative body or required by law or regulation," and that Axon must provide notice to the agency if disclosure is provided, so that an objection can be filed. This clause also limits Axon's "access to certain information from Agency" to performing troubleshooting services upon request or conducting an evaluation of the system.

Additionally, the City's standard contracts include an "Assignment" Clause, indicating that the company providing services cannot assign others to perform its scope of work. In addition, contractual terms can be added to include non-disclosure agreements, prohibiting a service company from disclosing, transferring, or selling information it receives while operating for the City, without City approval.

Finally, the City has, on numerous occasions, negotiated with service companies regarding the retention of ownership rights and the ability to audit. Standard language for retaining ownership of data could indicate the following:

> *Subject to the rights granted in this agreement, the City of Hayward and its licensors retain all right, title, and interest in and to the data and information obtained via the use of technology and Contractor acknowledges that it neither owns nor acquires any additional rights in and to the foregoing not expressly granted by this Agreement.*

Standard language for a right-to-audit clause could indicate the following:

The City of Hayward may conduct an audit of Contractor's financial, performance, and compliance records maintained in connection with the operations and services performed under this Contract. In the event of such audit, Contractor agrees to provide the City with reasonable access to Contractor's employees and make all such financial, performance and compliance records available to the City.

Personal Data Protections

To protect personal data, the City's contracts that concern retention of personal information include a "privacy" clause that limits the ability of the public to view certain items. For example, in the City's contract with Axon for Body Worn Cameras, the City included language that prohibits Axon from disclosing information to anyone, unless ordered to do so by a court or administrative body, or disclosure of the information is otherwise required by law (for instance if a Public Records Act request is made). As such, access will generally be limited to Hayward law enforcement, unless the City is ordered otherwise or the City has a legal duty to release the data.

Cloud-Hosted Data Security

In addition, the City's contracts with vendors can include clauses that ensure our vendors have proper protections in place to secure data, especially when this data is hosted in the cloud. Two examples of this are below:

Axon contract Section 4 – Security:

4 **Security**. Axon will implement commercially reasonable and appropriate measures to secure Agency Content against accidental or unlawful loss, access or disclosure. Axon will maintain a comprehensive information security program to protect Axon Cloud Services and Agency Content including logical, physical access, vulnerability, risk, and configuration management; incident monitoring and response; encryption of uploaded digital evidence; security education; and data protection. Axon agrees to the Federal Bureau of Investigation Criminal Justice Information Services Security Addendum.

Energov contract Sections 6.9 and 6.10:

6.9 Tyler data centers are accessible only by authorized personnel with a unique key entry. All other visitors to Tyler data centers must be signed in and accompanied by authorized personnel. Entry attempts to the data center are regularly audited by internal staff and external auditors to ensure no unauthorized access.

6.10 Where applicable with respect to our applications that take or process card payment data, we are responsible for the security of cardholder data that we possess, including functions relating to storing, processing, and transmitting of the cardholder data and affirm that, as of the Effective Date, we comply with applicable requirements to be considered PCI DSS compliant and have performed the necessary steps to validate compliance with the PCI DSS. We agree to supply the current status of our PCI DSS compliance program in the form of an official Attestation of Compliance, which can be found at https://www.tylertech.com/about-us/compliance, and in the event of any change in our status, will comply with applicable notice requirements. Should the requirements of compliance change, we will make all commercially reasonable efforts to reaffirm and remain in compliance.

Data Sharing with Other Agencies

It is the City's practice to protect the privacy rights of its residents, while also recognizing that the sharing of information between law enforcement agencies can be very beneficial to public safety. In reviewing information requests from other agencies, the City, to the best of its ability, restricts access to private information of its residents. The City works with information requestors to find alternative solutions, narrow down broad requests, and only release the information necessary for the purpose of protecting public safety. Nevertheless, given the legal requirements of disclosure of records, as set forth in the Public Records Act, SB 1421, and AB 748, the City is sometimes limited in its ability to restrict disclosure of surveillance type data (body worn camera footage, statistical data, etc.) unless there are grounds for objecting to the request or the material requested is exempt from disclosure.

Third-Party Data Protections

The City has the ability to negotiate a separate Non-Disclosure Agreement, or to include a Non-Disclosure Agreement clause in a contract, which would prohibit the sharing or sale of data by third parties without the City's consent. Below are two examples as to how data ownership are addressed in contract form. With these clauses in place, the City would have legal recourse to pursue action should these clauses be violated.

Section 3 – Agency Owns Agency Content of the Axon Contract, is an example of contract language which states the City is the owner of the data.

> 3 **Agency Owns Agency Content**. Agency controls and owns all right, title, and interest in Agency Content. Except as outlined herein, Axon obtains no interest in Agency Content, and Agency Content are not business records of Axon. Agency is solely responsible for uploading, sharing, managing, and deleting Agency Content. Axon will have limited access to Agency Content solely for providing and supporting Axon Cloud Services to Agency and Agency end users.

There is a Use of Data clause in the Microsoft contract, which is an example of prohibiting the use of City data.

> Use of Data. Consultant shall not utilize any non-public City information it may receive by reason of this Contract, for pecuniary gain not contemplated by this Contract, regardless whether Consultant is or is not under contract at the time such gain is realized. City specific information contained in the report, survey, or other product developed by Consultant pursuant to this Contract is the property of City, and shall not be used in any manner by Consultant unless authorized in writing by City

FISCAL IMPACT

The applications and solutions in this item are currently being used by the City. This report is only to offer information, so there is no fiscal impact associated with it.

STRATEGIC ROADMAP

This agenda item is a routine operational item and does not relate to one of Council's Strategic Roadmap priorities.

NEXT STEPS

This report has focused on information technology data security, legal review of vendor contracts, and third-party data protections to provide information on how the City works to protect data records, especially police records. The City has analyzed what peers in this area are reporting on for data transparency and there is minimal information that is publicly available. Based on feedback from other municipalities, requests for this type of data must be embarked upon with caution due to data security risks. Cities that the City looks to emulate when it comes to generating reports in this area do not produce similar reports ad-hoc or annually. The City is continuing discussions with other cities about these topics with the understanding that data security and protection warrant caution and must be handled delicately. Staff is still working on an overarching policy document related to use of surveillance technology as has previously been requested by the CIC. This report has been presented to share current best practices for privacy and data security in order to move forward with the UAS program. IT staff will bring any feedback from Council on this report and further discussion of a broader surveillance policy at the next available Council Infrastructure Committee meeting to discuss in greater detail.

Prepared by: Nathaniel Roush, IT Manager

Recommended by: Adam Kostrzak, CIO / Director of Information Technology

Approved by:

Kelly McAdoo, City Manager