

INTRADEPARTMENTAL CORRESPONDENCE

August 19, 2026
1.10

TO: The Honorable Board of Police Commissioners

FROM: Chief of Police

SUBJECT: 2025 ANNUAL COMPREHENSIVE TECHNOLOGY REPORT

RECOMMENDED ACTION

It is recommended that the Board of Police Commissioners REVIEW and APPROVE the Los Angeles Police Department's (Department) 2025 Annual Comprehensive Technology Report (CTR).

DISCUSSION

In 2022, *Department Manual Section 1/140.15, Acquisition and Annual Reporting of Certain Information Systems and Technologies*, was established to monitor and evaluate the use of new systems and emerging technologies by the Department. For this policy, "technology" means systems, hardware, or software, including data aggregators, that are owned, licensed, used, or shared by or with the Department and can access non-public places or information, or that aggregates publicly available information that can reveal considerable personal information about individuals.

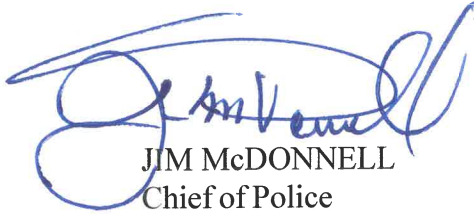
These technologies play a crucial role in equipping officers with investigative and enforcement tools to deter crime and provide evidence for investigation, improving the Department's performance in solving crimes and bringing those responsible to the criminal justice system. In addition, the established policy provides transparency and considers the potential impact on civil liberties and constitutional rights while implementing appropriate safeguards and oversight mechanisms to protect those rights.

The CTR records the applicable technologies that were implemented or were currently in use when the policy was established. It's important to note that the following technologies have specific Department policies governing their use, and they require comprehensive periodic audits that are reported to the Board of Police Commissioners.

- Automated License Plate Reader systems
- Photo Comparison Technology
- Small Unmanned Aerial Systems

Should you have any additional questions, please contact Commander Randy Goddard, Assistant Commanding Officer, Information Technology Bureau, at (213) 486-0370.

Respectfully,

A handwritten signature in blue ink, appearing to read "Jim McDonnell", is written over a large, stylized blue circular mark.

JIM McDONNELL
Chief of Police

Attachment

LOS ANGELES POLICE DEPARTMENT

2025 COMPREHENSIVE TECHNOLOGY REPORT



Completed by
INFORMATION TECHNOLOGY BUREAU

JIM McDONNELL
Chief of Police

August 19, 2026

TABLE OF CONTENTS

Comprehensive Technology Report
ITB

Page
No.

OVERVIEW	1
BACKGROUND	1
REPORTABLE TECHNOLOGIES	1
A. Automated License Plate Recognition (ALPR)	1
1. Technology Met the Expectations	3
2. Frequency of Use	3
3. Efficacy of the Technology	3
4. Personnel Compliance of All End Users	3
5. The Cost of the Technology and Cost-Benefits Analysis	4
6. Identified Concerns and Proposed Mitigations	5
7. Efficacy of the Existing Policy and Any Proposed Changes	5
8. Efficacy of the Training on the Existing Policy and Any Proposed Changes	6
Other Related Matters	6
Data Retention/Data Security	6
Privacy, Civil Rights, and Civil Liberties	6
Inspections/Audits	8
B. Whooster	9
1. Technology Met the Expectations	9
2. Frequency of Use	10
3. Efficacy of the Technology	10
4. Personnel Compliance of All End Users	10
5. The Cost of the Technology and Cost-Benefits Analysis	11
6. Identified Concerns and Proposed Mitigations	11
7. Efficacy of the Existing Policy and Any Proposed Changes	11
8. Efficacy of the Training on the Existing Policy and Any Proposed Changes	12
Other Related Matters	12
Data Retention	12
Data Security	12
Privacy, Civil Rights, and Civil Liberties	13
Inspections/Audits	14
C. Skopenow	15
1. Technology Met the Expectations	15
2. Frequency of Use	15
3. Efficacy of the Technology	16
4. Personnel Compliance of All End Users	16
5. The Cost of the Technology and Cost-Benefits Analysis	16
6. Identified Concerns and Proposed Mitigations	17

7. Efficacy of the Existing Policy and Any Proposed Changes	17
8. Efficacy of the Training on the Existing Policy and Any Proposed Changes	17
Other Related Matters	17
Data Retention	17
Data Security	18
Privacy, Civil Rights, and Civil Liberties	18
Inspections/Audits	19
D. Penlink Tangles (formerly known as Cobwebs Technologies)	20
1. Technology Met the Expectations	20
2. Frequency of Use	20
3. Efficacy of the Technology	21
4. Personnel Compliance of All End Users	21
5. The Cost of the Technology and Cost-Benefits Analysis	21
6. Identified Concerns and Proposed Mitigations	22
7. Efficacy of the Existing Policy and Any Proposed Changes	22
8. Efficacy of the Training on the Existing Policy and Any Proposed Changes	22
Other Related Matters	22
Data Retention	22
Data Security	23
Privacy, Civil Rights, and Civil Liberties	23
Inspections/Audits	24

COMPREHENSIVE TECHNOLOGY REPORT

Completed by
Innovation Management Section
2026

OVERVIEW

Technological advancements in law enforcement provide critical real-time information that supports criminal investigations. New and emerging technologies increasingly play a vital role in the daily tasks of sworn and civilian personnel, providing enforcement and investigative tools. These tools enhance officer effectiveness and help keep our communities safer. At the same time, these technologies may raise public concerns about the amount of data the Los Angeles Police Department (LAPD or Department) collects, stores, and uses.

BACKGROUND

The Department's mandate is to oversee the adoption, deployment, and use of technology to enhance community safety while safeguarding individuals' civil liberties and their reasonable expectations of privacy. Protecting data collected, stored, and used is crucial to ensure the effective and sustainable implementation of new technologies while maintaining public trust. This report is intended to comply with the requirements outlined in Special Order No. 11, Acquisition and Annual Reporting of Certain Information Systems and Technologies, dated August 2022, for reporting new technologies.

REPORTABLE TECHNOLOGIES

A. Automated License Plate Readers

Automated License Plate Readers (ALPR) use optical character recognition to read vehicle license plates and record the license plate photograph, vehicle location, and date and time. All of this data and its metadata are referred to as "ALPR data." This technology can scan license plates faster than human operators. Using computer algorithms, each scanned license plate is checked against crime databases. The ALPR alerts law enforcement officers if a "hit" occurs (e.g., a stolen vehicle, an AMBER alert, or an arrest warrant).¹

The Department is deploying two types of ALPR systems: mobile and fixed cameras. Mobile cameras are installed in police vehicles, trailers, and smartphones. Fixed cameras are placed at stationary locations. The ALPR system consists of the following three components:

- A camera that captures license plates within its field of view as well as the dates, times, and locations associated with the photos;
- Software that reads and converts images of license plates into data; and
- A searchable database that stores the data.

¹ A "hit" refers to a match between a license plate and a system alert tied to the specific license plate.

On January 22, 2022, the Department contracted with Vigilant Solutions (Vigilant), a subsidiary of Motorola Solutions, for mobile ALPR systems. In 2023, the Department upgraded the Axon Fleet 3 Digital In-Car Video System (DICVS) with an ALPR feature and began using Flock Safety's (Flock) user interface to view data from both Axon and Flock.

In 2025, Flock deployed 50 ALPR cameras in the Palisades Fire burn area to help prevent looting and burglaries. Additionally, the Los Angeles Police Foundation (LAPF) donated 63 Flock Safety fixed ALPR cameras to the Department.

- Vigilant

On January 22, 2022, the Department signed a contract with Vigilant to replace outdated cameras with new mobile ALPR systems. The contract is valid for five years and includes the installation of 28 mobile ALPR cameras per year, totaling 140 across all geographic areas and traffic divisions by the end of the contract in 2027. As of the end of 2025, 112 Vigilant mobile ALPR cameras have been installed on vehicles. Additionally, 100 Vigilant fixed ALPR cameras were installed in 2024, funded by Council District 12.

- Axon Enterprise, Fleet 3 DICVS, and ALPR

The Axon Fleet 3 DICV system offers many features, including ALPR. In November 2023, the Department activated the Fleet 3 ALPR feature. Currently, 1,500 Axon Fleet 3 mobile units have been installed.

- Flock Safety ALPR Data

Flock provides ALPR services to private subscribers. Subscribers include residential and commercial communities, such as individuals, homeowners' associations (HOAs), retail and wholesale businesses, shopping malls, business improvement districts (BIDs), and other entities. Flock owns and maintains the ALPR cameras, which it leases to subscribers.

On July 11, 2023, the Department and Flock signed a Memorandum of Understanding (MOU). The MOU authorizes the Department to access private subscribers' ALPR data for investigative purposes, in accordance with the Department's policies and the law.

For all ALPR cameras donated to the Department, for which the Department is now the "subscriber," the Department owns the data, which is stored in accordance with the Department's ALPR Policy.

In 2025, the LAPD had access to 99 fixed Flock ALPR cameras inside the city of Los Angeles.

This section was intentionally left blank

Findings

1. The Technology Met the Expectations of the Presentation to the Board of Police Commissioners and the Department when the Technology was Obtained

This technology helps field officers identify and locate specific vehicles wanted in connection with felony crimes, stolen vehicles, and other ongoing criminal investigations. It also assists officers in finding critical missing or endangered persons when the associated license plate is entered into a Department of Justice (DOJ) database (an AMBER alert). ALPR software references that database to populate a “hot list,” enabling Department personnel to locate these vehicles. Lastly, it allows investigators to use ALPR historical data to investigate vehicles linked to open cases.

In 2025, a total of 444,046 hits were recorded for real-time license plate scanning and data queries combined (see Findings Nos. 2 and 3). The inspection was conducted across two databases – Vigilant and Flock. All Flock cameras are fixed, resulting in 27,164 hits; all Fleet 3 cameras are mobile, resulting in 233,321 hits. Vigilant hits were broken down into 4,724 mobile and 178,837 fixed.

Most hits involved felony crimes and stolen-vehicle matches. The ALPR system has proven to be an invaluable tool for crime prevention and investigation because of its ability to provide real-time alerts and identify suspects.

2. Frequency of Use

In 2025, Department investigators conducted 765,736 ALPR data inquiries. The volume of inquiries highlights the value of the ALPR system as a vital tool in follow-up investigations involving missing, at-risk, or wanted persons who are using a vehicle.

3. Efficacy of the Technology

In 2025, ALPR cameras detected 1,092,434,536 license plates. Real-time scanning and data queries produced 444,046 hits. These hits were made possible by the efficiencies enabled by automation. The technology helps field officers identify and apprehend felony suspects, recover stolen vehicles, conduct criminal investigations, and locate missing or endangered people. It equips officers with tools to do their jobs more effectively, ultimately enhancing the safety of our communities.

4. Personnel Compliance of All End-users

Special Order No. 31, dated December 10, 2020, established Department Manual Section 3/568.53, *Automated License Plate Recognition Usage and Privacy Policy*, to ensure that all activities involving the capture, use, retention, and dissemination of information obtained through the ALPR system comply with applicable Federal, State, and local laws.²

² See Special Order No. 7, *Automated License Plate Recognition Usage and Privacy Policy - Revised*, dated February 7, 2023.

The ALPR policy limits the use of the ALPR system. The ALPR data shall only be retained, accessed, and used for the following official Department purposes:

- Criminal investigations or proceedings;
- Public Safety Investigations (e.g. missing or endangered persons);
- Administrative investigations or proceedings;
- Civil litigation or proceedings;
- Situational awareness operations;³ and
- Responses to cognizable threats to public safety.

Per Department Policy:

All ALPR data recorded and/or retained by the Department shall not be sold, shared, transferred, or otherwise disclosed for commercial purposes or to any person or entity not authorized to record, retain, access, or use ALPR data. ALPR data shall be shared only with California State local law enforcement agencies that have an interagency agreement with the Department. All current and future contracts shall include a clause prohibiting the sharing of Department ALPR data with any entity outside the agencies with which the Department has an agreement.

Interagency agreements or Memoranda of Agreement (MOAs) must be approved and signed by the Chief of Police. Currently, the following 16 California Law Enforcement Agencies have an MOU with the LAPD.

Torrance Police Department
Huntington Park Police Department
Ceres Police Department
Haward Police Department
Signal Hill Police Department
Madera County Sheriff's Department
San Luis Obispo Sheriff's Department,
Rohnert Police Department

Alhambra Police Department
West Covina Police Department
Livermore Police Department
Oakdale Police Department
Simi Valley Police Department
La Mesa Police Department
Los Angeles Port Police
Glendale Police Department

5. The Cost of the Technology and Cost-Benefit Analysis

- Vigilant Solutions, Inc.

The current five-year Vigilant ALPR contract, signed in 2022, has an annual cost of \$407,000. It includes 140 mobile ALPR cameras, data migration from the replaced PIPS to Vigilant, access to the Vigilant system training application, the Law Enforcement Archival Reporting Network (LEARN), and 10,000 user licenses. In 2022, the Department also purchased 60 fixed-pole ALPR cameras and four ALPR camera trailers for \$800,000 over five years. Additionally, 100 fixed ALPR cameras have been installed, funded by Council District 12.

³ An example of a situational awareness operation is to support specific evolving or critical incidents, emergencies, or credible threats to public safety.

- Axon Enterprise, Fleet 3 DICVS ALPR

Fleet 3 ALPR is an add-on feature included in the current Axon contract. At present, the Information Technology Bureau (ITB) and Axon Enterprise are negotiating the final costs and service contract terms for Fleet 3 ALPR as part of the upcoming contract renewal in August 2026.

- Flock Safety ALPR Data Only

The Department does not have a procurement contract for fixed ALPR cameras, including no contract with Flock in 2025. Flock and the Department signed an MOU under which Flock provides the Department with ALPR data from private subscribers for lawful and legitimate investigations. The data is available to the Department at no cost. For the 63 Flock ALPR cameras donated by the Los Angeles Police Foundation, no general funds were used; the donation consisted of private funds the Foundation used to purchase the cameras.

6. Identified Concerns and Proposed Mitigations

ITB, in conjunction with the City Attorney's Office, is drafting a contract with Flock Safety. The contract between the LAPD and Flock Safety will serve as the governing legal instrument defining the rights, responsibilities, and limitations of both parties regarding LAPD-generated data collected and processed through the Flock automated license plate recognition system. The contract will expressly establish that all data captured or processed through LAPD's deployment of Flock technology remains the exclusive property of the LAPD. The agreement will include API integration to enable interoperability between the Flock platform and authorized third-party LAPD systems. Flock Safety is strictly prohibited from sharing, disclosing, or transferring any LAPD data to any individual or entity without the Department's express prior written authorization. Any inter-agency data sharing shall further require the execution of a formal Inter-Agency Agreement, signed by the Chief of Police from both LAPD and the requesting agency, before any data is transmitted or made accessible, in compliance with all State Laws and Department policies. The contract shall also mandate cybersecurity standards, audit rights, and breach-notification protocols to ensure the integrity and confidentiality of LAPD data throughout its lifecycle on the Flock platform. Currently, these standard provisions are included in the purchase agreements between the Los Angeles Police Foundation and Flock Safety for cameras that the Foundation donates to the LAPD.

7. Efficacy of the Existing Policy and Any Proposed Changes

A review of the Department's ALPR Usage and Privacy Policy found that the policy aligns with the United States Constitution, the Fourth Amendment, and other relevant statutory authorities.

This section was intentionally left blank

8. Efficacy of the Training on the Existing Policy and Any Proposed Changes

Two types of users are authorized to use the ALPR system: administrators and data users.

- System Administrators:

Administrators are assigned to ITB and hold the highest-level access rights to the ALPR system. They are responsible for verifying the system's proper operation and maintaining the ALPR server. They also assist with any reports of inoperability or malfunctions in ALPR-equipped vehicles.

- Training:

All administrators must complete Department-approved training to fulfill their job responsibilities before accessing the ALPR system. Any ALPR data user or system administrator who has not used their ALPR account for one year must complete a reorientation training course before accessing the system.

- ALPR Data Users:

Data Users are active Department employees who have completed the ALPR Department training and ITB permission to query the ALPR system.

- Training:

Employees shall complete online Learning Management System (LMS) training to query the ALPR system. Once they complete the required LMS training, the system administrator grants access to the ALPR query capability.

Note: Employees with ALPR cameras in their Department vehicles may get an ALPR hit alert and review it to find the wanted vehicle. Employees receiving the hit alert cannot query, add, remove, or change any information in the ALPR system.

Other Related Matters

Data Retention/Data Security

All collected license plate data is uploaded to a secure, fully Criminal Justice Information System (CJIS)-compliant cloud storage provided by authorized vendors. Access to this CJIS-compliant cloud storage is restricted to authorized Department personnel.

Privacy, Civil Rights, and Civil Liberties (P/CRCL)

- Potential Impact on Privacy and Civil Rights

The Department's ALPR cameras collect and record only information visible to the public. The system captures the license plate number, date, time, and location. It does not collect vehicle owner details, registration records, or personal information. Due to existing data storage security and access controls, there is minimal impact on P/CRCL. All ALPR data requests are logged, used only for specified purposes, and are subject to periodic inspections and audits to ensure appropriateness.

ALPR Technology and Protected Activities: Addressing Groups' Concerns

Public comment received during the Board's review period has included concerns that Automated License Plate Recognition (ALPR) technology may be used to surveil individuals seeking reproductive health care or gender-affirming medical treatment. The Department takes these concerns seriously and responds directly.

The LAPD is bound by California Laws Protecting These Activities

In the State of California, access to abortion services and gender-affirming care are expressly protected under state law. The California Legislature enacted AB 1242 (Chapter 626, Statutes of 2022), which prohibits California law enforcement agencies from cooperating with any out-of-state investigation or proceeding seeking to impose civil or criminal liability on any person for seeking, obtaining, or facilitating an abortion that is lawful in California. Similarly, SB 107 (Chapter 810, Statutes of 2022) extends equivalent protections to individuals seeking gender-affirming health care. The LAPD, as a California law enforcement agency, is legally bound by both statutes.

ALPR Technology Does Not Capture Intent, Destination, or Medical Information

ALPR systems record a license plate number, the geographic location of the read, and a timestamp. The technology has no capability to determine where a vehicle is traveling, the purpose of a trip, or any personal or medical information about the vehicle's occupants. A license plate read near a medical facility is indistinguishable in the ALPR dataset from a read near any other business, residence, or point of interest on the same street. The inferential leap required to weaponize ALPR data against a person seeking medical care would require deliberate investigative targeting, which California law expressly prohibits for these protected activities.

LAPD Policy Governs Authorized Use Cases

LAPD's use of ALPR technology is governed by Department Manual Section 3/568.53 and Special Order No. 7, dated February 2023, which define the authorized purposes for ALPR data access. Authorized use cases are limited to specific law enforcement functions, including locating stolen vehicles, identifying vehicles associated with violent crimes, and supporting Amber/Silver Alert activations. Access to ALPR data requires documented justification tied to an authorized use case. The investigative targeting of individuals for exercising rights protected under California law is not an authorized use case and would constitute a violation of Department policy, state law, and the California Constitution's explicit right to privacy (Article I, Section 1).

The Assertion of ALPR Technology Being Used to Infringe on a Woman's Right to an Abortion Is Legally and Technically Unwarranted in Los Angeles

Concerns raised by groups, while understandable in the context of national discourse regarding ALPR misuse in states where abortion or gender-affirming care has been restricted or criminalized, do not translate to the legal and operational environment of the Los Angeles Police Department. California's statutory protections, LAPD's governing policy framework, and the inherent technical limitations of ALPR data collectively foreclose the scenario that ALPR technology infringes on issues such as women's rights to obtain an abortion, as described in public comment. The Department is committed to transparent governance of this technology.

- Measures Currently in Place to Maintain Data Security

The data is stored in CJIS-compliant cloud storage. Access is restricted to authorized Department personnel who have completed the required ALPR Data Users training. Additionally, the system shall be accessed and used only for official Department purposes.

- Plan to Safeguard Privacy and Civil Rights

The Department defines authorized ALPR system use as listed on Page 3 – *Personnel Compliance for All End-users*. The Department requires only that the license plate be visible in public view and that no information that could significantly reveal personal details be collected or maintained. Additionally, ITB conducts routine inspections to verify that the ALPR system complies with laws and policies, including ensuring that ALPR data is not shared outside of California or with any federal agency.

- Public Access to the Data

The public cannot access ALPR data. However, they may request information from the Risk Management & Legal Affairs Division (RMLAD), Discovery Section, under the California Public Records Act (CPRA) and the Freedom of Information Act (FOIA), as permitted by law.

Inspections/Audits

- The Innovation Management Section conducts monthly system inspections to verify that accounts for users who are no longer with the Department have been deactivated. System administrators who are no longer assigned to ITB have their accounts deactivated accordingly. Additionally, IMS performs routine inspections to ensure the ALPR system is used in compliance with laws and policies, including making sure ALPR data is not shared outside the State of California or with any federal entities.
- Audit Division conducts periodic inspections and audits of the ALPR system to ensure the Department adheres to existing policies and procedures.

This section was intentionally left blank

B. Whooster

Whooster is an investigative database and software platform that uses search technology to access both publicly available information and private data sources (such as commercial data brokers) to gather details on persons of interest. This information includes names, phone numbers, addresses, and email addresses. End users use this data for criminal investigations. Whooster is not limited to law enforcement and is also accessible to private-sector businesses.

The Department used two types of Whooster services:

- Whooster Web UI – Deployable from a computer (laptop) via a secure web-based login.
- Whooster SMS/TEXT – Deployable from a cellular telephone and requires no data usage.

Whooster is an investigative force multiplier that helps identify connections among persons of interest in criminal investigations and their contact information. It also serves as a resource for locating people based on their self-reports or self-registrations. Department investigators are tasked daily with finding individuals (such as suspects, victims, witnesses, and missing persons), identifying and apprehending suspects, and serving search warrants on services used or subscribed to by persons of interest. Whooster Web and SMS end-users query Whooster's secure platform for target-specific information. This essential "first step" provides investigators with the most current information.

Findings:

1. The Technology Met the Expectations of the Presentation to the Board of Police Commissioners and the Department when the Technology was Obtained

Whooster enables investigators to quickly and remotely access accurate, up-to-date information, including people, addresses, phone numbers, and vehicles, related to active criminal investigations. It also helps investigators locate missing persons and victims, such as in kidnap-for-ransom cases. Investigators are provided with the technology and capabilities to conduct these queries efficiently, helping to advance their respective criminal investigations.

Best practices recommend that information come from multiple sources rather than a single source. This technology enables investigators to manually cross-reference data from Whooster's secure platform with other law enforcement systems already in use by the Department. Once the information is verified, investigators can request additional details from service providers through search warrants. This technology conforms to and supports the Department's current policies and procedures.

2. Frequency of Use

Two LAPD entities were identified as using this technology in 2025. One contract was held by Robbery-Homicide Division (RHD). A separate contract was also held by RHD's South Bureau Section.⁴

- a. Robbery-Homicide Division has used Whooster for crimes such as homicide (e.g., multiple murders, arson-related murder, attempted murder involving police officers, and cold cases), robbery (e.g., robbery series, home invasion, and bank robbery), and kidnapping for ransom. On a regular basis, Robbery-Homicide Division personnel assist other LAPD entities with their criminal investigations. For 2025, Robbery-Homicide Division conducted 11,993 queries using Whooster Web and 3,963 queries using Whooster SMS.
- b. Robbery-Homicide Division's South Bureau Section has primarily used Whooster for murder investigations. In 2025, South Bureau Section conducted 4,305 queries using Whooster SMS.

3. Efficacy of the Technology

This technology has been queried thousands of times in 2025 and has proven vital for quickly generating relevant investigative leads. These leads have led to the successful identification, location, and apprehension of numerous felony suspects. Whooster has been used in a wide variety of criminal investigations.

Whooster is best known for its remote access, current addresses, and telephone data. It allows investigators to cross-check and verify information obtained through Whooster against data from other technologies already used by the Department. Investigators have found this tool to be a valuable addition to their resources. Additionally, best practices recommend that actionable information should not come from a single source.

4. Personnel Compliance of All End-users

Whooster Web and Whooster SMS have been provided to a limited number of personnel with access to ongoing training, user manuals, and usage standards. Whooster is used during the course and scope of the end-user's assignment for criminal investigations, in accordance with "right to know" and "need to know" standards.

Whooster's secure CJIS compliant servers store all end-user activity, including the date and time of searches, the content queried, and corresponding case numbers. The Department's search history information cannot be edited or removed from Whooster's platform. Whooster provides administrators with access to audit all search inquiries conducted by assigned end-users. An annual inspection is conducted to

⁴ As part of the Department's reorganization in August 2025, South Bureau Homicide Division, which had been a separate command, was made a section, under RHD.

ensure all end-users comply with Department policies and procedures. The designated administrators will perform the inspection, and the respective lieutenant and commanding officer will review the results. Additional periodic and targeted inspections may be conducted as necessary.

5. The Cost of the Technology and Cost-Benefit Analysis

Breakdown of cost for Fiscal Year 2025/2026:

Robbery-Homicide Division - \$26,671.83 (Whooster Web & Whooster SMS)

Robbery-Homicide Division's South Bureau Section - \$4,816.20 (Whooster SMS)

This technology can be accessed remotely, allowing investigators to query for new information at crime scenes. Funding for this technology was obtained through a grant from the Robbery-Homicide Division and from Los Angeles Police Department Information Technology Bureau funds (South Bureau Section). The cost of this technology is considerably offset by the time it saves investigators when gathering similar information through other resources. Ultimately, this saves the Department both time and money by reducing the travel time needed to access such information via a Departmental computer at a Departmental facility. This technology decreases investigative hours by providing relevant results quickly.

6. Identified Concerns and Proposed Mitigations

No concerns or proposed mitigations are indicated at this time.

Administrators have worked with Whooster and will continue to do so to identify, address, and resolve any concerns in the future (e.g., Federal or State law and Department policy changes).

7. Efficacy of the Existing Policy and Any Proposed Changes

Like other technologies and databases used by law enforcement, this system adheres to the “right to know” and “need to know” standards. Administrators require the entry of criminal case numbers for inquiries, which are later subject to audit or review.

The number of end-users is limited, and personnel are selected based on their assignment and need for the technology. End-users are informed of the designated administrator(s), that the system securely stores inquiries, and that their queries may be audited later.

This section was intentionally left blank

8. Efficacy of the Training on the Existing Policy and Any Proposed Changes

Whooster provides training during the initial “onboarding” process and offers ongoing training, resources, and support. Additionally, Whooster supplies a user guide and conducts weekly virtual training sessions. This technology is easy to use and has a short learning curve. End-users are also informed about their designated administrator(s). Administrators are primarily responsible for keeping end-users updated on any relevant changes to the technology, policy, and usage.

Other Related Matters

Data Retention

All cases involving queries of information through Whooster are investigative, with a criminal predicate and for legitimate law enforcement purposes. Data may be retained for ongoing investigations and criminal court proceedings. Data may be kept for extended periods due to the length of an open investigation and the duration of court proceedings. This aligns with Department policies and procedures, as well as all criminal court requirements, including discovery, court proceedings, and appellate processes. Data no longer needed for an investigation or court case will be properly disposed of in accordance with Department procedures and criminal court standards.

Data Security

All data is initially and exclusively stored on Whooster’s secure servers. End-users can access this information only through the designated applications (Whooster Web and Whooster SMS). End-users cannot add any information to Whooster’s platform without corresponding case numbers for any searches conducted.

Investigators may retain information in accordance with standardized data retention periods (see the data retention heading). Retained information is maintained in accordance with current Department standards. The Robbery-Homicide Division and its South Bureau Section operate within secure facilities in areas with secondary levels of restricted access.

Access to Whooster Web requires a password and Multi-Factor Authentication (MFA) to access Whooster data. Computers used to access the Whooster Web application are password-protected. Whooster SMS is used on cellular telephones that comply with the Department’s cellular telephone policy (e.g., password-protected). Whooster SMS also requires an active account for each cellular telephone number.

In addition, the designated cellular telephone number authorized to have a Whooster account must send an SMS message to a designated Whooster telephone number for any case number updates and inquiries.

Privacy, Civil Rights, and Civil Liberties (P/CRCL)

- Potential Impact on Privacy and Civil Rights

Whooster is a commercially available application used by private- and public-sector entities. No negative impacts or foreseen infringements on privacy and civil rights have been identified. Informational inquiries conducted by end-users via Whooster's platform involve investigatory cases with a criminal predicate. This is in accordance with Federal and State law and the Department's policies and procedures.

- Measures Currently in Place to Maintain Data Security

Whooster data is stored on Whooster's secure servers. Investigators (end-users) maintain extracted and stored data in accordance with Department policies and procedures, as well as any court-mandated requirements. Devices that access and query the Whooster platform are secured with passwords (Whooster Web and SMS) and MFA (Whooster Web). Investigators are familiar with technical safeguards, including encryption and other digital and physical safeguards. The Whooster system supports an audit process, providing additional protection.

- Plan to Safeguard Privacy and Civil Rights

The Department and designated end-users follow established best practices and standards to protect privacy, civil rights, and civil liberties (P/CRCL) while maintaining Operations Security (OPSEC). This includes administrators and technology coordinators who work with vendors and personnel on P/CRCL issues. Ongoing training between vendors and end-users also helps achieve this goal. Protocols for redacting information related to court cases prevent unnecessary and unwarranted public disclosure of data. In balancing situational awareness with First Amendment-protected activities, right-to-release protocols ensure that all relevant factors are reviewed.

- Public Access to the Data

While the Whooster platform isn't publicly accessible without license agreements, the raw data Whooster collects and maintains is mostly available to the public through manual search methods. Reports and discoveries from Whooster may remain confidential due to the nature of the investigation, court proceedings, and sealing orders. The public seeking Whooster-collected information can submit a request to the RMLAD Discovery Section in accordance with the CPRA and FOIA, as permitted by law.

This section was intentionally left blank

Inspections/Audits

A 2025 annual audit was completed to verify that all end-users complied with Department policies and procedures as outlined in Special Order No. 11, 2022. The audit was carried out by designated administrators. The respective lieutenant and commanding officer reviewed and approved the inspection. The methodology and results are stored at the Robbery-Homicide Division and are available for review. In addition to the annual inspection, periodic and targeted audits may be conducted on a case-by-case basis when necessary (Refer to Finding No. 4).

This section was intentionally left blank.

C. Skopenow

Skopenow is an advanced search engine that analyzes social media, the deep web, and the dark web to support investigations into individuals or businesses. Skopenow is not limited to law enforcement; it is also available to private-sector companies.

Skopenow is an investigative force multiplier that gathers and displays publicly available information. Because of the vast volume of data online—spread across various websites, applications, and services—it takes investigators significant time to search for, compile, and organize it. Additionally, traditional search engines like Google are not built for investigative use; they serve commercial purposes, including showing advertising. In contrast, Skopenow is designed to simplify the process of finding internet content related to a specific person involved in a criminal case, making it easier to interpret, document, and store in a format that can be easily found later. Once found, this content can open new investigative avenues, such as obtaining search warrants from service providers or exploring other investigative leads. Skopenow also saves time by capturing online content in a court-ready format.

Findings:

1. The Technology Met the Expectations of the Presentation to the Board of Police Commissioners and the Department when the Technology was Obtained

Skopenow is available to both public- and private-sector clients. It functions as a data processor that uses publicly available data from across the internet to generate a digital analytical report for each target-specific search related to a criminal case. Skopenow is not a database; the digital reports are based solely on public content. If content is made private, Skopenow does not retain that information. Additionally, users of Skopenow do not contribute any data to the system. Skopenow replaces the tedious and time-consuming task of investigators “hand searching” the internet by providing a search engine that aggregates relevant data into a report.

Skopenow has met the Department’s expectations by completing this task, saving many employee hours. It also quickly gathers relevant data that can be reviewed, vetted, and used to support an active criminal investigation. All end-user searches comply with a “right to know” and “need to know” basis.

2. Frequency of Use

For 2025, Robbery-Homicide Division was identified as using this technology. Robbery-Homicide Division (RHD) routinely assists other Department entities in criminal investigations when RHD determines that the request for the software’s use would apply to the criminal case.

This technology has been used in various cases and investigations, including but not limited to murder, attempted murder, kidnapping for ransom, and robbery. Robbery-Homicide Division has used Skopenow as an investigative force multiplier and has seen significant time savings. The usage level for the year 2025 was approximately 397 queries. In comparison, the number of individual queries to separate databases and websites would be much higher if an end-user (investigator) had to query and gather the same amount of information manually.

3. Efficacy of the Technology

Skopenow has been used in a wide variety of criminal investigations and cases. This technology has been queried hundreds of times in 2025 and has proven vital for quickly generating relevant investigative leads. These leads have resulted in the successful identification, location, and apprehension of numerous felony suspects.

Investigators have found this tool to be a valuable addition to other technologies. Skopenow is well known for quickly gathering and analyzing data and presenting it in a practical format. Best practices also specify that actionable information should not come from a single source. Skopenow enables investigators to cross-check and cross-reference information obtained through Skopenow with data from other technologies already used by the department.

4. Personnel Compliance of All End-Users

Skopenow enables the Department's administrator(s) to audit all search inquiries made by assigned end-users. Skopenow's servers record all end-user activity, including the date and time of searches, the content queried, and corresponding case numbers. End-users cannot modify or delete any logged activity (search history) from Skopenow's servers. Skopenow is assigned to a limited number of investigators in cases where its use is most relevant. It is used during the course of and within the scope of end-users' assignments for criminal investigations, in accordance with "right to know" and "need to know" standards.

An annual audit is conducted to ensure that all end-users comply with Department policies and procedures. The designated administrator(s) conduct the audit. The respective lieutenant and commanding officer review the audit results. Additionally, periodic and targeted audits may be conducted as needed.

5. The Cost of the Technology and Cost-Benefit Analysis

Robbery-Homicide Division's cost for Fiscal Year 2025/2026 is \$90,903.50.

Funding for this technology was obtained through a grant. The cost is significantly offset by the time it saves investigators when gathering similar information through other methods, such as "hand searching" the internet. This technology can be accessed remotely, allowing investigators to quickly query for new information at crime scenes. This fresh data is often very useful in advancing an investigation in its early stages. It also helps identify suspects

and victim accounts, as well as any connections between them, enabling the preservation of data from service providers that a suspect might later remove. Additionally, Skopenow reduces total employee work hours by providing relevant results promptly.

6. Identified Concerns and Proposed Mitigations

There are no concerns or suggested mitigations. Administrators have coordinated with the vendor to enable specific features, aligning this technology with Special Order No. 11, 2022, and current Department policies and procedures.

Administrators have collaborated with Skopenow and will continue to do so to identify, address, and resolve any concerns in the future (e.g., changes in Federal or State law and Department policy).

7. Efficacy of the Existing Policy and Any Proposed Changes

Like other technologies or databases used by law enforcement, this technology adheres to the “right to know” and “need to know” standards. Entering criminal case numbers along with inquiries is mandatory and subject to audit or inspection. The number of end-users is small, only 10, and personnel are selected based on their assignment and need to use the technology. End-users are informed of the designated administrators, that the system securely stores inquiries, and that their inquiries are later subject to audit.

8. Efficacy of the Training on the Existing Policy and Any Proposed Changes

Skopenow offers training during the initial onboarding process and provides ongoing training, resources, and support. It supplies a user guide and offers virtual training. This technology is easy to use, with a short learning curve. End-users are informed of their designated administrators, who are primarily responsible for updating end-users on any changes to the technology, policy, and usage.

Other Related Matters

Data Retention

All cases involving the query of information through Skopenow are investigatory, with a criminal predicate and legitimate law enforcement purposes. Data may be retained during ongoing investigations and criminal court proceedings. Data may be stored for extended periods due to the duration of open investigations and court cases. This aligns with Department policies and procedures, as well as all criminal court expectations, including discovery requirements, court proceedings, and appellate processes. Data no longer needed for an investigation or court case will be disposed of properly in accordance with Department procedures and criminal court standards.

Data Security

Skopenow does not maintain a database of information, nor do end-users contribute to any databases. If a person changes certain aspects of their “internet footprint” to “private,” Skopenow can no longer access the “private” information. The information is no longer available or stored.

Investigators may retain information according to standardized data retention periods (see the data retention heading). Retained information will be kept in accordance with current Department standards. The Robbery-Homicide Division operates within a secure facility with an additional restricted-access level. Personnel in the division are provided with locking desks and have access to storage cabinets as additional physical safeguards.

Computers used to access Skopenow’s web-based application or portal are password-protected desktop, laptop, or tablet devices. If a cellular phone is used to access Skopenow’s platform, the Department’s current cellular phone policy (such as password protection) applies.

Privacy, Civil Rights, and Civil Liberties (P/CRCL)

- Potential Impact on Privacy and Civil Rights

Skopenow is a commercially available application used by private and public sector entities. No negative impacts or expected infringements on privacy and civil rights have been identified. Informational inquiries made by end-users through Skopenow’s platform involve investigations with a criminal predicate. This complies with Federal and State law, as well as the Department’s policies and procedures.

- Measures Currently in Place to Maintain Data Security

Skopenow does not maintain a database. Investigators (end-users) store any extracted and saved data in accordance with Department policies, procedures, and court-mandated requirements. Devices used to access and query the Skopenow platform are password-protected. Facilities where printed records are stored are secured and inaccessible to unauthorized law enforcement or the public. Most investigators are familiar with digital safeguards, including encryption, and other physical and digital security measures. The Skopenow platform includes an audit process, providing an additional layer of protection.

- Plan to Safeguard Privacy and Civil Rights

The Department and assigned end-users have established best practices and standards to protect privacy, civil rights, and civil liberties (P/CRCL) while maintaining OPSEC. This includes administrators and technology coordinators who engage with vendors

and personnel on P/CRCL issues. Ongoing training between vendors and end-users also supports this goal. Protocols for redacting information related to court cases help prevent the unnecessary and unwarranted public release of data. Given the need for situational awareness and First Amendment rights, right-to-release protocols ensure that all relevant factors are considered.

- Public Access to the Data

Although the Skopenow platform itself is not publicly accessible, the raw data Skopenow collects through its publicly available searches is accessible to the public through manual search techniques and processes. Reports and discovery generated from Skopenow may be confidential due to the investigated case, court proceedings, and sealing orders. The public can submit a request for information to RMLAD, Discovery Section, in accordance with the CPRA and FOIA, as the law permits.

Inspections/Audits

A 2025 annual audit was completed to verify that all end-users complied with Department policies and procedures as outlined in Special Order No. 11, 2022. The audit was carried out by designated administrators. The respective lieutenant and commanding officer reviewed and approved the inspection. The methodology and results are stored at the Robbery-Homicide Division and are available for review. In addition to the annual inspection, periodic and targeted audits may be conducted on a case-by-case basis when necessary (Refer to Finding No. 4).

This section was intentionally left blank.

D. Penlink Tangles (formerly known as Cobwebs Technologies)

Penlink (Tangles) is a web-based platform that searches for and analyzes open-source information (OSINT), publicly available data, and anonymized commercial data. The technology is used for criminal investigations and public safety threat assessments. Once the technology produces relevant results, they are filtered and vetted by an investigator or crime analyst to confirm their relevance. Tangles creates products for both law enforcement and private-sector enterprises.

Findings:

1. The Technology Met the Expectations of the Presentation to the Board of Police Commissioners and the Department when the Technology was Obtained

Tangles helps users quickly and effectively analyze publicly available data for criminal cases, critical incidents, and threats to public safety. Tangles acts as a force multiplier, replacing the tedious, time-consuming task of manually searching the internet for open-source information related to an investigation.

Tangles has met the Department's expectations by completing investigative tasks accurately and quickly, ultimately saving many human resource hours. With Tangles, searches are performed swiftly and with greater accuracy. Once the information is obtained and verified, investigators can request additional data from service providers via search warrants. This technology aligns with and adheres to the Department's current policies and procedures. All end-user searches follow the principles of the "right to know" and "need to know."

2. Frequency of Use

The Department initially acquired Tangles on July 28, 2022. It purchased three concurrent licenses, supporting a total of 13 users, which were allocated between Robbery-Homicide Division and Major Crimes Division (MCD). The investigative responsibilities of RHD include, but are not limited to, homicides such as multiple murders, arson-related murders, murders involving police officers, and cold cases. Their scope also covers robberies like series of robberies, home invasions, and bank robberies, as well as kidnappings for ransom. Major Crimes Division's investigative duties encompass, but are not limited to, crimes threatening public safety, such as mass shootings, bomb threats, and serial arsons, as well as threats to critical infrastructure. In addition to utilizing the technology in their investigations, assigned personnel frequently employ it to assist other Department units with criminal investigations when needed and appropriate.

3. Efficacy of the Technology

Within the Tangles platform, activity is organized into “projects.” A total of 390 projects were initiated during the calendar year 2025. The Tangles platform has proven essential for quickly generating relevant investigative leads. Investigators can accurately and effectively sort open-source leads, which have led to the use of other investigative techniques (e.g., search warrants, interviews, and forensic investigation). Results have included the successful identification, location, and apprehension of numerous felony suspects. Tangles has been used in a wide variety of criminal investigations and cases.

Investigators have found Tangles to be a valuable and complementary addition to other technologies already used by the Department. Additionally, Tangles allows investigators to cross-check and cross-reference information obtained against other Department technologies. This is significant because “best practices” dictate that actionable information should not be derived from a single source.

4. Personnel Compliance of All End-Users

Tangles enables the Department’s Administrator(s) to monitor all search inquiries made by assigned end-users. Tangles’ servers securely store all end-user activity, including, but not limited to, search date/time, queried content, and related case numbers. End-users cannot edit or delete any logged activity (search history) from Tangles’ servers. Tangles is assigned to a small group of investigators in cases where this software's use is most relevant. It is used during the course and scope of end-users' assignments for criminal investigations, in accordance with “right to know” and “need to know” standards.

An annual inspection has been introduced to ensure that all end-users comply with Department policies and procedures. The designated administrators conduct the annual inspections. The respective lieutenant and commanding officer review these inspections. Additionally, periodic and targeted inspections may be conducted as needed.

5. The Cost of the Technology and Cost-Benefit Analysis

The total cost for both RHD and MCD for Fiscal Year 2025/2026 is \$174,742.47.

Funding for this technology was secured through a grant. Its cost is largely offset by the time it saves investigators when gathering similar information from other sources, such as “hand searching” the internet. This technology can be accessed remotely, allowing investigators to quickly query for new information at crime scenes. This fresh data is often very helpful in advancing an investigation during its early stages. It also helps identify suspects and victim accounts, as well as any connections between them, enabling the preservation of relevant data stored with service providers that the suspect may later remove. Tangles also reduced the total number of employee work hours by providing relevant results quickly.

6. Identified Concerns and Proposed Mitigations

No concerns or proposed mitigations are required. Administrators have collaborated with the vendor to make specific features accessible and to align this technology with Special Order No. 11, 2022, and current Department policies and procedures.

Administrators have worked with Tangles and will continue to do so to identify, address, and resolve any concerns in the future (e.g., changes in Federal or State law and Department policy).

7. Efficacy of the Existing Policy and Any Proposed Changes

Like other technologies or databases accessed by law enforcement, this technology adheres to the “right to know” and “need to know” standards. Entering criminal case numbers with inquiries is mandatory and will be reviewed during audits. The number of end-users is small—only six—and personnel are selected based on their assignment and need to use the technology. End-users are informed of the designated administrators, that the system securely stores inquiries, and that their inquiries are later subject to audit.

8. Efficacy of the Training on the Existing Policy and Any Proposed Changes

Tangles offers training during the initial onboarding process and provides ongoing training, resources, and support. Tangles supplies a user guide and offers virtual training. This technology is easy to use and has a short learning curve. End-users are informed of their designated administrators. Administrators are primarily responsible for updating end-users on any relevant changes to the technology, policy, and usage.

Other Related Matters

Data Retention

All cases involving the inquiry of information through Tangles are investigatory and have a criminal predicate for legitimate law enforcement purposes. Data may be retained during an ongoing investigation and criminal court proceedings, and may also be retained for extended periods due to the duration of open investigations and court processes. This approach complies with Department policies and procedures, as well as all criminal court requirements, including discovery, court proceedings, and appellate processes. Data no longer needed for an investigation or court case will be properly disposed of in accordance with Department procedures and criminal court standards.

Data Security

Investigators may retain information in accordance with standardized data retention periods (see the data retention section). Retained information will comply with current Department standards. Both RHD and MCD operate within secure facilities with a secondary restricted-access level. Personnel within the divisions are provided with locking desks and access to storage cabinets as additional physical safeguards.

Computers used to access Tangles' web-based application or portal are password-protected desktops, laptops, or tablets. If a cellular telephone is used to access Tangles' platform, the Department's current cellular telephone policy (e.g., password protection) applies.

Privacy, Civil Rights, and Civil Liberties (P/CRCL)

- Potential Impact on Privacy and Civil Rights

There are no identified negative effects or anticipated violations of privacy and civil rights. End-users conducting informational inquiries through Tangles' platform are involved in investigative cases with a criminal basis. This aligns with Federal and State law and the Department's policies and procedures.

- Measures Currently in Place to Maintain Data Security

Tangles does not maintain a database. Investigators (end-users) are responsible for maintaining any extracted and stored data in accordance with Department policies and procedures and court-mandated requirements. Devices used to access and query the Tangles platform are password-protected. Facilities where printed records are stored are secured and off-limits to unauthorized law enforcement or the public. Most investigators are familiar with security measures such as encryption and other digital or physical safeguards. The Tangles platform includes an audit process that provides additional protection.

- Plan to Safeguard Privacy and Civil Rights

The Department and assigned end-users follow established best practices and standards to protect privacy, civil rights, and civil liberties (P/CRCL) while balancing OPSEC. This includes administrators and technology coordinators who interact with vendors and personnel on P/CRCL issues. Ongoing training between vendors and end-users also supports this goal. Protocols for properly redacting information related to court cases prevent the unnecessary and unwarranted public release of data. Considering the need for situational awareness and First Amendment-protected activity, right-to-release protocols ensure that all relevant factors are taken into account.

- Public Access to the Data

While the Tangles platform itself is not publicly accessible, the raw data Tangles collects through its publicly available searches is accessible to the public via manual search techniques and processes. Reports and discoveries generated by Tangles may be confidential due to the case under investigation, court proceedings, or sealing orders. The public can submit a request for information to the Risk Management and Legal Affairs Division, Discovery Section, in accordance with the CPRA and FOIA, as permitted by law.

Inspections/Audits

The 2025 annual audit was completed to ensure all end-users were compliant with Department policies and procedures per Special Order No. 11. The annual inspection was conducted by the designated administrators. The respective lieutenant and commanding officer reviewed and approved the audit. The audit's methodology and results are maintained by the Robbery-Homicide Division and are available for inspection. In addition to the annual inspection, periodic and targeted inspections may be conducted on a case-by-case basis when necessary (Refer to Finding No. 4).

END OF REPORT