McMillan, Acquanette (Netta)

From: Black Rose Security
Sent: Tuesday, November 17, 2026 11:45 AM
To: PublicComment-AutoResponse
Subject: AGENDA ITEM #9 FOR TONIGHT

Some people who received this message don't often get email from Learn why this is important

[!] **CAUTION:** This email was delivered from the Internet. Do not click links or open attachments unless you ***know*** the content is safe. Report phish using the Phish Alert Button (PAB). For more information about the PAB view article "KB0011474" on the DoIT portal.

Hi my name is Atom Ward and I live/work/visit in Pasadena. I am urging you to vote NO on Item 9 and reject Flock and to immediately turn off and cover the ALPR cameras across Pasadena. Do not spend one more dollar into expanding a mass surveillance system with such an untrustworthy vendor like Flock.

It is widely known that Flock has violated agreements in other cities regarding data sharing, and has refused to turn off and take down their cameras after cities cancel their contracts. Even though Flock said they wouldn't share license plate data with ICE or Border Patrol, they were caught doing it anyway. They cannot be trusted with our data, they don't follow California state law and do not care about our safety.

Warrantless mass surveillance like Flock and other ALPR undermine civil liberties, and puts all of us at risk. This is not the opportunity to sell us on more surveillance like Real Time Crime Centers. Don't get left behind whiie hundreds of other cities across the nation are rejecting Flock. THANK YOU!

McMillan, Acquanette (Netta)

From: Kristina Denstitt
Sent: Tuesday, November 17, 2026 11:45 AM
To: PublicComment-AutoResponse
Subject: Public Comment: No Flock Cameras in Pasadena

Some people who received this message don't often get email from .earn why this is important

[!] **CAUTION:** This email was delivered from the Internet. Do not click links or open attachments unless you ***know*** the content is safe. Report phish using the Phish Alert Button (PAB). For more information about the PAB view article "KB0011474" on the DoIT portal.

Hello,

I am a concerned Pasadena resident who does not want Flock or any other ALPR cameras in our community. I do not feel safer with these mass surveillance tools deployed on our streets. Flock steals our data and is known to make mistakes, endangering law-abiding civilians who may one day be wrongly accused of a crime.

Traditional police work has addressed crime for decades, and Pasadena is already a relatively safe community. Creating a digital dragnet with Flock cameras is unnecessary.

Further, I did not consent to having my data collected while driving on a public street, and it is frankly dystopian for my city and police department to give me no choice to opt out.

Please know this is not a niche issue that only a minority of citizens care about. Many cities have already ended their Flock contracts due to public resistance. I hope Pasadena will soon be among them.

Thank you for your time.

Kristina Denstitt

/cMillan, Acquanette (Netta)

rom: Kristina Denstitt <noreply@adv.actionnetwork.org>
ent: Tuesday, November 17, 2026 11:59 AM
o: PublicComment-AutoResponse
ubject: I Do Not Want Mass Surveillance in Our Community

[ ] **CAUTION:** This email was delivered from the Internet. Do not click links or open attachments unless you ***know*** the content is safe. Report phish using the Phish Alert Button (PAB). For more information about the PAB view article "KB0011474" on the DoIT portal.

City Council Member,

I urge you to end warrantless mass surveillance like dystopian Flock Safety cameras and not turn Pasadena into a nanny state. Automated license plate readers (ALPR) are dragnet surveillance tech that tracks everyone indiscriminately without a warrant and without suspicion of crime.

While Flock, some law enforcement, and government continue to defend mass surveillance for public safety, they are subjecting the general public to surveillance without consent that threatens our right to privacy and our civil liberties. This is not the kind of society we want to live in.

Rather than spending our tax dollars on dystopian and dangerous surveillance technology, Pasadena needs to restore trust, uphold our constitutional rights, and invest in resources that are proven to keep communities safe. End ties with Flock, don't replace them with another vendor, and commit to fund community-based safety programs.

I'm calling on you to join the dozens cities and towns across the country that have cut ties with Flock. Take a stand against Big Brother and keep dystopian surveillance out of Pasadena.

Kristina Denstitt

Pasadena, California 91101

McMillan, Acquanette (Netta)

From: River Good
Sent: Tuesday, November 17, 2026 11:46 AM
To: PublicComment-AutoResponse
Subject: Public comment for Agenda Item 9. Flock

Some people who received this message don't often get email from Learn why this is important

[!] **CAUTION:** This email was delivered from the Internet. Do not click links or open attachments unless you ***know*** the content is safe. Report phish using the Phish Alert Button (PAB). For more information about the PAB view article "KB0011474" on the DoIT portal.

Good morning!

different ones. I want all cameras to be taken down. My opinion is shared with that of the Fourth Amendment; "

I look forward to hearing from our city tonight. Have a great day!

River Good

McMillan, Acquanette (Netta)

From: joel.yoshonis
Sent: Tuesday, November 17, 2026 12:02 PM
To: PublicComment-AutoResponse; Jones, Justin
Subject: Public comment for agenda item 9. Flock

Some people who received this message don't often get email from j Learn why this is important

[!] **CAUTION:** This email was delivered from the Internet. Do not click links or open attachments unless you ***know*** the content is safe. Report phish using the Phish Alert Button (PAB). For more information about the PAB view article "KB0011474" on the DoIT portal.

Dear City Council,

As a District 3 resident, PUSD parent, and faith leader in Pasadena I am writing to demand that the city CANCEL its contract with Flock and NOT replace this contract with another ALPR company.

Flock and other ALPR technology is warrantless mass surveillance. Automated license plate readers (ALPR) are dragnet surveillance tech that tracks everyone indiscriminately without a warrant and without suspicion of crime.

While Flock, some law enforcement, and government continue to defend mass surveillance for public safety, they are subjecting the general public to surveillance without consent that threatens our right to privacy and our civil liberties. This is not the kind of society we want to live in.

Not only is this technology unconstitutional and unnecessary, I cannot understand why City Council continues to approve these new tools for PPD when the department repeatedly demonstrates a pattern of reckless behavior.

For instance, the now infamous "horseplay" incident where a PPD officer inadvertently shoots a fellow officer on camera while attempting to joke around is an example of both PPD's unprofessional conduct and its lack of transparency with the community as this incident was only learned of when local media discovered and reported on it. If officers cannot be trusted with their own firearms, and given the department's delay in disclosing this incident to the public, it is mind-boggling to me that we would entrust them with MORE tools and technology.

Another recent example that comes to mind is a community event I attended with Mayor Gordo and Chief Harris hosted by the Clergy Community Coalition at PazNaz. Just weeks later, NBA LA journalists discovered that ICE and the FBI had, in fact, been given access to Pasadena PD's Flock database. It is not surprising, then, to learn from local org Pasadena Privacy that the majority of ICE kidnappings in Pasadena have taken place in areas most concentrated with Flock cameras. It is a stain on the City of Pasadena's racist history that these cameras are predominantly located in Pasadena's historic Black and Hispanic neighborhoods. Why should we entrust ALPR technology to a department that lies to us about its use?

A final recent example: I live on the 200 block of N Oakland where recently a Pasadena PD officer shot at a vehicle multiple times during an investigation. I have lived in this neighborhood for 7 years with my wife and 3 young kids. I have NEVER felt unsafe here—until that night. We, including my children, heard the gunshots go off followed by police helicopters and a swarm of officers racing down our street. When I called the PPD non-emergency line to find out what was going on—in particular regarding the police helicopter that had been circling for 30 minutes—I was told there was a suspect and led to believe this was who fired the shots. It is

11/17/2026 Item 9

understandable that the operator may not have had the full incident report, but I spent several hours worried about a gunman on the loose based on this discussion and continued helicopter activity.

Upon learning it was an officer who fired a weapon, I could not understand why the PPD helicopter continued to circle the area. I was told by the PPD operator to contact the heliport line where I left a message and request for a call back.

I never received a call back.

A related aside: in Chief Harris' report regarding new military equipment acquisitions to the police oversight commission, a mere 7 or 8 noise complaints from helicopter activity (from my memory) were listed. I know for a fact that my phone calls — which have been frequent about this — were not listed. When I asked the operator about this the night of the police shooting on N Oakland and how to get my complaints officially recorded, they were unable to answer—very alarming to me. That's when they told me to call the heliport line.

Why are we expanding surveillance for a department that won't listen to or record residents' concerns or even bother to help residents understand the process to do so? What recourse will we have to address further misuse of police technologies when they aren't aven fielding the current ones?

This raises serious questions regarding PPD's engagement with community concerns and the department's integrity in relating these to City Council and other oversight committees. I raise these individual issues not as comprehensive examples but to demonstrate an ongoing pattern of dismissal of community concerns and safety by PPD.

Rather than spending our tax dollars on dystopian and dangerous surveillance technology, Pasadena needs to restore trust, uphold our constitutional rights, and invest in resources that are proven to keep communities safe. End ties with Flock, don't replace them with another vendor, and commit to fund community-based safety programs.

I'm calling on you to join the dozens cities and towns across the country that have cut ties with Flock. Take a stand against Big Brother and keep dystopian surveillance out of Pasadena.

Sincerely,
Rev. Joel Yoshonis
District 3 Resident
Fuller Seminary '22

Sent from Proton Mail for iOS.

McMillan, Acquanette (Netta)

From: Francesca Mariani
Sent: Tuesday, November 17, 2026 12:13 PM
To: PublicComment-AutoResponse
Subject: No to Flock Cameras near PUSD schools

Some people who received this message don't often get email from earn why this is important

[!] **CAUTION:** This email was delivered from the Internet. Do not click links or open attachments unless you ***know*** the content is safe. Report phish using the Phish Alert Button (PAB). For more information about the PAB view article "KB0011474" on the DoIT portal.

Dear Mayor Gordo and Members of the Pasadena City Council,

I am writing to urge the City Council to reject the continued expansion of Flock Safety surveillance cameras in Pasadena and, in particular, to prohibit their placement near schools, playgrounds, parks, and other places where children and families gather.

Our schools should be places where children can learn, grow, and feel safe—not locations surrounded by automated surveillance technology that tracks people entering and leaving the area.

There are several reasons why I believe this deserves serious consideration:

1. Children deserve privacy

Families should not have to worry that their daily routines—dropping off children, attending school events, visiting playgrounds, or seeking services—are being logged in a surveillance database. Children cannot meaningfully consent to this type of monitoring, and their families should not have to accept it simply to participate in everyday community life.

2. Schools should not become surveillance zones.

Placing automated license plate readers near schools creates a record of who visits those campuses and when. This could include parents, students who drive, teachers, school employees, volunteers, contractors, and visitors. The implications extend well beyond law enforcement investigations.

3. Data collection creates risks beyond its original purpose.

Even when a system is introduced for legitimate public safety reasons, the collection, storage, searching, and sharing of sensitive location data raises serious questions about access, oversight, misuse, and future changes in policy. Promises about appropriate use today do not eliminate the possibility of misuse tomorrow.

4. Public safety should not come at the expense of civil liberties.

We all want safer neighborhoods and schools. But safety and privacy should not be treated as mutually exclusive. The City should prioritize approaches that protect residents without creating an extensive infrastructure for tracking their movements.

I ask the City Council to take the following actions:

- **Reject any placement of Flock cameras near schools**, including school entrances, drop-off and pickup areas, playgrounds, and school-adjacent streets.
- Direct staff to identify and remove any existing cameras located near schools and other child-centered facilities.
- Suspend expansion of the Flock network and reconsider the City's continued relationship with the company.
- Provide full transparency regarding camera locations, data retention, access, sharing agreements, and independent audits.
- Hold meaningful public discussions with parents, students, educators, and community members before making decisions about surveillance technology.
- Explore investments in community-based safety measures that do not require the mass collection of residents' location data.

Pasadena has an obligation to protect its children, respect families, and preserve the trust of its residents. The presence of surveillance technology near our schools deserves a much higher level of scrutiny than a routine technology procurement decision.

Please do not normalize surveillance as part of the school experience. Our children deserve safe schools, and our families deserve privacy.

I urge you to put children, families, and civil liberties at the center of this decision.

Sincerely,

Francesca Mariani
Parent of 2 kids in PUSD

McMillan, Acquanette (Netta)

From: Millie R <noreply@adv.actionnetwork.org>
Sent: Tuesday, November 17, 2026 12:20 PM
To: PublicComment-AutoResponse
Subject: I Do Not Want Mass Surveillance in Our Community

[!] **CAUTION:** This email was delivered from the Internet. Do not click links or open attachments unless you ***know*** the content is safe. Report phish using the Phish Alert Button (PAB). For more information about the PAB view article "KB0011474" on the DoIT portal.

City Council Member,

I urge you to end warrantless mass surveillance like dystopian Flock Safety cameras and not turn Pasadena into a nanny state. Automated license plate readers (ALPR) are dragnet surveillance tech that tracks everyone indiscriminately without a warrant and without suspicion of crime.

While Flock, some law enforcement, and government continue to defend mass surveillance for public safety, they are subjecting the general public to surveillance without consent that threatens our right to privacy and our civil liberties. This is not the kind of society we want to live in.

Rather than spending our tax dollars on dystopian and dangerous surveillance technology, Pasadena needs to restore trust, uphold our constitutional rights, and invest in resources that are proven to keep communities safe. End ties with Flock, don't replace them with another vendor, and commit to fund community-based safety programs.

I'm calling on you to join the dozens cities and towns across the country that have cut ties with Flock. Take a stand against Big Brother and keep dystopian surveillance out of Pasadena.

Millie R

, 91105

McMillan, Acquanette (Netta)

From: Laura MacPherson <noreply@adv.actionnetwork.org>
Sent: Tuesday, November 17, 2026 12:27 PM
To: PublicComment-AutoResponse
Subject: I Do Not Want Mass Surveillance in Our Community

[⚠] **CAUTION:** This email was delivered from the Internet. Do not click links or open attachments unless you ***know*** the content is safe. Report phish using the Phish Alert Button (PAB). For more information about the PAB view article "KB0011474" on the DoIT portal.

City Council Member,

I urge you to end warrantless mass surveillance like dystopian Flock Safety cameras and not turn Pasadena into a nanny state. Automated license plate readers (ALPR) are dragnet surveillance tech that tracks everyone indiscriminately without a warrant and without suspicion of crime.

While Flock, some law enforcement, and government continue to defend mass surveillance for public safety, they are subjecting the general public to surveillance without consent that threatens our right to privacy and our civil liberties. This is not the kind of society we want to live in.

Rather than spending our tax dollars on dystopian and dangerous surveillance technology, Pasadena needs to restore trust, uphold our constitutional rights, and invest in resources that are proven to keep communities safe. End ties with Flock, don't replace them with another vendor, and commit to fund community-based safety programs.

I'm calling on you to join the dozens cities and towns across the country that have cut ties with Flock. Take a stand against Big Brother and keep dystopian surveillance out of Pasadena.

Laura MacPherson

Altadena, California 91001

McMillan, Acquanette (Netta)

From: bea lamar <noreply@adv.actionnetwork.org>
Sent: Tuesday, November 17, 2026 12:29 PM
To: PublicComment-AutoResponse
Subject: I Do Not Want Mass Surveillance in Our Community

[⚠] **CAUTION:** This email was delivered from the Internet. Do not click links or open attachments unless you ***know*** the content is safe. Report phish using the Phish Alert Button (PAB). For more information about the PAB view article "KB0011474" on the DoIT portal.

City Council Member,

I urge you to end warrantless mass surveillance like dystopian Flock Safety cameras and not turn Pasadena into a nanny state. Automated license plate readers (ALPR) are dragnet surveillance tech that tracks everyone indiscriminately without a warrant and without suspicion of crime.

While Flock, some law enforcement, and government continue to defend mass surveillance for public safety, they are subjecting the general public to surveillance without consent that threatens our right to privacy and our civil liberties. This is not the kind of society we want to live in.

Rather than spending our tax dollars on dystopian and dangerous surveillance technology, Pasadena needs to restore trust, uphold our constitutional rights, and invest in resources that are proven to keep communities safe. End ties with Flock, don't replace them with another vendor, and commit to fund community-based safety programs.

I'm calling on you to join the dozens cities and towns across the country that have cut ties with Flock. Take a stand against Big Brother and keep dystopian surveillance out of Pasadena.

bea lamar

Pasadena, California 91101

McMillan, Acquanette (Netta)

From: Bea Lamar
Sent: Tuesday, November 17, 2026 12:45 PM
To: PublicComment-AutoResponse
Subject: Vote NO on Item 9. Reject Flock.

Some people who received this message don't often get email from [redacted] arn why this is important

[⚠] **CAUTION:** This email was delivered from the Internet. Do not click links or open attachments unless you ***know*** the content is safe. Report phish using the Phish Alert Button (PAB). For more information about the PAB view article "KB0011474" on the DoIT portal.

Dear Pasadena City Council,

I urge you to vote NO on Item 9, reject Flock, and immediately deactivate and cover every ALPR camera in Pasadena.

Public safety demands public trust, civil liberties, and the freedom to move through our city without being tracked. Flock's record of data misuse, unauthorized access, false identifications, and broken promises makes it an UNACCEPTABLE choice for Pasadena.

Cities across California -including Los Angeles, San Diego, Santa Cruz, and South Pasadena -are walking away. Pasadena should lead with them.

Every dollar invested deepens a surveillance infrastructure that compromises our privacy, exposes our residents, and places our civil liberties at risk.

Vote NO. Protect Pasadena.

Sincerely,
Bea Lamar
Pasadena Resident

McMillan, Acquanette (Netta)

From: Yadi
Sent: Tuesday, November 17, 2026 12:28 PM
To: PublicComment-AutoResponse
Subject: Fwd: Public comment - Pasadena CPOC - 08/13/26
Attachments: Public Comment - CPOC 08-13-26 ALPR Audit.pdf

[⚠] **CAUTION:** This email was delivered from the Internet. Do not click links or open attachments unless you ***know*** the content is safe. Report phish using the Phish Alert Button (PAB). For more information about the PAB view article "KB0011474" on the DoIT portal.

Hi,

Please include my public comment below for the November 17, 2026 City Council agenda item 9. ALPR.

Thank you,

Yadi

---------- Forwarded message ---------
From: **Yadi** ·
Date: Thu, Aug 13, 2026 at 3:48 PM
Subject: Public comment - Pasadena CPOC - 08/13/26
To: <cpoc@cityofpasadena.net>

Hi,

Please find attached my public comment for the August 13, 2026 Pasadena Community Police Oversight Commission meeting, general comment on items not on the agenda.

Thanks,

Yadi
(Attachments: 1)

Comment about Pasadena Police ALPR Audit

On July 10, 2026 the Los Angeles Office of Inspector General (OIG) published a review of the Los Angeles Police Department's use of Automatic License Plate Readers (ALPR) during a two-month period, from August 1, 2025, through September 30, 2025.[1] [2] The LA OIG ALPR review is attached for your reference.

The Pasadena Police Oversight Commission needs to instruct the IPA to redo its "audit" of Pasadena's ALPR to provide the public, the CPOC and Council with true transparency and facts of PPD's ALPR. This should be done at no cost to the City.

At the bare minimum, any report or audit should include factual background such as the vendor contract, and equipment details. It is imperative for the public to understand Pasadena's ALPR system to be able to weigh in on Flock as a vendor and ALPR as a technology.

In comparison, the LA OIG's report "sought to identify the impact ALPRs had to the recovery of stolen vehicles, arrests, and overall crime suppression efforts. The OIG also sought to evaluate the governance, oversight, and contractual limitations of ALPR service providers in addition to security measures associated with information sharing. The report concludes with recommendations for consideration intended to address the identified operational and contractual limitations."

Moreover, the OIR Group's "Review" of Pasadena's ALPR is factually incorrect or misleading at best. The "review" states: "The ALPR program appears to be operating consistent with California law and Department policy" does it or does it not operate in accordance with state law? What exactly does the IPA mean by "appears"? We know that's not true, as PPD has historically shared data out of state and its ALPR systems were accessed for federal purposes and against policy for the infringement of protected activities like the right to protest.[3] The record must be corrected.

"Continued oversight remains important as the program expands".. excuse us, what??

Please provide the public with an actual review and audit or get us an independent auditor who will.

Yadi
Pasadena Community Police Oversight Commission
August 13, 2026
Pasadena Police ALPR audit

---

1 https://www.oig.lacity.org/significant-reports
2 https://lapdonlinestrgeacc.blob.core.usgovcloudapi.net/lapdonlinemedia/071426.pdf
3 https://pasadenaprivacy.org/nbc-pasadena-flock

Comment about Pasadena Police ALPR Audit

On July 10, 2026 the Los Angeles Office of Inspector General (OIG) published a review of the Los Angeles Police Department's use of Automatic License Plate Readers (ALPR) during a two-month period, from August 1, 2025, through September 30, 2025.[1] [2] The LA OIG ALPR review is attached for your reference.

The Pasadena Police Oversight Commission needs to instruct the IPA to redo its "audit" of Pasadena's ALPR to provide the public, the CPOC and Council with true transparency and facts of PPD's ALPR. This should be done at no cost to the City.

At the bare minimum, any report or audit should include factual background such as the vendor contract, and equipment details. It is imperative for the public to understand Pasadena's ALPR system to be able to weigh in on Flock as a vendor and ALPR as a technology.

In comparison, the LA OIG's report "sought to identify the impact ALPRs had to the recovery of stolen vehicles, arrests, and overall crime suppression efforts. The OIG also sought to evaluate the governance, oversight, and contractual limitations of ALPR service providers in addition to security measures associated with information sharing. The report concludes with recommendations for consideration intended to address the identified operational and contractual limitations."

Moreover, the OIR Group's "Review" of Pasadena's ALPR is factually incorrect or misleading at best. The "review" states: "The ALPR program appears to be operating consistent with California law and Department policy" does it or does it not operate in accordance with state law? What exactly does the IPA mean by "appears"? We know that's not true, as PPD has historically shared data out of state and its ALPR systems were accessed for federal purposes and against policy for the infringement of protected activities like the right to protest.[3] The record must be corrected.

"Continued oversight remains important as the program expands".. excuse us, what??

Please provide the public with an actual review and audit or get us an independent auditor who will.

Yadi
Pasadena Community Police Oversight Commission
August 13, 2026
Pasadena Police ALPR audit

---

1 https://www.oig.lacity.org/significant-reports
2 https://lapdonlinestrgeacc.blob.core.usgovcloudapi.net/lapdonlinemedia/071426.pdf
3 https://pasadenaprivacy.org/nbc-pasadena-flock

INTRADEPARTMENTAL CORRESPONDENCE

July 10, 2026 **BPC #26-184**
1.0

TO: The Honorable Board of Police Commissioners

FROM: Inspector General, Police Commission

SUBJECT: REVIEW OF LOS ANGELES POLICE DEPARTMENT AUTOMATIC LICENSE PLATE READER SYSTEM AND USE IN THE FIELD

RECOMMENDED ACTION

REVIEW and APPROVE the Inspector General's Report on its Review of the Los Angeles Police Department's Automatic License Plate Reader System and Use in the Field.

DISCUSSION

The OIG conducted a review of the Los Angeles Police Department's (Department) use of Automatic License Plate Readers (ALPR) to assess the operational efficacy during a two-month period from August 1, 2025, through September 30, 2025. During the review period, the OIG sought to identify the impact ALPRs had to the recovery of stolen vehicles, arrests, and overall crime suppression efforts. The OIG also sought to evaluate the governance, oversight, and contractual limitations of ALPR service providers in addition to security measures associated with information sharing. The report concludes with recommendations for consideration intended to address the identified operational and contractual limitations.

I am available to provide any information the Board may require.



MATTHEW J. BARRAGAN
Inspector General
Police Commission

Attachment

LOS ANGELES POLICE COMMISSION

REVIEW OF THE DEPARTMENT'S ALPR SYSTEM AND USE IN THE FIELD

OFFICE OF THE INSPECTOR GENERAL

MATTHEW BARRAGAN

Inspector General

July 10, 2026

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY 1
II. BACKGROUND 3
A. ALPR Providers, Distribution, and Contracts 4
B. Funding 7
C. System Use 9
D. Data Access 9
E. Data Sharing 10
F. Data Retention, Storage, and Department Oversight 11
G. Hot Lists 13
H. Hot List Alerts 13
III. OIG REVIEW OF ALPR ALERTS 14
A. Review Period and Available Alert Outcome Data 14
IV. OIG REVIEW RESULTS AND FINDINGS 15
A. No Action Taken 15
B. Duplication of Action Taken 15
C. Determined Not Stolen 16
D. Stolen Vehicles and Stolen License Plates Recovered 16
E. Arrests and High-Risk Stops 16
F. Vehicle Pursuits 17
V. RECOMMENDATIONS 17
VI. DEPARTMENT RESPONSE 19
Appendix A 68
Appendix B 72
Appendix C 75
Appendix D 79
Appendix E 82
Appendix F 83
Appendix G 85

REVIEW OF THE DEPARTMENT'S ALPR SYSTEM AND USE IN THE FIELD

I. EXECUTIVE SUMMARY

The Los Angeles Police Department (LAPD or Department) operates an Automated License Plate Reader (ALPR) system that initially consisted of a limited number of cameras mounted on police vehicles and traffic poles throughout Los Angeles. Over time, the Department has expanded both the system's use and the number of cameras in operation, prompting questions regarding data retention practices, privacy protections, and the overall effectiveness of ALPR technology in reducing crime.

California Senate Bill 34, enacted in 2015, requires law enforcement agencies operating ALPR systems to maintain and make available a usage and privacy policy.[1] The law establishes requirements related to the collection, access, retention, sharing, and security of ALPR information and requires agencies to implement reasonable safeguards to protect ALPR data. However, it does not itself create a comprehensive statewide transparency or oversight regime.

In 2023, the California Attorney General issued a bulletin providing guidance to help agencies ensure that their collection, storage, and use of ALPR information comply with state law.[2] In response, the Department issued Special Order No. 7, *Automated License Plate Recognition Usage and Privacy Policy – Revised*, approved by the Board of Police Commissioners (BOPC) in February 2023. The revised Special Order established procedures governing authorized uses of ALPR data, access controls, training, information sharing, retention, deletion, and data security. [3]

Despite these legal and policy safeguards, concerns regarding the potential misuse and unauthorized sharing of ALPR data continue to arise. Recent reports have documented instances in which license plate data collected through Flock Safety, an ALPR provider used by law enforcement agencies nationwide, including the LAPD, was accessible to federal agencies. These reports also raised concerns regarding the adequacy of internal oversight and safeguards designed to prevent unauthorized access and dissemination of ALPR data.

Public concerns about privacy, information sharing, and the reliability of ALPR technology prompted the Office of the Inspector General (OIG) to review the Department's policies and practices. Although state law prohibits California law enforcement agencies from sharing ALPR data with federal agencies, recent developments in federal immigration enforcement have raised concerns that the federal government may seek access to that data. The OIG also examined the extent of law enforcement activity generated by ALPR real-time alerts during a two-month period.

---

[1] Cal. Civ. Code §§ 1798.90.5–1798.90.55 (added by Sen. Bill No. 34)
[2] https://oag.ca.gov/system/files/media/2023-dle-06.pdf
[3] Department Manual, Volume III, Section 568.53, Automated *License Plate Recognition Usage and Privacy Policy*.

Key Findings

The OIG's findings are as follows:

- The Department's ALPR system includes 248 pole-mounted cameras, 140 cameras mounted on police vehicle roofs, approximately 1,500 cameras installed inside police vehicles, and seven mobile trailer cameras.
- An additional 50 pole-mounted cameras in the Pacific Palisades area have been temporarily loaned to the Department at no cost.
- Three vendors provide ALPR technology and related services. However, the Department does not have formal contracts or agreements in place for all services to address ALPR data-security, privacy, and access-control requirements.
- The Department shares ALPR data with 15 California law enforcement agencies under a Memorandum of Agreement that establishes specific conditions and safeguards for data sharing.
- Department personnel must complete ALPR policy training before receiving authorization to access and query ALPR databases.
- Department policy requires the Department's Audit Division to conduct periodic audits of access to and use of ALPR data. Audit Division has issued one report in 2022.
- The policy also requires Information Technology Bureau (ITB) conduct regular inspections of the ALPR system operations and usage. The ITB conducts monthly reviews of specific search terms entered by Department personnel when querying ALPR data.
- Police vehicles equipped with both in-car and roof mounted ALPR cameras generate an alert on the vehicle's mobile computer when a scanned license plate matches a plate on a Hot List.
- Police vehicles equipped with both camera systems generate duplicate alerts when the same license plate is scanned by both systems.
- The Department's current process does not fully or accurately document the law enforcement actions taken in response to ALPR alerts.
- The Department's ALPR cameras generated 210,568,103 license plate reads between August 1 and September 30, 2025.
- The OIG identified the following outcomes from in-car ALPR alerts generated between August 1 and September 30, 2025:
    - Officers confirmed 161 alerts as accurate matches to the scanned license plate; however, subsequent investigation determined that the vehicles had not been stolen.
    - Three hundred, thirty-seven alerts resulted in the recovery of stolen vehicles.
    - Sixty-eight alerts resulted in 74 arrests.
    - Nine alerts resulted in pursuits.

Recommendations

The OIG makes the following recommendations:

1. Suspend the deployment of new ALPR cameras and the execution of new ALPR-related contracts pending public input and a broader reassessment of vendors and data practices. If the Department continues to use ALPR technology, it shall obtain approval from the BOPC for formal contracts or agreements with all ALPR vendors, regardless of the contract amount or whether the agreement involves an exchange of funds. Those contracts or agreements shall establish enforceable requirements governing data security, privacy, access controls, retention, and auditing to protect Department ALPR data and ensure accountability for its collection, use, and disclosure.

   Note: In 2020, the California State Auditor recommended the LAPD update ALPR vendor contracts with necessary data safeguards to address shortcomings the audit identified.[4]

2. Strengthen oversight of ALPR data access by amending Department policy to require annual audits to ensure that Department personnel are using the ALPR systems for authorized purposes and to clearly communicate that misuse of ALPR data may result in disciplinary action.

3. Develop and implement a standardized process for documenting traffic stops initiated by ALPR alerts to ensure complete and accurate records and facilitate meaningful analysis of officer actions and stop outcomes.

II. BACKGROUND

Given the complexity of the Department's ALPR system — including its technology, operational use, and governing policies — the OIG provides the following background to place its review and findings in context:

A. ALPR Providers, Distribution, and Contracts
B. Funding
C. System Use
D. Data Access
E. Data Sharing
F. Data Retention, Storage, and Department Oversight
G. Hot Lists
H. Hot List Alerts

[4] https://information.auditor.ca.gov/pdfs/reports/2019-118.pdf

A. ALPR Providers, Distribution, and Contracts

When in operation, ALPR cameras will capture a vehicle's license plate number, date, time, and location in addition to a photo of the vehicle. The ALPR cameras collect and record license plate images that are visible to the public, including unenclosed driveways of private property. Once an image is captured, the software converts the photo's metadata into a searchable format within a database. The ALPR scans typically record moving vehicles and may not always be accurate, necessitating officer verification prior to any action.

In 2022, the Department signed a five-year contract, expiring on June 21, 2027, with the first of three ALPR vendors — Motorola Solutions (Motorola)[5] — to install 140 ALPR cameras on police vehicles (roof-mounted cameras), 60 pole-mounted cameras, and three trailer cameras.[6] The Department repurposed three salvaged trailers with spare ALPR equipment, resulting in a total of seven trailer cameras available for deployment in the field. Due to an increase in vehicle thefts, Newton Division was the first to receive roof-mounted ALPR cameras. The remaining cameras were evenly distributed throughout the Department by March 2026.[7]

The second ALPR vendor, Flock Safety (Flock), typically services businesses, residential communities, and public sector agencies with pole-mounted cameras and data storage. Of the 138 pole-mounted cameras serviced to the LAPD, 50 are in the Pacific Palisades area to assist in the aftermath of the January 2025 Palisades Fire, 49 are in West Los Angeles Area, and 39 are distributed throughout Council District 11.[8] In total, the Department has access to the data collected by 298 pole-mounted cameras throughout Los Angeles (160 through Motorola and 138 through Flock).

The Department's partnership with the third ALPR vendor, Axon Enterprise (Axon), is the most widely used, as the ALPR feature is integrated into the existing Digital In-Car Video (DICV) system. In 2023, the ALPR feature was activated in approximately 1,500 police vehicles.[9] Axon data — including DICV, Body-Worn Video (BWV), and ALPR images — is stored in Evidence.com, an application used by the Department to access video evidence. Evidence.com does not have the capability to query ALPR data. As a result, Axon partnered with Flock to use

---

[5] The OIG reviewed the related contract, signed by the former Chief of Police and former Los Angeles City Attorney. The ALPR system was originally serviced by Vigilant Solutions, which was acquired by Motorola in 2019. The contract is available at: https://cityclerk.lacity.org/onlinecontracts/2022/C-140535_c_6-22-22.pdf

[6] A trailer camera is a mobile portable vehicle equipped with a camera mounted on a pole designed to capture license plate images. Trailer cameras are primarily used during major events, such as sporting events or parades.

[7] The delay in the final implementation of the roof mounted cameras occurred because of operational and tactical planning priorities, such as the Dodgers World Series Championship parade.

[8] *See* Appendix A. The Flock MOU provided by the Department outlines the terms and conditions of use for the 50 Flock donated cameras currently being used in the Palisades area in response to the January 2025 fires. The document was signed by Flock general counsel in January 2025 and signed by the Chief of Police (undated). Additionally, the document includes a signature block for the City Attorney for approval; however, it remains unsigned.

[9] This is an approximate number, as police vehicles may be out of service on any given day due to maintenance or other issues.

their application to search Axon-captured ALPR information. Although Axon ALPR data is owned by the LAPD and not Flock, the Department does not currently have a written agreement with Flock or Axon outlining security measures and protocols to secure Axon ALPR data within Flock's system. Flock's access to Axon data is unknown in the absence of a written agreement.

In 2016, the Department entered a 10-year contract with Axon, expiring July 31, 2026, to equip officers with BWV cameras and intermediate force electronic weapons (TASERs). In 2022, the Department attested the contract with Axon to include the use of the ALPR feature integrated within the DICV system.[10] The contract outlined several security provisions and requirements regarding data ownership, sharing, and storage to ensure the Department remained the sole and exclusive owner of the collected data, prohibiting data sharing. As with Motorola and Flock, Axon must meet the FBI's Criminal Justice Information Services (CJIS) data storage requirements to ensure data security. The OIG did note that while the Axon contract does emphasize data ownership, it lacks specific language to address retention, search capability, and information sharing with other law enforcement organizations. The contract contains clear language establishing data ownership, security, portability, and data deletion but does not specifically address compliance with California ALPR statutes.

California law limits the use of local resources for federal immigration enforcement and establishes safeguards governing the collection, use, and sharing of personal information.[11] Recent federal immigration enforcement actions, however, have heightened scrutiny of law enforcement technology and data-sharing practices, particularly where contractual arrangements, technological capabilities, or third-party access may permit uses that are inconsistent with the intent of those safeguards.

On June 11, 2023, the Department entered into a Memorandum of Understanding (MOU) with Flock that remained in effect until June 2026.[12] The MOU provided the terms and conditions for which the Department had the right to access the features and functions of the Flock service during the term. The MOU states that Flock retains the right to any recordings or data provided through Flock and it may use the data for any purpose.

On January 23, 2025, the Department signed an MOU with Flock detailing the terms of use associated with the 50 cameras loaned to the Department in the Pacific Palisades area.[13] The MOU outlines the terms and conditions associated with data optimization, liability, insurance, and operational use. The City and City Users are named as the responsible parties for all acts

---

[10] The OIG reviewed the related contract, signed by the former Chief of Police and former Los Angeles City Attorney. The contract is available at: https://cityclerk.lacity.org/onlinecontracts/2022/C-140744_C_07-01-22.pdf

[11] Senate Bill 34 (2015) and Senate Bill 54 (2017) — the California Values Act of 2017 is also known as the 'Sanctuary State' law. The law limits state and local law enforcement agencies from using resources to assist with federal immigration enforcement. Additionally, in December 2024, the City of Los Angeles passed Ordinance 188441, which prohibits the use of any City resources, personnel, property and data to support federal immigration enforcement.

[12] See Appendix A. The MOU was signed on June 11, 2023, for a three-year term.

[13] *See* Appendix B. The MOU was signed on January 23, 2025, for a six-month term.

and omissions of data captured. The MOU lacks provisions to address data breaches or other liability caused by Flock.

According to the MOU, "*LAPD is the sole and exclusive owner of all data and information provided to Flock by or on behalf of LAPD as well as any data collected by the Flock Equipment in the City of Los Angeles (City Data)*."[14] Although the MOU highlights the Department's ownership of the information collected by Flock cameras, Flock retains the right to analyze and anonymize City Data and City generated data to improve and enhance Flock services and system development. Specifically, the MOU states "*Flock shall have the right to collect, analyze, and anonymize City Data and City generated data to the extent such anonymization renders the data non-identifiable."* The MOU notes Flock's intent behind the collection and anonymization of data is to *"improve and enhance the services for other development, diagnostic and corrective purposes*," or to assist in the enhancement of technology in vehicle identification.

The OIG requested any contracts or other agreements related to the Flock cameras and Flock's access to Axon data. The Department could not produce documentation establishing the contractual authority that identify applicable data-sharing terms and other governing provisions. The absence of formal agreements is particularly concerning given the growing national concern over third-party access to ALPR data and the limited understanding within law enforcement of how such data is accessed, shared, and used.

In October 2025, the University of Washington's Center for Human Rights reported that Flock had implemented an information-sharing pilot program that allowed federal agencies to access license plate data collected by local law enforcement agencies without those agencies' knowledge or consent. [15] The report raised questions about whether agencies fully understand the scope of data access available through the platform and whether existing agreements adequately protected against unauthorized information sharing.

Since that report, public allegations of data sharing and misuse have prompted other jurisdictions to deactivate cameras or terminate contracts with Flock. In 2025, Hillsborough, North Carolina[16] announced that it would end its contract with Flock, followed by Flagstaff, Arizona.[17] In 2026, additional jurisdictions cancelled their contracts with Flock including Santa Cruz,[18] Santa Clara County,[19] Mountain View,[20] and South Pasadena.[21]

[14] The Flock MOU defines "City Data" as data collected by Flock equipment in the City of Los Angeles.
[15] https://jsis.washington.edu/humanrights/2025/10/21/leaving-the-door-wide-open/
[16] https://www.hillsboroughnc.gov/Home/Components/News/News/856/14
[17] https://www.azfamily.com/2025/12/20/flagstaff-cancels-controversial-contract-flock-safety-cameras/
[18] https://santacruzlocal.org/2026/01/13/santa-cruz-leaders-vote-to-terminate-contract-with-flock/
[19] https://www.kqed.org/news/12074467/santa-clara-county-leaders-cut-out-flock-safety-in-new-surveillance-policy
[20] https://www.mountainview.gov/Home/Components/News/News/1211/284
[21] https://www.foxla.com/news/south-pasadena-remove-flock-safety-cameras-over-privacy-concerns

B. Funding

As of the date of this report, the Department has access to ALPR data captured by 298 pole-mounted cameras, approximately 1,500 police vehicles equipped with in-car cameras, 140 roof-mounted cameras, and seven mobile trailer cameras that can be deployed anywhere in the City of Los Angeles. Of the 298 pole-mounted cameras, 139 were funded by Council Districts 11 and 12, 60 were purchased by the Department,[22] 49 were acquired by the Los Angeles Police Foundation (LAPF) using donated funds from local Homeowners Associations, and the remaining 50 cameras are currently on loan and strictly for use in the Pacific Palisades area to support law enforcement efforts after the Palisades Fire. All pole cameras have been distributed throughout the City, with placement focused on high-traffic pedestrian areas, freeway entrances and exits, and areas known for high-risk crime.

In 2023, former Chief of Police Michael Moore presented to the BOPC the Department's 2023-2025 Strategic Plan outlining an intention to increase pole camera placement throughout the City of Los Angeles by 50% in the 2023-2024 fiscal year and again by another 50% in the 2024-2025 fiscal year. [23] The funds used to purchase and install some cameras were provided by the LAPF, with former Chief Moore noting earmarked monies to support the maintenance of the cameras moving forward. A review of BOPC agenda items between December 2024 and May 2025 revealed $619,302 provided on behalf of the LAPF in support of ALPR technology.[24, 25] The table below shows the Department's ALPR camera distribution and funding source.[26]

[INTENTIONALLY LEFT BLANK]

[22] The Department purchased the cameras using the Urban Areas Securities Initiative (UASI) Grant. UASI is a grant provided by the Department of Homeland Security to fund dense high-risk regions to prevent, prepare for, and respond to threats.
[23] https://www.lapdpolicecom.lacity.org/072523/BPC_23-122.pdf.
[24] The Los Angeles Police Foundation is the primary non-profit partner and largest source of private funding for the Los Angeles Police Department.
[25] This total was determined upon review of the 2025 BOPC approved items. BOPC agenda archives can be found at: https://www.lapdonline.org/police-commission/police-commission-meetings-archives/
[26] *See* Appendix C for a map of the distribution of the pole cameras and related purchase orders, where available.

Camera Type	No. of Cameras	Location	Funder
FLOCK SAFETY CAMERAS			
Pole Mounted	50	West Los Angeles (Palisades)	On loan for use by the Department due to the January 2025 Palisades Fire
Pole Mounted	49	West Los Angeles	Los Angeles Police Foundation[27]
Pole Mounted	39	Council District 11	Council District 11[28]
MOTOROLA SOLUTIONS CAMERAS			
Pole Mounted	100	Devonshire	Council District 12[29]
Pole Mounted	8	77th St.	Los Angeles Police Department [30]
Pole Mounted	5	Hollywood	Los Angeles Police Department
Pole Mounted	3	Central	Los Angeles Police Department
Pole Mounted	4	Olympic	Los Angeles Police Department
Pole Mounted	5	Southeast	Los Angeles Police Department
Pole Mounted	5	Wilshire	Los Angeles Police Department
Pole Mounted	4	Hollenbeck	Los Angeles Police Department
Pole Mounted	3	Mission	Los Angeles Police Department
Pole Mounted	4	North Hollywood	Los Angeles Police Department
Pole Mounted	3	Newton	Los Angeles Police Department
Pole Mounted	3	Rampart	Los Angeles Police Department
Pole Mounted	3	West Valley	Los Angeles Police Department
Pole Mounted	1	Foothill	Los Angeles Police Department
Pole Mounted	2	Harbor	Los Angeles Police Department
Pole Mounted	2	Northeast	Los Angeles Police Department
Pole Mounted	2	Topanga	Los Angeles Police Department
Pole Mounted	2	Van Nuys	Los Angeles Police Department
Pole Mounted	1	Southwest	Los Angeles Police Department
Trailer	4[31]	Various	Los Angeles Police Department
Roof Mounted	140	Department-Wide	Los Angeles Police Department
AXON CAMERAS			
Police Vehicles	Approx. 1,500	Department-Wide	Los Angeles Police Department

[27] All donations are presented to and approved by the BOPC. Agenda archives can be found at: https://www.lapdonline.org/police-commission/police-commission-meetings-archives/. Donations to purchase the 49 cameras were approved between December 2024 and May 2025.
[28] https://cd11.lacity.gov/press-releases/councilmember-traci-park-launches-comprehensive-public-safety-package-make-council. The funds were transferred from Council District 11 to the Department, then the Department submitted a Purchase Order to the City of Los Angeles, General Services Division (GSD).
[29] https://cd12.lacity.gov/articles/automated-license-plate-reader-program-launches. The funds were transferred from Council District 12 to the Department, then the Department submitted a Purchase Order to GSD.
[30] The Department purchased 60 pole cameras and 4 trailer cameras using UASI grant funds.
[31] The Department repurposed three salvaged trailers with spare ALPR equipment, resulting in a total of seven trailer cameras available for deployment in the field.

C. System Use

In June 2025, ITB presented its annual Comprehensive Technology Report to the BOPC which included the Department's use of ALPR technology.[32] The report highlighted the frequency and efficacy of ALPR usage, emphasizing its value in follow-up investigations. The Department's ALPR system is used by investigators to develop leads for existing investigations, while officers in the field rely on real-time alerts to initiate a traffic stop on vehicles linked to crimes, involve at-risk or missing persons, or are stolen.

Department policy outlines the following authorized uses of ALPR data for official Department purposes:[33]

- criminal investigations or proceedings,
- non-criminal investigations,
- administrative investigations or proceedings,
- civil investigations or proceedings,
- situational awareness operations, and
- responses to cognizable threats to public safety.

The purpose of the ALPR system is to capture and store images of license plates and associated vehicle information. The system does not perform analytical functions, identify trends, patterns, or incorporate facial recognition capabilities. Additionally, ALPR data is not used to support predictive policing strategies or generate forecasts about potential criminal activity.

D. Data Access

Access to ALPR data requires Department personnel to complete a course through the LAPD's online training platform — Learning Management System (LMS) — to demonstrate proficiency and understanding of the system. The two-hour training course provides officers with an overview of ALPR functionality, use, and current Department policy. Once the training is successfully completed and the user has demonstrated an understanding by passing a quiz, the user is granted an investigator account with access to query ALPR data. Recertification and follow up training of the ALPR system is not required; however, Department employees are encouraged to participate in various trainings provided by the vendor, free of charge.

Once an account has been granted, a user can query ALPR data through either the Motorola or Flock applications. Department personnel access both Flock and Axon ALPR data through the Flock application, while Motorola remains a standalone application. To query the Flock application, the user must enter the related case identification details in the free-form text box in addition to providing a reason for the query in another free-form box. The user must then select

---

[32] Department report titled, "Comprehensive Technology Report," dated May 16, 2025. *See* https://www.lapdpolicecom.lacity.org/062525/BPC_25-164.pdf

[33] Department Manual, Volume III, Section 568.53, *Automated License Plate Recognition Usage and Privacy Policy – Authorized Uses*.

an "offense type" from a dropdown menu to expand upon the search reason. The Motorola application shares similar characteristics to Flock, requiring the user to list casefile identification details in a free-form text box, followed by selecting a reason for the license plate query from a dropdown menu.[34] Because both applications permit users to enter case information in a largely unstructured manner, the resulting records lack consistency. As a result, auditing user activity and identifying potential misuse requires significantly greater effort.

E. Data Sharing

Department policy states that ALPR data recorded or retained by the Department shall not be sold, shared, transferred, or disclosed and shall only be shared with local law enforcement agencies in which the Department has entered an Memorandum of Agreement (MOA).[35] MOAs require partnering law enforcement agencies to take various measures to ensure data security, including: (a) provide quality assurance of information entered, (b) maintain data sharing protections, and (c) ensure data security and privacy. MOAs typically expire after three years from the date of the last signature, unless terminated early by written agreement.

At present, the Department has an MOA with the following law enforcement agencies: (1) Huntington Park Police Department, (2) La Mesa Police Department, (3) Livermore Police Department, (4) San Luis Obispo Sheriff's Department, (5) West Covina Police Department, (6) Los Angeles Port Police, (7) Torrance Police Department, (8) Ceres Police Department, (9) Hayward Police Department, (10) Signal Hill Police Department, (11) Glendale Police Department, (12) Alhambra Police Department, (13) Simi Valley Police Department, (14) Rohner Police Department, and (15) Madera County Sheriff's Department.[36] MOAs prohibit the sharing of ALPR data outside the contracted parties.

While the terms of the MOA require partnering agencies to maintain data confidentiality, sharing protections, security and privacy, the MOA does not require the partnering agency to conduct periodic audits to evaluate compliance. Further, the Department does not conduct any regular inspections of the search queries submitted by partnering agencies. However, any violation of an MOA identified by the Department would result in the termination of the agreement.

Public concern regarding safeguards and information sharing of ALPR data with federal agencies has grown since June 2025. This concern was heightened following the publication of a 2026 internal audit of the Mountain View Police Department's use of Flock.[37] According to the audit, a pattern of concerning search terms, such as "ICE" and "immigration" emerged suggesting

---

[34] The dropdown list includes, "be on the lookout," "crime analysis," and other general reasons for conducting a query of the data.
[35] Department Manual, Volume III, Section 568.53, *Automated License Plate Recognition Usage and Privacy Policy – Sharing of ALPR Data*.
[36] *See* Appendix C. The OIG reviewed all the signed MOAs between the Department and each participating agency and found that all agreements contained identical terms and provisions. This list is current as of the date of this report.
[37] https://content.govdelivery.com/accounts/CAMOUNTAINVIEW/bulletins/406f640

Mountain View Police Department officers were conducting searches on behalf of federal agencies. Considering these public concerns, the OIG requested ITB conduct an audit of the ALPR applications.

In July 2025, ITB inspected both the Flock and Motorola applications for search terms including "immigration" and "ICE" and reported no instances of those terms being used to query ALPR data.[38] The Department's written agreement with Motorola outlines the guidelines for maintaining the confidential information collected by their ALPR cameras and, specific to the sharing of information, the agreement states that Motorola is prohibited from sharing any ALPR data or information with ICE.[39]

Department policy states that the Department's ALPR system shall only be accessed and used on a "need to know" and "right to know" basis.[40] On November 6, 2025, the Department disseminated an e-mail titled, *"Sensitive and Confidential Department Records and Information Reminder,"* to remind all personnel of the Department's policies governing confidential records, reports, and information release and to reinforce that all Department records — even those not classified as sensitive or confidential — remain the property of the Department.[41] Access to ALPR data applications is restricted through unique login credentials, requiring authorized LAPD usernames and passwords.

F. Data Retention, Storage, and Department Oversight

Department policy outlines the guidelines for the management, storage, and security of ALPR data captured, noting all data shall be stored on a Department approved storage system compliant with CJIS.[42, 43] Specifically, Axon and Motorola data are stored for five years in their application specific databases but are searchable by users for only two years. It is only upon

---

[38] The OIG's request was limited ICE and did not encompass other agencies within the Department of Homeland Security.

[39] Section titled "Information Sharing" of the agreement states, "For the avoidance of any doubt, no ALPR data collected by the Contractor for the LAPD pursuant to this Agreement shall be provided by the Contractor to any person or entity outside of the LAPD, except at the prior and express written direction of the Commanding Officer of Information Technology Bureau. Further, and notwithstanding anything in this Agreement to the contrary, the Contractor shall not provide any ALPR data or information, gathered from or for the LAPD as part of performing the services of this Agreement, with the U.S. Immigration and Customs Enforcement agency of the U.S. Department of Homeland Security."

[40] Department Manual, Volume III, Section 568.53, *Automated License Plate Recognition Usage and Privacy Policy - Limitations on Use of ALPR Data.*

[41] E-mail dated November 6, 2025, cited Department Manual, Volume III, Section 406.10, *Guidelines and Restrictions for the Release of Police Record Information*, and Section 408.16, *Releases of CORI - Determination of Right - To -Know/Need - To - Know*.

[42] Department Manual, Volume III, Section 568.53, *Automated License Plate Recognition Usage and Privacy Policy*.

[43] The Federal Bureau of Investigations' approved storage system compliant with information security standards is called the Criminal Justice Information System (CJIS). Flock, Axon, and Motorola meet CJIS standards.

special request that an ALPR manager may view data for the remaining three years. Flock data is stored on Flock servers for a period of five years.[44]

When searching for a license plate captured by Motorola, Flock, or Axon, an authorized user can query either the Motorola or Flock applications. Motorola and Flock have capability to conduct a license plate only search, as opposed to Axon which does not. While all Axon captured data is stored in Evidence.com, the information is not searchable by license plate number only. As a result, Axon partnered with Flock which provides one way query and data retrieval of Axon data. As previously reported, the Department does not currently have a written agreement with Flock or Axon outlining security measures and protocols to ensure data security between Axon and Flock.

The ALPR applications operate under the assumption a user has the appropriate accesses, purpose, and "need to know" associated with the application. Because an investigator must go through an approval and training process to obtain an account, there is an expectation the investigator adheres to mandated access and data sharing rules. The Department regularly monitors employee investigator accounts, which are automatically deactivated when inactive for more than 90 days. Investigator accounts are also deactivated when Department personnel have been terminated, retired, or resigned. The Department's System Administrator is responsible for the deactivation of the investigator accounts, which occurs daily, Monday–Friday. This practice stems from a 2022 Department Audit of the ALPR system, which identified inactive user accounts that had not been deactivated.[45]

The 2025 Comprehensive Technology Report outlines the Department's technology oversight efforts — both ITB and the Department's Audit Division are responsible for conducting compliance inspections to ensure alignment with established policies and procedures, including data access. In addition, Department policy requires Audit Division to conduct periodic audits of access and use of ALPR data in accordance with their Annual Audit Plan.[46] Further, Department policy requires the Department's ITB to maintain ALPR data access records for five years.[47]

Department policy also states that ITB should conduct regular inspections on the use and the operations of the ALPR system. Accordingly, ITB conducts monthly inspections of the search terms used by Department investigators to query ALPR data. These inspections are not formally documented or memorialized and are intended to ensure administrative compliance with

---

[44] *See* Appendix B. 'Confidentiality' – Flock shall retain all data collected for five years at no charge to the Department or City.

[45] The Department presented its 2022 Audit, "Automated License Plate Recognition Audit" to the BOPC in October 2022.

[46] Department Manual, Volume III, Section 568.53, *Automated License Plate Recognition Usage and Privacy Policy-Records of Access and Periodic System Audits*.

[47] Records of access include:

- the date and time the information is accessed;
- the license plate number or other data elements used to query the ALPR System;
- the username of the person who accessed the information; and,
- the identified authorized purpose for accessing the information.

Department policy, rather than identify employee misconduct or misuse of access. The inspection results may be provided to the ITB Commanding Officer upon request.

Motorola allows for additional data management oversight by allowing the Department to audit the vendor's data privacy and security program once per calendar year with 30 days' advance notice.[48]

G. Hot Lists

The ALPR alerts are generated when a scanned license plate matches an entry on a Hot List maintained in one of three databases. These databases include records of vehicles connected to a crime, are stolen, or involve missing or at-risk individuals. The first database is maintained by the California Department of Justice (CalDOJ) and contains license plate details of vehicles identified by law enforcement officers throughout the state of California. The vehicles entered in the CalDOJ database remain there until the vehicle has been located and the corresponding law enforcement entity that entered the plate details removes it from the database. The Department's Vehicle Identification and Processing Unit (VIPU) has access to the CalDOJ database and is responsible for entering and removing stolen vehicles identified by LAPD, and only LAPD. The VIPU operates 24 hours a day and is staffed by civilian employees.

The second and third databases are generated and maintained by LAPD and Los Angeles County Sheriff's Department (LASD). Both databases provide instructions connected to the license plate for officer awareness when encountering and engaging the vehicle. The LASD entries are entered and removed by LASD and do not have an automatic expiration date, as opposed to manual entries made by the Department, which expire after three days.

H. Hot List Alerts

Roof-mounted and DICV ALPR cameras are always active and continuously scanning license plate numbers whenever the police vehicle is turned on. As the camera is scanning license plates, the ALPR system is comparing those details to the Hot Lists, in real-time. When a license plate matches with a vehicle of interest on a Hot List, an alert will appear on the police vehicle's Mobile Digital Computer (MDC).[49] The camera lens on a DICV will capture what is directly in front of the lens, where as a roof-mounted camera will capture a higher angle and will therefore capture different surrounding images due to its placement. If a police vehicle has both ALPR cameras and they scan and match with the same license plate, two separate alerts will appear on the vehicle's MDC screen simultaneously.

Officers may acknowledge if the hit was correct or incorrect, as errors with scanning and matching license plates do occur.[50] For a correct hit, officers may take further action but are not

[48] *See* Motorola contract: https://cityclerk.lacity.org/onlinecontracts/2022/C-140535_c_6-22-22.pdf.
[49] The MDC is a mobile computer that connects to Department databases and resources for use by officers when in the field.
[50] Letters, numbers, or registration State can be misread.

required to take further action as they may be actively investigating another incident or unable to safety change direction to peruse the vehicle from the alert.

An ALPR alert does not immediately inform field officers of the reason for the license plate's placement on the Hot List.[51] Officers must utilize Department resources available through the MDC to gather more information to safely approach the vehicle. Often, officers will approach the vehicle with extreme caution or conduct a "high-risk" stop. This involves calling for back up, air support, and a supervisor and ordering the suspect out of their vehicle. Department policy requires officers to attempt to verify the accuracy of the ALPR alert prior to conducting a stop.[52]

III. OIG REVIEW OF ALPR ALERTS

The ALPR system assists field officers by providing real-time alerts of vehicles wanted in connection with felony crimes, stolen vehicles, or other criminal investigations. These alerts enable officers to respond promptly and take appropriate enforcement action when they are available, in accordance with Department policy. The OIG sought to assess the overall outcomes resulting from Hot List alerts during the defined review period: August 1 to September 30, 2025.

A. Review Period and Available Alert Outcome Data

All police vehicles have one ALPR camera integrated in the DICV system, while a limited number of police vehicles have an additional camera mounted on the roof (approximately 140 of 1,500 or roughly 10%). Both camera systems overlap a portion of their field of view but also scan slightly different areas based on their placement. Police vehicles with both ALPR camera systems will simultaneously provide officers with an alert from both the Motorola and Axon applications — where the same license plate is scanned prompting officers to confirm whether the license plate read is accurate. The Axon application also enables officers to document any action taken in response to a confirmed Hot List alert. Accordingly, the results and outcomes of alerts generated by roof-mounted ALPR cameras are not documented within the application and therefore not available for inclusion in this review.

The Department provided the OIG with all Hot List alert data extracted from the Axon application for the two-month review period of August 1 to September 30, 2025. The raw data indicated that 50,180 ALPR hits through Axon were reported to field officers during the review period.[53] The OIG removed all duplicate alerts and organized the remaining data by date, time,

[51] Officers are unable to respond to every ALPR alert due to various circumstances encountered during patrol, including responding to a critical incident, traffic safety considerations, or not hearing the alert while outside the vehicle.
[52] Department Manual, Volume III, Section 568.53, *Automated License Plate Recognition Usage and Privacy Policy – Quality Assurance* states "Department personnel shall attempt to verify records obtained prior to conducting an investigative stop."
[53] The OIG identified numerous duplicate alerts caused by multiple police vehicles responding to the same scene and simultaneously capturing the targeted license plate. These multi vehicle responses also result in multiple actions reported for a single incident.

involved officer serial number, vehicle description and license plate number of vehicle of interest, and the action taken, if any.[54]

The Axon application enables field officers to select from a list of actions taken, including but not limited to "no action taken," "citation issued," "arrest – felony," "not stolen," "not wanted (person)," and "vehicle recovered/towed/impounded." The application only allows for one option from the list to be selected. In the absence of a selection, the default will record the disposition of "no action taken." The Axon application is not designed to analyze or track actions taken. As a result, the OIG was unable to accurately identify primary unit officers or determine the overall outcomes of law enforcement actions in response to ALPR hits during the review period.

For stops resulting in an arrest, the OIG reviewed BWV recordings, incident details, and related reports to corroborate and document the actions taken and to ensure a clear understanding of the incident outcome.

IV. OIG REVIEW RESULTS AND FINDINGS

The roof-mounted ALPR system does not capture actions taken in response to Hot List alerts, and the DICV ALPR system data is not structured in a manner that allows for efficient analysis. Accordingly, the compiled data cannot be considered a complete or accurate measure of all actions taken in response to alerts during the two-month review period.

Based on available Axon data, the OIG determined that of the 50,183 total alerts, 5,911 were unique license plates. During the two-month review period, the Department's ALPR cameras generated 210,568,103 license plate reads.

A. No Action Taken

Of those 5,911 license plate hits, for 4,575 alerts officers verified the license plate match was accurate and selected "no action taken" or did not make any selection which also records the disposition as "no action taken."

B. Duplication of Action Taken

Multiple police vehicles that respond to the same incident and get an alert will result in multiple actions taken for the same incident. The OIG identified 1,182 alerts for which officers confirmed the license plate information was correct, but the action taken selected was not accurate and consistent with what occurred. Ideally, only the primary unit officers should document the outcome of the stop. When multiple officers enter or select an action in the system, this can result in duplicate, inconsistent, or incorrect entries about what happened.

[54] Despite extensive analysis, the results of the police action taken may be inaccurate, as multiple officers and police vehicles report differing dispositions for the same incident.

C. Determined Not Stolen

When records are not updated in a timely manner, officers may act on inaccurate or outdated information, increasing the risk of unnecessary enforcement actions, including vehicle stops and wrongful detentions, or a confrontation with serious consequences. Department policy dictates that officers attempt to verify all records prior to conducting an investigative stop; however, conditions outside the officer's control can also impact a stop. For example, delays in updating records may cause a license plate to remain on a Hot List after the vehicle has been recovered or is no longer considered stolen.

During the review period, officers acknowledged 161 alerts as accurate license plate matches; however, subsequent investigations determined the vehicles were not stolen.

In addition to creating an inconvenience for vehicle owners, these inaccuracies can affect individual liberty interests, erode public trust, and potentially create substantial legal and financial liability concerns.

D. Stolen Vehicles and Stolen License Plates Recovered

The OIG found that during the two-month review period, 337 stolen vehicles were recovered without incident. Valley Bureau recovered the most vehicles, with 144 recoveries, followed by Central Bureau with 72, South Bureau with 70, West Bureau with 44, and seven with Traffic Services Division.

Additionally, the OIG noted the recovery of 24 stolen license plates attached to a vehicle not reported stolen. The tactic of stealing a license plate from an inconspicuous vehicle to place on a stolen vehicle is used to deter investigators and evade capture.

E. Arrests and High-Risk Stops

The OIG identified 74 arrests resulting from 68 stops generated by Hot List alerts.[55] Of those, five stops involved the arrest of the driver and occupants.[56] Of the 68 arrests, 15 suspects were charged with Grand Theft Auto, 34 were charged with Taking of a Vehicle without the Owner's Consent, four were charged with Evading, and three were charged as a Felon in Possession of a Firearm. The remaining charges include Robbery, Battery, Assault with a Deadly Weapon, Receiving Stolen Property, and Terrorizing Causing Fear.

Of those 68 stops, officers used high-risk stop tactics to remove the vehicle occupants from the vehicle and take them into custody during 46 stops. The Department manual states officers must broadcast Code Six Charles when encountering a license number connected with suspects or vehicles considered armed and dangers—generally leading to a responding officer using high-

[55] When querying the data, arrests were categorized in three ways: 'arrest' (7 occasions), 'Criminal Charge' (3 occasions), 'Arrest-Felony' (69 occasions), and 'Arrest – Misdemeanor' (6 occasions).
[56] Occupants taken into custody had existing arrest warrants.

risk stop tactics for safety purposes.[57] Patrol officers will determine the necessity of a high-risk stop based on the information listed when verifying the license plate number.

F. Vehicle Pursuits

The OIG identified nine vehicle pursuits that resulted from Hot List alerts during the review period. Of these nine pursuits:

- Five concluded with the suspects surrendering and being taken into custody without incident;
- One involved a foot pursuit ending in a surrender;
- One involved both a foot pursuit and a non-categorical use of force as officers used body force to subdue the suspect to the ground, placing them into handcuffs prior to taking them into custody;
- One involved a traffic collision resulting in undercarriage damage to the suspect vehicle, followed by a foot pursuit that concluded with the suspect's surrender;[58]
- The final pursuit was handed off to CHP and ended in a surrender.
- Only one of the nine pursuits involved a vehicle containing more than one occupant where all suspects were arrested.[59]

V. RECOMMENDATIONS

The OIG makes the following recommendations:

1. Suspend the deployment of new ALPR cameras and the execution of new ALPR-related contracts pending public input and a broader reassessment of vendors and data practices. If the Department continues to use ALPR technology, it shall obtain approval from the BOPC for formal contracts or agreements with all ALPR vendors, regardless of the contract amount or whether the agreement involves an exchange of funds. Those contracts or agreements shall establish enforceable requirements governing data security, privacy, access controls, retention, and auditing to protect Department ALPR data and ensure accountability for its collection, use, and disclosure.

   Note: In 2020, the California State Auditor recommended the LAPD update ALPR vendor contracts with necessary data safeguards to address shortcomings the audit identified.

[57] When engaging in a high-risk stop, officers will typically request back up units and an airship to assist in taking the driver and other occupants into custody. Officers will draw their weapons, using their vehicle as a barrier—calling commands to the driver and any vehicle occupants.
[58] The suspect's erratic driving caused the vehicle's undercarriage to hit the road, causing damage.
[59] The arrests associated with the nine pursuits are included in the total of 74 arrests.

2. Strengthen oversight of ALPR data access by amending Department policy to require annual audits to ensure that Department personnel are using the ALPR systems for authorized purposes and to clearly communicate that misuse of ALPR data may result in disciplinary action.

3. Develop and implement a standardized process for documenting traffic stops initiated by ALPR alerts to ensure complete and accurate records and facilitate meaningful analysis of officer actions and stop outcomes.

VI. DEPARTMENT RESPONSE

INTRADEPARTMENTAL CORRESPONDENCE

June 29, 2026
1.1

TO: Office of the Inspector General

FROM: Chief of Police

SUBJECT: LOS ANGELES POLICE DEPARTMENT'S RESPONSE TO THE OFFICE OF THE INSPECTOR GENERAL'S REVIEW OF THE DEPARTMENT'S AUTOMATED LICENSE PLATE READER (ALPR) SYSTEM AND USE IN THE FIELD

The Los Angeles Police Department (LAPD or Department) has received the Office of the Inspector General's (OIG) draft report of the Review of the Department's Automated License Plate Reader (ALPR) System and Use in the Field. The Department appreciates the OIG's thorough and balanced review and welcomes the opportunity to respond.

ALPR technology is a vital, lawful public-safety tool that helps officers identify and apprehend criminal suspects, recover stolen vehicles and license plates, locate missing and at-risk persons, and advance active investigations, all while operating within the privacy framework established by California law and Department policy. Objective results from the OIG's two-month review (August 1 through September 30, 2025) demonstrate this value. During that period, in-car ALPR alerts contributed to the recovery of 337 stolen vehicles, each recovered without incident, and 24 stolen license plates that had been affixed to other vehicles to evade detection. ALPR alerts led to 68 stops resulting in 74 arrests, including 15 for Grand Theft Auto, 34 for unlawful taking of a vehicle, four for evading, and three for felon in possession of a firearm, along with arrests for robbery, assault with a deadly weapon, and criminal threats. Nine vehicle pursuits arising from alerts were resolved, with every suspect taken into custody. In addition, 50 pole-mounted cameras, donated at no cost, continue to support public safety and recovery efforts in Pacific Palisades following the devastating January 2025 Palisades Fire. For these reasons, the Department is committed to the continued, responsible use of ALPR technology and, as set forth below, to strengthening the contractual, oversight, and documentation safeguards that protect the data it generates.

The report includes three recommendations to be made as follows:

SECTION V. RECOMMENDATIONS

1. Suspend the deployment of new ALPR cameras and the execution of new ALPR-related contracts pending public input and a broader reassessment of vendors and data practices. If the Department continues to use ALPR technology, it shall obtain approval from the Board of Police Commissioners for formal contracts or agreements with all ALPR vendors, regardless of the contract amount or whether the agreement involves an exchange of funds. Those contracts or agreements shall establish enforceable requirements governing data security, privacy, access controls, retention,

and auditing to protect Department ALPR data and ensure accountability for its collection, use, and disclosure.

2. Strengthen oversight of ALPR data access by amending Department policy to require annual audits to ensure that Department personnel are using the ALPR systems for authorized purposes and to clearly communicate that misuse of ALPR data may result in disciplinary action.

3. Develop and implement a standardized process for documenting traffic stops initiated by ALPR alerts to ensure complete and accurate records and facilitate meaningful analysis of officer actions and stop outcomes.

Department Response

The Department appreciates the OIG's review and concurs with the intent of each of the three recommendations, which is to ensure that ALPR technology is governed by enforceable agreements, rigorous oversight, and accurate records. The Department's responses to each recommendation are set forth below. The Department also respectfully offers several clarifications to ensure the final report is accurate and complete.

1) In response to Recommendation No. 1: The Department concurs. The Information Technology Bureau (ITB) has already paused the deployment of additional ALPR cameras and the acceptance of any further camera donations through the Los Angeles Police Foundation, pending completion of the contractual work described below. The Department also affirms that no ALPR contract or agreement with any vendor can proceed without approval from the Board of Police Commissioners and transmittal to the Mayor's Office. This requirement applies regardless of the dollar value of the agreement or whether it involves an exchange of funds, and it is already the Department's established practice.

   As part of this pause, ITB is working with the Office of the City Attorney and other major US cities through the Major City Chiefs Association to develop standardized contractual language to govern all ALPR vendor agreements going forward. A copy of this draft language is provided as Attachment A for the OIG's review. The draft directly addresses each contractual gap the OIG identified. It establishes that the City is the sole and exclusive owner of all City Data, including all metadata and all derived or algorithmic outputs (Section 10.2); it prohibits the vendor from using City Data for any purpose other than providing the contracted service to the Department, and specifically bars the vendor from selling, sharing, aggregating, anonymizing for resale, or using City Data to train, fine-tune, or improve any algorithm or artificial-intelligence system (Sections 10.2 through 10.4); it requires that data be stored in the continental United States and secured in a manner compliant with the FBI Criminal Justice Information Services (CJIS) Security Policy and Security Addendum (Sections 10.4, 10.10, 10.18, and 10.19); it requires breach notification within 24 hours and makes the vendor responsible for, and requires the vendor to indemnify the City against, costs and liability arising from a data breach (Section 10.11); it reserves to the City the exclusive right to

determine whether and with whom City Data is shared (Sections 10.5 and 10.8); and it grants the City the right to audit the vendor's data privacy and security program (Section 10.14). The agreement becomes effective only upon execution by the parties and signature by the City Attorney as to form and legality (Section 2.1), which resolves the unsigned City Attorney approval block the OIG noted on the current Palisades Flock agreement. This language will close the remaining gaps the OIG identified, including the absence of a written agreement governing the security of Axon-captured ALPR data accessed through the Flock application.

The Department further affirms, clearly and unequivocally, that it does not share ALPR data with U.S. Immigration and Customs Enforcement (ICE) or for federal immigration enforcement, and that it will not do so. This prohibition is grounded in the Department's ALPR Usage and Privacy Policy (Manual Section 568.53), California Senate Bill 34 (2015), and Senate Bill 54 (2017, the California Values Act), as well as City of Los Angeles Ordinance No. 188441 (2024), which prohibits the use of City resources, personnel, property, and data to support federal immigration enforcement. The Department's contract with Motorola Solutions expressly prohibits the vendor from providing any ALPR data to ICE. In July 2025, in response to public concern, ITB inspected the Flock and Motorola applications for the search terms "immigration" and "ICE" and found no instances of those terms being used to query ALPR data. The standardized contract language in Attachment A reinforces these protections by prohibiting vendor data sharing and reserving all interagency sharing decisions to the City.

With respect to data shared with other law-enforcement agencies, the Department shares ALPR data only with vetted California law-enforcement agencies under Memoranda of Agreement (MOAs) that require data confidentiality, sharing protections, and data security, and that are terminable upon any violation. All such partner agencies are bound by the same California law that prohibits sharing ALPR data with federal agencies or with agencies outside California. Each agency maintains its own internal audits and controls over its use of shared data. Consistent with standard practice among partner agencies, this is a reciprocal arrangement in which neither the Department nor its partners audit one another's personnel.

Finally, the Department respectfully requests a factual correction regarding its vendor contracts. The 2022 contract with Motorola Solutions (Contract No. C-140535) covers 140 mobile ALPR cameras mounted on police vehicles and access to the vendor's user interface; it does not include fixed pole-mounted or trailer cameras. The 60 fixed pole-mounted cameras and the related trailer cameras were acquired separately via a Department purchase order processed through the City's General Services Department using Urban Areas Security Initiative (UASI) grant funds, the same procurement path used for the Motorola pole cameras funded by Council District 12. The Department respectfully requests that the report be revised to reflect this distinction.

The Department notes the OIG's reference to the 2020 California State Auditor recommendation and agrees that the standardized contract language described above directly addresses that recommendation by incorporating the necessary data safeguards into every ALPR vendor agreement.

2) In response to Recommendation No. 2: The Department concurs with the objective of strengthening oversight of ALPR data access and agrees to amend Department policy to clearly state that misuse of ALPR data may result in disciplinary action. The Department proposes the following approach to the audit requirement. The Department's Audit Division is the only Department entity that performs official, certified audits, applying the specialized training, methodology, and professional certifications that such audits require. Given Audit Division's annual audit calendar and finite resources, the Department recommends that Audit Division conduct a certified audit of ALPR data access on a biennial basis (every two years) rather than annually.

   This certified audit will be complemented by inspections conducted by ITB. ITB will continue to conduct monthly inspections, which will be formalized, documented, and reviewed at the executive level, specifically by the Commanding Officer or Assistant Commanding Officer of ITB. The monthly inspections review Department users' queries for consistency with California law and Department policy. The results of this oversight, including both the biennial certified audits and the monthly ITB inspections, will be reported to the Board of Police Commissioners annually through the Department's Comprehensive Technology Report. The Department believes this layered structure, combining certified biennial audits, documented monthly executive-reviewed inspections, annual public reporting, and explicit language regarding disciplinary consequences, fully satisfies the intent of the recommendation while making responsible use of the Department's audit resources.

   The Department also acknowledges the OIG's observation that the free-form text fields in the ALPR applications make auditing more labor-intensive. As part of the documentation improvements described in response to Recommendation No. 3, the Department will work with its vendors to develop more structured query fields to improve the consistency and auditability of access records.

3) In response to Recommendation No. 3: The Department concurs. Capturing accurate, structured data on law-enforcement actions and outcomes resulting from ALPR alerts, particularly the identification and arrest of criminal suspects, will provide objective, fact-based information documenting the substantial public-safety benefits of ALPR technology and supporting future inspections, audits, and reports to the Board of Police Commissioners. The Department will research and work with its vendors to identify the most efficient and reliable method for capturing this data.

   In doing so, the Department will address the specific limitations the OIG identified. At present, officers are not required to select a disposition following an alert, and an absence of any selection is recorded by default as "no action taken"; this accounts for a substantial portion of the 4,575 alerts the OIG categorized as "no action taken". The Department will evaluate requiring a disposition selection so that the resulting metrics accurately reflect

officer actions. The Department will also work to reduce the duplicate and inconsistent entries that arise when multiple units respond to the same incident and each receives and acts on the same alert, with the goal of having the primary unit document the outcome. The Department further notes that the roof-mounted (Motorola) cameras do not currently capture disposition data within the Axon application; the Department will pursue a documentation method that captures outcomes across both camera systems.

Two additional points of context bear on the accuracy of any outcome analysis. First, for the 161 alerts in which officers confirmed an accurate license-plate match but the vehicle was later determined not to be stolen: these situations generally result from the timing of record updates outside the Department's control, such as delays by another jurisdiction or a vehicle owner in clearing a plate from a Hot List after a vehicle has been recovered or is no longer wanted. Department policy requires officers to attempt to verify the accuracy of an ALPR alert before conducting a stop (Manual Section 568.53, Quality Assurance), and the Department's Vehicle Identification and Processing Unit operates 24 hours a day to enter and promptly remove LAPD-entered stolen-vehicle records. The Department takes the liberty and privacy interests at stake seriously and will continue to emphasize verification.

Second, the Department notes that an ALPR alert does not, by itself, explain why a license plate is on a Hot List. This is a deliberate safeguard: an alert serves as an investigative lead that an officer must independently verify using Department resources before taking any enforcement action. Officers approach such vehicles with appropriate caution, including high-risk stop tactics when the information warrants. This verification-before-action requirement protects both the public and officers and reflects the layered safeguards already built into the Department's ALPR program.

Should you have any questions or concerns regarding this matter, please contact Chief Information Officer Dean Gialamas, Information Technology Bureau, at (213) 486-0370.

Respectfully,

JIM McDONNELL
Chief of Police

Attachment

DRAFT

PROFESSIONAL SERVICES AGREEMENT

CONTRACTOR: FLOCK GROUP, INC.

ALPR CAMERA DATA MANAGEMENT SERVICES

Agreement Number _____

TABLE OF CONTENTS

1.0 PARTIES TO THE AGREEMENT AND REPRESENTATIVES
1.1 Parties to the Agreement
1.2 Representatives of the Parties

2.0 TERM OF THE AGREEMENT
2.1 Term of the Agreement

3.0 PERSONNEL
3.1 Project Manager

4.0 STATEMENT OF WORK
4.1 Statement of Work to be Performed
4.2 Time of Performance

5.0 ACCESS TO CITY FACILITIES AND RESOURCES SUPPLIED BY CITY

6.0 COMPENSATION AND METHOD OF PAYMENT
6.1 Compensation
6.2 Taxes
6.3 Method of Payment

7.0 DISPUTES

8.0 REPRESENTATIONS AND WARRANTIES
8.1 General
8.2 Warranties of Function
8.3 Warranty of Originality
8.4 Warranty of Authority
8.5 Deliverables
8.6 Pass through Warranties
8.7 Compliance with Law
8.8 Software
8.9 System Security

9.0 CONFIDENTIALITY, RESTRICTIONS ON DISCLOSURE, AND BACKGROUND CHECKS
9.1 Confidentiality and Restrictions on Disclosure
9.2 Document Control Procedure
9.3 Background Checks
9.4 Provisions Apply to Subcontracts
9.5 Survival of Provisions

10.0 DATA OWNERSHIP, DATA PROTECTION, OPEN API
10.1 **DEFINITIONS**
10.2 **Data Ownership**
10.3 **Artificial Intelligence and Automated Processing**
10.4 **Data Protection**
10.5 **OPEN API ACCESS — CITY'S UNRESTRICTED RIGHT TO DATA INTEGRATION**
10.6 **SUPPLEMENTAL SENSOR SYSTEM DATA RIGHTS**
10.7 **Scope; Relationship to Section 10.3**
10.8 **INTER-AGENCY AND MULTI-PARTY DATA SHARING**
10.9 **Compliance with Privacy Laws**
10.10 **Data, Development, and Access Point Location**
10.11 **Data Breach**
10.12 **Firewalls and Access Controls**
10.13 **Vulnerability Management and Patching**
10.14 **Right of Audit by City**
10.15 **Written Information Security Policy**
10.16 **Change in Service**
10.17 **Third Party Software**
10.18 **Criminal Justice Information Systems**
10.19 **Security Addendum**
10.20 **Provisions Apply to Subcontracts**
10.21 **Survival of Provisions**

11.0 AMENDMENTS

12.0 MISCELLANEOUS
12.1 Standard Provisions for City Contracts
12.2 Border Wall Disclosure
12.3 Severability/Ambiguity
12.4 Use of Marks
12.5 Media, Publicity, Case Studies
12.6 No Third Party Beneficiaries
12.7 Non-Exclusive Agreement
12.8 Not a Waiver
12.9 Audit Rights
12.10 Payment Does Not Imply Acceptance of Work

13.0 ENTIRE AGREEMENT
13.1 Complete Agreement
13.2 Counterparts/Electronic Signatures
13.3 Number of Originals and Attachments

13.4 Order of Precedence.....

SIGNATURE PAGE.....

AGREEMENT NUMBER _____
BETWEEN THE CITY OF LOS ANGELES
AND
FLOCK GROUP, INC.

This Agreement is made and entered into by and between the City of Los Angeles, California, a municipal corporation (hereinafter referred to as the "City"), acting by and through the Los Angeles Police Department (hereinafter referred to as the "LAPD" or the "Department"), and Flock Group, Inc., a Georgia corporation with a place of business at 1170 Howell Mill Road NW, Suite 210, Atlanta, GA 30318 (hereinafter referred to as the "Contractor")(each a "Party" and collectively, the "Parties").

RECITALS

WHEREAS, the City, acting by and through LAPD, owns and operates an automatic license plate recognition ("ALPR") system composed of a computerized database resulting from the deployment and usage of one or more mobile or fixed cameras and supporting hardware and software (the "LAPD ALPR System"); and

WHEREAS, on February 7, 2023 the Board of Police Commissioners approved a revised Automatic License Plate Recognition Usage and Privacy Policy which governs the LAPD ALPR System; and

WHEREAS, the City has purchased or received via donation certain of Contractor's ALPR cameras and hardware ("Contractor's Hardware"); and

WHEREAS, the usage by LAPD of Contractor's Hardware, and the integration of Contractor's software into the LAPD ALPR System requires Contractor's compliance with governing law and LAPD policy and the execution of an agreement containing necessary obligations and controls; and

WHEREAS, City requires and Contractor agrees to provide an open application programming interface that meets City's specifications; and

WHEREAS, pursuant to Charter Section 1022, City does not have staff or resources with sufficient time or the necessary expertise to undertake these specialized professional tasks in a timely manner, and it is therefore more feasible and in Department's best interest to secure these services by contract; and

WHEREAS, the services required are expert, professional, and technical in nature, and are temporary and occasional in character; therefore, pursuant to Charter Section 371(e)(2), competitive bidding is neither practicable, advantageous, nor consistent with the City's interests; and

WHEREAS, the services required by the LAPD are of a professional and expert and temporary nature; and

WHEREAS, the Parties hereto wish to enter into an Agreement pursuant to which the Contractor will perform the work and furnish the deliverables as described herein for consideration and upon the terms and conditions as hereinafter provided.

NOW THEREFORE, in consideration of the above promises and of the terms, covenants and considerations set forth herein, the parties do agree as follows:

SECTION 1.0
PARTIES TO THE AGREEMENT AND REPRESENTATIVES

1.1 Parties to Agreement

The parties to this Agreement are:

A. City – The City of Los Angeles, a municipal corporation, acting by and through the LAPD, having its principal office at 100 West First Street, Los Angeles, California, 90012.

B. Contractor – Flock Group, Inc., a Georgia corporation with a place of business at 1170 Howell Mill Road NW, Suite 210, Atlanta, GA 30318.

1.2 Representatives of the Parties

A. The representatives of the parties who are authorized to administer this Agreement and to whom formal notices, demands and communications will be given are as follows:

1) The City's representative is, unless otherwise stated in the Agreement:

Chief of Police
Los Angeles Police Department
100 West First Street, Tenth Floor
Los Angeles, California 90012

With copies to:

Commanding Officer
Information Technology Bureau
Los Angeles Police Department

100 West First Street, Suite 842
Los Angeles, California 90012

2) The Contractor's representative is, unless otherwise stated in the Agreement:

_____, CEO
Flock Group, Inc.
2588 Winslow Drive
Atlanta, GA 30305

B. Formal notices, demands and communications to be given hereunder by either party must be made in writing and may be affected by electronic mail (e-mail), personal delivery or by registered or certified mail, postage prepaid, return receipt requested and will be deemed communicated as of the date of mailing or email transmission.

C. If the name of the person designated to receive the notices, demands or communications or the address of such person is changed, written notice will be given in accordance with this Section, within five (5) business days of said change.

SECTION 2.0
TERM OF THE AGREEMENT

2.1 The term of this Agreement will commence on the date by which each of the parties have executed the Agreement and the City Attorney has signed as to form and legality (the "Effective Date"). The Agreement will terminate 360 days thereafter unless otherwise terminated pursuant to PSC-9 (Termination) of the Standard Provisions for City Contracts (Rev. 1/25 [v.2]), attached hereto as Attachment A.

SECTION 3.0
PERSONNEL

3.1 Project Manager

Contractor shall assign a project manager with full authority to administer the Agreement for Contractor and with relevant experience in implementing the Statement of Work to be performed.

SECTION 4.0
STATEMENT OF WORK

4.1 Statement of Work to be Performed

A. During the term of this Agreement, Contractor shall provide the services, implement the tasks, and provide the deliverables identified herein and in Attachment B, Statement of Work ("SOW"), which is attached hereto and incorporated herein by reference.

B. All work, tasks, and deliverables are subject to City approval in accordance with the SOW. Failure to receive approval may result in the withholding of compensation for such deliverable(s) pursuant to Section 6, Compensation and Method of Payment, of this Agreement.

C. Notwithstanding any other provision of this Agreement, the Contractor shall perform such other work and deliver such other items within the scope of services as are necessary to ensure that the deliverables provided under this Agreement meet the requirements set forth in this Agreement and all Attachments.

D. In the event that City requires services in addition to those specified in this Agreement, Contractor shall provide such services in accordance with Section 10, Amendments, of this Agreement. Prior to performance of additional work, this Agreement will be amended to include the additional work and payment.

E. Contractor's performance of the work under this Agreement must not interfere unnecessarily with the operation of LAPD or any other City Department. If City, as a result of its own operations, delays, disrupts, or otherwise interferes with and materially affects Contractor's performance hereunder, adjustments will be determined by mutual agreement of the parties and may be accomplished in accordance with Section 10, Amendments, of this Agreement. Contractor shall notify City immediately if delays, regardless of the cause, begin to put the schedule of services in jeopardy.

4.2 Time of Performance

A. Normal Business Hours – The Contractor will be available to the LAPD, during normal business hours, upon receiving at least twenty-four (24) hours advance notice. Normal business hours will mean the hours between 8:00 a.m. and 5:00 p.m., Monday through Friday, Pacific Time, excluding City holidays.

B. Outside Normal Business Hours–Upon receiving at least twenty-four (24) hours advance notice, the Contractor will be available to the LAPD as needed during weekends, City holidays, and after normal business hours.

C. Emergencies – The Contractor will be available for emergency calls on an as-needed, twenty-four (24) hours a day, seven (7) days a week basis when requested to respond with less than twenty-four (24) hours' notice.

SECTION 5.0
ACCESS TO CITY FACILITIES AND RESOURCES SUPPLIED BY CITY

At City's sole discretion, the City shall provide the Contractor access to City facilities and personnel as necessary to perform the services under this Agreement.

SECTION 6.0
COMPENSATION AND METHOD OF PAYMENT

6.1 Compensation

A. For complete and satisfactory performance of the services and delivery of the deliverables of this Agreement, City shall pay Contractor a total cumulative amount not to exceed one dollar ($1), including state and local taxes.

B. Contractor shall invoice City, and City shall pay Contractor, as provided herein

C. The Contractor further understands and agrees that execution of this Agreement does not guarantee that any or all of these funds will be expended.

D. Notwithstanding any other provision of this Agreement, including any exhibits or attachments incorporated therein, and in order for the City to comply with its governing legal requirements, the City shall have no obligation to make any payments to Contractor unless the City shall have first made an appropriation of funds equal to or in excess of its obligation to make any payments as provided in said Agreement. Contractor agrees that services provided by Contractor, purchases made by Contractor, or expenses incurred by Contractor in excess of said appropriation(s) shall be free and without charge to City and City shall have no obligation to pay for said services, purchases or expenses. Contractor shall have no obligation to provide any services, provide any equipment or incur any expenses in

excess of the appropriated amount(s) until City appropriates additional funds for this Agreement.

6.2 Taxes

To the extent that any of the services or deliverables to be provided by Contractor hereunder are subject to any California sales and use taxes, City and Contractor acknowledge and agree that such taxes shall be collected from the City. Contractor acknowledges and agrees to remit the same to the appropriate tax collection authorities in the manner set forth under applicable law. Contractor shall be solely responsible for any uncollected and unremitted taxes due and owing to the appropriate tax collection authorities and shall indemnify the City for any losses in connection with any uncollected and unremitted taxes due.

6.3 Method of Payment

A. Invoices. The City shall pay the Contractor pursuant to the requirements of this Section 6.0 after receipt and approval of the Contractor's invoices by the City. To ensure that services provided under personal services contracts are measured against services as detailed in this Contract, the Controller of the City of Los Angeles has developed a policy requiring the following supporting documentation to be submitted with all invoices:

Billing and Invoicing Requirements

The Contractor shall submit invoices that conform to City standards and include, at a minimum, the following information:

1) Name and address of contractor
2) Division and Department name and address where services were provided
3) Date of invoice and period covered
4) Contract number or authority (purchase order) number
5) Description of completed task and amount due for task, including (if applicable):
   a. Name of personnel working on task
   b. Hours spent on task and timesheet supporting charges
   c. Rate per hour and total due
6) Certification by a duly authorized officer
7) Taxes (indicate taxable and non-taxable items on invoice)
8) Discount and terms (if applicable)
9) Remittance Address (if different from company address)

B. All invoices must be submitted on Contractor's letterhead, contain Contractor's official logo, or other unique and identifying information such

as the name and address of the Contractor. Evidence that tasks have been completed, in the form of detailed description of tasks performed per hours billed, shall be attached to all invoices. Invoices shall be submitted as per Section 6.3 and shall be payable to the Contractor no later than 30 days after City determination that the invoice is complete. Invoices are considered complete when appropriate documentation or services provided are signed off as satisfactory by the Commanding Officer, Information Technology Bureau, which approval shall not be unreasonably withheld, and which approval shall be provided within a reasonable amount of time. Notwithstanding the foregoing, and subject to any rules or regulations necessitated by the Office of the Los Angeles City Controller or as otherwise required by law, there shall exist a rebuttable presumption that invoices are complete upon submission by Contractor. Should there be any reason for which the invoices should not be deemed complete upon delivery, and for which reason payment should not occur upon 30 days of delivery of the invoices, City shall immediately notify Contractor and the parties shall work together in good faith to immediately rectify any deficiencies. In no event shall City be responsible for any late fees, late charges, interest, or penalties.

C. Invoices and supporting documentation shall be prepared at the sole expense and responsibility of the Contractor. The City will not compensate the Contractor for costs incurred in invoice preparation. The City may request, in writing, changes to the content and format of the invoice and supporting documentation at any time. The City reserves the right to request additional supporting documentation to substantiate costs at any time.

D. Failure to adhere to these policies may result in nonpayment or non-approval of demands, pursuant to Charter Section 262(a), which requires the Controller to inspect the quality, quantity, and condition of services, labor, materials, supplies, or equipment received by any City office or department, and approve demands before they are drawn on the Treasury.

E. Invoices must be sent to:

Commanding Officer
Information Technology Bureau
Los Angeles Police Department
100 West 1st Street, Eighth Floor
Los Angeles, CA 90012

SECTION 7.0
DISPUTES

Both parties shall undertake to reach an amicable settlement in cases of dispute. If an amicable settlement cannot be reached, or in the event of default that could result in termination of this Agreement, City and Contractor shall schedule a meeting of their representatives in a good faith attempt to resolve the issues in dispute. The meeting shall allow for a detailed presentation of each party's views on the issues and potential solutions to the dispute or default. If possible, the meeting should result in an agreed upon course of action to resolve the dispute or default.

Contractor and City shall continue to perform any obligations under this Agreement during any dispute.

The provisions of Sections 5.169 and 5.170 (Div. 5, Ch. 10, Art. 1) of the Los Angeles Administrative Code and Section 350 of the City Charter shall govern the procedure and rights of the parties with regard to claims arising from this Agreement.

SECTION 8.0
REPRESENTATIONS AND WARRANTIES

8.1 General

The warranties in this section are nonexclusive and are cumulative of any other representations and warranties from Contractor in this Agreement or otherwise available to City under law.

8.2 Warranties of Function

A. Contractor represents and warrants that for one year following the final acceptance of any deliverable provided by Contractor, the deliverable will perform materially as described in the technical specifications set forth in this Agreement.

B. Contractor represents and warrants that no deliverable, when installed, will impair or degrade the performance of any existing system, during the period from installation until Final System Acceptance.

8.3 Warranty of Originality

Contractor represents and warrants that any deliverable will be its own original work, without incorporation of software, text, images, or other assets created by third parties, except to the extent that City consents to such incorporation in writing.

8.4 Warranty of Authority

Contractor represents and warrants that it has the full right and authority to enter into, execute, and perform its obligations under this Agreement and that no pending or threatened claim or litigation known to it would have a material adverse impact on its ability to perform as required by this Agreement.

8.5 Deliverables

Contractor represents and warrants that any and all deliverables shall at the time of delivery and acceptance conform to the applicable specifications; shall be free from any error, malfunction, or defect; shall be fit for the particular purpose for which the deliverable is developed and of which City advises Contractor; and if intended to serve as one or more components of an associated system, program, device, network or data, such deliverable shall comply with the warranties and other requirements of this Agreement when integrated or used with the System.

8.6 Pass through Warranties

Without limiting City's rights with respect to Contractor's warranties under this Agreement, if Contractor provides any deliverables covered by a third-party manufacturer's warranty or indemnity, or both, Contractor shall: (i) provide City with a copy of each such warranty or indemnity; and (ii) if such warranty or indemnity does not by its terms pass through to the end-user, then to the extent permitted, Contractor shall assign to City or otherwise cause the manufacturer to grant to City all warranties and indemnities provided by such manufacturer.

8.7 Compliance with Law

Contractor represents and warrants that the services provided under this Agreement will comply with all applicable laws, including without limitation federal, state, and local laws.

8.8 Software

Contractor represents and warrants that any software licensed or developed hereunder and any media used to distribute such software contain no viruses or other computer instructions or technological means intended to disrupt, damage, or interfere with the use of computers or related systems.

Contractor represents and warrants to City that all software developed or licensed hereunder does not contain any undisclosed disabling code (defined as computer code designed to interfere with the normal operation of the software or City's hardware or software) or any program routine, device or other undisclosed feature, including but not limited to, a time bomb, virus, drop-dead device, malicious logic, worm, Trojan horse, or trap door which is designed to delete, disable, deactivate, interfere with or otherwise harm the software or City's hardware or software.

Contractor represents and warrants to City that: (a) Contractor has used its best efforts to scan for viruses within the any software developed or licensed hereunder, and (b) no malicious system, component of a system or work product will be supplied under this Agreement.

8.9 System Security

Contractor represents and warrants that it will employ industry standard or better protections to prevent unauthorized disclosure or exposure of sensitive or confidential information that City provides to any system developed or licensed hereunder or to any system for which a component or deliverable is developed or licensed hereunder.

SECTION 9.0
CONFIDENTIALITY, RESTRICTIONS ON DISCLOSURE, AND BACKGROUND CHECKS

9.1 Confidentiality and Restrictions on Disclosure

A. All documents, records, and information provided by the City to the Contractor, or accessed or reviewed by the Contractor, during performance of this Agreement, including but not limited to Criminal Offender Records Information (CORI) will remain the property of the City. All documents, records and information provided by the City to the Contractor, or accessed or reviewed by the Contractor during the performance of this Agreement, are confidential (hereinafter collectively referred to as "Confidential Information"). The Contractor shall not provide Confidential Information, or disclose their content or any information contained in them, either orally or in writing, to any other person or entity. The Contractor agrees that all Confidential Information used or reviewed in connection with the Contractor's work for the City will be used only for the purpose of carrying out City business and cannot be used for any other purpose. The Contractor is responsible for protecting the confidentiality and maintaining the security of City documents and records in its possession.

B. The Contractor shall make the Confidential Information provided by the City to the Contractor, or accessed or reviewed by the Contractor during performance of this Agreement, available to its employees, agents and subcontractors, only on a need to know basis. Further, the Contractor shall provide written instructions to all of its employees, agents and subcontractors, with access to the Confidential Information about the penalties for its unauthorized use or disclosure.

C. The Contractor shall store and process Confidential Information in an electronic format in such a way that unauthorized persons cannot retrieve the information by computer, remote terminal or other means.

D. The Contractor shall not remove Confidential Information or any other documents or information used or reviewed in connection with the Contractor's work for the City from City facilities without prior approval from the City. The Contractor shall not use, other than in direct performance of work required pursuant to the Agreement, or make notes of any home address or home telephone numbers contained in Confidential Information provided by the City that are reviewed during work on this Agreement. The Contractor shall, at the conclusion of this Agreement, or at the request of the City, promptly return any and all Confidential Information and all other written materials, notes, documents, or other information obtained by the Contractor during the course of work under this Agreement to the City. The Contractor shall not make or retain copies of any such information, materials, or documents.

E. Any reports, findings, deliverables, analyses, studies, notes, information, or data generated as a result of this Agreement are to be considered confidential. The Contractor shall not make such information available to any individual, agency, or organization except as provided for in this Agreement or as required by law.

F. The Contractor and its employees, agents, and subcontractors may have access to confidential criminal record and Department of Motor Vehicle record information, whose access is controlled by statute. Misuse of such information may adversely affect the subject individual's civil rights and violates the law. The Contractor shall implement those measures necessary to keep secure and private criminal history information accessed by its employees, agents, and subcontractors during the performance of this Agreement. The Contractor shall advise its employees, agents, and subcontractors of the confidentiality requirements of Title 42, United States Code, Section 3789(g) [42 U.S.C. 3789(g)], California Penal Code Sections 11075 through 11144, California Penal Code, Sections 13301 through 13305, and California Vehicle Code Section 1808.45.

G. The Contractor shall require that all its employees, agents, and subcontractors who will review, be provided, or have access to Confidential Information, during the performance of this Agreement, execute a confidentiality agreement that incorporates the provisions of this Section, prior to being able to access Confidential Information.

9.2 Document Control Procedure

The Contractor shall develop and administer a mutually acceptable Document Control Procedure over documents flowing to and from the City, in such a manner as to ensure that the confidentiality requirements of this Agreement are met. Each document will be controlled through the use of a Document Control Number.

9.3 Background Checks

To the extent permitted by applicable law, the City may conduct background checks at its expense on the Contractor, its employees, designated replacement employees, agents, and subcontractors who will have, or may have, access to City information and data during performance of this Agreement. The Contractor recognizes the highly sensitive nature of such information and data and agrees to cooperate with the City and provide, to the extent permitted by applicable law, whatever information, including verification of education and previous employment, the City requires in order to conduct background checks. The City may request changes to Contractor personnel in response to background check information, and the Contractor will accommodate such request for personnel changes. Both parties agree to keep the results of any background checks confidential in accordance with the provisions of Section 9.0, as permitted by applicable law.

9.4 Provisions Apply to Subcontracts

Any subcontract entered into pursuant to the terms of this Agreement will be subject to, and incorporate, the provisions of this Section 9.0.

9.5 Survival of Provisions

The provisions of this Section 9.0 will survive expiration or termination of this Agreement.

SECTION 10.0
DATA OWNERSHIP, DATA PROTECTION, OPEN API

10.1 DEFINITIONS

10.1.1. "AI System" means any machine-based system, including any generative artificial intelligence, large language model, machine learning model, algorithmic or automated decision system, or similar technology, that infers from the inputs it receives how to generate outputs such as text, images, audio, video, code, classifications, scores, predictions, recommendations, or decisions.

10.1.2. "City Data" means all data, content, records, information, text, audio, video, images, software, documents, Personal Information, credentials, metadata, logs, prompts, inputs, outputs, feedback, configurations, and other information, in any form, that is: (i) provided by or on behalf of City to Contractor; (ii) made available to Contractor by City's personnel, residents, users, agents, systems, or devices; or (iii) collected, received, accessed, stored, hosted, transmitted, generated, derived, created, or otherwise processed by Contractor or its Subprocessors in connection with this Contract, in each case where such information identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked to City, any individual or household or vehicle, City operations, or City systems. City Data includes any data embodied in Work Product and any prompts, inputs, outputs, logs, and evaluation data used or generated in connection with any AI System under this Contract. City Data does not include Contractor Materials, and does not include De-Identified Data solely to the extent Contractor is expressly permitted to use such De-Identified Data as provided below. For the avoidance of doubt, in deployments involving automated recognition or sensor-based detection systems (including, without limitation, automated license plate recognition ("ALPR") systems, IoT platforms, or similar instrumentation), City Data includes all read records, scan records, match results, event logs, alert outputs, hotlist results, vehicle or object classification outputs, movement or pattern analyses, and all associated imagery, geolocation coordinates, device telemetry, and confidence scores.

10.1.3. "Contractor Materials" means preexisting or independently developed materials, services, software, source code, object code, models, algorithms, routines, templates, know-how, tools, methods, documentation, and other intellectual property that were not created specifically for City under this Contract and were not developed using City Data or City funding.

10.1.4. "Data Breach" means any unauthorized acquisition, access, use, disclosure, exfiltration, loss, theft, destruction, alteration, or compromise of City Data, or of the security, confidentiality, or integrity of City Data, whether or not such event constitutes a breach under applicable law.

10.1.5. "De-Identified Data" means data that cannot reasonably be used to infer information about, or otherwise be linked to, City, any individual, household, vehicle, device, or City system, and with respect to which Contractor has implemented technical and organizational measures designed to prohibit re-identification and onward disclosure except as permitted by law.

10.1.x "Metadata" means all descriptive, structural, administrative, and technical information associated with City Data, including without limitation: timestamps; geolocation coordinates; device identifiers; camera or sensor identifiers; scan and read records; query logs; user access logs; API call logs; confidence scores; match probabilities; image hashes; system-generated event records; firmware version records; calibration records; and any other information that describes, characterizes, indexes, or provides context for City Data. All Metadata is City Data for all purposes under this Agreement.

10.1.x "Derived Data" or "Algorithmic Output" means any data, result, output, inference, prediction, score, classification, alert, recommendation, or analytical product generated by Contractor's algorithms, artificial intelligence models, machine learning models, or automated analytical processes when applied to or trained upon City Data or Metadata, including without limitation: recognition match results; object or vehicle classification outputs; movement or behavior pattern analyses; frequency or anomaly scores; hotlist alert outputs; risk or confidence scores; and any data product that would not exist but for the application of an automated analytical process to City Data. All Derived Data is City Data for all purposes under this Agreement.

10.1.x "Open API" or "API Interface" means an Application Programming Interface, or suite of such interfaces, that provides City with standardized, programmatic, machine-readable access to City Data, Metadata, and Derived Data, enabling seamless integration with City's existing records management systems, third-party software platforms, inter-agency or inter-organizational data-sharing frameworks, and any other systems authorized by City, without restriction, additional licensing fee, or Contractor approval.

10.1.x "Third-Party Integration Partner" means any vendor, agency, platform, system, or authorized party to which City, in its sole discretion, elects to provide access to City Data through the Open API, including without limitation: other agencies or organizations, information-sharing systems, analytics platforms, records management systems, dispatch and computer-aided dispatch ("CAD") systems, case management platforms, fusion centers, and any other system designated by City.

10.1.x "Proprietary Technology" means Contractor's pre-existing and independently developed intellectual property, including the software source code, hardware designs, firmware, algorithms, machine learning model architectures, and trade secrets that Contractor owned prior to the Effective Date of this Agreement or that Contractor develops independently without use of City Data.

10.1.x "Raw Sensor Data" means the raw, unprocessed output of any physical sensors, IoT devices, edge-computing components, or other hardware

instrumentation deployed by or on behalf of City ("Sensor Systems"), including all original sensor readings at their native sampling resolution, prior to any filtering, aggregation, normalization, compression, or other processing applied by Contractor's platform.

10.1.6. "Personal Information" means any information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual or household or vehicle, and any other data subject to privacy, confidentiality, security, breach notification, consumer protection, identity theft, employment, or similar laws, including sensitive personal information, personally identifiable information, protected health information, payment card data, financial account information, biometric information, credentials, education records, and government-issued identifiers.

10.1.7. "Security Incident" means any actual or reasonably suspected event that materially threatens or adversely affects the confidentiality, integrity, availability, or resilience of City Data or of the systems used to provide the services, including malware, ransomware, denial of service, unauthorized access attempts, or material outages, but excluding unsuccessful routine scans, pings, or blocked attacks that do not result in unauthorized access to City Data or material degradation of the services.

10.1.8. "Subprocessor" means any subcontractor or other third party, including any cloud, hosting, support, analytics, payment, or AI provider, engaged by Contractor or its Subcontractors to host, access, receive, store, transmit, or otherwise process City Data or to provide a material technology service used in performance of this Contract.

10.2 Data Ownership

10.2.1. City Data. City retains all right, title, and interest in and to City Data. No rights in City Data are granted to Contractor except the limited, nonexclusive, nontransferable right to use City Data solely as necessary to perform this Contract and solely in accordance with this Contract and City's written instructions. Contractor shall not sell, license, rent, disclose, release, transfer, assign, encumber, or otherwise exploit City Data and shall not assert any lien, withholding right, setoff, or other encumbrance against City Data.

For the avoidance of doubt, the fact that City Data is stored on, processed by, transmitted through, or hosted within Contractor's infrastructure shall not create, transfer, or vest in Contractor any ownership interest, proprietary right, license, or other legal claim with respect to such data. City Data does not become Contractor property by virtue of its presence within Contractor's systems.

All Metadata associated with City Data, whether automatically generated by the Services, produced by Contractor's infrastructure, or derived from system logs, is and shall remain City Data for all purposes under this Agreement. Contractor shall have no right, title, or interest in any Metadata originating from City's use of the Services, and shall not use, retain, license, sell, aggregate, or otherwise exploit such Metadata for any purpose except as explicitly authorized in writing by City.

All Derived Data and Algorithmic Outputs — including any data product, inference, score, classification, match result, or analytical output produced by Contractor's algorithms or artificial intelligence systems when applied to City Data — are and shall be the exclusive property of City. The application of Contractor's Proprietary Technology to City Data does not create, and shall not be construed to create, any Contractor ownership interest in the resulting Derived Data. The intellectual labor of algorithmic transformation does not diminish, qualify, or transfer City's exclusive ownership of the outputs of such transformation when applied to City Data.

City shall retain all rights to Derived Data regardless of: (a) the computational complexity of the process by which it was produced; (b) the degree of Contractor skill or proprietary methodology incorporated in the analytical process; (c) the commercial value of the output; or (d) whether City could have independently produced equivalent output. Contractor expressly waives any claim of data authorship, data copyright, or ownership interest in Derived Data based on the application of its technology to City Data.

Contractor shall not use, copy, aggregate, anonymize, de-identify, re-identify, sell, license, publish, disclose, share, or otherwise exploit City Data, Metadata, or Derived Data for any purpose not expressly authorized in writing by City. Without limiting the foregoing, Contractor is specifically prohibited from:

- Using City Data to train, fine-tune, test, validate, benchmark, or improve any algorithm, machine learning model, or artificial intelligence system, whether for Contractor's own benefit or for the benefit of any third party;
- Aggregating City Data with data from other Contractor customers for any analytical, research, development, or commercial purpose;
- Creating or selling any product, service, report, or derivative work based in whole or in part on City Data without express written authorization from City;
- Sharing City Data with any parent company, subsidiary, affiliate, investor, or successor of Contractor without prior written City authorization;
- Using City Data for any marketing, advertising, promotional, or commercial purpose;
- Retaining City Data beyond the periods specified in this Agreement for any purpose not expressly authorized herein.

To the extent that any right, title, or interest in City Data, Metadata, or Derived Data may be deemed by operation of law to vest in Contractor by reason of its creation,

production, processing, or hosting of such data, Contractor hereby irrevocably assigns, transfers, and conveys to City all such right, title, and interest, including all intellectual property rights therein, without further consideration and without reservation. Contractor shall execute any additional instruments of assignment or transfer reasonably requested by City to perfect or evidence City's ownership rights under this Section.

10.2.2. Work Product. Unless otherwise expressly provided in this Contract, all finished and unfinished works, tangible or intangible, originated and prepared by Contractor or its Subcontractors specifically for City under this Contract, including, without limitation, documents, reports, analyses, studies, specifications, manuals, software, code, configurations, interfaces, databases, designs, audiovisual materials, websites, domain names, inventions, discoveries, and other deliverables (each, a "Work Product"; collectively, "Work Products"), together with all intellectual property rights therein, shall be and remain the exclusive property of City for its use in any manner City deems appropriate. Contractor hereby assigns to City all right, title, and interest worldwide in and to such Work Products. Contractor shall execute any documents reasonably necessary for City to perfect, memorialize, or record City's ownership of rights provided herein.

10.2.3. AI-Generated Output. To the extent any Work Product or portion thereof is generated or assisted by an AI System or is not capable of assignment or exclusive ownership as a matter of law, Contractor hereby grants to City a perpetual, irrevocable, worldwide, royalty-free, fully paid-up license, with the right to sublicense to City's contractors and service providers acting on City's behalf, to use, reproduce, modify, display, perform, distribute, create derivative works from, and otherwise exploit such Work Product or output for any City purpose.

10.2.4. Contractor Materials. Contractor retains ownership of Contractor Materials. To the extent any Contractor Materials are incorporated into, delivered with, or reasonably necessary for City to use any Work Product or receive the benefits of the services, Contractor grants to City a nonexclusive, perpetual, irrevocable, worldwide, royalty-free, fully paid-up license, with the right to sublicense to City's contractors and service providers acting on City's behalf, to use, execute, reproduce, display, perform, configure, maintain, support, and, if delivered in source or editable form, modify such Contractor Materials solely as necessary for City to use the Work Product and receive the benefits of the services.

10.2.5. Third-Party Materials. For all materials, software, data, or other items delivered to City that are not originated or prepared by Contractor or its Subcontractors under this Contract, Contractor shall secure for City, at no additional cost to City, all rights necessary for City to use such items for City purposes and to receive the full benefit of this Contract.

10.2.6. Restrictions on Disclosure. Contractor shall not provide or disclose any Work Product or City Data to any third party except as expressly permitted under this Contract or approved in writing by City.

10.2.7. Subcontracts. Any subcontract or other agreement entered into by Contractor relating to this Contract shall preserve and protect City's rights in City Data and Work Product and shall state that no Subprocessor or subcontractor obtains any ownership interest in either.

10.2.8. Equitable Relief. Contractor agrees that a monetary remedy for breach of this Section 10 may be inadequate, impracticable, or difficult to prove and that a breach may cause City irreparable harm. City may therefore enforce this Section 10 by seeking injunctive relief and specific performance, without any necessity of showing actual damage or irreparable harm. Seeking injunctive relief or specific performance does not preclude City from seeking or obtaining any other relief to which City may be entitled.

10.3 Artificial Intelligence and Automated Processing

Disclosure and Approval. Contractor shall not use any AI System that processes City Data, generates deliverables for City, interacts with the public or City personnel on City's behalf, or materially informs services or decisions under this Contract, or permit any Subprocessor to do so, without prior written disclosure to City of the AI System or provider, intended use case, categories of City Data processed, hosting region, retention practices, and material limitations reasonably known to Contractor that may affect accuracy, reliability, security, confidentiality, intellectual property, or bias. No such AI System or material AI feature may be enabled for City without City's prior written consent if it materially changes how City Data is processed or materially changes the risk profile of the services.

No Model Training or Secondary Use. Except as expressly authorized in a written amendment signed by City, Contractor shall not, and shall cause its Subprocessors and AI providers not to, use City Data to train, retrain, fine-tune, or otherwise improve any AI System or model, whether general-purpose or customer-specific. Any retention of prompts, inputs, outputs, or feedback for abuse monitoring, safety review, or troubleshooting must be disclosed to City in advance, limited to the minimum necessary, protected as City Data, and not used for model training or generalized product improvement.

Responsibility and Human Oversight. Contractor remains fully responsible for all services performed with or through an AI System. Contractor shall implement reasonable governance and quality controls appropriate to the use case, including documented intended use, change management, testing for material errors and security risks, and human review before any AI-generated output is relied upon for material legal, financial,

employment, eligibility, benefits, enforcement, or safety decisions affecting any individual, unless City expressly authorizes otherwise in writing and applicable law permits such use.

Output and Records. Any output, report, recommendation, code, content, or other deliverable generated by an AI System for City under this Contract shall be treated as Work Product or City Data, as applicable. Upon City's reasonable request, Contractor shall identify whether a deliverable was materially generated or modified using an AI System. Contractor shall, upon City's reasonable request, maintain and provide records sufficient to identify the AI System used, the material version or model family, the date of use, and the categories of City Data processed in connection with the services, except to the extent disclosure would reveal Contractor's trade secrets unrelated to City's use, in which case Contractor shall provide a reasonably informative summary.

Changes and Suspension. Contractor shall provide City with reasonable advance written notice of any material change in an AI System or AI provider used to perform the services that is reasonably likely to affect City Data, security, confidentiality, functionality, or the risk profile of the services. If City reasonably determines that an AI System presents a material risk to City Data, City systems, or affected individuals, City may direct Contractor to suspend the applicable AI-enabled processing until the risk is remediated to City's reasonable satisfaction.

This provision shall survive expiration or termination of this Agreement.

10.4 Data Protection

General Standard. Contractor shall protect City Data using administrative, technical, physical, and organizational safeguards no less rigorous than accepted industry standards and no less protective than those Contractor uses for its own information of similar sensitivity, and in all events consistent with applicable law and the nature of the services and City Data. Contractor shall maintain a written information security program, incident response plan, and business continuity and disaster recovery capabilities appropriate to the services.

Permitted Use; Restricted Use. Contractor shall collect, access, use, retain, disclose, store, and otherwise process City Data only for the limited and specified purpose of performing this Contract, complying with applicable law, and as otherwise expressly authorized in writing by City. Contractor shall limit access to City Data to personnel and approved Subprocessors with a need to know for performance of this Contract and who are bound by written confidentiality and data protection obligations at least as protective as this Contract. Contractor shall not: (i) sell, share, rent, release, disclose, disseminate, make available, transfer, or otherwise communicate City Data to any third party except as expressly authorized by City or required by law; (ii) use City Data for advertising, marketing, profiling for unrelated purposes, product development unrelated to the services, or any commercial purpose other than performance of this Contract; (iii) combine City Data with data from other customers or sources except as necessary to

provide the services and subject to written controls that prevent unauthorized use or disclosure; or (iv) move, store, or permit access to City Data outside the United States without City's prior written approval.

Data Minimization and Retention. Contractor shall collect and use only the minimum City Data reasonably necessary to perform this Contract, and shall retain City Data only for the duration reasonably necessary for the permitted purpose or as otherwise required by law or City's written instructions. If retention is required by law or PSC-16, such retained City Data shall remain subject to all protections of this Contract.

Security Controls. Without limiting the foregoing, Contractor shall, to the extent applicable to the services, implement and maintain: (i) logical access controls based on least privilege and unique user identification; (ii) multi-factor authentication for remote access, privileged access, and access to systems hosting City Data where technically feasible; (iii) encryption of City Data in transit and at rest, to the extent commercially reasonable and appropriate to the sensitivity of the City Data and the architecture of the services, and in all cases for portable media and internet transmissions; (iv) malware protection, endpoint monitoring, and timely security patching and vulnerability management appropriate to risk; (v) logging and monitoring reasonably sufficient to detect, investigate, and respond to unauthorized access or use; (vi) secure configuration, secure development where software or AI-based services are provided, and change management; (vii) secure disposal of media containing City Data; (viii) periodic privacy and security training for personnel with access to City Data; and (ix) segregation of City Data from other data through logical or physical separation appropriate to the services.

Subprocessors. Contractor shall not permit any Subprocessor to access or process City Data without City's prior written approval as required hereunder and a written agreement binding the Subprocessor to obligations no less protective than this Contract, including the restrictions in this PSC-22 and PSC-23. Contractor remains fully responsible for all acts and omissions of its Subprocessors.

Security Incidents and Data Breaches. Contractor shall notify City in writing without unreasonable delay, and in any event no later than twenty-four (24) hours after discovery of any Security Incident or Data Breach. Such notice shall include, to the extent known at the time, the nature of the incident, the categories of City Data affected, the date and time or estimated date and time of the incident, the systems affected, the measures taken or proposed to address it, and a point of contact. Contractor shall promptly take all reasonable steps to contain, investigate, mitigate, and remediate the incident; preserve relevant evidence; provide City with regular status updates at least daily until resolution, or more frequently if reasonably requested by City; and cooperate fully with City, its representatives, insurers, auditors, and law enforcement. Contractor shall not notify any third party, regulator, or affected individual, or issue any public statement, regarding any Security Incident or Data Breach involving City Data without City's prior written approval, unless required by law, in which case Contractor shall, to the extent legally permitted, consult with City in advance and provide City a copy of the proposed notice. Contractor

shall reimburse City for reasonable documented third-party costs incurred by City to investigate, respond to, mitigate, notify, and remediate any Security Incident or Data Breach to the extent caused by Contractor or its Subprocessors, including legally required notice, call center support, credit or identity monitoring where reasonably appropriate, forensic services, data restoration, and other reasonable incident response costs.

Assessments and Audit Cooperation. Upon City's reasonable request, not more than once annually except following a Security Incident, Data Breach, or material change in Contractor's security controls, Contractor shall provide City with then-current summaries of relevant independent security assessments, certifications, or audit reports, such as SOC 2 Type II, ISO 27001, or comparable reports, if available, together with remediation status for material findings relevant to the services. If such reports are unavailable, Contractor shall complete City's reasonable security questionnaire and provide reasonable supporting documentation sufficient to demonstrate compliance with this PSC-22. City or its designated representative may, upon reasonable notice and during normal business hours, perform a reasonable review of Contractor's compliance with this PSC-22 and PSC-23, subject to reasonable confidentiality, security, and operational safeguards. Any such review shall be limited to information and systems relevant to the services and City Data and shall not unreasonably interfere with Contractor's business operations or expose data of other customers.

Return, Transition, and Deletion. Upon City's request, expiration, or termination of this Contract, Contractor shall promptly, and in no event later than thirty (30) days unless otherwise directed by City, return to City all City Data in a reasonably usable format designated by City and securely delete all copies of City Data in Contractor's and its Subprocessors' possession or control, except to the extent retention is required by law or by immutable backup media not reasonably accessible in the ordinary course. Any retained City Data shall remain subject to this Contract until deleted. Upon request, Contractor shall certify in writing its completion of the return and deletion obligations. The return of City Data in a reasonably usable format and the deletion certification required by this subsection shall be provided at no additional charge. Additional transition services requested by City beyond those ordinary obligations shall be provided at the rates, if any, set forth in this Contract, or otherwise at mutually agreed rates.

Legal Requests and Public Records. Contractor shall promptly notify City of any subpoena, court order, public records request, or other legal demand seeking City Data or Confidential Information, unless prohibited by law. Contractor shall not respond or produce City Data except as required by law and after giving City a reasonable opportunity to seek protective relief or otherwise direct the response. Contractor shall reasonably assist City in responding to requests for records relating to this Contract.

Limited Use of De-Identified Data. Contractor may use De-Identified Data solely for internal security, fraud prevention, service support, capacity planning, and improvement of the services provided to City, provided that Contractor does not identify City, any individual, household, vehicle, device, or City system, does not sell or share such data,

and does not use such data to train or improve any general-purpose or third-party AI System without City's prior written approval.
By entering into this Contract, Contractor certifies that it understands and will comply with the restrictions in this PSC-22 and PSC-23. This PSC-22 shall survive expiration or termination of this Contract.

10.5 OPEN API ACCESS — CITY'S UNRESTRICTED RIGHT TO DATA INTEGRATION

10.5.1 Mandatory Provision of Open API
Contractor shall provide and maintain, throughout the Term and for a period of no less than one hundred eighty (180) days following expiration or termination of this Agreement for any reason, a documented, machine-readable Open API that enables City to access, retrieve, and export all City Data in its entirety. This API access shall be:

(i) Provided at no additional cost, charge, licensing fee, or subscription fee beyond the base services compensation set forth in this Agreement;

(ii) Available without requiring City to seek, apply for, or obtain any additional Contractor approval, certification, or authorization;

(iii) Documented with complete, current, and accurate technical specifications, including all endpoints, authentication methods, data schemas, query parameters, response formats, rate limits, error codes, and versioning information, made available to City at no charge via a dedicated developer portal or equivalent resource;

(iv) Supported with full technical assistance from Contractor's engineering personnel during City's integration and ongoing operations; and

(v) Maintained in a stable, backwards-compatible manner, with no less than one hundred eighty (180) days' advance written notice of any material changes to API structure, endpoints, authentication protocols, or data schemas, and with backward compatibility or a functionally equivalent replacement maintained throughout such notice period.

10.5.2 Scope of API Access

The API access provided under this Section shall encompass, at minimum:

(i) Real-time and batch query capabilities for all City Data and associated Metadata (including, by way of illustration, all license plate read records, scan records, hotlist match results, alert outputs, and event data captured within City's environment or jurisdiction);

(ii) Full export and retrieval functionality for all City Data in machine-readable, industry-standard, non-proprietary formats (JSON, CSV, and XML at minimum), without encoding or encryption that would prevent standard programmatic access;

(iii) Access to all Derived Data and Algorithmic Outputs produced by Contractor's systems from City Data (including, by way of illustration, vehicle or object classification outputs, movement pattern analyses, frequency scores, confidence scores, and anomaly or risk scores);

(iv) Search and filter capabilities across all City Data attributes including date ranges, geographic areas, device or camera identifiers, object or subject attributes, and confidence or match levels;

(v) Audit log access, including complete records of all API calls, queries, and data access events associated with City's account;

(vi) Webhook or push-notification capabilities enabling real-time data streaming to City systems and authorized Third-Party Integration Partners; and

(vii) Bulk data export functionality capable of producing complete datasets upon City request within a commercially reasonable timeframe not to exceed forty-eight (48) hours. Upon City's written request for a bulk data export, Contractor shall provide elevated or unlimited rate access for the duration of such export.

10.5.3 Third-Party Integration — Unrestricted Right

City shall have the unconditional right to use the Open API to integrate City Data with any third-party system, platform, agency, or authorized partner of City's choosing, without Contractor consent, approval, review, or notification, subject only to City's own legal and policy obligations. This right expressly includes, without limitation:

(i) Integration with other agency or organizational platforms, including regional, state, or national information systems (including, by way of illustration, law enforcement information systems, criminal justice information systems, or inter-agency data-sharing networks authorized under applicable law, including the California Public Records Act, the Stored Communications Act, and any applicable inter-agency data-sharing agreements);

(ii) Integration with City's Records Management System ("RMS"), Computer-Aided Dispatch ("CAD") system, case management platform, and any successor or replacement systems;

(iii) Integration with licensed third-party analytics, investigative, or operational platforms selected by City;

(iv) Integration with fusion centers, joint task force systems, and multi-party or multi-agency data-sharing networks authorized under applicable law; and

(v) Development of City's own custom applications, dashboards, or analytical tools using data retrieved via the Open API.

10.5.4 No Contractor Restrictions on Integration Partners

Contractor shall not impose, directly or indirectly, any restriction, condition, approval requirement, certification requirement, or commercial term that limits, discourages, penalizes, or conditions City's ability to integrate City Data with any Third-Party Integration Partner. Specifically, Contractor shall not:

(i) Require that Third-Party Integration Partners be approved, certified, or listed by Contractor as a precondition to City's use of the Open API for such integration;

(ii) Impose additional fees, charges, or licensing costs based on the number of Third-Party Integration Partners or the volume of data shared through the Open API;

(iii) Impose technical restrictions (such as rate limits, data throttling, or format limitations) on API use that disproportionately affect City's ability to integrate with third parties;

(iv) Include in any Contractor end-user license agreement, terms of service, or platform policy any provision that would restrict or prohibit City's right to share City Data with authorized third parties via the Open API; or

(v) Claim any contractual right to review, approve, or veto City's selection of Third-Party Integration Partners.

10.5.5 API Interoperability Standards

To ensure seamless integration and maximum data portability, Contractor shall design and maintain the Open API in conformance with the following standards and requirements:

(i) RESTful API architecture conforming to industry standards, with support for OAuth 2.0 or equivalent industry-standard authentication protocol, credential rotation capabilities, and access logging;

(ii) All data shall be made available in open, non-proprietary formats including JSON and CSV at minimum, without proprietary encoding, compression, or encryption that would prevent standard programmatic access;

(iii) API responses shall include complete data records without truncation, redaction, or omission of any fields accessible within Contractor's own platform;

(iv) All data transmitted via the Open API shall be encrypted in transit using TLS 1.2 or higher;

(v) The API shall support pagination, filtering, and sorting capabilities sufficient to support large-scale data retrieval operations;

(vi) Contractor shall maintain API uptime at a level consistent with or exceeding the uptime commitments applicable to the Services generally under this Agreement;

(vii) Contractor shall provide a dedicated API test environment (sandbox) enabling City and its designated Third-Party Integration Partners to develop and test integrations without affecting production data; and

(viii) Contractor warrants that the Open API will perform without material degradation in data completeness, accuracy, or functionality relative to the access available through Contractor's own user interface or platform.

10.5.6 No Export Fees

Contractor shall not impose fees for data exports via the Open API.

10.5.7 No Lock-In; Data Return

Contractor acknowledges that all City Data remains the sole and exclusive property of City at all times. Contractor shall not: (i) technically or contractually restrict City's ability to access, export, or migrate City Data to any competing service or system; (ii) impose fees for data access or export via the Open API except as expressly permitted under Section 10.3.6 above; or (iii) degrade or throttle Open API performance in response to City's exercise of its data portability rights.

City shall have the unconditional right, exercisable at any time during or upon termination or expiration of this Agreement, to obtain a complete export of all City Data, Metadata, and Derived Data in machine-readable, open formats. Upon such request or upon termination or expiration of this Agreement, Contractor shall, at City's election, either:

(i) Deliver a complete export of all City Data, Metadata, and Derived Data within fifteen (15) business days of City's written request, at no additional charge, in formats agreed upon by the parties, defaulting to JSON and CSV if no format is specified, with written certification upon completion that the export is complete and accurate as of the date of export; or

(ii) Continue to make the Open API available for City's self-service export for no less than one hundred eighty (180) days following the effective date of termination or expiration, at no additional charge, and cooperate in good faith with City's transition to any successor contractor or system during such period.

10.5.8 Audit Rights

City shall have the right, upon reasonable prior written notice, to test the Open API against the requirements of this Section, to request written confirmation from Contractor that all City Data categories — including Metadata, Derived Data, and device-generated telemetry data — are accessible via the Open API, and to audit Contractor's compliance with the data access and portability requirements herein. Contractor shall respond to any such written request within ten (10) business days. Contractor shall provide written certification of API compliance upon City's request, including confirmation that no data categories accessible through Contractor's platform are unavailable through the Open API.

10.5.9 Security of API Access

All access to and transmission of City Data via the Open API shall be subject to the security standards and requirements set forth in Section [___] of this Agreement. Contractor shall ensure that the Open API incorporates encryption in transit (TLS 1.2 or higher), credential rotation capabilities, and access logging consistent with the requirements of such Section. In the event of any conflict between the requirements of this Section and Section [___], the more protective standard shall govern.

10.6 SUPPLEMENTAL SENSOR SYSTEM DATA RIGHTS

10.7 Scope; Relationship to Section 10.3

This Section applies to any Services that involve the collection, transmission, storage, or processing of data generated by physical sensors, IoT devices, edge-computing components, automated recognition systems (including, by way of illustration, ALPR cameras, imaging sensors, acoustic sensors, and environmental sensors), or other hardware instrumentation deployed by or on behalf of City ("Sensor Systems"). The rights set forth in this Section are supplemental to, and shall be read together with, the requirements of Section 10.3. In the event of any conflict between this Section and Section 10.3, the provision more favorable to City shall govern.

10.7.1 Raw Data Preservation and Export

Contractor shall store and make available for export via the Open API the Raw Sensor Data from all Sensor Systems, including all original sensor readings at their native sampling resolution, prior to any filtering, aggregation, normalization, compression, or other processing applied by Contractor's platform. Contractor shall not substitute

processed, aggregated, or downsampled data in satisfaction of its export obligations under this Agreement unless City has expressly elected in writing to receive only processed data in lieu of Raw Sensor Data. Where both raw and processed data are available, the Open API shall provide access to each independently.

For deployments involving automated recognition systems, Raw Sensor Data includes without limitation:

(i) Raw image or video frames captured by recognition cameras;
(ii) Unfiltered read or scan records prior to confidence thresholding;
(iii) Raw classifier outputs prior to post-processing; and
(iv) All associated sensor telemetry generated at the time of each capture event.

10.7.2 Sampling Resolution and Timestamp Integrity

All Sensor System data exported via the Open API shall:

(i) Be exported at the original sampling frequency at which the data was generated and received by Contractor's platform, without reduction in temporal resolution;

(ii) Include precise, unmodified timestamps for each data point in Coordinated Universal Time (UTC) with no less than millisecond resolution, or such higher resolution as is native to the Sensor System; and

(iii) Preserve the original sequence and continuity of the data stream, including any gaps, dropouts, or anomalies that occurred during collection, without interpolation or artificial fill.

10.7.3 Device Metadata and Configuration Export

Contractor shall ensure that all Sensor System data exported via the Open API is accompanied by, or exportable together with, the complete device metadata and configuration state associated with each Sensor System, including without limitation:

(i) Device identifiers (serial numbers, hardware IDs, and any platform-assigned identifiers);

(ii) Firmware and software version history for each device as recorded by Contractor's platform;

(iii) Calibration records, calibration coefficients, and calibration dates applicable to each sensor;

(iv) Sensor configuration parameters, threshold settings, alert rules, hotlist configurations, and any other operational configuration stored on or managed through Contractor's platform; and

(v) Physical installation and location mapping data (including GPS coordinates, zone assignments, field-of-view descriptors, or logical placement descriptors) to the extent maintained by Contractor's platform.

Such metadata and configuration data shall be exported in a structured, machine-readable format and shall be logically associated with the corresponding sensor data records to enable accurate reconstruction of the operational context of each data point.

10.7.4 Open Format Decoding Requirement

Where Contractor stores Sensor System data in a proprietary binary format, compressed format, or any encoding that cannot be interpreted without Contractor's proprietary tools or software, Contractor shall ensure that the Open API decodes and delivers such data in a non-proprietary, open, human-readable or standard machine-readable format (e.g., JSON, CSV, or Protocol Buffers with a published schema) prior to transmission to City. Contractor shall not deliver raw binary or proprietary-encoded data through the Open API in satisfaction of its export obligations under this Agreement unless accompanied by complete, publicly available decoding specifications and tooling sufficient to enable City to independently interpret the data without ongoing reliance on Contractor.

10.7.5 Data Integrity and Chain of Custody

For City environments subject to regulatory requirements, evidentiary standards, legal hold obligations, or operational audit requirements, Contractor shall, upon City's written request, accompany each bulk data export with:

(i) A cryptographic hash (SHA-256 or stronger) of each exported data file or dataset, generated by Contractor's platform at the time of export;

(ii) A signed manifest or export certificate identifying the data ranges, device identifiers, and timestamps covered by the export, the export timestamp, and the identity of the exporting system; and

(iii) Written confirmation that the exported dataset is complete and unaltered relative to the data stored on Contractor's platform for the requested period and device set.

Contractor shall retain the capability to regenerate export manifests for any export performed during the Term for a period of no less than three (3) year following the date of export.

10.7.6 Data Retention; Prohibition on Downsampling

Contractor shall retain all Sensor System data, including Raw Sensor Data, at its original sampling resolution for a minimum period of [___] months ("Full-Resolution Retention Period"). Contractor shall not reduce the sampling resolution of, compress, or purge any Sensor System data within the Full-Resolution Retention Period without City's prior written consent. Following the Full-Resolution Retention Period, if Contractor applies any downsampling or data reduction to historical sensor data, Contractor shall:

(i) Provide City with no less than sixty (60) days' prior written notice of the intended reduction;

(ii) Specify the post-reduction resolution and the data to be affected; and

(iii) Provide City an opportunity to perform a full-resolution export prior to the reduction taking effect.

10.7.7 Security of Sensor Data Transmission

All transmission of Sensor System data, including Raw Sensor Data and device metadata, via the Open API shall comply with the security requirements of Section [___] of this Agreement. In addition, Contractor shall implement and maintain end-to-end encryption for data in transit between Sensor Systems and Contractor's platform to the extent technically feasible given the hardware constraints of the applicable Sensor Systems, and shall document any hardware-imposed limitations on encryption capability in the technical specifications provided to City.

10.8 INTER-AGENCY AND MULTI-PARTY DATA SHARING

Note to Drafters: This Section addresses inter-agency and multi-party data sharing obligations. It is drawn from specialized law enforcement instrument language and should be applied, adapted, or omitted based on City's operational and regulatory context. Statutory references are carried from the source instrument and should be verified and updated to reflect City's applicable jurisdiction.

10.8.1 City's Right to Share Data with Other Agencies and Authorized Parties

City retains the unconditional right to share City Data with other agencies, organizations, criminal justice entities, and authorized governmental or private bodies pursuant to applicable law, court order, inter-agency agreement, or City policy. Contractor shall not impose any contractual restriction on City's ability to share City Data with authorized third parties, nor shall Contractor require that such parties become Contractor customers or enter into any Contractor agreement as a condition of receiving City-shared data.

10.8.2 Support for Inter-Party Integrations

Contractor shall provide technical support, documentation, and API credentials necessary to enable authorized inter-agency and inter-party integrations at no additional cost to City or to the receiving party. Contractor shall cooperate in good faith with other parties' technical personnel to facilitate integration of City Data into multi-agency or multi-organization analytical and operational platforms, including without limitation:

(i) Records management systems;
(ii) Computer-aided dispatch systems;
(iii) Fusion centers and joint task force systems; and
(iv) Crime analysis or operations analysis platforms.

10.9 Compliance with Privacy Laws

Contractor shall ensure that Contractor's performance of Contractor's obligations under this Agreement complies with all applicable local, state, and federal privacy laws and regulations, including, but not limited to, laws relating to consent to make visual and audio recordings of individuals and consent to collect information from individuals. If this Agreement or any practices which could be, or are, employed in performance of this Agreement are inconsistent with or do not satisfy the requirements of any of these privacy laws and regulations, City and Contractor shall in good faith execute an amendment to this Agreement sufficient to comply with these laws and regulations and Contractor shall complete and deliver any documents necessary to compliance.

10.10 Data, Development, and Access Point Location

Storage of City Data shall be located in the continental United States of America. Contractor shall not allow its personnel or contractors to store City Data on portable devices, including personal computers, except for devices that are used and kept only at Contractor's continental United States of America headquarters or data centers. Contractor shall neither access, nor allow a third party to access systems housing City Data from any location outside of the continental United States of America. Contractor shall obtain the City's prior written approval for each of its employees, contractors, officers, partners, consultants, principals, agents, affiliates, or subsidiaries who are essential for the purpose of providing the services under this Agreement ("Authorized Persons"). When Contractor submits a request for City's prior written approval, it shall describe the proposed Authorized Person's role and the necessity for the proposed Authorized Person to access City Data. Contractor shall at all times cause such Authorized Persons to abide strictly by Contractor's obligations under this Agreement and the industry standards for information security. Contractor hereby agrees that only Authorized Persons who are bound in writing by confidentiality and other obligations sufficient to protect City Data in accordance with the terms and conditions of this Agreement will access

City Data, and will do so only for the purpose of enabling Contractor to perform its obligations under this Agreement.

10.11 Data Breach

Contractor shall protect City Data using the most secure means and technology that is consistent with industry standards for the type of data at issue. Contractor shall notify City as soon as reasonably feasible, but in any event, within twenty-four (24) hours in writing and telephonically of Contractor's discovery or reasonable belief of any unauthorized access of City Data (a "Data Breach"), or of any incident affecting, or potentially affecting City Data related to cyber security (a "Security Incident"), including, but not limited to, denial of service attack, and system outage, instability or degradation due to computer malware or virus. Contractor shall begin remediation immediately. Contractor shall provide daily updates, or more frequently if required by City, regarding findings and actions performed by Contractor until the Data Breach or Security Incident has been effectively resolved to City's satisfaction. Contractor shall conduct an investigation of the Data Breach or Security Incident and shall share the report of the investigation with City. If directed by City, Contractor shall retain an independent third party to conduct the investigation at Contractor's sole cost. At City's sole discretion, City and/or its authorized agents shall have the right to lead or participate in the investigation. Contractor shall cooperate fully with City, its agents and law enforcement. Contractor is responsible for all costs associated with a Data Breach or Security Incident, including, if directed by City, the provision of identity theft protection and/or credit monitoring services to individuals affected by the Security Incident. If required by law or directed by City, Contractor will be responsible for notifying individuals impacted by the Security Incident or Data Breach, with City having final approval of the content of the notification. In the event City incurs any costs related to the breach referenced above, City will seek reimbursement from Contractor or reduce Contractor's invoice for costs associated with breach of security.

A. Data Breach Liability. If City is subject to any claims relating to any Data Breach or Security Incident, Contractor shall fully indemnify and hold harmless City and defend City against any such claims, including reimbursement of any costs incurred by City relating to those claims. This obligation is in addition to any of Contractor's other indemnification obligations in this Agreement.

10.12 Firewalls and Access Controls

A. Access Precautions. Contractor shall use precautions, including, but not limited to, physical software and network security measures, employee screening, training and supervision, and appropriate agreements with employees to:

1) Prevent anyone other than City, Contractor, and authorized City or Contractor personnel from monitoring, using, gaining access to, or learning the import of City Data; and

2) Protect appropriate copies of City Data from loss, corruption, or unauthorized alteration; and

3) Prevent the disclosure of City and Contractor passwords and other access control information to anyone other than authorized City personnel.

B. Security Best Practices. Contractor shall implement the following security best practices with respect to any service provided:

1) Least Privilege: Contractor shall authorize access only to the minimum amount of resources required for a function.

2) Separation of Duties: Contractor shall divide functions among its staff members to reduce the risk of one person committing fraud undetected.

3) Role-Based Security: Contractor shall restrict access to authorized users and base access control on the role a user plays in an organization.

C. Access Restrictions. Contractor shall restrict the use of, and access to, administrative credentials for City accounts and Contractor's systems to only those of Contractor's employees and other agents whose access is essential for the purpose of providing the services of this Agreement. Contractor shall require these personnel to log on using an assigned user-name and password when administering City accounts or accessing City Data. These controls must enable Contractor to promptly revoke or change access in response to terminations or changes in job functions, as applicable. Contractor shall encrypt all passwords, passphrases, and PINs, using solutions that are certified against U.S. Federal Information and Processing Standard 140-2, Level 2, or equivalent industry standard, and verify that the encryption keys and keying material are not stored with any associated data. Contractor will implement any City request to revoke or modify user access within twenty-four (24) hours or the next business day of receipt of City's request. Contractor will disable user accounts after at most ten (10) consecutive invalid authentication attempts.

10.13 Vulnerability Management and Patching

At least annually, Contractor shall perform at Contractor's expense vulnerability tests and risk assessments of all systems that contain City Data. For Contractor's internet perimeter network, and any of Contractor's applications that process City Data, such testing must also include (i) penetration tests, including by use of intercept proxies to identify security vulnerabilities that cannot be discovered using automated tools, and (ii) code review or other manual verification. All tests must be performed by Contractor's compliance team using industry recommended network security tools to identify vulnerability information. Upon written request from City, Contractor shall provide to City a Vulnerability Testing & Risk Assessment Report at the organization level including an executive summary of the results.

10.14 Right of Audit by City

Without limiting any other audit rights of City, upon reasonable advance notice of at least thirty (30) days, and no more than once per calendar year, City may review Contractor's data privacy and data security program prior to the commencement of this Agreement and from time to time during the term of this Agreement. During the performance of this Agreement, upon reasonable advance notice of at least thirty (30) days, and no more than once per calendar year, City, may, by itself or by retaining a certified public accounting firm or information security professional, perform, or have performed, an on-site audit of Contractor's data privacy and information security program. In lieu of an on-site audit, at City's discretion and upon request by City, Contractor agrees to complete, within fourteen (14) days of receipt, an audit questionnaire provided by City regarding Contractor's data privacy and information security program. These audit rights are in addition to any other audit rights set forth Attachment A, Standard Provisions for City Contracts (Rev. 1/25 [v.2]).

10.15 Written Information Security Policy

Contractor shall establish and maintain a formal, documented, mandated, company-wide information security program, including security policies, standards, and procedures (collectively "Information Security Policy"), and communicate the Information Security Policy to all of its respective employees and contractors in a relevant, accessible, and understandable form. Contractor shall regularly review and evaluate the Information Security Policy to ensure its operational effectiveness, compliance with all applicable laws and regulations, and to address new threats and risks. Upon execution of this Agreement and thereafter within three (3) business days of City's request, Contractor shall make available for City's review Contractor's Information Security Policy and any related SOC audits, information security certifications, or other evidence that Contractor has in place appropriate policies and procedures regarding information protection and security.

10.16 Change in Service

Contractor shall notify City of any changes, enhancement, and upgrades to Contractor's systems, or changes in other related software services, as applicable, which could impact the security of the services.

10.17 Third Party Software

In the event Contractor provides any third-party software (the "Third-Party Software"), including Open Source Software, to City in connection with this Agreement for which City would be obligated to accept and be bound by any third-party terms and conditions, the following shall apply: (1) Contractor shall specifically identify in writing all Third-Party Software in the relevant Task Order; (2) Contractor shall attach to the relevant Task Order written copies of all third-party license agreements applicable to City; and (3) Contractor warrants that (i) it has the right to license any Third-Party Software licensed to City under this Agreement; (ii) to the best of Contractor's knowledge, the Third-Party Software does not, and the use of the Third-Party Software by City as contemplated by this Agreement will not, infringe any intellectual property rights of any third party; and (iii) unless specifically provided otherwise herein, City shall have no obligation to pay any third party any fees, royalties, or other payments for City's use of any Third-Party Software in accordance with the terms of this Agreement. With regard to (i) Open Source Software, (ii) any Third-Party Software that Contractor fails to identify in the relevant Task Order, and (iii) any third-party software embedded in the Licensed Software for which City is not required to accept any third-party terms and conditions, all such software shall be considered, as appropriate, part of and included in the definition of "Licensed Software" and subject to all warranties, indemnities, and other requirements of this Agreement, including scope of license and maintenance and support, relating to the Licensed Software. To the extent permitted by law or contract, Contractor shall pass through to City the warranties for the Third-Party Software. For purposes of this provision, "Open Source Software" means any software, programming, or other intellectual property that is subject to (i) the GNU General Public License, GNU Library General Public License, Artistic License, BSD license, Mozilla Public License, or any similar license, including, but not limited to, those licenses listed at www.opensource.org/licenses or (ii) any agreement with terms requiring any intellectual property owned or licensed by City to be (a) disclosed or distributed in source code or object code form; (b) licensed for the purpose of making derivative works; or (c) redistributable.

10.18 Criminal Justice Information Systems

Contractor agrees to and shall comply with the Federal Bureau of Investigation Criminal Justice Information Systems Security Policy (the "CJIS Security Policy"),

as amended from time to time, which document is incorporated into and made a part of this Agreement by reference. Contractor shall ensure that Contractor's security, technical, personnel, and administrative practices, meet no less than those standards articulated in the Security Policy.

Contractor agrees to, and shall comply with, Attachment D, The Federal Bureau of Investigation Criminal Justice Information Systems Security Addendum (the "Security Addendum"), which document is incorporated into and made a part of this Agreement by reference as though fully stated herein.

Contractor shall provide each of Contractor's employees with a copy of the Security Addendum and the CJIS Security Policy. Contractor shall further require each of Contractor's employees to execute the certification document contained in Attachment D, and Contractor shall provide LAPD a copy of each executed certification.

10.19 Security Addendum

Contractor agrees to and shall comply with Attachment D, The Federal Bureau of Investigation Criminal Justice Information Systems Security Addendum, which document is incorporated into and made a part of this Agreement by reference.

10.20 Provisions Apply to Subcontracts

Any subcontract entered into pursuant to the terms of this Agreement will be subject to, and incorporate, the provisions of this Section 10.0.

10.21 Survival of Provisions

The provisions of this Section 10.0 will survive termination of this Agreement.

SECTION 11.0
AMENDMENTS

Any change in the terms of this Agreement must be incorporated into this Agreement by a written amendment properly executed and signed by the person(s) authorized to bind the parties thereto.

SECTION 12.0
MISCELLANEOUS

12.1 Standard Provisions for City Contracts

The Contractor shall comply with the applicable requirements of the *Standard Provisions for City Contracts (Rev. 1/25 [v.2])*, attached hereto as Attachment A and incorporated herein by reference.

12.2 Border Wall Disclosure

Contractor shall comply with Los Angeles Administrative Code ("LAAC") Section 10.50 et seq., "Disclosure of Border Wall Contracting." City may terminate this Contract at any time if City determines that Contractor failed to fully and accurately complete the required affidavit and disclose all Border Wall Bids and Border Wall Contracts, as defined in LAAC Section 10.50.1. The required affidavit must be submitted online at www.rampLA..org.

12.3 Severability/Ambiguity

In the event a court of competent jurisdiction holds any provision of this Agreement to be invalid, such holding shall have no effect on the remaining provisions of this Agreement, and they shall continue in full force and effect. No ambiguity in this Agreement may be interpreted against any one party by virtue of that party being drafter of the Agreement. The parties acknowledge that they have read and understood this Agreement and had the opportunity to consult with counsel of their choosing regarding this Agreement.

12.4 Use of Marks

Except as expressly provided in this Agreement, Contractor shall not use the City or LAPD's names, logos, seals, insignia or other words, names, symbols or devices that identify the City or LAPD, for any purpose except with the prior written consent of, and in accordance with restrictions required by the City.

12.5 Media, Publicity, and Case Studies

Contractor shall refer all inquiries from the news media to LAPD, shall immediately contact LAPD to inform City of the inquiry, and shall comply with the procedures of LAPD's Public Affairs staff regarding statements to the media relating to this Agreement or Contractor's services under this Agreement. Contractor shall not use City as a reference or case study absent receipt of City's prior written approval. Contractor shall further provide City with the opportunity to review and approve any such reference or case study prior to publication, which approval City shall not unreasonably withhold.

12.6 No Third-Party Beneficiaries

Nothing herein is intended to create a third-party beneficiary in any subcontractor. City has no obligation to any subcontractor. No privity is created with any subcontractor by this Agreement. Even if Contractor uses subcontractors, Contractor remains responsible for complete and satisfactory performance of the terms of this Agreement.

12.7 Non-Exclusive Agreement

City and Contractor understand and agree that this is a non-exclusive Agreement to provide services to the City and the LAPD and that the City and the LAPD reserve the right to enter into one or more agreements with other contractors to provide similar services during the term of this Agreement.

12.8 Not a Waiver

Contractor acknowledges and agrees that nothing contained in this Agreement is, represents, or is intended to be construed as: a release, compromise, settlement, or waiver by City of any cause of action that City may have against Contractor. City reserves its rights in full, including, but not limited to, the right to bring any claim, cause of action, or request for reimbursement against Contractor in relation to this Agreement and other transactions between City and Contractor.

12.9 Audit Rights

In addition to those rights available to City elsewhere in this Agreement, including pursuant to PSC-16, Retention of Records, Audit and Reports, of Attachment A – Standard Provisions for City Contracts *(Rev. 1/25 [v.2])*. Contractor shall provide City, or City's duly authorized representatives, access for the purposes of audit and investigation, to any and all books, documents, papers, records, deliverables, and software documentation pertaining to any past, current, or future (i) transactions between City and Contractor, (ii) work requested to be performed of Contractor, or (iii) demands for payment by Contractor.

12.10 Payment Does Not Imply Acceptance of Work

The granting of any payment by City, or the receipt thereof by Contractor, in no way lessens the liability of Contractor to replace unsatisfactory work, equipment, or materials although the unsatisfactory character of this work, equipment or materials may not have been apparent or detected at the time the payment was made. Materials, equipment, components, or workmanship that do not conform to the requirements of this Agreement may be rejected by City and upon rejection must be replaced by Contractor without delay.

SECTION 13.0
ENTIRE AGREEMENT

13.1 Complete Agreement

This Agreement contains the full and complete Agreement between the two parties. No verbal agreement or conversation with any officer or employee of either party will affect or modify any of the terms and conditions of this Agreement. No-shrink-wrap, click-wrap, privacy policy, or other terms and conditions or agreements ("Additional Contractor Software Terms") provided with any products, services, documentation, or software hereunder shall be binding on the City, even if use of the foregoing requires an affirmative "acceptance" of those Additional Contractor Software Terms before access is permitted. All such Additional Contractor Software Terms shall be of no force or effect and shall be deemed rejected by the City in their entirety.

13.2 Counterparts/Electronic Signatures

This Agreement may be executed in one or more counterparts, and by the parties in separate counterparts, each of which when executed shall be deemed to be an original but all of which taken together shall constitute one and the same agreement. The parties further agree that facsimile signatures or signatures scanned into .pdf (or signatures in another electronic format designated by City) and sent by e-mail shall be deemed original signatures.

13.3 Number of Originals and Attachments

This Agreement includes twenty four (24) pages and four (4) attachments. Attachments A-D listed below are incorporated herein by this reference:

Attachment A – Standard Provisions for City Contracts (Rev. 1/25 [v.2])
Attachment B – Statement of Work
Attachment C – Confidentiality Agreement
Attachment D – The Federal Bureau of Investigation Criminal Justice Information Systems Security Addendum

13.4 Order of Precedence

In the event of any inconsistency between the terms, attachments, specifications or provisions which constitute this Agreement, the following order of precedence shall apply in the order listed herein:

1) This Agreement between the City of Los Angeles and Flock Group, Inc.
2) Attachment A, Standard Provisions for City Contracts (Rev. 1/25 [v.2])

3) Attachment B, Statement of Work
4) Attachment C, Confidentiality Agreement
5) Attachment D, The Federal Bureau of Investigation Criminal Justice Information Systems Security Addendum

Notwithstanding any other language in this Agreement, this Agreement shall be enforced and interpreted under the laws of the State of California.

[Signature Page Follows]

[Remainder of the Page Intentionally Left Blank]

IN WITNESS WHEREOF, the City of Los Angeles and the Contractor have caused this Agreement to be executed by their duly authorized representatives.

For: THE CITY OF LOS ANGELES,
a Municipal Corporation

By signing below, the signatory attests that they have no personal, financial, beneficial, or familial interest in this contract.

By: _____
JIM McDONNELL
Chief of Police
Los Angeles Police Department

Date: _____

APPROVED AS TO FORM:

HYDEE FELDSTEIN SOTO, City Attorney

By: _____
SAMUEL PETTY
Deputy City Attorney

Date: _____

[Contractor Name]
**Approved Signature Methods:*
1) Two signatures: One of the Chairman of the Board of Directors, President, or Vice-President, and one of the Secretary, Assistant Secretary, Chief Financial Officer, or Assistant Treasurer.

2) One signature of a Corporate-designated individual together with a properly attested resolution of the Board of Directors authorizing the individual to sign.

By: _____
[Name]
[Title]

By: _____
[Name]
[Title]

Date: _____

ATTEST:

PATRICE Y. LATTIMORE, City Clerk

By: _____
Deputy City Clerk

Date: _____

City Business License Number: _____

Internal Revenue Service Taxpayer Identification Number: _____

Said Agreement is Number _____ of City Contracts

Appendix A

flock safety

MEMORANDUM OF UNDERSTANDING

This Memorandum of Understanding (hereinafter "**MOU**") is entered into by and between Flock Group, Inc. ("**Flock**"), with a place of business at 1170 Howell Mill Rd NW Suite 210, Atlanta, GA 30318 and the Los Angeles Police Department ("LAPD" or "Department"), each a "**Party**," and together, the "**Parties**."

Whereas, the Department desires to access Flock's technology platform and Flock Safety dashboard (together, the "**Flock Service**") for the purposes of facilitating the submission of photos and videos ("**Recordings**") to the Department for investigative purposes, consistent with LAPD policy, applicable law, while utilizing Flock's software for automatic license plate detection. Whereas, Flock desires to share such Recordings and supplemental data with the Department pursuant to the following terms and conditions:

1. **Purpose**. To allow the Department to utilize the Flock Services to gain awareness with respect to the communities for which they serve, and to protect and facilitate investigations (the "Purpose").

2. **Access Rights to Flock Services**. Subject to the terms and conditions contained in this MOU, Flock hereby grants to the Department a non-exclusive, non-transferable right to access the features and functions of the Flock Service during the Term (as defined below), solely for use by Authorized Users in accordance with the terms and conditions herein, and only through the Department's official email account. For the purposes of this MOU, "Authorized Users" means employees, agents, or officers of the Department accessing or using the Flock Services for the Purpose. The Department shall undertake reasonable efforts to make all Authorized Users aware of the provisions of this MOU as applicable to such Authorized User's use of the Flock Service, and shall cause Authorized Users to comply with such provisions.

3. **Restrictions on Use**. The Department shall use the Flock Service solely for governmental purposes, consistent with LAPD policy and applicable law.

4. **Suspension of Service.** Flock may immediately suspend and/or revoke the Department's and any Authorized User's access to any portion or all of the Flock Service if Flock determines that (a) there is a threat or attack on any of the Flock Service by Department; (b) the Department's or any Authorized User's use of the Flock Service disrupts or poses a security risk to the Flock Service or any other customer or vendor of Flock; (c) the Department or any Authorized User uses the Flock Service for fraudulent or illegal activities; (d) any unauthorized user has accessed Flock Service through the Department's account; or (e) the Department violates any term of this MOU, including, but not limited to, utilizing the Flock Service for anything other than the Purpose.

5. **Ownership**. As between the Parties, subject to the rights granted in this MOU, Flock and its licensors retain all right, title and interest in and to the Flock Service and its components, and any Recordings or data provided by Flock through the Flock Service, and the Department acknowledges that it neither owns nor acquires any additional rights in and to the foregoing not expressly granted by this MOU. The Department further acknowledges that Flock retains the right to use the foregoing for any purpose in Flock's sole discretion.

6. **Warranty**. Flock makes no express or implied warranty as to the: Conditions of the Recordings, their fitness for a particular research, data, investigative purpose, resulting actions or omissions resulting from Recordings, or supplemental data obtained by the Department through the use of Flock Services.

7. **Financial Implications to Department**. No financial commitment by the Department is required to access the Flock Service or Recordings.

flock safety

8. **Term; Termination.**

A. **Term.** This MOU will commence once executed by both Parties and shall continue for a period of three (3) years.

B. **Termination.** Prior to expiration of the Term, either Party may terminate this MOU for its convenience, and in its sole discretion, by providing thirty (30) days prior written notice of termination to the other Party. Additionally, either Party may terminate this MOU upon written notice if the other Party has breached a material term of this MOU and has not cured such breach within thirty (30) days of receipt of notice from the non-breaching party specifying the breach. Upon termination of this MOU, LAPD will immediately cease all access or use of the Flock Service.

9. **Indemnification.** Except for the active negligence or willful misconduct of LAPD, or any of its boards, officers, agents, employees, assigns and successors in interest, Flock shall defend, indemnify and hold harmless LAPD and any of its boards, officers, agents, employees, assigns, and successors in interest from and against all lawsuits and causes of action, claims, losses, demands and expenses, including, but not limited to, attorney's fees (both in house and outside counsel) and cost of litigation (including all actual litigation costs incurred by LAPD, including but not limited to, costs of experts and consultants), damages or liability of any nature whatsoever, for death or injury to any person, including Flock's employees and agents, or damage or destruction of any property of either party hereto or of third parties, arising in any manner by reason of an act, error, or omission by Flock, Flock's subcontractors, or their boards, officers, agents, employees, assigns, and successors in interest. The rights and remedies of LAPD provided in this section shall not be exclusive and are in addition to any other rights and remedies provided by law or under this MOU. This provision will survive expiration or termination of this MOU.

10. **Confidentiality.**

Obligations. During the performance of services and the Department's use of the Flock Service under this Agreement, it may be necessary for a party to provide the other with certain information considered to be proprietary or confidential by the disclosing party. The disclosure of such confidential information shall be subject to the following terms and conditions.

i. The term, "Department Confidential Information," shall mean any material, data, systems, procedures and other information of, or with respect to the Department that is not accessible or known to the general public, including information concerning its hardware, software, business plans or opportunities, business strategies, finances, employees, and third-party proprietary or other information that the Department treats as confidential. Flock shall not use, publish or divulge any Department Confidential Information except:

(a) In connection with Flock's provision of Software and services pursuant to this Agreement;
(b) To Flock's officers, directors, employees, agents and contractors who need to know such information to enable Flock to provide Software and services pursuant to this Agreement; or,
(c) With the prior written consent of the Department, which consent the Department may withhold in its sole discretion.

ii. The term "Flock Confidential Information" means any material, data, systems, procedures and other information of or with respect to Flock that is not accessible to or known to the general public, including, without limitation, the software, object code, source code, formulae, algorithms, financial data, clients, employees, software development plans, software support third-party proprietary or other information that Flock treats as confidential. The Department shall not use, publish or divulge any Flock Confidential Information except:

flock safety

(a) To its employees, agents and officers who need to know such information to enable Department to use the Flock Service;
(b) With the prior written consent of Flock, which consent Flock may withhold in its sole discretion; or,
(c) Each Party shall protect the other's confidential information with the same degree of care normally used to protect its own similar confidential information, but in no event less than that degree of care that a reasonably prudent business person would use to protect such information. The obligations of each Party to protect confidential information received from the other Party shall not apply to information that is publicly known, or becomes publicly known, through no act, or failure to act, on the part of the recipient. All provisions of this MOU concerning the Confidentiality section herein, shall survive any termination of this MOU.

B. **Exclusions.** Confidential Information shall not include any information that is:

i Already known to the receiving party at the time of the disclosure;
ii Publicly known at the time of the disclosure or becomes publicly known through no wrongful act or failure of the receiving party;
iii Subsequently disclosed to the receiving party on a non-confidential basis by a third-party not having a confidential relationship with the other party hereto that rightfully acquired such information; or,
iv Communicated to a third party by the receiving party with the express written consent of the other party hereto.

A disclosure of Confidential Information that is legally compelled to be disclosed pursuant to a subpoena, summons, order or other judicial or governmental process or the California Public Records Act shall not be considered a breach of this MOU.

12. **Entire Agreement**. This MOU is complete and contains the entire understanding between the Parties relating to the sharing of Recordings and Confidential Information by and between Flock and the Department. This MOU supersedes any and all other agreements between the Parties. This Agreement is non-assignable by both Parties.

13. **Severability.** Nothing in this MOU is intended to conflict with or violate state or federal laws, regulations, policies, etc. If a term or provision of this MOU is inconsistent with a law or authority, then that term or provision shall be invalid, but the remaining terms and provisions shall remain in full force and effect. If any provision of this MOU is found to be unenforceable, unlawful, or void, the provision shall be deemed severable from the MOU and shall not affect the validity of the remaining provisions.

14. **Miscellaneous**. All notices, requests, demands, or other communications required or permitted to be given hereunder must be in writing and must be addressed to the parties at their respective addresses set forth below and shall be deemed to have been duly given when (a) delivered in person (b) one (1) business day after being deposited with a reputable overnight air courier service; or (c) three (3) business days after being deposited with the United States Postal Service, for delivery by certified or registered mail, postage pre-paid and return receipt requested. This MOU shall be governed by the laws of the State California, excluding its conflict of laws rules. The Parties agree that the United Nations Convention for the International Sale of Goods is excluded in its entirety from this MOU.

IN WITNESS WHEREOF, Flock and the Department have caused this MOU to be signed on the date set forth below and be effective on the last date specified below.

flock safety

FLOCK GROUP, INC.		Los Angeles Police Department	
By:		By:	
Name:	MARK SMITH	Name:	Michel R. Moore
Title:	GENERAL COUNSEL	Title:	Chief of Police
Date:	23 JUNE 2023	Date:	7-11-23

Appendix B

Memorandum of Understanding

Between

The Los Angeles Police Department (LAPD)

And

Flock Group Inc.

Regarding Temporary Use of Flock Safety Falcon LPR Cameras

1. Purpose

This Memorandum of Understanding ("MOU") outlines the terms and conditions under which Flock Group Inc. ("Flock") will donate the use of its Safety Falcon License Plate Reader (LPR) technology to the Los Angeles Police Department ("LAPD" or "Department") for a period of six months at no cost to the Department or the City of Los Angeles ("City"). The purpose of the donation is to help the Department deter, detect, and investigate any looting activity in the restricted areas affected by recent fires in the City of Los Angeles.

2. Key Operational Aspects

Flock will provide the following resources:

- **Up to 50 Flock Safety Falcon Systems ("Flock Equipment")**
- **Installation and removal of the LPRs by Flock employees or agents**
- **Cloud storage for collected data**
- **Technical means for Department Personnel to access the collected data**
- **Training for Department Personnel as needed**
- **Insurance related to the installation and removal of the Flock Equipment**

The Department will provide the following resources:

- **Police escort and traffic control during installation of the Flock Equipment**
- **Coordination with the Department of Street Services on use of City poles**

Flock hereby grants to City a non-exclusive, non-transferable right to access the features and functions of the Flock Equipment and services during the term, solely for use by the City. The footage will be available for City user to access and download via the Flock web interface for the retention period. City will be required to sign up for an account and select a password and username. City shall be responsible for all acts and omissions of City users. City shall undertake reasonable efforts to make all City users aware of all applicable provisions of this MOU and shall cause City users to comply with such provisions.

Flock shall have the right to collect, analyze, and anonymize City Data and City generated data to the extent such anonymization renders the data non-identifiable to create Anonymized Data to use and perform the services and related systems and technologies, including the training of machine learning algorithms. City hereby grants Flock a non-exclusive, worldwide, perpetual, royalty-free right to use and distribute such Anonymized Data to improve and enhance the

services and for other development, diagnostic and corrective purposes, and other Flock offerings. The parties understand that the aforementioned license is required for continuity of services. Flock does not own and shall not sell Anonymized Data. For purposes of this MOU, "Anonymized Data" means City Data permanently stripped of identifying details and any potential personally identifiable information, by commercially available standards which irreversibly alters data in such a way that a data subject (i.e., individual person or entity) can no longer be identified directly or indirectly.

3. Confidentiality

LAPD is the sole and exclusive owner of all data and information provided to Flock by or on behalf of LAPD pursuant to this Agreement, as well as any data collected by the Flock Equipment in the City of Los Angeles ("City Data"). Flock shall retain all data collected for five years at no charge to the Department or City. Flock shall not use City Data for any purpose other than as specified in Section 1, nor shall Flock sell, assign, lease, dispose of, or otherwise use City Data for any other purpose. City may require Flock to export City Data stored within Flock's systems or held by Flock, in any form or format, at no charge to City within 3 business days of any request.

4. Term and Termination

This MOU shall terminate six months from the date it is signed, unless terminated earlier. Either party may terminate this MOU with 14 days' written notice. Upon termination, Flock will remove all Flock-provided hardware within a reasonable time, and LAPD will be given the opportunity to download all City Data, as defined in Section 3, remaining on Flock's servers before it is deleted.

5. Waiver, Indemnification and Hold Harmless Agreement

Flock agrees to and hereby does release, discharge, waive and relinquish any and all claims, demands, actions, or causes of action for personal injury, property damage, or wrongful death that may arise from the installation and removal of the Flock Equipment, and agrees that under no circumstances will Flock prosecute or present any such claims, demands, actions, or causes of action against the Department or City arising from this agreement. To the extent that any claim of injury, loss, damages, or liability against the City arising from an act or omission of Flock or its agents, or by defective or malfunctioning Flock Equipment or software used in connection with the Flock Equipment, Flock agrees to indemnify, defend, and hold harmless the City from any and all such claims, including reasonable attorney's fees and/or any other associated costs.

6. Insurance Requirement

Flock hereby agrees to provide and maintain, at its own expense, insurance that has coverage and limits not less than: $1,000,000 for workers' compensation; and $1,000,000 for general liability. Such insurance must add the City as an additional named insured to cover the City's liability arising out of the acts of Flock employees or agents during the installation and removal of the Flock Equipment. Such insurance must include a waiver of subrogation that waives the insurer's right to recover from the City any worker's compensation paid to the injured employee or agent of Flock. Flock agrees to provide LAPD with proof of insurance that meets these

requirements prior to installation of the Flock Equipment. All required insurance must be maintained in full force for the duration of this agreement.

Acknowledgment and Acceptance

By signing below, both parties acknowledge their understanding of, and agreement to, the terms outlined in this MOU.

Los Angeles Police Department

By: _____

Name: _____

Title: _____

Date: _____

Flock Group Inc.

Signed by:
By: Mark Smith
AC5C831454C24F8...

Name: Mark Smith

Title: General Counsel

Date: 1/23/2025

Approved

_____, 20__

Hydee Feldstein Soto, City Attorney

By: _____

Appendix C

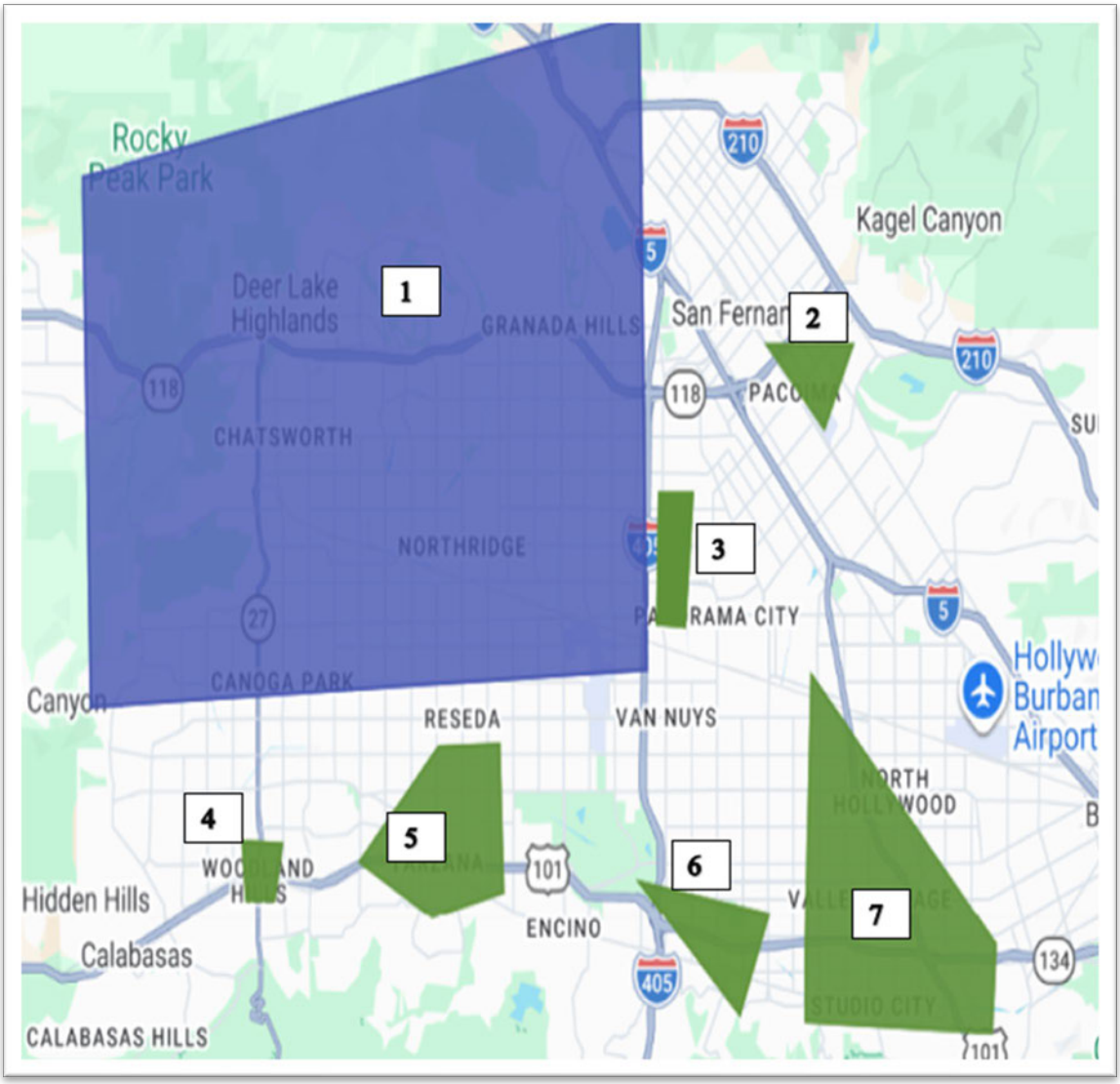
Map Key for following Three Maps

Blue Polygon represents Flock Cameras
Green Polygon represents Motorola Cameras

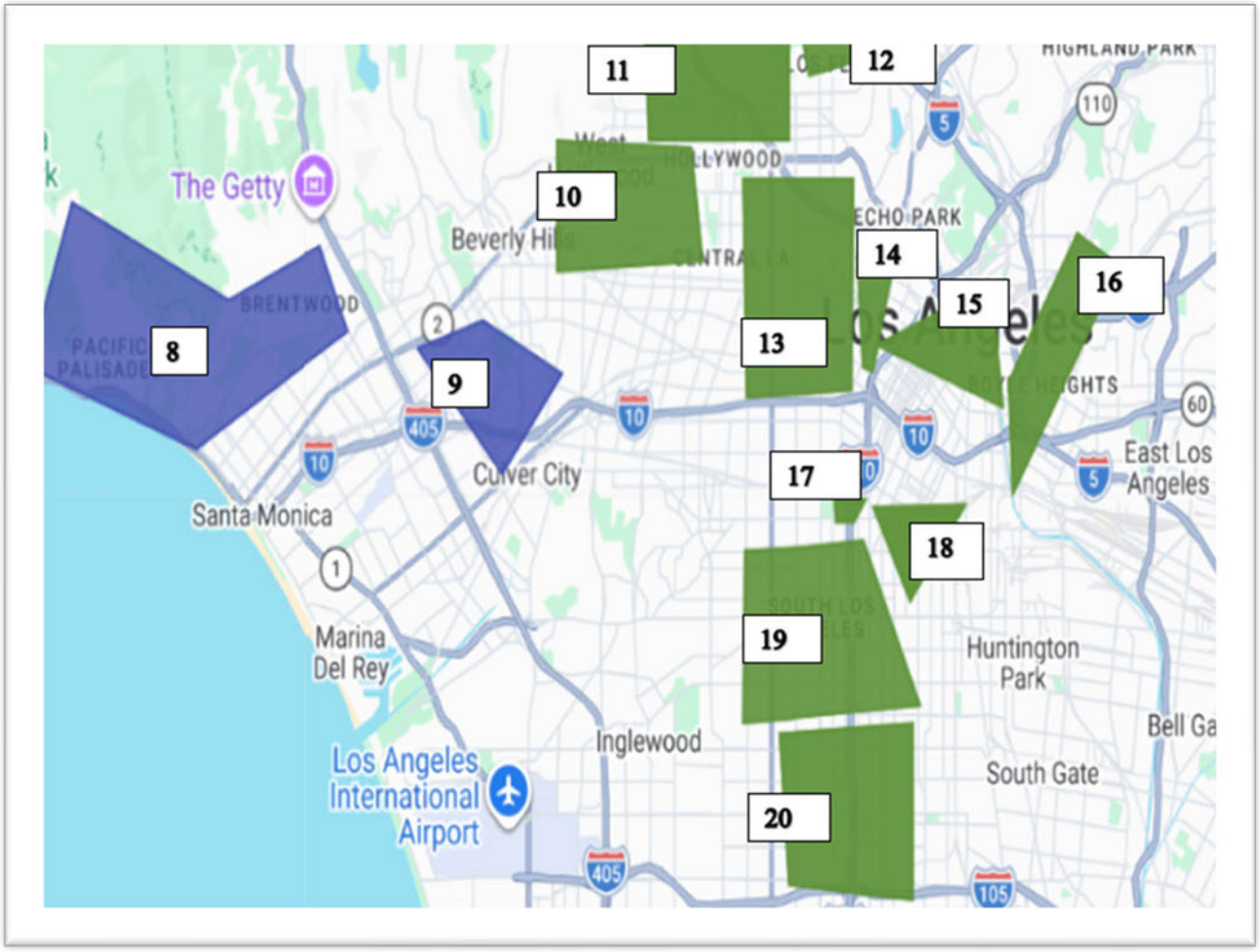
Numbers Represent the following Divisions

1. Devonshire
2. Foothill
3. Mission
4. Topanga
5. West Valley
6. Van Nuys
7. North Hollywood
8. West LA (Pacific Palisades)
9. West LA
10. Wilshire
11. Hollywood
12. Northeast
13. Olympic
14. Rampart
15. Central
16. Hollenbeck
17. Southwest
18. Newton
19. 77th
20. Southeast
21. Harbor

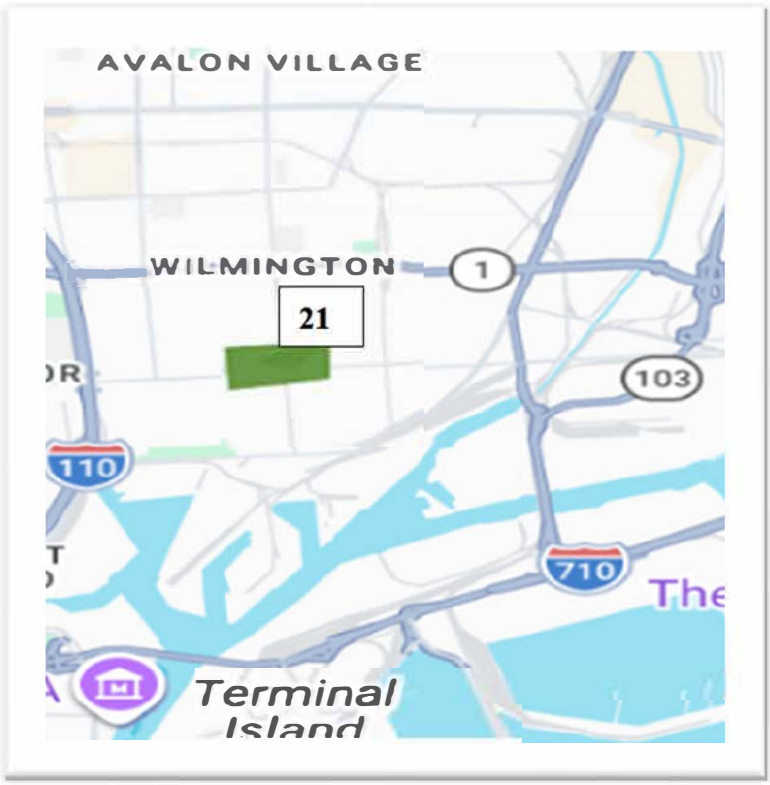
Map 1


Rocky Peak Park
Deer Lake Highlands
1
GRANADA HILLS
CHATSWORTH
NORTHRIDGE
CANOGA PARK
Canyon
RESEDA
VAN NUYS
Kagel Canyon
San Fernan
2
PACOIMA
3
RAMA CITY
Hollyw
Burban
Airport
4
5
6
7
WOODLAND
Hidden Hills
Calabasas
CALABASAS HILLS
ENCINO
STUDIO CITY
118
210
5
27
101
405
134

Map 2


11
12
10
14
15
16
13
8
9
17
18
19
20
The Getty
Beverly Hills
HOLLYWOOD
ECHO PARK
BRENTWOOD
PACIFIC PALISADES
Culver City
Santa Monica
Marina Del Rey
Los Angeles International Airport
Inglewood
Huntington Park
South Gate
East Los Angeles
Bell Ga
110
405
10
5
60
105

Map 3



Appendix D
Purchase Order for pole-mounted cameras located in Council District 12

CITY OF LOS ANGELES

City of Los Angeles Purchasing Agent
111 E 1ST STREET
ROOM 110
LOS ANGELES CA 90012

ONE-TIME PURCHASE ORDER

Purchase Order Number	Record Date	Requester Name
OPO 70 240000302682 1	05-03-24	[redacted]
Payment Terms	**Freight Terms**	**Ship Via**
0% Net 30	FOB Dest, Freight Prepaid	Vendor
Bill To	**Vendor**	**Ship To**
City of Los Angeles Supply Svcs., Accounts Payable 555 Ramirez St., Space 312 Los Angeles CA 90012	MOTOROLA SOLUTIONS INC 000028442 13108 COLLECTIONS CENTER DR CHICAGO, IL 60693	LAPD - INFO TECH BUREAU ITBWAREHOUSE 555 RAMIREZ STREET Space 212 LOS ANGELES, CA 90012

Additional Info

Please include this first page with your shipment.

You are hereby notified of the award of this Purchase Order (PO) with the City of Los Angeles in accordance with the Vendor Renewal Quote listed herein for the items thereof. The Quotation document signed by the appropriate contractor and by duly authorized City officials is on file in the Purchasing Agent's office.

MOTOROLA SOLUTIONS INC quote LQW-0892-01, Date 04/04/2024

The PO is awarded for the following:

**** ALPR CAMERAS FOR IMD ****

SUPPLIER CONTACT:
Contact Person: [redacted]
Telephone No.: [redacted]
E-Mail Address: [redacted]

DEPARTMENT CONTACT:
Contact Person: [redacted]
Direct: [redacted]
E-mail Address: [redacted]

RQS 240000602778

The new IT-Receiving Policy applies to this purchase. End-users must scan and attach one of the supporting documentation below to the RC document in FMS 2.0.

Shipping Additional Info: *** ELECTRONIC SOFTWARE DELIVERY: LICENSES@LAPD ONLINE *** DELIVERY INSTRUCTIONS: MONDAY-FRIDAY, 8:00 AM - 3:00 PM PLEASE DELIVER TO THE PIPER TECHNICAL CENTER AT 555 RAMIREZ STREET SECOND LEVEL, SPACE 212 (ITB WAREHOUSE), LOS ANGELES, CA 90012 ITB WAREHOUSE: (213) 473-9900, PRESS OPTION 4

Issuer: [redacted]
Phone Number [redacted] Email Address [redacted]

Requestor: [redacted]
Phone Number: [redacted] Email Address: [redacted]

Line Items

Line	Commodity Code	CL Description	Quantity	UOM	Unit Price	Sub Total	Sales Tax	Line Total
1	3116	L5F Fixed LPR Camera with Sun Shield - 25mm Lens with Camera	100	EA	$2,500.00	$250,000.00	$23,750.00	$273,750.00
Extended Description:	Dual-lens camera with infrared LEDs for plate illumination - 55ft 85ft capture distance and up to 2 lane coverage Internal trigger for capture of plate alphanumerics, vehicle make and model Camera housing with included sunshield is IP67 rated for reliable use in varied weather conditions - 60' camera cable included - Includes CarDetector LPR software for local server hosting LPR vehicle license plate scanning / real time alerting - Full suite of LPR tools including data analytics							
Delivery Date:	09-24-24							
Shipping Add'l Info:	*** ELECTRONIC SOFTWARE DELIVERY: LICENSES@LAPD.ONLINE *** DELIVERY INSTRUCTIONS: MONDAY-FRIDAY, 8:00 AM - 3:00 PM PLEASE DELIVER TO THE PIPER TECHNICAL CENTER AT 555 RAMIREZ STREET SECOND LEVEL, SPACE 212 (ITB WAREHOUSE), LOS ANGELES, CA 90012 ITB WAREHOUSE: (213) 473-9900, PRESS OPTION 4							
2	3116	Fixed LPR Camera Bracket	100	EA	$250.00	$25,000.00	$2,375.00	$27,375.00
Extended Description:	Pole or Wall Mount - UPR ARM ASSY POLE & WALL MOUNT BLK REV B							
Delivery Date:	09-24-24							
Shipping Add'l Info:	*** ELECTRONIC SOFTWARE DELIVERY: LICENSES@LAPD.ONLINE *** DELIVERY INSTRUCTIONS: MONDAY-FRIDAY, 8:00 AM - 3:00 PM PLEASE DELIVER TO THE PIPER TECHNICAL CENTER AT 555 RAMIREZ STREET SECOND LEVEL, SPACE 212 (ITB WAREHOUSE), LOS ANGELES, CA 90012 ITB WAREHOUSE: (213) 473-9900, PRESS OPTION 4							
3	3116	Vigilant FixedCamera Communications Box	50	EA	$2,636.00	$131,800.00	$12,521.00	$144,321.00
Extended Description:	Linux Comms Box using VLP5200 Manages power and communications for up to four (4) Vigilant fixed LPR cameras - Includes modem for communication with cellular carriers - SIM Card not included							
Delivery Date:	09-24-24							
Shipping Add'l Info:	*** ELECTRONIC SOFTWARE DELIVERY: LICENSES@LAPD.ONLINE *** DELIVERY INSTRUCTIONS: MONDAY-FRIDAY, 8:00 AM - 3:00 PM PLEASE DELIVER TO THE PIPER TECHNICAL CENTER AT 555 RAMIREZ STREET SECOND LEVEL, SPACE 212 (ITB WAREHOUSE), LOS ANGELES, CA 90012 ITB WAREHOUSE: (213) 473-9900, PRESS OPTION 4							
4	3116	Vigilant LPR Basic Service Package for Hosted/Managed LPR De	1	EA	$25,000.00	$25,000.00	$0.00	$25,000.00
Extended Description:	Managed/hosted server account services by Vigilant -Includes access to all LEARN or Client Portal and CarDetector software updates Priced per camera per year for over 60 total camera units - Requires new/existing Enterprise Service Agreement (ESA)							
Delivery Date:	09-24-24							
Shipping Add'l Info:	*** ELECTRONIC SOFTWARE DELIVERY: LICENSES@LAPD.ONLINE *** DELIVERY INSTRUCTIONS: MONDAY-FRIDAY, 8:00 AM - 3:00 PM PLEASE DELIVER TO THE PIPER TECHNICAL CENTER AT 555 RAMIREZ STREET SECOND LEVEL, SPACE 212 (ITB WAREHOUSE), LOS ANGELES, CA 90012 ITB WAREHOUSE: (213) 473-9900, PRESS OPTION 4							

Line	Commodity Code	CL Description	Quantity	UOM	Unit Price	Sub Total	Sales Tax	Line Total
5	3116	Vigilant System Start Up & Commissioning of In Field LPR sys	50	EA	$450.00	$22,500.00	$0.00	$22,500.00
Extended Description:		Vigilant technician to visit customer site Includes system start up, configuration and commissioning of LPR system Includes CDM/CDF Training Applies to mobile (1 System) and fixed (1 Camera) LPR systems						
Delivery Date:		09-24-24						
Shipping Add'l Info:		*** ELECTRONIC SOFTWARE DELIVERY: LICENSES@LAPD.ONLINE *** DELIVERY INSTRUCTIONS: MONDAY-FRIDAY, 8:00 AM - 3:00 PM PLEASE DELIVER TO THE PIPER TECHNICAL CENTER AT 555 RAMIREZ STREET SECOND LEVEL, SPACE 212 (ITB WAREHOUSE), LOS ANGELES, CA 90012 ITB WAREHOUSE: (213) 473-9900, PRESS OPTION 4						
6	78121601	Vigilant Shipping Charges - Fixed or Comms	100	EA	$40.03	$4,003.00	$0.00	$4,003.00
Extended Description:		SHIPPING CHARGES						
Delivery Date:		09-24-24						
Shipping Add'l Info:		*** ELECTRONIC SOFTWARE DELIVERY: LICENSES@LAPD.ONLINE *** DELIVERY INSTRUCTIONS: MONDAY-FRIDAY, 8:00 AM - 3:00 PM PLEASE DELIVER TO THE PIPER TECHNICAL CENTER AT 555 RAMIREZ STREET SECOND LEVEL, SPACE 212 (ITB WAREHOUSE), LOS ANGELES, CA 90012 ITB WAREHOUSE: (213) 473-9900, PRESS OPTION 4						

Sub Total:	$458,303.00
Sales Tax:	$38,646.00
Total PO Amount:	$496,949.00

Appendix E
Purchase Order for Axon in-car ALPR feature

CITY OF LOS ANGELES

City of Los Angeles Purchasing Agent
111 E 1ST STREET
ROOM 110
LOS ANGELES CA 90012

ONE-TIME PURCHASE ORDER

Purchase Order Number	Record Date	Requester Name
OPO 70 250000302683 1	05-13-25	[redacted]
Payment Terms	**Freight Terms**	**Ship Via**
0% Net 30		Vendor
Bill To	**Vendor**	**Ship To**
City of Los Angeles Supply Svcs., Accounts Payable 555 Ramirez St., Space 312 Los Angeles CA 90012	AXON ENTERPRISE INC 000038831 17800 N. 85TH ST SCOTTSDALE, AZ 85255	LAPD - INFO TECH BUREAU ITBWAREHOUSE 555 RAMIREZ STREET Space 212 LOS ANGELES, CA 90012

Additional Info

Please include this first page with your shipment.

You are hereby notified of the award of this Purchase Order (PO) with the City of Los Angeles in accordance with the Vendor Renewal Quote listed herein for the items thereof. The Quotation document signed by the appropriate contractor and by duly authorized City officials is on file in the Purchasing Agent's office.

AXON ENTERPRISE INC Quote # Q-578400-45602-866MH Dated 11/6/2024

The PO is awarded for the following:

**** Axon - Fleet 3 ALPR License Renewal - 1 year ****

SUPPLIER CONTACT:
Contact Person: [redacted]
Telephone No.:
E-Mail Address:

DEPARTMENT CONTACT:
Contact Person:
Direct:
E-mail Address:

RQS 250000603010
Previous PO # 240000300593

The new IT-Receiving Policy applies to this purchase.

Issuer: [redacted]
Phone Number: [redacted] Email Address: [redacted]

Requestor: MARK NAVARRO
Phone Number: [redacted] Email Address [redacted]

Line Items

Line	Commodity Code	CL Description	Quantity	UOM	Unit Price	Sub Total	Sales Tax	Line Total
1	4316	AXON FLEET 3 - ALPR LICENSE - 1 CAMERA	1	EA	$531,000.00	$531,000.00	$0.00	$531,000.00
Extended Description: QTY. 1500 @ 29.50/EA X 12 MONTHS Delivery Date: NULL								

OPO 70 250000302683 1 Page 1

Appendix F
Purchase Order for pole-mounted cameras and trailer cameras using UASI grant fund

CITY OF LOS ANGELES

City of Los Angeles Purchasing Agent
111 E 1ST STREET
ROOM 110
LOS ANGELES CA 90012

CONTRACT PURCHASE ORDER

Purchase Order Number	Contract Number	Record Date
CPO 46 230000431593 1	ARC 40 230000000019 1	11-02-22
Payment Terms	**Freight Terms**	**Ship Via**
0% Net 30	FOB Dest, Freight Prepaid	Vendor
Ship To	**Vendor**	**Bill To**
LAPD - INFO TECH BUREAU ITBWAREHOUSE 555 RAMIREZ STREET Space 212 LOS ANGELES, CA 90012	MOTOROLA SOLUTIONS INC 000028442 725 S FIGUEROA SUITE 1870 LOS ANGELES, CA 90071	City of Los Angeles Supply Svcs., Accounts Payable 555 Ramirez St., Space 312 Los Angeles CA 90012

Additional Info

Please include this first page with your shipment.

Grant Guidance:
https://www.ecfr.gov/current/title-2/subtitle-A/chapter-II/part-200/appendix-Appendix%20II%20to%20Part%20200

END-USER CONTACT:
Requestor Name: Scott [redacted]
Requestor Phone Number: [redacted]
Requestor Address:
LAPD ITD
555 Ramirez St, Sp 212
Los Angeles, CA 90012
Requestor Mail Stop: 422-212
Requestor E-mail Address: [redacted]
Are Federal Grant Funds being used for this purchase? X Yes ___ No

GRANT: UASI'20 64 E/46T970/530/21 LAPD LINE# B-3/21
GRANT SPECIALIST: [redacted]
SMS PR INQUIRIES:

==========Quote Attached==========

PLEASE DELIVER ASAP

Shipping Additional Info: Attn: [redacted]

Issuer: [redacted]
Phone Number: [redacted] Email Address: [redacted]

Requestor [redacted]
Phone Number: [redacted] Email Address: [redacted]

Line Items

Line	Commodity Code	CL Description	Quantity	UOM	Unit Price	Sub Total	Sales Tax	Line Total
1	451215	L6Q Quick Deploy Camera item VSFS-L6Q-S-SUB	60	EA	$1,975.00	$118,500.00	$11,257.50	$129,757.50

Extended Description: Cameras
Contract Line: 1
Delivery Date: NULL
Shipping Add'l Info: Attn [redacted]

Line	Commodity Code	CL Description	Quantity	UOM	Unit Price	Sub Total	Sales Tax	Line Total
2	451215	L6Q Solar Panel Ext Battery item VS-L6Q-SPEB	60	EA	$325.00	$19,500.00	$1,852.50	$21,352.50
Extended Description: Cameras Contract Line: 1 Delivery Date: NULL Shipping Add'l Info: Attn [redacted]								
3	451215	L6Q External LTE Antenna item VS-L6Q-EANT	60	EA	$125.00	$7,500.00	$712.50	$8,212.50
Extended Description: Cameras Contract Line: 1 Delivery Date: NULL Shipping Add'l Info: Attn [redacted]								
4	451215	L6Q Annual Replacement Plan item VS-L6Q-REPPLAN	300	EA	$100.00	$30,000.00	$0.00	$30,000.00
Extended Description: Cameras Contract Line: 1 Delivery Date: NULL Shipping Add'l Info: Attn [redacted]								
5	451215	Annual Prepaid Subscription item Prepaid-L6Q-S	240	EA	$1,975.00	$474,000.00	$0.00	$474,000.00
Extended Description: Cameras Contract Line: 1 Delivery Date: NULL Shipping Add'l Info: Attn [redacted]								
6	451215	Standard 2-Camera LPR Trailer item VSS-STD-SPD-VLT	4	EA	$18,000.00	$72,000.00	$6,840.00	$78,840.00
Extended Description: Cameras Contract Line: 1 Delivery Date: NULL Shipping Add'l Info: Attn: [redacted]								
7	451215	4 Yr Extended Hardware Warranty	4	EA	$5,000.00	$20,000.00	$0.00	$20,000.00
Extended Description: Cameras Contract Line: 1 Delivery Date: NULL Shipping Add'l Info: Attn: [redacted]								
8	451215	System Start Up & Commissioning item SSU-SYS-L6Q-COM	60	EA	$350.00	$21,000.00	$0.00	$21,000.00
Extended Description: Cameras Contract Line: 1 Delivery Date: NULL Shipping Add'l Info: Attn: [redacted]								
9	451215	Vigilant Travel item VS-TRVL-01	9	EA	$1,550.00	$13,950.00	$0.00	$13,950.00
Extended Description: Cameras Contract Line: 1 Delivery Date: NULL Shipping Add'l Info: Attn: [redacted]								
10	781216010000	Vigilant Shipping item VS-SHP-02	60	EA	$48.10	$2,886.00	$0.00	$2,886.00
Extended Description: FREIGHT, SHIPPING Contract Line: 1 Delivery Date: NULL Shipping Add'l Info: Attn: [redacted]								

Sub Total:	$779,336.00
Sales Tax:	$20,662.50
Total PO Amount:	$799,998.50

Appendix G
Information Sharing Memorandum of Agreement

AGREEMENT NO. ___20_____

MEMORANDUM OF AGREEMENT
BETWEEN
THE LOS ANGELES POLICE DEPARTMENT
AND
Huntington Park Police Department
REGARDING
THE SHARING OF AUTOMATED LICENSE PLATE RECOGNITION (ALPR) SYSTEM INFORMATION FOR LAW ENFORCEMENT PURPOSES

I. OVERVIEW

A. Introduction

This Memorandum of Agreement (MOA) is entered into on December 4, 2023 by and between the Los Angeles Police Department, located in the City of Los Angeles, and Huntington Park Police Department, located at 6542 Miles Ave, Huntington Park CA 90255, collectively referred to as the "Parties."

WHEREAS, both Parties maintain Automated License Plate Recognition (ALPR) systems that capture and record license plate data in public view for law enforcement purposes; and

WHEREAS, both Parties maintain an ALPR privacy and usage policy to ensure that the collection, use, maintenance, sharing, and dissemination of ALPR information is consistent with respect for individuals' privacy and civil liberties.

WHEREAS, the Parties recognize the value of sharing ALPR data in support of law enforcement investigations and activities; and

WHEREAS, the Parties seek to establish a formal agreement to govern the sharing of ALPR data between the Parties.

NOW, THEREFORE, the Parties agree as follows:

B. Background

ALPR system technology is a computerized database resulting from the operation of one or more mobile or fixed ALPR cameras which read and convey images of license plates and the characters they contain into computer-readable data. The data collected by the ALPR cameras consists of a photo of the vehicle license plate, the date, time and location the photo was taken, and the identification number of the ALPR camera capturing the information. The captured data can be automatically compared against a law enforcement database (i.e. "hotlist") of stolen or wanted vehicles as well as vehicles associated with Amber Alerts or outstanding warrants. When used effectively and in accordance with established laws and policies, the ALPR data can be used as an effective tool in law

enforcement investigations, situational awareness operations and responses to cognizable threats to public safety.

C. Purpose

The purpose of this MOA is to outline the terms, conditions and responsibilities under which the Parties shall reciprocally share and use "scanned plate" and "hotlist" ALPR information for official law enforcement purposes.

II. SCOPE

The scope of the data sharing includes all ALPR data captured by each Agency's system, including license plate numbers, dates and times of capture, and associated location information.

A. Responsibilities of the Parties

Parties shall designate a point of contact who will be responsible for coordinating the data sharing activities under this MOA.

Parties shall comply with all applicable federal, state, and local laws and regulations governing the use and sharing of ALPR data, including but not limited to data security, privacy, and retention requirements.

Parties shall establish appropriate technical and administrative safeguards to ensure the integrity, confidentiality, and security of ALPR data shared under this MOA.

B. Data Sharing Procedures

As between the Parties, the Party sharing ALPR data is the sole and exclusive owner of the ALPR data provided to the other Party pursuant to this MOA, and all intellectual property rights in the foregoing, whether or not provided to any other Party. Subject to the restrictions of this MOA, each Party grants the other Party a non-transferable, non-exclusive, terminable at-will license, solely for the term of this MOA, to use the ALPR data shared pursuant to this MOA consistent with the requirements of this MOA, and solely for law enforcement purposes, including but not limited to criminal investigations.

The Parties shall make best efforts to ensure the accuracy of all data provided pursuant to this MOA. Notwithstanding the foregoing, all data provided by or on behalf of either Party pursuant to this MOA is "as is." Neither Party makes any representation or warranty, express or implied, regarding the data's accuracy, completeness, or use. There are no express or implied warranties of merchantability or fitness for a particular purpose or that the use of the data will not infringe any patent, copyright, trademark, or other proprietary rights.

Parties shall exchange ALPR data electronically via an approved secure system and network connection.

ALPR data shared under this MOA shall be retained in accordance with Party policy and applicable laws and regulations governing the retention of law enforcement records.

C. Authorization

The Parties are authorized to share other ALPR license plates and "hotlist" information from their respective databases or networks as permitted by law and in accordance with established policies and procedures. The Parties are responsible for withholding any information it does not want to share with the other. The Parties are not required by the Agreement to share any ALPR information with the other.

This MOA authorizes only the Parties to share ALPR information with each other. ALPR information shall only be shared with other law enforcement agencies that have sharing agreements with the respective Parties. The sharing of ALPR information of the respective Parties outside of the agency with whom the respective Parties have an agreement is prohibited.

The sharing and use of ALPR information shall be for authorized and official law enforcement purposes only. Only authorized and trained law enforcement personnel currently employed by and in good standing with their respective agency shall access and use ALPR information. Shared ALPR information shall not be sold, shared, transferred, or otherwise disclosed for commercial purposes or to persons or entities that are not authorized to access or use ALPR information.

ALPR information shall not be shared or used for the primary purpose of immigration enforcement in accordance with law.

D. Audits and Quality Assurance

The Parties shall verify that the most current "hotlists" have been refreshed and uploaded.

The Parties shall periodically review, inspect and audit their respective ALPR systems and networks, including access and use of ALPR information, in accordance with each Party's respective audit policies.

E. Mutual Indemnity

Pursuant to the provisions of Sections 895.4 et seq. of the California Government Code, each Party agrees to indemnify and hold the other harmless from all loss or liability for injury or damage, actual or alleged, to

person or property arising out of or resulting from the indemnifying Party's acts or omissions in the performance of this Agreement. In the event of third-party loss caused by the negligence, wrongful act or omission of more than one party, each Party shall bear financial responsibility in proportion to its percentage of fault as may be mutually agreed between them or judicially determined. The provisions of California Civil Code Section 2778 regarding interpretation of indemnity agreements are hereby incorporated into this agreement.

F. Dispute Resolution

Any disputes arising from this MOA shall be resolved in accordance with the laws of California and through the Parties' mutual agreement. In the event that a dispute cannot be resolved through mutual agreement, the Parties may seek legal remedies available under applicable law.

G. Term and Termination

The term of this MOA will commence on and will expire three years from the date of the last signature to this MOA, unless terminated early by written agreement. Either Party may terminate this Agreement without cause by providing the other Party with at least 30-days written notification of its intent to terminate and specifying the termination date, served on a representative of the Party by certified mail. Unless written notice is provided by one Party to the other Party of non-extension of the MOA at least thirty (30) days prior to the date of expiration, this Agreement will be automatically extended for a one-year term commencing the next day after expiration, subject to the same terms and conditions as the initial term. Either Party may re-negotiate the terms of the Agreement during the term of the Agreement and up to 30 days prior to the renewal date.

Signatures

This MOA may be executed in counterparts and may be signed electronically. By signing below, the Parties agree to be bound by the terms and conditions of this MOA.

LOS ANGELES POLICE DEPARTMENT:

By: [redacted] Date: 7/2/24

DOMINIC H. CHOI
Chief of Police
Los Angeles Police Department

Agency: Huntington Park Police Department

Signature: [redacted] Date: 12.4.23

[Chief of Police or Authorized Representative]

INTRADEPARTMENTAL CORRESPONDENCE

July 10, 2026 **BPC #26-184**
1.0

TO: The Honorable Board of Police Commissioners

FROM: Inspector General, Police Commission

SUBJECT: REVIEW OF LOS ANGELES POLICE DEPARTMENT AUTOMATIC LICENSE PLATE READER SYSTEM AND USE IN THE FIELD

On July 10, 2026, the Office of the Inspector General (OIG) received the Department's amended response to the OIG's Review of LAPD's Automatic License Plate Reader System and Use in the Field. The response is attached for your review.

I am available to provide any additional information the Board may require.



MATTHEW J. BARRAGAN
Inspector General
Police Commission

Attachment

INTRADEPARTMENTAL CORRESPONDENCE

June 29, 2026
1.1

TO: Office of the Inspector General

FROM: Chief of Police

SUBJECT: LOS ANGELES POLICE DEPARTMENT'S RESPONSE TO THE OFFICE OF THE INSPECTOR GENERAL'S REVIEW OF THE DEPARTMENT'S AUTOMATED LICENSE PLATE READER (ALPR) SYSTEM AND USE IN THE FIELD

The Los Angeles Police Department (LAPD or Department) has received the Office of the Inspector General's (OIG) draft report of the Review of the Department's Automated License Plate Reader (ALPR) System and Use in the Field. The Department appreciates the OIG's thorough and balanced review and welcomes the opportunity to respond.

ALPR technology is a vital, lawful public-safety tool that helps officers identify and apprehend criminal suspects, recover stolen vehicles and license plates, locate missing and at-risk persons, and advance active investigations, all while operating within the privacy framework established by California law and Department policy. Objective results from the OIG's two-month review (August 1 through September 30, 2025) demonstrate this value. During that period, in-car ALPR alerts contributed to the recovery of 337 stolen vehicles, each recovered without incident, and 24 stolen license plates that had been affixed to other vehicles to evade detection. ALPR alerts led to 68 stops resulting in 74 arrests, including 15 for Grand Theft Auto, 34 for unlawful taking of a vehicle, four for evading, and three for felon in possession of a firearm, along with arrests for robbery, assault with a deadly weapon, and criminal threats. Nine vehicle pursuits arising from alerts were resolved, with every suspect taken into custody. In addition, 50 pole-mounted cameras, donated at no cost, continue to support public safety and recovery efforts in Pacific Palisades following the devastating January 2025 Palisades Fire. For these reasons, the Department is committed to the continued, responsible use of ALPR technology and, as set forth below, to strengthening the contractual, oversight, and documentation safeguards that protect the data it generates.

The report includes three recommendations to be made as follows:

SECTION V. RECOMMENDATIONS

1. Suspend the deployment of new ALPR cameras and the execution of new ALPR-related contracts pending public input and a broader reassessment of vendors and data practices. If the Department continues to use ALPR technology, it shall obtain approval from the Board of Police Commissioners for formal contracts or agreements with all ALPR vendors, regardless of the contract amount or whether the agreement involves an exchange of funds. Those contracts or agreements shall establish enforceable requirements governing data security, privacy, access controls, retention,

and auditing to protect Department ALPR data and ensure accountability for its collection, use, and disclosure.

2. Strengthen oversight of ALPR data access by amending Department policy to require annual audits to ensure that Department personnel are using the ALPR systems for authorized purposes and to clearly communicate that misuse of ALPR data may result in disciplinary action.

3. Develop and implement a standardized process for documenting traffic stops initiated by ALPR alerts to ensure complete and accurate records and facilitate meaningful analysis of officer actions and stop outcomes.

Department Response

The Department appreciates the OIG's review and concurs with the intent of each of the three recommendations, which is to ensure that ALPR technology is governed by enforceable agreements, rigorous oversight, and accurate records. The Department's responses to each recommendation are set forth below. The Department also respectfully offers several clarifications to ensure the final report is accurate and complete.

1) In response to Recommendation No. 1: The Department concurs. The Information Technology Bureau (ITB) has already paused the deployment of additional ALPR cameras and the acceptance of any further camera donations through the Los Angeles Police Foundation, pending completion of the contractual work described below. The Department also affirms that no ALPR contract with any vendor can proceed without approval from the Board of Police Commissioners and transmittal to the Mayor's Office. This requirement applies regardless of the dollar value of the contract, and it is already the Department's established practice.

   As part of this pause, ITB is working with the Office of the City Attorney and other major US cities through the Major City Chiefs Association to develop standardized contractual language to govern all ALPR vendor contracts going forward. A copy of this draft language is provided as Attachment A for the OIG's review. The draft directly addresses each contractual gap the OIG identified. It establishes that the City is the sole and exclusive owner of all City Data, including all metadata and all derived or algorithmic outputs (Section 10.2); it prohibits the vendor from using City Data for any purpose other than providing the contracted service to the Department, and specifically bars the vendor from selling, sharing, aggregating, anonymizing for resale, or using City Data to train, fine-tune, or improve any algorithm or artificial-intelligence system (Sections 10.2 through 10.4); it requires that data be stored in the continental United States and secured in a manner compliant with the FBI Criminal Justice Information Services (CJIS) Security Policy and Security Addendum (Sections 10.4, 10.10, 10.18, and 10.19); it requires breach notification within 24 hours and makes the vendor responsible for, and requires the vendor to indemnify the City against, costs and liability arising from a data breach (Section 10.11); it reserves to the City the exclusive right to

determine whether and with whom City Data is shared (Sections 10.5 and 10.8); and it grants the City the right to audit the vendor's data privacy and security program (Section 10.14). The contract becomes effective only upon execution by the parties and signature by the City Attorney as to form and legality (Section 2.1), which resolves the unsigned City Attorney approval block the OIG noted on the current Palisades Flock agreement. This language will close the remaining gaps the OIG identified, including the absence of a written agreement governing the security of Axon-captured ALPR data accessed through the Flock application.

The Department further affirms, clearly and unequivocally, that it does not share ALPR data with U.S. Immigration and Customs Enforcement (ICE) or for federal immigration enforcement, and that it will not do so. This prohibition is grounded in the Department's ALPR Usage and Privacy Policy (Manual Section 568.53), California Senate Bill 34 (2015), and Senate Bill 54 (2017, the California Values Act), as well as City of Los Angeles Ordinance No. 188441 (2024), which prohibits the use of City resources, personnel, property, and data to support federal immigration enforcement. The Department's contract with Motorola Solutions expressly prohibits the vendor from providing any ALPR data to ICE. In July 2025, in response to public concern, ITB inspected the Flock and Motorola applications for the search terms "immigration" and "ICE" and found no instances of those terms being used to query ALPR data. The standardized contract language in Attachment A reinforces these protections by prohibiting vendor data sharing and reserving all interagency sharing decisions to the City.

With respect to data shared with other law-enforcement agencies, the Department shares ALPR data only with vetted California law-enforcement agencies under Memoranda of Agreement (MOAs) that require data confidentiality, sharing protections, and data security, and that are terminable upon any violation. All such partner agencies are bound by the same California law that prohibits sharing ALPR data with federal agencies or with agencies outside California. Each agency maintains its own internal audits and controls over its use of shared data. Consistent with standard practice among partner agencies, this is a reciprocal arrangement in which neither the Department nor its partners audit one another's personnel.

Finally, the Department respectfully requests a factual correction regarding its vendor contracts. The 2022 contract with Motorola Solutions (Contract No. C-140535) covers 140 mobile ALPR cameras mounted on police vehicles and access to the vendor's user interface; it does not include fixed pole-mounted or trailer cameras. The 60 fixed pole-mounted cameras and the related trailer cameras were acquired separately via a Department purchase order processed through the City's General Services Department using Urban Areas Security Initiative (UASI) grant funds, the same procurement path used for the Motorola pole cameras funded by Council District 12. The Department respectfully requests that the report be revised to reflect this distinction.

The Department notes the OIG's reference to the 2020 California State Auditor recommendation and agrees that the standardized contract language described above directly addresses that recommendation by incorporating the necessary data safeguards into every ALPR vendor agreement.

2) In response to Recommendation No. 2: The Department concurs with the objective of strengthening oversight of ALPR data access and agrees to amend Department policy to clearly state that misuse of ALPR data may result in disciplinary action. The Department proposes the following approach to the audit requirement. The Department's Audit Division is the only Department entity that performs official, certified audits, applying the specialized training, methodology, and professional certifications that such audits require. Given Audit Division's annual audit calendar and finite resources, the Department recommends that Audit Division conduct a certified audit of ALPR data access on a biennial basis (every two years) rather than annually.

   This certified audit will be complemented by inspections conducted by ITB. ITB will continue to conduct monthly inspections, which will be formalized, documented, and reviewed at the executive level, specifically by the Commanding Officer or Assistant Commanding Officer of ITB. The monthly inspections review Department users' queries for consistency with California law and Department policy. The results of this oversight, including both the biennial certified audits and the monthly ITB inspections, will be reported to the Board of Police Commissioners annually through the Department's Comprehensive Technology Report. The Department believes this layered structure, combining certified biennial audits, documented monthly executive-reviewed inspections, annual public reporting, and explicit language regarding disciplinary consequences, fully satisfies the intent of the recommendation while making responsible use of the Department's audit resources.

   The Department also acknowledges the OIG's observation that the free-form text fields in the ALPR applications make auditing more labor-intensive. As part of the documentation improvements described in response to Recommendation No. 3, the Department will work with its vendors to develop more structured query fields to improve the consistency and auditability of access records.

3) In response to Recommendation No. 3: The Department concurs. Capturing accurate, structured data on law-enforcement actions and outcomes resulting from ALPR alerts, particularly the identification and arrest of criminal suspects, will provide objective, fact-based information documenting the substantial public-safety benefits of ALPR technology and supporting future inspections, audits, and reports to the Board of Police Commissioners. The Department will research and work with its vendors to identify the most efficient and reliable method for capturing this data.

   In doing so, the Department will address the specific limitations the OIG identified. At present, officers are not required to select a disposition following an alert, and an absence of any selection is recorded by default as "no action taken"; this accounts for a substantial portion of the 4,575 alerts the OIG categorized as "no action taken". The Department will evaluate requiring a disposition selection so that the resulting metrics accurately reflect

officer actions. The Department will also work to reduce the duplicate and inconsistent entries that arise when multiple units respond to the same incident and each receives and acts on the same alert, with the goal of having the primary unit document the outcome. The Department further notes that the roof-mounted (Motorola) cameras do not currently capture disposition data within the Axon application; the Department will pursue a documentation method that captures outcomes across both camera systems.

Two additional points of context bear on the accuracy of any outcome analysis. First, for the 161 alerts in which officers confirmed an accurate license-plate match but the vehicle was later determined not to be stolen: these situations generally result from the timing of record updates outside the Department's control, such as delays by another jurisdiction or a vehicle owner in clearing a plate from a Hot List after a vehicle has been recovered or is no longer wanted. Department policy requires officers to attempt to verify the accuracy of an ALPR alert before conducting a stop (Manual Section 568.53, Quality Assurance), and the Department's Vehicle Identification and Processing Unit operates 24 hours a day to enter and promptly remove LAPD-entered stolen-vehicle records. The Department takes the liberty and privacy interests at stake seriously and will continue to emphasize verification.

Second, the Department notes that an ALPR alert does not, by itself, explain why a license plate is on a Hot List. This is a deliberate safeguard: an alert serves as an investigative lead that an officer must independently verify using Department resources before taking any enforcement action. Officers approach such vehicles with appropriate caution, including high-risk stop tactics when the information warrants. This verification-before-action requirement protects both the public and officers and reflects the layered safeguards already built into the Department's ALPR program.

Should you have any questions or concerns regarding this matter, please contact Chief Information Officer Dean Gialamas, Information Technology Bureau, at (213) 486-0370.

Respectfully,

JIM McDONNELL
Chief of Police

Attachment