Daniel Negrete-Gonzalez
4007 Caminito Meliado
San Diego, CA 92122
(202) 643-6306
dnegreteg@proton.me

In Pro Per

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF RIVERSIDE

DANIEL NEGRETE-GONZALEZ Petitioner, v. **THE REGENTS OF THE UNIVERSITY OF CALIFORNIA,** Respondent.	Case No.: CVRI2602862 **FIRST AMENDED VERIFIED PETITION FOR WRIT OF MANDATE AND COMPLAINT FOR DECLARATORY RELIEF** [Cal. Const. Art. I, § 3; Gov. Code § 7920.000 et seq.; Code Civ. Proc. §§ 1060, 1085]

INTRODUCTION

1. This petition arises from the University of California, Riverside's refusal to conduct an adequate search for records responsive to a California Public Records Act ("CPRA") request. In response to Petitioner's request for audit logs and data-sharing records relating to the UC Riverside Police Department's ("UCRPD") Automated License Plate Reader ("ALPR") system, Respondent produced internal audit logs and a vendor-generated Data *Sharing Report*, but refused to produce the corresponding external/network audit logs documenting access to UCRPD's ALPR data by outside agencies. Respondent's sole justification is that these records "do not exist for UCR" because UCRPD is merely an "end user" of vendor-operated systems.

2. This position appears inconsistent with Respondent's own records. UCRPD's published ALPR policy designates its personnel as “system operators” and requires the maintenance of access records under Civil Code section 1798.90.52—the operator provision of the ALPR statute.

(Ex. 9, UCRPD Policy 468, § 468.3.1(d).) The ALPR vendors' own published documentation indicates that the system provides full auditing capability, including audit records of all users from shared agencies who query the data, and that such records are retained for a minimum of one year unless the customer specifies otherwise. (Exs. 10, 11.) Respondent has not explained why the external/network audit logs maintained in the same system as the produced documents cannot also be obtained.

3. Respondent has not described what search, if any, it conducted for the withheld records. It has not stated whether it inquired of its vendors—Flock Safety or Motorola Solutions (Vigilant)—to produce the requested audit logs, whether it reviewed account-level administrative tools or contracts, and it has cited no statutory exemption for withholding any responsive record.

4. Petitioner seeks a writ of mandate compelling Respondent to: (a) conduct a reasonable search for all responsive records, including records maintained by Respondent's ALPR vendors; (b) provide a sworn declaration describing the search methodology employed, the custodians consulted, and the vendor inquiries made; and (c) produce all nonexempt responsive records or identify, with specificity, each statutory exemption claimed for any record withheld.

PARTIES

5. Petitioner Daniel Negrete-Gonzalez is a member of the public within the meaning of Government Code sections 7920.515 and 7920.520 and is the requester of the public records at issue in this proceeding.

6. Respondent The Regents of the University of California is a public agency subject to the California Public Records Act. Respondent governs the University of California system, including UC Riverside and the UC Riverside Police Department ("UCRPD").

JURISDICTION AND VENUE

7. This Court has jurisdiction pursuant to Government Code sections 7923.000 and 7923.100 and Code of Civil Procedure section 1085. Article VI, Section 10 of the California Constitution vests this Court with original jurisdiction over proceedings for extraordinary relief.

8. Venue is proper in this Court pursuant to Code of Civil Procedure section 393 because the records at issue are situated in Riverside County, the acts and omissions complained of

occurred in Riverside County, and Respondent conducts business in Riverside County through UC Riverside.

LEGAL BACKGROUND

9. The CPRA provides that "access to information concerning the conduct of the people's business is a fundamental and necessary right of every person in this state." (Gov. Code, § 7921.000.) All public records not subject to a statutory exemption must be made available for inspection and copying upon request. (Gov. Code, §§ 7922.525(a)—(b).) The burden is on the agency to justify withholding by identifying an applicable statutory exemption. (Gov. Code, § 7922.000(a).)

10. An agency receiving a CPRA request has a duty to conduct a search reasonably calculated to locate responsive records, including communicating the request to the custodians of agency records and pressing the inquiry to a reasonable extent. The CPRA's disclosure obligations extend to records within an agency's constructive possession—records that the agency has the right to control, either directly or through another person. (*City of San Jose v. Superior Court of Santa Clara Cnty.* (2017) 2 Cal.5th 608, 623.)

11. Whenever it is made to appear by verified petition that public records are being improperly withheld, the Court shall order the agency to disclose the records or show cause why it should not do so. (Gov. Code, § 7923.100.) Such proceedings take precedence over all other civil matters. (Gov. Code, § 7923.005.)

FACTUAL BACKGROUND

A. UCRPD's ALPR System and Vendor Relationships

12. UCRPD operates an Automated License Plate Reader system through contracts or service arrangements with two vendors: Flock Safety and Motorola Solutions, the latter operating the platform known as "Vigilant" or "VehicleManager." (Exs. 3, 10.)

13. Motorola Solutions' published documentation establishes that all ALPR data collected by its law enforcement customers is the property of the respective customer agency, and that agencies manage and control all access to their data, including retention periods. (Ex. 10.) The documentation further states that data sharing is accomplished by the "Agency Manager employing

configurable resource restrictions and role-based access privileges." (Ex. 11.)

14. The same vendor documentation confirms that VehicleManager provides: (a) full auditing capability, including of any users from a shared agency querying the data; (b) printable audit reports for record management; and (c) robust audits and accountability based on users, search parameters, and system IP address logging. (Ex. 10.) Audit records are retained for a minimum of one year, unless the customer specifies otherwise. (Ex. 11.)

15. The VehicleManager CJIS Security Compliance Guide states that for every transaction—whether successful or unsuccessful—Agency Managers can monitor the originating IP address, the specific activity performed, and the precise timing of each event. The guide further states that all events and content, with specified exceptions, are "captured and available to the end user auditor in the audit module." (Ex. 11.) The vendor also states that it "assists clients in obtaining necessary audit data." (Ex. 11.)

16. UCRPD Policy 468 establishes that: (a) the ALPR Administrator shall develop procedures for "system operators" to maintain records of access in compliance with Civil Code section 1798.90.52 (§ 468.3.1(d)); (b) all ALPR data shall be accessible only through a login/password-protected system "capable of documenting all access of information by name, date and time" (§ 468.6(a)); and (c) ALPR system audits shall be conducted on a regular basis (§ 468.6(c)). (Ex. 9.)

17. Civil Code section 1798.90.52 requires ALPR operators to maintain a record of access that includes, at minimum, the date and time of access, the license plate or data element queried, and the username and organizational affiliation of the individual accessing the system.

B. Petitioner's CPRA Request and Respondent's Partial Production

18. On February 17, 2026, Petitioner submitted a CPRA request to UC Riverside's Office of Legal Affairs seeking: (A) ALPR audit logs, including both internal and external/network audit logs, from January 1, 2024 through February 16, 2026; (B) records identifying agencies with which UCRPD shares or receives ALPR and hot-list data; and (C) current ALPR sharing configuration settings. (Ex. 1.) Petitioner's request included step-by-step retrieval instructions identifying, for each vendor platform, the specific administrative tools and menu paths through

which the requested records could be obtained. For Flock Safety, the instructions identified the "Insights" tab on the agency's admin dashboard, from which audit logs can be downloaded as spreadsheets. For Vigilant, the instructions directed Respondent to the "Agency Management" auditing interface and specified that two datasets should be created: one for searches conducted by the agency's own users, and another for searches and lookups performed on the agency's network by outside agencies. (Ex. 1.) As used in this petition, Petitioner's request for "external/network audit logs" encompasses any existing records ordinarily maintained that reflect access to or queries of UCRPD's ALPR data by outside agencies, regardless of the vendor's internal label for such records.

19. Respondent failed to provide a written determination—or any substantive response—within the ten-day period required by Government Code section 7922.535(a).

20. On March 3, 2026, after the statutory deadline had expired, Petitioner sent follow-up correspondence advising Respondent that no compliant determination had been issued. (Ex. 2.) Respondent thereafter provided only an acknowledgment containing a generalized estimate of "eight weeks." (Ex. 1.) That acknowledgment did not state whether the request sought disclosable public records in Respondent's possession, whether responsive records would be produced, the reasons for any determination, or the estimated date and time when records would be made available, as required by Government Code section 7922.535(a). Nor did it invoke an extension under Government Code section 7922.535(b).

21. On March 5, 2026, Petitioner sent Respondent a memorandum memorializing the relevant communications and events. Shortly thereafter, Respondent sent a follow-up correspondence purporting to invoke a fourteen-day extension under Government Code section 7922.535(b). (Ex. 1.) Petitioner then spoke with Respondent's counsel and advised that section 7922.535(b) does not permit an agency to retroactively invoke an extension after the initial ten-day determination period has already expired.

22. On March 11, 2026, Respondent produced a partial response consisting of: (a) internal audit logs from Flock Safety; (b) approximately 470 pages of internal audit logs from Vigilant, reflecting searches and queries conducted by UCRPD's own personnel within the vendor's

system; and (c) a Vigilant *Data Sharing Report* dated February 26, 2026. (Exs. 1, 3.)

23. The *Data Sharing Report* identified no fewer than 121 out-of-state and federal law enforcement agencies listed in connection with UCRPD's ALPR data-sharing relationships, spanning over thirty states as well as federal entities including U.S. Customs and Border Protection (CBP-NTC), the Bureau of Alcohol, Tobacco, Firearms and Explosives (national account), the Internal Revenue Service Criminal Investigations Division, the Bureau of Indian Affairs, the U.S. Postal Inspection Service, and Camp Pendleton Provost Marshal's Office. (Ex. 3.)

24. Respondent did not produce any external/network audit logs requested in Part A.2 of Petitioner's CPRA request, in whatever form ordinarily maintained, reflecting access to or queries of UCRPD's ALPR data by outside agencies—records which the vendor's own documentation describes as the product of its "audit module" providing "auditing capability, including ANY users from a shared agency querying the data." (Ex. 10.) Respondent cited no statutory exemption for these omissions and did not identify whether the omission was based on nonexistence, lack of possession, retention limitations, technical inaccessibility, or any other ground. (Ex. 1.)

C. Petitioner's Efforts to Resolve the Dispute

25. On March 24, 2026, Petitioner sent a formal letter notifying Respondent of apparent violations of Civil Code section 1798.90.55(b) and demanding production of the withheld records. (Ex. 4.) On March 25, 2026, Chief Campus Counsel Lorena Peñaloza acknowledged receipt. (Ex. 5.)

26. On April 7, 2026, Ms. Peñaloza responded. She stated: "UCR neither owns or operates ALPR cameras or an ALPR system, nor does UCR maintain or control any stored data associated with them." She further stated that UCR is an "end user" of ALPR networks operated by Flock and Vigilant and "does not separately maintain its own ALPR database." (Ex. 5.)

27. Respondent's characterization of UCRPD as an "end user" appears inconsistent with UCRPD's own published policy, which designates UCRPD personnel as "system operators" and requires the maintenance of access records under the operator provision of the ALPR statute. (Ex. 9, Policy 468, § 468.3.1(d).) It also appears inconsistent with the vendor documentation indicating that each customer agency manages and controls its own data, retention settings, and sharing

configurations. (Exs. 10, 11.)

28. On May 5, 2026, Petitioner wrote to Respondent again demanding confirmation of compliance and production of the withheld records by May 8, 2026. (Ex. 6.) Respondent did not respond by that deadline.

29. On May 11, 2026, Ms. Peñaloza responded and attached an updated *Data Sharing Report* dated April 20, 2026, which removed all previously listed sharing agencies. (Exs. 7, 8.) However, she reiterated Respondent's position that the external/network audit logs and agency-sharing records "do not exist for UCR." (Ex. 7.) That assertion is contradicted by Respondent's own production of two Vigilant Data Sharing Reports, which are themselves records responsive to the request for agency-sharing records.

30. With respect to the external/network audit logs, at no point in the parties' correspondence did Respondent: (a) describe the search it conducted for the requested records; (b) identify the custodians consulted; (c) state whether it asked Flock Safety or Motorola Solutions/Vigilant to produce the requested audit logs; (d) explain why audit records that the vendor's own documentation indicates are available through the system could not be obtained; (e) identify whether any requested records were unavailable because of retention settings, deletion, or date limitations; or (f) identify any statutory exemption applicable to any record not produced.

D. Respondent's Final Refusal

31. By stating in its May 11, 2026 correspondence that the requested external/network audit logs "do not exist for UCR," Respondent made a final refusal to produce those records. Respondent's position was unequivocal and was reiterated after multiple rounds of correspondence in which Petitioner identified the specific records at issue and the basis for believing they exist. No further informal exchange appears likely to resolve the dispute.

E. Respondent's Search for Responsive Records

32. Respondent's own production raises substantial questions about the scope of its search. Respondent produced approximately 470 pages of internal audit logs from the Vigilant system—records generated by the vendor's audit module reflecting UCRPD personnel's own searches and queries. The vendor documentation describes that same audit module as providing

"auditing capability, including ANY users from a shared agency querying the data." (Ex. 10.) Petitioner's request included instructions directing Respondent to create two datasets from Vigilant's auditing interface: one for internal searches and one for searches performed on the agency's network by outside agencies. (Ex. 1.) Respondent appears to have followed the instructions for the first dataset but not the second. It has not explained why the external/network audit records generated by the same system—through the same administrative interface—could not also be obtained. Respondent additionally produced a vendor-generated *Data Sharing Report* (Ex. 3), further demonstrating that vendor-maintained records concerning UCRPD's account are retrievable.

33. Upon information and belief, based on the vendor documentation described in Paragraphs 14—15 and Exhibits 10—11, the vendor platforms used by UCRPD are capable of maintaining the requested external/network audit records in connection with UCRPD's ALPR account, and such records may be retrievable through Respondent's vendor accounts, administrative tools, or contractual rights as described in the vendor's own published documentation. Respondent has not stated whether it attempted to retrieve such records through any available means.

34. Even assuming some requested records may no longer be available due to retention limitations, the vendor documentation states that audit records are retained for a minimum of one year unless the customer specifies otherwise. (Exs. 10, 11.) Respondent did not state whether it searched for records within that documented retention period or what retention settings applied to UCRPD's account. Nor did it state whether responsive records were unavailable due to retention limitations or whether it took any steps to preserve responsive records after receiving Petitioner's request.

FIRST CAUSE OF ACTION

(Writ of Mandate — Gov. Code, §§ 7920.000 et seq., 7923.000–7923.110; Code Civ. Proc., § 1085)

35. Petitioner incorporates herein by reference the preceding paragraphs of this petition.

36. Under the CPRA, a public agency receiving a request for identifiable records must conduct a search reasonably calculated to locate all responsive records, communicate the request to the custodians of those records, and press the inquiry to a reasonable extent. (Gov. Code, §

7922.525; *City of San Jose v. Superior Court of Santa Clara Cnty.* (2017) 2 Cal.5th 608, 623.) Respondent has not described the search, if any, it conducted for records responsive to Petitioner's request. It has not identified the custodians consulted, stated whether it inquired of its ALPR vendors, or explained why records that the vendor's own documentation indicates are available through the system could not be obtained. It has cited no statutory exemption for any record not produced. Its assertion that the requested records "do not exist for UCR," without any account of the search conducted, does not satisfy these obligations.

37. The vendor documentation and UCRPD's own policy indicate that the customer agency owns all data collected in connection with its account, manages and controls access to that data including retention periods, and has administrative tools for auditing and sharing configuration. (Exs. 10, 11.) Respondent's correspondence did not address these portions of the vendor documentation or explain whether UCRPD has account-level administrative or contractual rights relevant to the requested records.

38. Respondent's failure to produce responsive records or to justify withholding constitutes improper withholding within the meaning of Government Code section 7923.100. Petitioner has no plain, speedy, and adequate remedy in the ordinary course of law other than the relief sought in this petition. (Code Civ. Proc., § 1086.)

SECOND CAUSE OF ACTION

(Declaratory Relief — Gov. Code, § 7923.000; Code Civ. Proc., § 1060)

39. Petitioner incorporates herein by reference the preceding paragraphs of this petition.

40. An actual controversy has arisen and now exists between Petitioner and Respondent. Specifically, the parties dispute:

a. Whether audit and access records maintained by Respondent's ALPR vendors in connection with UCRPD's use of ALPR systems constitute "public records" within the meaning of the CPRA, to the extent they are writings relating to the conduct of the public's business that are prepared, owned, used, retained, or constructively possessed by Respondent;

b. Whether Respondent's obligations under the CPRA include conducting a search for records maintained by third-party vendors on Respondent's behalf, where the vendor's own documentation identifies the agency as the data owner;

c. Whether Respondent satisfied its search obligations by asserting that it is an "end user" without inquiring with vendors, examining contractual access rights, or attempting to retrieve vendor-maintained records; and

d. Whether Respondent may refuse to produce responsive records on the ground that they "do not exist for UCR" without describing what search was conducted, whether vendors were contacted, or why vendor-maintained records cannot be obtained.

41. The CPRA authorizes declaratory relief to enforce a person's right to inspect or receive a copy of any public record. (Gov. Code, § 7923.000.) Declaratory relief is appropriate where it would resolve an ongoing dispute regarding the parties' rights and obligations in a manner that has some likelihood of affecting future requests or future conduct. (*City of Gilroy v. Superior Court* (2026) 19 Cal.5th 38.)

42. This dispute is likely to recur. UCRPD continues to operate its ALPR system through the same vendor arrangements, and Respondent has adopted a categorical position—not limited to this request—that records accessible through its vendor platform are beyond its disclosure obligations. Multiple UC campuses operate ALPR systems through similar vendor arrangements, and Petitioner has submitted and intends to submit substantially similar requests to other UC campuses.

<u>REQUEST FOR RELIEF</u>

Wherefore, Petitioner prays that this Court:

1. Issue a writ of mandate directing Respondent to conduct a reasonable search for all records responsive to Petitioner's February 17, 2026 CPRA request, including any existing audit logs, audit reports, access logs, query logs, or audit-module exports, in whatever form ordinarily maintained, reflecting access to or queries of UCRPD's ALPR data, maintained by Respondent's ALPR vendors — Flock Safety and Motorola Solutions/Vigilant — and to produce all nonexempt

responsive records;

2. Order Respondent to file a sworn declaration describing the search methodology it has employed in response to Petitioner's request, identifying the custodians consulted, the repositories searched, the contracts or service agreements reviewed, the administrative tools or account settings examined, and whether and when it inquired of each ALPR vendor regarding the existence and availability of the requested records. To the extent Respondent contends responsive records are unavailable because of retention limitations or deletion schedules, Respondent should identify that position in its responsive declaration;
3. Order Respondent to justify any withholding of responsive records by identifying each withheld record or category of records, each specific statutory exemption claimed, and the factual basis for applying that exemption, in the form of a declaration or index sufficient to permit judicial assessment of any claimed exemption;
4. Order Respondent to produce all reasonably segregable portions of any responsive records not properly exempt from disclosure;
5. If records are withheld under a claimed exemption, order Respondent to submit the records for in camera review to determine whether the claimed exemption applies;
6. Issue a declaratory judgment that, where responsive records may be maintained by ALPR vendors in connection with UCRPD's account and may be within Respondent's contractual or administrative control, the CPRA requires Respondent to make reasonable efforts to inquire of those vendors and search those sources before representing that no responsive records exist;
7. Set times for hearings and responsive pleadings "with the object of securing a decision as to the matters at issue at the earliest possible time" in accordance with Government Code section 7923.005;
8. Award Petitioner costs of suit as authorized by Government Code section

7923.115;

9. For such other and further relief as the Court deems proper.

DATED: May 18, 2026

Daniel Negrete

Daniel Negrete-Gonzalez
In Pro Per

VERIFICATION

I, Daniel Negrete-Gonzalez, am the Petitioner in this action. I have read the foregoing First Amended Verified Petition for Writ of Mandate and Complaint for Declaratory Relief and know its contents.

The factual matters alleged in this Petition are true of my own knowledge, except as follows: The matters alleged in Paragraphs 13, 14, 15, and 33, insofar as they describe the capabilities, configuration, retention settings, or account-level functionality of Respondent's vendor systems, are alleged upon information and belief based on the vendor's published documentation (Exhibits 10 and 11), and as to those matters I believe them to be true.

All other factual allegations are based on records produced by Respondent, correspondence exchanged between the parties, publicly available UCRPD policy documents, and publicly available vendor documentation. Allegations concerning legal standards and authorities state Petitioner's contentions of law and are not verified as factual matters.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct.

DATED: May 18, 2026

Daniel Negrete

Daniel Negrete-Gonzalez
Petitioner

EXHIBIT "1"

From: PublicRecords PublicRecords <publicrecords@ucr.edu>
To: elliscollective <elliscollective@proton.me>, PublicRecords PublicRecords <publicrecords@ucr.edu>
Date: Wed, 11 Mar 2026 16:28:05 -0700
Subject: Re: CPRA Request
Attachments: ALPR Sharing Configuration.pdf, vigilant.pdf, Shared Data.pdf, Flock report.pdf

---

Hello,

This email responds to your request for access to public records, which was received by this office on February 17, 2026. You specifically request the following:

Part A: ALPR audit logs (internal + external/network) from January 1, 2024 through February 16, 2026. Include the fields available in your export such as

timestamp/date, searching/requesting agency, user/account, search type, justification/reason, and search scope., STAC):

1. Searches/lookups performed by this agency's users/accounts;

2. Searches/lookups performed by external agencies that queried or included this agency's ALPR network/data (network audit logs).

Part B: Lists of agencies and networks with Automated License Plate Reader (ALPR) sharing relationships (including, but not limited to fusion centers such as ARJIS, JRIC, NCRIC, OCIAC, STAC)

3. The names of agencies and organizations with which this agency shares

ALPR data;

4. The names of agencies and organizations from which this agency receives

ALPR data;

5. The names of agencies and organizations with which this agency shares "hot

list" information;

6. The names of agencies and organizations from which this agency receives

"hot list" information;

Part C: Current ALPR sharing settings/configuration, STAC):

7. Records sufficient to show the current ALPR sharing configuration, including whether each partner listed in Part A has query/search access to this agency's

ALPR data and whether access is full vs hit-only vs hotlist-only (screenshots or configuration export acceptable)

Enclosed are documents responsive to the above requested categories. After reviewing the relevant records, the University has determined that certain portions are exempt

from disclosure under applicable provisions of the California Public Records Act. The applicable exemptions are:

• Law enforcement investigatory records (Gov. Code § 7923.600)

• Privacy (Gov. Code §§ 7927.700 and 7922.000)

Accordingly, the University has redacted those portions of the records to which the exemption(s) applies. This message concludes the University's response to your

request.

If you have any questions, please feel free to contact Information Practices at publicrecords@ucr.edu.

Kristen

Erving

Senior

Paralegal Specialist

Information

Practices Coordinator

University

of California, Riverside

900

University Ave.

Hinderaker

Hall 3148

Riverside,

CA 92521

Office: (951)

827-5983

Fax: (951)

888-3074

Kristen.Erving@ucr.edu

https://legalaffairs.ucr.edu/

On Thu, Mar 5, 2026 at 4:27 PM PublicRecords PublicRecords <publicrecords@ucr.edu> wrote:

Hello,

Thank you for your message.

I’m writing to inform you that we are taking the 14-day extension to the 10-day time limit for the initial response in order to properly research your request and determine the availability and estimated date for production of responsive records, as permitted by Government Code § 7922.535. This extension is necessitated by the need to search for records from facilities and establishments separate from the Office of Legal Affairs and the need to consult with stakeholders with a substantial interest in the determination of the request.

The initial response to your public records request will be provided on or before March 12, 2026.

In the meantime, the campus is continuing to conduct searches for records potentially responsive to Parts A, B, and C of your request and coordinating with relevant offices regarding review and potential production.

If you have any questions or wish to discuss this further, you may reply to this email directly.

Kristen

Erving

Senior

Paralegal Specialist

Information

Practices Coordinator

University

of California, Riverside

900

University Ave.

Hinderaker

Hall 3148

Riverside,

CA 92521

Office: (951)

827-5983

Fax: (951)

888-3074

Kristen.Erving@ucr.edu

https://legalaffairs.ucr.edu/

On Tue, Mar 3, 2026 at 9:37 AM elliscollective <elliscollective@proton.me> wrote:

Hello,

Thank you for your acknowledgment.

Government Code § 7922.535(a) requires the agency, within 10 calendar days of receipt, to make and dispatch a written determination as to whether the request seeks disclosable records in the agency's possession and to promptly notify the requester of that determination and the reasons.

Your message provides an acknowledgment and a general estimate ("eight weeks"), but it does not state (1) whether UC Riverside has located responsive records, (2) whether it will produce them (in whole or in part), or (3) the basis for any extension beyond the statutory determination period. Please therefore provide, in writing, the statutory determination under § 7922.535(a), including:

Whether UC Riverside has responsive records for each of Parts A, B, and C, and whether UC Riverside will produce them; and

A rolling production plan with (a) the date of first production and (b) an estimated completion date.

The items I requested are readily available and do not require compilation or extraordinary effort beyond ordinary retrieval and review. My request was submitted on February 17, 2026. UC Riverside did not provide any written determination or written notice of extension within the statutory determination period. Although § 7922.535(b) permits a limited extension only in "unusual circumstances," it does so only by written notice stating the specific reasons and the date the determination is expected to be dispatched (up to 14 additional calendar days). No timely written extension notice was provided. Accordingly, the time for invoking an extension under § 7922.535(b) has passed.

Thank you,

The Ellis Collective

On Tuesday, 3 March 2026 at 8:55 AM, PublicRecords PublicRecords <publicrecords@ucr.edu> wrote:

Hello,

This is to acknowledge your California Public Records Act (CPRA) request. Appropriate UC Riverside offices are being notified of your request. Records identified as responsive to your request will be reviewed, and made available for your access, in accordance with relevant law and University policy. The estimated date of production for all new requests is eight weeks, though we are often able to provide records more quickly.

Please note that there is no central repository for all University records. The identification and collection of potentially responsive records is only the first step in the CPRA response process. The collected records must be reviewed by this office to ensure that they are in fact responsive to your request and to assess whether any legal privileges or exemptions from disclosure are applicable and whether redactions may be required to protect individuals' rights to privacy. Please also bear in mind that we are concurrently fulfilling numerous other requests, many of which were received before yours and that we generally process requests in the order in which they are received.

Although the requested records have not yet been fully gathered and reviewed, it is possible that the requested material may contain information exempt from disclosure pursuant to the CPRA. However, this is not a determination that the requested records are necessarily exempt from disclosure. This office will provide you with a status update after the requested records have been thoroughly reviewed.

Kristen

Erving

Senior

Paralegal Specialist

Information

Practices Coordinator

University

of California, Riverside

900

University Ave.

Hinderaker

Hall 3148

Riverside,

CA 92521

Office: (951)

827-5983

Fax: (951)

888-3074

Kristen.Erving@ucr.edu

https://legalaffairs.ucr.edu/

On Tue, Feb 17, 2026 at 10:12 PM elliscollective <elliscollective@proton.me> wrote:

Pursuant to the California Public Records Act, I request the following records from UCR PD:

Part A: ALPR audit logs (internal + external/network) from January 1, 2024 through February 16, 2026. Include the fields available in your export such as timestamp/date, searching/requesting agency, user/account, search type, justification/reason, and search scope., STAC):

1. Searches/lookups performed by this agency's users/accounts;

2. Searches/lookups performed by external agencies that queried or included this agency's ALPR network/data (network audit logs).

Part B: Lists of agencies and networks with Automated License Plate Reader (ALPR) sharing relationships (including, but not limited to fusion centers such as ARJIS, JRIC, NCRIC, OCIAC, STAC)

3. The names of agencies and organizations with which this agency shares ALPR data;

4. The names of agencies and organizations from which this agency receives ALPR data;

5. The names of agencies and organizations with which this agency shares "hot list" information;

6. The names of agencies and organizations from which this agency receives "hot list" information;

Part C: Current ALPR sharing settings/configuration, STAC):

7. Records sufficient to show the current ALPR sharing configuration, including whether each partner listed in Part A has query/search access to this agency's ALPR data and whether access is full vs hit-only vs hotlist-only (screenshots or configuration export acceptable)

The requested documents will be made available to the general public, and this request is not being made for commercial purposes. I prefer to receive responsive records electronically via the request portal or email attachment. If any fees may apply, please provide an itemized estimate in advance.

These audit/search logs are required as part of ALPR operation under California Civil Code § 1798.90.52(a) and can help the public understand how often ALPR data is being queried and by whom. Similar records have been disclosed by multiple agencies in response to prior CPRA requests. If records responsive to any portion of this request are maintained by another department, division, or office, please identify the appropriate custodian and provide reasonable assistance in locating the records as required by Government Code §§ 7922.535 and 7922.600. If any portion of a responsive record is exempt, please redact only the exempt material and produce the remainder, consistent with Government Code § 7922.525(b) (reasonably segregable portions must be disclosed).

For your convenience, I have compiled brief instructions on how these records can be seen here: https://drive.proton.me/urls/JFC930F0G4#BVewJLnWPNEr

If documents will be sent on a rolling basis, please do so in chronological order (ALPR audit logs first). Thank you. I look forward to your response within 10 calendar days.

Instructions on How to Share Information

Request of all documents in this page are allowed and required upon request, persuant to SB 34 (2015). Failure to provide all request material will comsitute violations of SB 34 and the California Public Record Act, which can result in litigation.

Flock:

Items 1-2: The audit logs can be accessed via your agency's Flock admin dashboard on the "Insights" tab. These logs in the user download as spreadsheets in monthly increments, provide all spreadsheets for the timeframe stated in the request. Keep all columns in the logs, including agency performing search/loopup, date/time of search, user ID, and search parameters and reason.

Items 3-6: With Flock Safety, this information is available through the transparency portal function.

Item 7: This information can be obtained via through a few different tools in Flock Safety. If all agencies in the "agencies sharing with me" section of the sharing report (*items 3-6)* have the capability to automatically search through your network, no report or screenshot is needed. Simply confirm in writing if that is the case.

Vigilant:

Items 1-2: Logs can be obtained by going to Agency Management → Auditing. Create one dataset on searches/lookup made by this agency's users, and another for Searches/lookups performed on your agency's network. You must include the Agency name (conducting the search), date(s), officer, query, and reason.

Items 3-6: Data sharing agreements can be downloaded through the the Data Sharing interface : "The Output Report button allows you to download a PDF report listing of shared agency data. The report will consist of all Detection and Hot List shares that are currently being shared, as well as all Detection and Hot List shares being received."

Item 7: This information can also be accessed through the data sharing interface. If all agencies in the "agencies sharing with me" section of the sharing report (*items 3-6)* have the capability to automatically search through your network, no report or screenshot is needed. Simply confirm in writing if that is the case.

EXHIBIT "2"

From: elliscollective <elliscollective@proton.me>
To: kristen.erving@ucr.edu, lorena.penaloza@ucr.edu, Jamie.lopez@ucr.edu
Date: Tue, 03 Mar 2026 09:47:31 +0000
Subject: CPRA Request Determination Overdue
Attachments: Requested Material.pdf, help.pdf

To Office of Legal Affairs,

I am following up on the CPRA request I submitted on February 17th, 2026, seeking records from UCR PD regarding ALPR audit logs, ALPR sharing partners, and current ALPR sharing configuration (Parts A–C listed in the forwarded email below). To date, I have received no acknowledgment, no written determination, and no written notice of extension.

Government Code § 7922.535(a) required UC Riverside to issue a written determination within 10 calendar days of receipt. If UC Riverside believed "unusual circumstances" applied, § 7922.535(b) permitted a single extension of up to 14 additional calendar days, but only if UC Riverside provided written notice setting forth the reasons for the extension and the date on which the determination was expected to be dispatched. No such written extension notice was provided within the statutory determination period. Accordingly, the time for invoking an extension under § 7922.535(b) has passed, and UC Riverside remains obligated to provide the required determination and proceed with prompt production.

Please provide no later than March 5, 2026:

Written confirmation of the date UC Riverside received my request;

UC Riverside's written CPRA determination under § 7922.535(a) (whether responsive records exist and will be produced); and

A rolling production schedule, including the date of first release and an estimated completion date.

If any portion is withheld or redacted, please identify the specific exemption(s) and produce all reasonably segregable non-exempt portions. (Gov. Code § 7922.525(b).) If records are maintained by another office, please identify the appropriate custodian and provide reasonable assistance in locating the records. (Gov. Code § 7922.600.)

If UC Riverside does not provide the required determination and a reasonable production schedule by the deadline above, I will treat the continued nonresponse as a denial and will pursue judicial enforcement under the CPRA.

Best,

The Ellis Collective

------- Forwarded Message -------

From: elliscollective <elliscollective@proton.me>

Date: On Tuesday, 17 February 2026 at 10:12 PM

Subject: CPRA Request

To: publicrecords@ucr.edu <publicrecords@ucr.edu>

Pursuant to the California Public Records Act, I request the following records from UCR PD:

Part A: ALPR audit logs (internal + external/network) from January 1, 2024 through February 16, 2026. Include the fields available in your export such as timestamp/date, searching/requesting agency, user/account, search type, justification/reason, and search scope., STAC):

1. Searches/lookups performed by this agency's users/accounts;

2. Searches/lookups performed by external agencies that queried or included this agency's ALPR network/data (network audit logs).

Part B: Lists of agencies and networks with Automated License Plate Reader (ALPR) sharing relationships (including, but not limited to fusion centers such as ARJIS, JRIC, NCRIC, OCIAC, STAC)

3. The names of agencies and organizations with which this agency shares ALPR data;

4. The names of agencies and organizations from which this agency receives ALPR data;

5. The names of agencies and organizations with which this agency shares "hot list" information;

6. The names of agencies and organizations from which this agency receives "hot list" information;

Part C: Current ALPR sharing settings/configuration, STAC):

7. Records sufficient to show the current ALPR sharing configuration, including whether each partner listed in Part A has query/search access to this agency's ALPR data and whether access is full vs hit-only vs hotlist-only (screenshots or configuration export acceptable)

The requested documents will be made available to the general public, and this request is not being made for commercial purposes. I prefer to receive responsive records electronically via the request portal or email attachment. If any fees may apply, please provide an itemized estimate in advance.

These audit/search logs are required as part of ALPR operation under California Civil Code § 1798.90.52(a) and can help the public understand how often ALPR data is being queried and by whom. Similar records have been disclosed by multiple agencies in response to prior CPRA requests. If records responsive to any portion of this request are maintained by another department, division, or office, please identify the appropriate custodian and provide reasonable assistance in locating the records as required by Government Code §§ 7922.535 and 7922.600. If any portion of a responsive record is exempt, please redact only the exempt material and produce the remainder, consistent with

Government Code § 7922.525(b) (reasonably segregable portions must be disclosed).

For your convenience, I have compiled brief instructions on how these records can be seen here: https://drive.proton.me/urls/JFC930F0G4#BVewJLnWPNEr

If documents will be sent on a rolling basis, please do so in chronological order (ALPR audit logs first). Thank you. I look forward to your response within 10 calendar days.

EXHIBIT "3"

Detections Shared

The University of California Riverside Police Department (CA) Agency is Sharing its Detection data with the following Agencys:

81st Judicial District Attorneys Office TX	Abilene Police Department (TX)
Addison Police Department (TX)	Anaheim Police Department
Antioch Police Department CA	Arizona Department of Public Safety
ATF National Account	Baldwin County Sheriffs Office (AL)
Bellevue Police Department (NE)	Boulder City Police Department (NV)
Brea Police Department	Bridgeport Police Department (WV)
Buckeye Police Department (AZ)	Bureau of Indian Affairs
Burlington County Prosecutors Office (NJ)	Butte County Sheriffs Department (CA)
CAL FIRE	Calcasieu Parish Sheriffs Office
California Department of Fish And Wildlife (CA)	California Department Of Insurance (CA)
California Highway Patrol (CA)	Camden County Police Department
Cameron Parish Sheriffs Office (LA)	Camp Pendleton Provost Marshall Office
Canton Police Department (TX)	CBP - NTC
Ceres Police Department (CA)	Chenango County Sheriffs Office (NY)
Chico Police Department (CA)	Clanton Police Department (AL)
County of San Mateo Sheriffs Office	Coweta County Sheriffs Office
Crockett Police Department (TX)	Desoto Parish Sheriffs Office (LA)
Deuel County Sheriffs Department (NE)	District 21 Drug Task Force
Eagle County Sheriffs Office (CO)	East Carroll Parish Sheriffs Office (LA)
East Lampeter Township Police Department (PA)	El Cajon Police Department (CA)
El Dorado County Sheriff	El Segundo Police Department (CA)
Fairfax County Police - Criminal Intelligence Division (VA)	Fayette County Sheriffs Office (TX)
Fillmore County Sheriffs Office (NE)	Folsom Police Department

Fontana Police Department	Fresno County District Attorney (CA)
Fresno County Sheriffs Office (CA)	Fresno Police Department
Globe Police Department (AZ)	Gove County Sheriffs Office (KS)
Grants Pass Police Department	Grapevine Police Department (TX)
Gray County Sheriffs Office (TX)	Grayson County Sheriffs Office (TX)
Greenville Police Department (TX)	Gresham Police Department
Gulf Shores Police Department	Haskell County Sheriffs Department (KS)
HERNANDO POLICE DEPT (MS)	Hidalgo County Sheriff (TX)
Hobart Police Department (IN)	Hoover Police Department
Hot Springs Police Department (AR)	Houston Police Department (TX)
Huntington Park Police Department (CA)	Huntsville Police Department (AL)
Inactive CSU Fullerton Police Department	Inactive Federal Bureau of Investigation
Inactive Pearl River County Sheriffs Office	Inactive Tooele City Police Department (UT)
Inactive Trinidad Police Department (CO)	IRS Criminal Investigations
Jack County Sheriffs Office (TX)	Jackson Parish Sheriffs Office (LA)
Jefferson County Sheriffs Office	Johnson City Police Department (NY)
Kimble County Sheriffs Office (TX)	Kingman Police Department (AZ)
La Habra Police Department	La Mesa Police Department (CA)
La Paz County Sheriffs Office (AZ)	LA Port Police
Lacy-Lakeview Police Department (TX)	Lamar County Sheriffs Department (MS)
Livingston County Sheriffs Office (MI)	Livingston Parish Sheriffs Office (LA)
Llano County Sheriffs Office (TX)	Long Beach Police Department (CA)
Lorena Police Department (TX)	Lowndes County Sheriffs Office (MS)
Lubbock County South Plains Auto Theft Task Force (TX)	Madera County Sheriffs Department (CA)
Mansfield Police Department (TX)	Moab Police Department (UT)
Mobile County Sheriffs Office (AL)	Mono County Sheriffs Office (CA)

Morris County Sheriffs Office (KS)	Mount Carmel Township Police Department (PA)
Murrieta Police Department	Nacogdoches County Sheriffs Office (TX)
Nacogdoches Police Department	Napa Police Department (CA)
Natchitoches Parish Sheriffs Office (LA)	New York State Police
Newaygo County Sheriffs Office (MI)	Newton County Sheriffs Office (MS)
North Dakota Bureau of Criminal Investigation (ND)	Ontario Police Department
Ottawa Police Department (KS)	Oxnard Police Department
Palm Springs Police Department (CA)	Philadelphia Police - Major Crimes Auto Squad (PA)
Plymouth Township Police Department (MI)	Porter County Sheriff (IN)
Prescott Police Department (AZ)	Region VI Drug Task Force Eddy County (NM)
Richland Parish Sheriffs Office (LA)	Riverside County District Attorneys Office (CA)
Riverside County Sheriffs Department (CA)	Riverside Police Department
Sacramento Police Department	Saint Martin Parish Sheriffs Office (LA)
Salt Lake County Sheriffs Office (UT)	Sampson County Sheriff (NC)
San Bernardino County Fire Dept	San Bernardino County Sheriffs
San Bernardino Police Department	San Diego County District Attorney (CA)
San Luis Obispo Sheriffs Office	Sandoval County Sheriffs Office K9 Unit
Santa Ana Police Department	Santa Rosa County Sheriff (FL)
Schaumburg Police Department	Scott County Sheriffs Office (IA)
Seal Beach Police Department	Seguin Police Department (TX)
Seward County Sheriffs Office (NE)	Signal Hill Police Department
Simi Valley Police Department	Skokie Police Department
South Charleston Police Department (WV)	South Dakota Division of Criminal Investigation (SD)
South Dakota Highway Patrol (SD)	South Lake Tahoe Police Department (CA)
Spartanburg County Sheriffs Office (SC)	Springfield MO Police Department
St George Police Department (UT)	Summit County Sheriffs Office (UT)

Sunnyvale Public Safety Services (CA)	Tennessee Highway Patrol (TN)
Teton County Sheriffs Office	Texas Financial Crimes Intelligence (TX)
Tinley Park Police Department (IL)	Torrance Police Department
Town of Dillon (CO)	Travis County SO
Tri-Dent Task Force (IL)	Trussville Police Department
UC Irvine Police Department	Unified Police Of Greater Salt Lake (UT)
Upland Police Department (CA)	US Postal Inspection Service
Ventura County District Attorneys Office (CA)	Vermilion Parish Sheriffs Office (LA)
Village of Clearview Police Department (WV)	Washoe County Sheriffs Office
Wayne County Airport Police (MI)	West Covina Police Department
Wharton Police Department (NJ)	Wheeler County Sheriffs Office (TX)
Winters Police Department (CA)	Wisconsin DNR
Woodstock Police Department (GA)	Wylie Police Department (TX)
Yavapai-Apache Police Department (AZ)	

Detections Received

The University of California Riverside Police Department (CA) Agency is receiving Detection data from the following Agencys:

Agency	City	State
Grand Junction Police Department (CO)	Grand Junction	CO
Coweta County Sheriffs Office	Newnan	GA
Coral Springs Police Department	Coral Springs	FL
Galveston Auto Theft Task Force	Dickinson	TX
Riverside Police Department	Riverside	CA
Vigilant Solutions Sales	Chicago	IL
Skokie Police Department	Skokie	IL
Santa Ana Police Department	Santa Ana	CA
Orange County Sheriffs Department	Aliso Viejo	CA
Anaheim Police Department	Anaheim	CA
Orange Police Department	Orange	CA
Tustin Police Department	Tustin	CA
Westminster Police Department	Westminster	CA

Laguna Beach Police Department	Laguna Beach	CA
Kemah Police Department	Kemah	TX
Seal Beach Police Department	Seal Beach	CA
Brea Police Department	Brea	CA
UC Irvine Police Department	Irvine	CA
La Habra Police Department	La Habra	CA
Irvine Police Department (CA)	Irvine	CA
Newport Beach Police Department	Newport Beach	CA
Palm Beach County Sheriffs	West Palm Beach	FL
Frisco Police Department	Frisco	TX
Sacramento Police Department	Sacramento	CA
Corona Police Department	Corona	CA
Sikeston Police Department	Sikeston	MO
Springfield MO Police Department	Springfield	MO
Joplin Police Department	Joplin	MO
Carrollton Police Department (GA)	Carrollton	GA
Jefferson County Sheriffs Office	Birmingham	AL
Beachwood Police Department (OH)	Beachwood	OH
City of Reno	reno	NV
Washoe County Sheriffs Office	Reno	NV
Nassau County Police Department	Massapequa Park	NY
Des Peres Police Department	Des Peres	MO
Lewisville Police Department	Lewisville	TX
Allen Police Department	Allen	TX
Belle Meade Police Department (TN)	Nashville	TN
Lake City Police Department	Lake City	GA
El Paso Police Department	El Paso	TX
San Bernardino County Sheriffs	San Bernardino	CA
Houston Police Department (TX)	Houston	TX
Hoover Police Department	Hoover	AL
Polk County Sheriff	Winter Haven	FL
Orange County Sheriff (FL)	Orlando	FL
Ontario Police Department	Ontario	CA
White Bear Lake Police Department	White Bear Lake	MN
Emerson Police Department (GA)	Emerson	GA
Lee County Sheriffs Office	Ft Myers	FL

US Postal Inspection Service	Washington	DC
Peoria Police Department (IL)	Peoria	IL
Travis County SO	Austin	TX
Claremont Police Department (CA)	Claremont	CA
Riverside County District Attorneys Office (CA)	Riverside	CA
Chino Police Department	Chino	CA
Lodi Police Department	Lodi	CA
Lamar County Sheriffs Department (MS)	Purvis	MS
Kirkwood Police Department	Kirkwood	MO
Kane County Sheriffs Office	St Charles	IL
Long Beach Police Department (CA)	Long Beach	CA
Fontana Police Department	Fontana	CA
Woodstock Police Department (GA)	Woodstock	GA
Jackson County Sheriffs Office (MS)	Pascagoula	MS
Georgia State Patrol	Atlanta	GA
Farmers Branch Police Department	Farmers Branch	TX
El Dorado County Sheriff	Placerville	CA
Houston HIDTA	Houston	TX
Beaumont Police Department	Beaumont	CA
Orange Police Department (TX)	Orange	TX
Rankin County Sheriffs Office	Brandon	MS
San Diego Regional Auto Theft Task Force	San Diego	CA
LA Port Police	San Pedro	CA
Chula Vista Police Department	Chula Vista	CA
Jackson County Sheriffs Office (MO)	Lees Summit	MO
Morton Police Department	Morton	MS
Adel Police Department (GA)	Adel	GA
Munster Police Department	Munster	IN
Riverside County Sheriffs Department (CA)	Riverside	CA
Baldwin County Sheriffs Office (AL)	Fairhope	AL
Meridian Police Department	Meridian	MS
Monroe County Sheriff NY	Rochester	NY
New Castle County Police Department (DE)	New Castle	DE
Livermore Police Department	livermore	CA
Fresno County Sheriffs Office (CA)	Fresno	CA
New York State Police	Albany	NY

Darien Police Department IL	Darien	IL
West Covina Police Department	West Covina	CA
Kings County District Attorneys Office	Hanford	CA
Cincinnati Police Department (OH)	Cincinnati	OH
Folsom Police Department	Folsom	CA
Inactive Belvedere Police Department	Belvedere	CA
Hinsdale Police Department	Hinsdale	IL
Lansing Police Department (IL)	Lansing	IL
California Franchise Tax Board (CA)	West Covina	CA
San Bernardino Police Department	San Bernardino	CA
Simi Valley Police Department	Simi Valley	CA
Harris County District Attorneys Office (TX)	Houston	TX
Burr Ridge Police Department	Burr Ridge	IL
West Palm Beach Police Department	West Palm Beach	FL
Indianapolis Metropolitan Police Department (IN)	Indianapolis	IN
Burnet County TX Law Enforcement	Burnet	TX
Windcrest Police Department	Windcrest	TX
Port Arthur Police Department	Port Arthur	TX
Stanislaus County Auto Theft Task Force	Modesto	CA
Missouri State Highway Patrol (MO)	Jefferson City	MO
San Diego Sector Border Patrol (CA)	Chula Vista	CA
Kansas Highway Patrol (KS)	Salina	KS
Antioch Police Department CA	Antioch	CA
Oxnard Police Department	Oxnard	CA
Calumet City Police Department	Calumet City	IL
West Sacramento Police Department	West Sacramento	CA
Petaluma Police Department (CA)	Petaluma	CA
Fayette County Sheriffs Office (TX)	La Grange	TX
Iberville Parish Sheriffs Office (LA)	Maringouin	LA
ATF National Account	Washington	DC
Inactive Griffith Police Department (IN)	Griffith	IN
CA Parole Apprehension Team (CA)	Sacramento	CA
Monterey County Sheriffs Office	Salinas	CA
Kennesaw Police Department	Kennesaw	GA
Summit County Sheriffs Office (UT)	Park City	UT
Grundy County States Attorney Office	Morris	IL

Pittsburgh Police Bureau (PA)	Pittsburgh	PA
Grapevine Police Department (TX)	Grapevine	TX
Johns Creek Police Department	Johns Creek	GA
Grosse Pointe Park Public Safety	Grosse Pointe Park	MI
Franklin County Sheriffs Office (TX)	Mount Vernon	TX
Pearl River County Sheriffs Office	Poplarville	MS
Modesto Police Department (CA)	Modesto	CA
Wylie Police Department (TX)	Wylie	TX
Arizona Department of Public Safety	Phoenix	AZ
Dooly County Sheriffs Office	Pinehurst	GA
Highland Police Department	Highland	IN
24th Judicial District Drug Task Force	Camden	TN
Kansas City Police Department (KS)	Kansas City	KS
New York State Office of the Attorney General	New York	NY
Desoto Parish Sheriffs Office (LA)	Mansfield	LA
Greenville Police Department (TX)	Greenville	TX
Hemet Police Department (CA)	Hemet	CA
San Bernardino County District Attorneys Office (CA)	San Bernardino	CA
Hammond Police Department	Hammond	IN
Inactive Selma Police Department (TX)	Selma	TX
Redondo Beach Police Department	Redondo Beach	CA
Wichita Falls Police Department (TX)	Wichita Falls	TX
Brandon Police Department (MS)	Brandon	MS
Nacogdoches Police Department	Nacogdoches	TX
Carlsbad Police Department	Carlsbad	CA
Van Buren County Sheriff (MI)	Paw Paw	MI
Signal Hill Police Department	Signal Hill	CA
Carrollton Police Department TX	Carrollton	TX
Saraland Police Department	Saraland	AL
Rohnert Park Police Department CA	Rohnert Park	CA
La Mesa Police Department (CA)	La Mesa	CA
Inactive Linn County Sheriffs Office (IA)	Cedar Rapids	IA
Indiana HIDTA	Hobart	IN
Rockville Centre Police Department	Rockville Center	NY
District 21 Drug Task Force	Norman	OK
Redlands Police Department (CA)	Redlands	CA

Grants Pass Police Department	Grants Pass	OR
Paradise Valley Police Department	Paradise Valley	AZ
Camden County Police Department	Camden	NJ
Pomona Police Department	Pomona	CA
Tallapoosa Police Department	Tallapoosa	GA
Smith County Sheriff Office	Tyler	TX
Burleson Police Department	Burleson	TX
Denton County Sheriff Office	Denton	TX
Reeve County Sherriffs Office	Pecos	TX
ICE ERO	Washington	DC
Wayne County Airport Police (MI)	Detroit	MI
Brentwood Police Department (TN)	Brentwood	TN
Hartford Police Department	Hartford	CT
Inactive Newington Police Department	Newington	CT
CAL FIRE	Sacramento	CA
South Windsor Police Department	South Windosr	CT
Louisiana State Police (LA)	Baton Rouge	LA
Calhoun County Sheriffs Office (AL)	Anniston	AL
Glendale Police Department (CA)	Glendale	CA
Gresham Police Department	Gresham	OR
Oklahoma Bureau of Narcotics (OK)	Oklahoma City	OK
Santa Monica Police Department (CA)	Santa Monica	CA
Nichols Hills Police Department	Nichols Hills	OK
Texas Attorney General (TX)	Austin	TX
Mississippi Department of Public Safety (MS)	Jackson	MS
Escondido Police Department	ESCONDIDO	CA
Upland Police Department (CA)	Upland	CA
Oceanside Police Department (CA)	Oceanside	CA
Inglewood Police Department (CA)	Inglewood	CA
Eastchester Police Department	Eastchester	NY
Flagler County Sheriffs Office	Bunnell	FL
Whiting Police Department	Whiting	IN
McEwen Police Department	McEwen	TN
Mississippi Bureau of Narcotics (MS)	Byram	MS
Knox County Sheriff (TN)	Knoxville	TN
Knoxville Police Department (TN)	Knoxville	TN

Biloxi Police Department (MS)	Biloxi	MS
Addison Police Department (TX)	Addison	TX
Genesee County Sheriffs Department (MI)	Flint	MI
Campbell Police Department (CA)	Campbell	CA
Chenango County Sheriffs Office (NY)	Norwich	NY
California Department of Fish And Wildlife (CA)	Sacramento	CA
Duncanville Police Department (TX)	Duncanville	TX
Harper Woods Police Department (MI)	Harper Woods	MI
Hays County Sheriffs Office (TX)	San Marcos	TX
Bergen County (NJ)	Paramus	NJ
Buckeye Police Department (AZ)	Buckeye	AZ
Chico Police Department (CA)	Chico	CA
Evesham Township Police Department (NJ)	Marlton	NJ
Huntington Park Police Department (CA)	Huntington Park	CA
Ocean County Prosecutors Office (NJ)	Toms River	NJ
Passaic County Prosecutors Office (NJ)	Totowa	NJ
Paterson Police Department (NJ)	Paterson	NJ
Vacaville Police Department (CA)	Vacaville	CA
West Orange Police Department (NJ)	West Orange	NJ
Wise County Sheriffs Office (TX)	Decatur	TX
South Orange Police Department (NJ)	South Orange	NJ
Wharton County Sheriffs Office TX	Wharton	TX
Yuma County Sheriffs Office (AZ)	Yuma	AZ
Eureka Police Department MO	Eureka	MO
Shelby County Sheriffs Office AL	Columbiana	AL
New Hampshire State Police (NH)	Concord	NH
Livingston Police Department (NJ)	Livingston	NJ
Cedar Park Police Department (TX)	Cedar Park	TX
Bureau of Indian Affairs	Albuquerque	NM
Livingston County Sheriffs Office (MI)	Howell	MI
San Luis Obispo Police Department (CA)	San Luis Obispo	CA
Scott County Sheriffs Office (IA)	Davenport	IA
Hidalgo County Sheriff (TX)	Edinburg	TX
University of Oklahoma Police Department (OK)	Norman	OK
Altoona Police Department (IA)	Altoona	IA
Alpharetta Police Department (GA)	Alpharetta	GA

Wayne County Sheriffs (IN)	Richmond	IN
Omaha Police Department (NE)	Omaha	NE
McLennan County Sheriff Department (TX)	Waco	TX
Madison Police Department (MS)	Madison	MS
University Of Central Florida Police Department	Orlando	FL
North Port FL PD	North Port	FL
Miramar Police Department (FL)	Miramar	FL
Wilton Manors Police Department	Wilton Manors	FL
City of Doral	Doral	FL
Leon County Sheriffs Office FL	Tallahassee	FL
Highlands County Sheriffs Office	Sebring	FL
Village Of Pinecrest Police Department (FL)	Pine Crest	FL
Martin County Sheriffs Office	Stuart	FL
Brevard County Sheriffs Office	Titusville	FL
Lee County Port Authority	Fort Meyers	FL
El Segundo Police Department (CA)	El Segundo	CA
Norman Police Department (OK)	Norman	OK
Marana Police Department (AZ)	Marana	AZ
Danbury Police Department (CT)	Danbury	CT
Palm Springs Police Department (CA)	Palm Springs	CA
Nacogdoches County Sheriffs Office (TX)	Nacogdoches	TX
Tucson Police Department (AZ)	Tucson	AZ
Flowood Police Department (MS)	Flowood	MS
Douglas County Sheriff (NV)	Minden	NV
Santa Rosa County Sheriff (FL)	Milton	FL
Gillespie County Sheriffs Office (TX)	Fredericksburg	TX
Hollister Police Department (CA)	Hollister	CA
San Diego Harbor Police Department (CA)	San Diego	CA
El Cajon Police Department (CA)	El Cajon	CA
La Paz County Sheriffs Office (AZ)	Parker	AZ
Plymouth Township Police Department (MI)	Plymouth	MI
Prescott Police Department (AZ)	Prescott	AZ
Battle Creek Police Department (MI)	Battle Creek	MI
McCook Police Department (IL)	McCook	IL
Orlando Police Department (FL)	Orlando	FL
Ellis County Sheriffs Office (TX)	Waxahachie	TX

Pflugerville Police Department (TX)	Pflugerville	TX
Utah County Sheriffs Office (UT)	Spanish Fork	UT
National City Police Department (CA)	National City	CA
Wharton Police Department (NJ)	Wharton	NJ
South Barrington Police Department (IL)	South Barrington	IL
Huntsville Police Department (AL)	Huntsville	AL
Clarksville Police Department (TN)	Clarksville	TN
Davie Police Department (FL)	Davie	FL
East Baton Rouge Sheriffs Office (LA)	Baton Rouge	LA
Columbia County Sheriffs (GA)	Appling	GA
Pinole Police Department (CA)	Pinole	CA
Fort Mohave Tribal Police Department (AZ)	Mohave Valley	AZ
West Des Moines Police Department (IA)	West Des Moines	IA
Ventura County District Attorneys Office (CA)	Ventura	CA
Elizabeth Police Department (NJ)	Elizabeth	NJ
Pueblo of Pojoaque Tribal Police Department (NM)	Santa Fe	NM
Haskell County Sheriffs Department (KS)	Sublette	KS
Abilene Police Department (TX)	Abilene	TX
St George Police Department (UT)	St George	UT
Crockett County Sheriffs Office (TX)	Ozona	TX
Hillsborough Police Department (CA)	Hillsborough	CA
Beatrice Police Department (NE)	Beatrice	NE
Three Affiliated Tribes MHA Nation LES (ND)	New Town	ND
Jefferson Davis Parish Sheriffs Office (LA)	Jennings	LA
Papillion Police Department (NE)	Papillion	NE
West Fargo Police Department (ND)	West Fargo	ND
Seward County Sheriffs Office (NE)	Seward	NE
Mesa County Sheriffs Office (CO)	Grand Junction	CO
Mono County Sheriffs Office (CA)	Bridgeport	CA
Scotts Bluff County Sheriffs Office (NE)	Gering	NE
Alhambra Police Department (CA)	Alhambra	CA
San Leandro Police Department (CA)	San Leandro	CA
Sunnyvale Public Safety Services (CA)	Sunnyvale	CA
Natchitoches Parish Sheriffs Office (LA)	Natchitoches	LA
Caddo Parish Sheriffs Office (LA)	Shreveport	LA
Winters Police Department (CA)	Winters	CA

Anderson Police Department (CA)	Anderson	CA
Franklin Parish Sheriffs Office (LA)	Winnsboro	LA
Plumstead Township Police Department (PA)	Pipersville	PA
Rapides Parish Sheriffs Office (LA)	Alexandria	LA
La Vista Police Department (NE)	La Vista	NE
Waller County Sheriffs Office (TX)	Hempstead	TX
Hernando County Sheriffs Office (FL)	Brooksville	FL
Escambia County Sheriffs Office (FL)	Pensacola	FL
Pharr Police Department (TX)	Pharr	TX
Chattanooga Police Department (TN)	Chattanooga	TN
Lubbock County South Plains Auto Theft Task Force (TX)	Lubbock	TX
Richland Parish Sheriffs Office (LA)	Rayville	LA
East Carroll Parish Sheriffs Office (LA)	Lake Providence	LA
Tuscaloosa Police Department (AL)	Tuscaloosa	AL
Tensas Parish Sheriffs Office (LA)	Saint Joseph	LA
Grayson County Sheriffs Office (TX)	Sherman	TX
North Brunswick Police Department (NJ)	North Brunswich Township	NJ
Caldwell Parish Sheriffs Office (LA)	Columbia	LA
Jackson Parish Sheriffs Office (LA)	Jonesboro	LA
Grand River Dam Authority Police Department (OK)	Shouteau	OK
Harlingen Police Department (TX)	Harlingen	TX
Beloit Police Department (WI)	Beloit	WI
Canadian County Sheriffs Office (OK)	El Reno	OK
Baltimore County Police Department (MD)	Towson	MD
Dallas Fort Worth Intl Airport Public Safety (TX)	Dallas	TX
Hamilton County Sheriffs Office (TN)	Chattanooga	TN
Durant Police Department (OK)	Durant	OK
Milam County Sheriffs Office (TX)	Cameron	TX
Spartanburg County Sheriffs Office (SC)	Spartanburg	SC
Deuel County Sheriffs Department (NE)	Chappell	NE
Wichita County Sheriffs Office (TX)	Wichita Falls	TX
Miami Police Department - POC	Miami	FL
Lake City Police Department (FL)	Lake City	FL
Hot Springs Police Department (AR)	Hot Springs	AR
Idaho Falls Police Department (ID)	Idaho Falls	ID

Azle Police Department (TX)	Azle	TX
Oklahoma State Bureau of Investigation (OK)	Oklahoma City	OK
Toms River Police Department (NJ)	Toms River	NJ
Rockland County Sheriffs Office (NY)	New City	NY
Imperial County District Attorney (CA)	El Centro	CA
Cleveland Police Department (TN)	Cleveland	TN
Ottawa Police Department (KS)	Ottawa	KS
Newton County Sheriffs Office (MS)	Decatur	MS
Hillside Police Department (IL)	Hillside	IL
West Valley City Police Department (UT)	West Valley City	UT
Arizona Attorney General (AZ)	Phoenix	AZ
Surprise Police Department (AZ)	Surprise	AZ
Gulf Shores Police Department	Gulf Shores	AL
Lehi Police Department (UT)	Lehi	UT
Florida Fish and Wildlife Conservation Commission (FL)	Tallahassee	FL
Vermilion Parish Sheriffs Office (LA)	Abbeville	LA
Pineville Police Department (LA)	Pineville	LA
Mills County Sheriffs Office (TX)	Goldthwaite	TX
Waverly Police Department (TN)	Waverly	TN
Aransas County Sheriffs Office (TX)	Rockport	TX
Alexandria Police Department (LA)	Alexandria	LA
Boulder City Police Department (NV)	Boulder City	NV
Humboldt County Sheriffs Office (CA)	Eureka	CA
Bellevue Police Department (NE)	Bellevue	NE
Yavapai-Apache Police Department (AZ)	Camp Verde	AZ
Port Washington Police Department (NY)	Port Washington	NY
McAllen Police Department (TX)	McAllen	TX
Clanton Police Department (AL)	Clanton	AL
Louisville Airport Authority (KY)	Louisville	KY
Lowndes County Sheriffs Office (MS)	Columbus	MS
Many Police Department (LA)	Many	LA
Sabine Parish Sheriffs Office (LA)	Many	LA
Bienville Parish Sheriffs Office (LA)	Arcadia	LA
Brownsburg Police Department (IN)	Brownsburg	IN
Woodworth Police Department (LA)	Woodworth	LA
Webster Parish Sheriff Office (LA)	Minden	LA

Sycuan Tribal Police Department (CA)	El Cajon	CA
Taylorsville Police Department (UT)	Taylorsville	UT
East Lampeter Township Police Department (PA)	Lancaster	PA
Grinnell Police Department (IA)	Grinnell	IA
South Texas Task Force (TX)	Kingsville	TX
Fort Wayne Police Department (IN)	Fort Wayne	IN
Sycamore Police Department (IL)	Sycamore	IL
Jonesboro Police Department (AR)	Jonesboro	AR
South Dakota Game Fish And Parks	Pierre	SD
Nephi Police Department (UT)	Nephi	UT
Canton Police Department (TX)	Canton	TX
Mount Carmel Township Police Department (PA)	Atlas	PA
Stater Bros Markets (CA)	N/A	N/A
Cameron Parish Sheriffs Office (LA)	Cameron	LA
Eagle Pass Police Department (TX)	Eagle Pass	TX
AZ HIDTA Investigation Support Center	Tucson	AZ
Polk County Sheriffs Office (TX)	Livingston	TX
Soddy Daisy Police Department (TN)	Soddy Daisy	TN
McKinney Police Department (TX)	McKinney	TX
Brenham Police Department (TX)	Brenham	TX
IRS Criminal Investigations	San Diego	CA
North Salt Lake City Police Department (UT)	North Salt Lake	UT
West Jordan Police Department (UT)	West Jordan	UT
Texas Financial Crimes Intelligence (TX)	Tyler	TX
Livingston Parish Sheriffs Office (LA)	Livingston	LA
Nogales Police Department (AZ)	Nogales	AZ
Reagan County Sheriffs Office (TX)	Big Lake	TX
Marinette Police Department (WI)	Marinette	WI
Tevare HOA (NV)	N/A	N/A
Wyoming County Sheriff (WV)	Pineville	WV
Columbus Police Department (MS)	Columbus	MS
Cabarrus County Sheriffs Office (NC)	Concord	NC
Freeport Police Department (IL)	Freeport	IL
North Caldwell Police (NJ)	North Caldwell	NJ
Stephenson County Sheriff (IL)	Freeport	IL
Grandview Police Department (MO)	Grandview	MO

Sampson County Sheriff (NC)	Clinton	NC
Philadelphia Police - Major Crimes Auto Squad (PA)	Philadelphia	PA
Pitkin County Sheriff (CO)	Aspen	CO
Fresno County District Attorney (CA)	Fresno	CA
Gonzales County Sheriffs Office (TX)	Gonzales	TX
Crockett Police Department (TX)	Crockett	TX
Smyrna Police Department (DE)	Smyrna	DE
Inactive Houston Arson Bureau (TX)	Houston	TX
Granbury Police Department (TX)	Granbury	TX
Jasper County Sheriffs Office (IN)	Renesselear	IN
Department Of Cannabis Control California (CA)	Rancho Cordova	CA
Wallkill Police Department (NY)	Middletown	NY
Madison County Sheriff (ID)	Rexburg	ID
Jersey Village Police Department (TX)	Jersey Village	TX
Kimble County Sheriffs Office (TX)	Junction	TX
Inactive Shiner Police Department (TX)	Shiner	TX
Winfield Police Department (IN)	Winfield	IN
Ogle County Sheriffs Office	Oregon	IL
Newaygo County Sheriffs Office (MI)	White Cloud	MI
Hobart Police Department (IN)	Hobart	IN
Hill County Sheriffs Office (TX)	Hillsboro	TX
Middletown Police Department (DE)	Middletown	DE
Lathrop Police Department (CA)	Lathrop	CA
Osage County Sheriff (KS)	Lyndon	KS
Forest Service USDA	Vallejo	CA
Comanche Police Department (TX)	Comanche	TX
Seymour Police Department (CT)	Seymour	CT
Globe Police Department (AZ)	Globe	AZ
Zachary Police Department (LA)	Zachary	LA
Edwards County Sheriffs Office (TX)	Rocksprings	TX
Menard County Sheriffs Office (TX)	Menard	TX
Northwest Regional Police Department (PA)	Elizabethtown	PA
Bryan County Sheriffs Office (GA)	Pembroke	GA
Murfreesboro Police Department (TN)	Murfreesboro	TN
East Feliciana Parish Sheriffs Office (LA)	Clinton	LA
Middle Tennessee State University Police Department (TN)	Murfreesboro	TN

San Miguel County Sheriffs Department (CO)	Telluride	CO
Sandy City Police Department (UT)	Sandy	UT
Woodcliff Lake Police (NJ)	Woodcliff Lake	NJ
Ohio Workers Compensation Bureau (OH)	Columbus	OH
Johnson City Police Department (TN)	Johnson City	TN
Ocean City Police Department (NJ)	Ocean City	NJ
Pocono Mountain Regional Police Department (PA)	Pocono Summit	PA
Bates County Sheriffs Office (MO)	Butler	MO
South Charleston Police Department (WV)	South Charleston	WV
Inactive Brantley Police Department (AL)	Brantley	AL
Hammond Police Department (LA)	Hammond	LA
Bellefonte Police Department (PA)	Bellefonte	PA
Maywood Police Department (IL)	Maywood	IL
Putnam County Sheriffs Office (TN)	Cookeville	TN
Lorena Police Department (TX)	Lorena	TX
Stony Creek Township Police Department (PA)	Johnstown	PA
Corpus Christi Police Department (TX)	Corpus Christi	TX
Lehigh County Regional Intelligence and Investigation Cent	Allentown	PA
Clearfield Police Department (UT)	Clearfield	UT
Clear Lake Shores (TX)	Clear Lake Shores	TX
Rio Blanco County Sheriffs Office (CO)	Meeker	CO
Cherokee County Sheriffs Office (TX)	Rusk	TX
West Chester Police Department (OH)	West Chester Township	OH
Tri-Dent Task Force (IL)	Oglesby	IL
Van Alstyne Police Department (TX)	Van Alstyne	TX
Inactive Prospect Heights Police Department (IL)	Prospects Heights	IL
South Dakota Division of Criminal Investigation (SD)	Pierre	SD
State Center Police Department (IA)	State Center	IA
JW Marriott Resort Palm Desert (CA)	N/A	N/A
Prairie Du Chien Police Department (WI)	Prairie Du Chien	WI
Clinton County Sheriffs Office (IN)	Frankfort	IN
Miami Police Department (OK)	Miami	OK
Franklin Police Department (TN)	Franklin	TN
Wills Point Police Department (TX)	Wills Point	TX
Calhoun County Sheriffs Office (MI)	Marshall	MI

Dickson County Sheriffs Office (TN)	Charlotte	TN
South Beloit Police Department (IL)	South Beloit	IL
Dodge County Sheriffs Office (WI)	Juneau	WI
Potosi Police Department (MO)	Potosi	MO
Wyoming County Sheriffs Office (NY)	Warsaw	NY
Murray Police Department (UT)	Murray	UT
Jackson Township Police Department (Luzerne County) (PA)	Shavertown	PA
Fredericksburg Police Department (TX)	Fredericksburg	TX
Seligman City Police Department (MO)	Seligman	MO
Brownsville Police Department (TX)	Brownsville	TX
Montgomery Police Department (IL)	Montgomery	IL
Jack County Sheriffs Office (TX)	Jacksboro	TX
South Jordan Police Department (UT)	South Jordan	UT
California Department of Motor Vehicles (CA)	Sacramento	CA
Chippewa County Sheriffs Office (MI)	Sault Ste Marie	MI
Windber Borough Police Department (PA)	Windber	PA
Sewickley Heights Borough Police Department (PA)	Sewickley	PA
Menominee Police Dept (MI)	Menominee	MI
Salt Lake County Sheriffs Office (UT)	Salt Lake City	UT
East Hempfield Township Police Department (PA)	Landisville	PA
Unified Police Of Greater Salt Lake (UT)	Salt Lake City	UT
Alexandria Police Department (IN)	Alexandria	IN
Town of Dillon (CO)	Dillon	CO
Beachwood Police Department (NJ)	Beachwood	NJ
South Toms River Police Department (NJ)	South Toms River	NJ
Manchester Township Police Department (NJ)	Manchester	NJ
Barnegat Police Department (NJ)	Barnegat	NJ
Pismo Beach Police Department (CA)	Pismo Beach	CA
Beauregard Parish Sheriffs Office (LA)	DeRidder	LA
Bay Head Police Department (NJ)	Bay Head	NJ
Glassport Borough Police (PA)	Glassport	PA
University Of North Texas (TX)	Denton	TX
Point Pleasant Borough Police Department (NJ)	Point Pleasant	NJ
Rock County Sheriffs Department (WI)	Janesville	WI
La Joya Police Department (TX)	La Joya	TX
Ward County Sheriffs Department (ND)	Minot	ND

Springdale Borough Police Department (PA)	Springdale	PA
Deephaven Police Department (MN)	Deephaven	MN
Churchill County Sheriffs Office (NV)	Fallon	NV
Girard Borough Police Department (PA)	Girard	PA
Alto Police Department (GA)	Alto	GA
Williston Police Department (ND)	Williston	ND
Iowa County Sheriffs Office (WI)	Dodgeville	WI
Coal City Police Department (IL)	Coal City	IL
Fox Chapel Borough Police Department (PA)	Pittsburgh	PA
Kerr County Sheriffs Office (TX)	Kerrville	TX
Longview Police Department (TX)	Longview	TX
Maui County Police Department (HI)	Wailuku	HI
University of South Carolina (SC)	Columbia	SC
Hancock County Sheriffs Office (MS)	Bay St Louis	MS
University of Central Missouri (MO)	Warrensburg	MO
Bethlehem Police Department (PA)	Bethlehem	PA
St Charles Police Department (IL)	St Charles	IL
Deridder Police Department	Deridder	LA
Livingston Police Department (IL)	Livingston	IL
Piatt County Sheriffs Office (IL)	Monticello	IL
Inactive Monee Police Department (IL)	Monee	IL
Inactive Willowbrook Police Department (IL)	Willowbrook	IL
Cottonwood Heights Police Department (UT)	Cottonwood Heights	UT
North Dakota Bureau of Criminal Investigation (ND)	Bismarck	ND
Laredo Police Department (TX)	Laredo	TX
Eastern Pike Regional Police Department (PA)	Matamoras	PA
Inactive Lake Forest Police Department (IL)	Lake Forest	IL
Trinity County Sheriffs Office (TX)	Groveton	TX
Star City Police Department (WV)	Star CIty	WV
Greenfield Township (PA)	Claysburg	PA
Grand County Sheriffs Department (UT)	Moab	UT
Howell County Sheriffs Office (MO)	West Plains	MO
Crafton Borough Police Department (PA)	Pittsburgh	PA
Mission Police Department (TX)	Mission	TX
Mount Vernon Police Department (NY)	Mount Vernon	NY
Eagle County Sheriffs Office (CO)	Eagle	CO

California State Lottery (CA)	Sacramento	CA
Union City Police Department (PA)	Union City	PA
New Braunfels Police Department (TX)	New Braunfels	TX
Inactive DuPage County Sheriffs Department (IL)	Wheaton	IL
Ardmore Police Department (OK)	Ardmore	OK
Presidio Police Department (TX)	Presidio	TX
Inactive Stinesville Police Department (IN)	Stinesville	IN
Manlius Police Department (NY)	Manlius	NY
Gove County Sheriffs Office (KS)	Gove City	KS
Manasquan Police Department (NJ)	Manasquan	NJ
Medina County Sheriffs Office (TX)	Hondo	TX
Oak Ridge North Police Department (TX)	Oak Ridge North	TX
Kingman Police Department (AZ)	Kingman	AZ
Winnebago Police Department (IL)	Winnebago	IL
Rocky Mount Police Department (VA)	Rocky Mount	VA
Buffalo County Sheriffs Office (NE)	Kearney	NE
Garvin County Sheriffs Office (OK)	Pauls Valley	OK
Williamsport Bureau of Police (PA)	Williamsport	PA
Mackinac County Sheriffs Office (MI)	St Ignace	MI
Big Spring Police Department (TX)	Big Spring	TX
University of Wisconsin Madison (WI)	Madison	WI
Mosheim Police Department (TN)	Mosheim	TN
Houma Terrebonne Airport Commission (LA)	Houma	LA
Upper Darby Township Police Department (PA)	Upper Darby	PA
Columbia Police Department (MS)	Columbia	MS
Dallas County Sheriffs Office (IA)	Adel	IA
Bayfield County Sheriffs Office (WI)	Washburn	WI
Holly Springs Police Department (NC)	Holly Springs	NC
Sunset Valley Police Department (TX)	Sunset Valley	TX
Park City Police Department (UT)	Park City	UT
South Dakota Highway Patrol (SD)	Pierre	SD
Richmond Police Department (IN)	Richmond	IN
Chippewa Twp Emergency Management (PA)	Beaver Falls	PA
Alabaster Police Department (AL)	Alabaster	AL
The Village Police Department (OK)	The Village	OK
Harrison County Sheriffs Office (MS)	Gulfport	MS

Hidalgo County Constable Prt 4	Mission	TX
Donna Police Department (TX)	Donna	TX
Kearney Police Department (NE)	Kearney	NE
Divide County Sheriffs Department (ND)	Crosby	ND
Upper Pottsgrove Police Department (PA)	Pottstown	PA
Victoria Police Department ATTF (TX)	Victoria	TX
Inactive Kenosha Police Department (WI)	Kenosha	WI
Woodville Police Department (TX)	Woodville	TX
Buffalo County Sheriffs Office (WI)	Alma	WI
Ozark Police Department (MO)	Ozark	MO
Muhlenberg Police Department (PA)	Reading	PA
Millcreek Township Police (PA)	Erie	PA
Elkhorn Police Department (WI)	Elkhorn	WI
White County Sheriffs Office (TN)	Sparta	TN
Plattsburgh Police Department (NY)	Plattsburgh	NY
Rosemont Public Safety Department (IL)	Rosemont	IL
Kennedy Township Police Department (PA)	Coraopolis	PA
Sandy Township Police Department (PA)	DuBois	PA
Wayne County Sheriffs Office (NY)	Lyons	NY
Burlington Township PD (NJ)	Burlington	NJ
Morgantown Police Department (WV)	Morgantown	WV
Palmview Police Department (TX)	Palmview	TX
Griswold Real Estate Management Inc (NV)	N/A	N/A
Reno Tahoe Airport Police Department	Reno	NV
Harrison County Sheriffs Office (TX)	Marshall	TX
Lewisburg Police Department (TN)	Lewisburg	TN
Campbell County Sheriffs Office (TN)	Jacksboro	TN
Red Oak Police Department (TX)	Red Oak	TX
Inactive Clarendon County Sheriffs Office (SC)	Manning	SC
Ohio State Highway Patrol (OH)	Columbus	OH
Garrison Police Department (TX)	Garrison	TX
North Texas Sheriffs Criminal Interdiction Unit	McKinney	TX
Inactive Palos Park Police Department (IL)	Palos Park	IL
Inactive Loup County Sheriffs Office (NE)	Taylor	NE
Arroyo Grande Police Department-CA	Arroyo Grande	CA
Bainbridge Police Department (GA)	Bainbridge	GA

Inactive Janesville Police Department (IA)	Janesville	IA
Nebraska State Patrol (NE)	Lincoln	NE
Franklin County Sheriffs Office (TN)	Winchester	TN
McKenzie County Sheriffs Office (ND)	Watford City	ND
Nevada DMV Compliance Enforcement (NV)	Carson City	NV
Cambria Township Police (PA)	Ebensburg	PA
Cleona Borough Police Department (PA)	Cleona	PA
Henry Police Department (TN)	Henry	TN
Pottawatomie County Sheriffs Office (OK)	Shawnee	OK
Cresson Borough Police Department (PA)	Cresson	PA
Dyersburg Police Department (TN)	Dyersburg	TN
Red Bank Police Department (TN)	Red Bank	TN
Comal County Constable Pct 3 (TX)	New Braunfels	TX
Tennessee District Attorneys General Conference (TN)	Nashville	TN
Morris County Sheriffs Office (KS)	Council Grove	KS
Littlestown Police Department (PA)	Littlestown	PA
The Dalles Police Department (OR)	The Dalles	OR
Whitehall Borough Police Department (PA)	Pittsburgh	PA
Dodgeville Police Department (WI)	Dodgeville	WI
Lincoln Police Department (ND)	Lincoln	ND
Bristol Police Department (TN)	Bristol	TN
Lewistown Police Department (PA)	Lewistown	PA
Marshalltown Police Dept (IA)	Marshalltown	IA
Westfield Police Dept (MA)	Westfield	MA
Frackville Borough Police Department (PA)	Frackville	PA
Lamb County Sheriffs Department (TX)	Littlefield	TX
Royse City Police Department (TX)	Royse City	TX
Mauldin Police Department (SC)	Mauldin	SC
Mattapoisett Police Department (MA)	Mattapoisett	MA
Valley Falls Police Department (KS)	Valley Falls	KS
Inactive Labette County Sheriffs Office (KS)	Oswego	KS
Gregg County Sheriffs Office (TX)	Longview	TX
Morgan County UT	Morgan	UT
East Texas Anti-Gang Center (TX)	Tyler	TX
Schulenburg Police Department (TX)	Schulenburg	TX
Grand Valley State University PD (MI)	Allendale	MI

Inactive Winthrop Police Department (MA)	Winthrop	MA
Inactive Revere Police Department (MA)	Revere	MA
Teton County Sheriffs Office	Driggs	ID
HERNANDO POLICE DEPT (MS)	Hernando	MS
Freeport Police Department (ME)	Freeport	ME
BROWN COUNTY SHERIFFS OFFICE (MN)	New Ulm	MN
Gray County Sheriffs Office (TX)	Pampa	TX
Hardeman County Sheriffs Office (TN)	Bolivar	TN
Seguin Police Department (TX)	Seguin	TX
Saint Martin Parish Sheriffs Office (LA)	Saint Martinville	LA
Gonzales Police Department (TX)	Gonzales	TX
Inactive Guthrie County Sheriffs Office (IA)	Guthrie Center	IA
Torrance Police Department (CA)	N/A	N/A
Franklin County Sheriffs Office (VA)	Rocky Mount	VA
Bee County Sheriffs Office (TX)	Beeville	TX
Grosse Pointe Woods Department of Public Safety (MI)	Grosse Pointe Woods	MI
Grosse Pointe City Department of Public Safety (MI)	Grosse Pointe City	MI
Grosse Pointe Farms Department of Public Safety (MI)	Grosse Pointe Farms	MI
Arkansas County Sheriffs Office (AR)	Stuttgart	AR
Seneca County Sheriff (NY)	Romulus	NY
Inactive Outagamie County Sheriffs Office (WI)	Appleton	WI
Eastland County Sheriffs Office (TX)	Eastland	TX
Monroe County Sheriff (IL)	Waterloo	IL
Village of Maple Bluff Police Department (WI)	Madison	WI
Page Police Department (AZ)	Page	AZ
Brigham City Police Department (UT)	Brigham City	UT
Barton County Sheriffs Office (KS)	Great Bend	KS
Amory Police Department (MS)	Amory	MS
Inactive Trinidad Police Department (CO)	Trinidad	CO
Monroeville Police Department (PA)	Monroeville	PA
Urbandale Police Department (IA)	Urbandale	IA
Carroll Police Department (IA)	Carroll	IA
Angelo State University Police Department (TX)	San Angelo	TX
81st Judicial District Attorneys Office TX	Floresville	TX
Franklin County Sheriffs Office (KY)	Frankfort	KY
25th Judicial Drug Task Force (TN)	Ripley	TN

Monroe County Sheriffs Office (MS)	Aberdeen	MS
Union City Police Department (TN)	Union City	TN
Moab Police Department (UT)	Moab	UT
Terrell County Sheriffs Office (TX)	Terrell	TX
Lawrenceburg Police Department (TN)	Lawrenceburg	TN
Rockdale Police Department (TX)	Rockdale	TX
Mount Vernon Police Department (TX)	Mount Vernon	TX
Ada County Sheriffs Office (ID)	Boise	ID
Hoosick Falls Village Police Department (NY)	Hoosick Falls	NY
Bryan County Sheriffs Office (OK)	Durant	OK
Elm Ridge Police Department (TX)	Savannah	TX
Shoshoni Police Department (WY)	Shoshoni	WY
Ohio HIDTA	Cleveland	OH
Essex County Sheriffs Office (VA)	Tappahannock	VA
Rhea County Sheriffs Office (TN)	Dayton	TN
Inactive Joliet Police Department (IL)	Joliet	IL
Hurricane City Police Department (UT)	Hurricane	UT
Coffee County Sheriffs Office (AL)	New Brockton	AL
Greenwood County Sheriffs Office (SC)	Greenwood	SC
Shenandoah Police Department (PA)	Shenandoah	PA
Llano County Sheriffs Office (TX)	LLANO	TX
Brighton Township Police Department (PA)	Beaver	PA
Terrell Hills Police Department (TX)	San Antonio	TX
West Deer Township Police (PA)	Cheswick	PA
Hummelstown Police Department (PA)	Hummelstown	PA
Tooele County Sheriffs Department (UT)	Tooele	UT
Lampasas Police Department (TX)	Lampasas	TX
Kendall County Sheriffs Office (TX)	Boerne	TX
Inactive Flagstaff Police Department (AZ)	Flagstaff	AZ
Washington Parish Sheriffs Office (LA)	Franklinton	LA
Brighton Police Department (NY)	Rochester	NY
Motorola Solutions_VME	N/A	N/A
Hutchins Police Department (TX)	Hutchins	TX
Grand Saline Police Department (TX)	Grand Saline	TX
Los Lunas Police Department (NM)	Los Lunas	NM
North Woodbury Twp Police (PA)	Martinsburg	PA

Sandoval County Sheriffs Office K9 Unit	Bernalillo	NM
Inactive Milwaukie Police Department (OR)	Milwaukie	OR
Onondaga County Sheriffs Office (NY)	Syracuse	NY
Porter County Sheriff (IN)	Valparaiso	IN
Jefferson Hills Police Dept (PA)	Jefferson Hills	PA
Auburn Police Department (MA)	Auburn	MA
Williams County Sheriffs Office	Williston	ND
Kilgore Police Department	Kilgore	TX
Ashland City Police Department (TN)	233 Tennessee Waltz Parkway	TN
Yankton Police Department (SD)	Yankton	SD
BROWN COUNTY SHERIFFS DEPARTMENT (IL)	Mount Sterling	IL
Greensburg Police Department City of (PA)	Greensburg	PA
Kent County Sheriffs Office (TX)	Jayton	TX
Selbyville Police Department (DE)	Selbyville	DE
Williamson County Sheriffs Office (TN)	Franklin	TN
Findlay Township Police Department (PA)	Clinton	PA
Marysville Police Department (KS)	Marysville	KS
McMinn County Sheriffs Office (TN)	Athens	TN
Round Lake Beach Police Department (IL)	Round Lake Beach	IL
Greenwood County Sheriffs Office (KS)	Eureka	KS
Alger County Sheriffs Office (MI)	Munising	MI
Clyde Police Department (NY)	Clyde	NY
Jefferson County Sheriffs Office (WV)	Kearneysville	WV
Manchester Police Department (MO)	Manchester	MO
Kidder Township Police Department (PA)	Lake Harmony	PA
Inactive Gibson County Sheriffs Office (IN)	Princeton	IN
Perry Township Police Department (OH)	DUBLIN	OH
Cuero Police Department (TX)	Cuero	TX
Rountree Neighborhood (CA)	N/A	N/A
Iowa Tribe Police Department (OK)	Perkins	OK
New London Police Department (WI)	New London	WI
Gladewater Police Department (TX)	Gladewater	TX
Cattaraugus County Sheriffs Office (NY)	Little Valley	NY
Henderson Police Department (TX)	Henderson	TX
Bridgeport Police Department (WV)	Bridgeport	WV

Hannahville Tribal Police Department (MI)	Wilson	MI
Woodridge Village Police Department (NY)	Woodridge	NY
New Boston Police Department (TX)	New Boston	TX
Coffey County Sheriffs Department (KS)	BURLINGTON	KS
Lancaster Police Department (TX)	Van Alstyne	TX
Ames Police Department (IA)	Ames	IA
Monroe Township Police Department (NJ)	Williamstown	NJ
Dwight Police Department (IL)	Dwight	IL
Inactive Schoolcraft College Police Department (MI)	Livonia	MI
Alma Police Department (TX)	Alma	TX
Liberty Township Police (PA)	Saxton	PA
Sallisaw Police Department (OK)	Sallisaw	OK
Madison County Sheriffs Office (NY)	Wampsville	NY
Covington Police Department (KY)	Covington	KY
Park Forest Police Department (IL)	Park Forest	IL
Town and Country Police Department (MO)	St Louis	MO
Coalinga Police Department (CA)	Fresno	CA
Butte County Sheriffs Department (CA)	Oroville	CA
Bradley County Sheriffs Office (TN)	Cleveland	TN
Lee County Sheriffs Office (IL)	Dixon	IL
Camp Pendleton Provost Marshall Office	Oceanside	CA
Poweshiek County Sheriffs Department (IA)	MONTEZUMA	IA
Grosse Pointe Shores (MI)	Grosse Pointe Shores	MI
Venice Police Department (FL)	Venice	FL
Karnes County Sheriffs Office (TX)	KARNES CITY	TX
Inactive Corvallis Police Department (OR)	Corvallis	OR
Inactive Dekalb County Sheriffs Office (IL)	Sycamore	IL
Utah Attorney Generals Office (UT)	Salt Lake	UT
Inactive Cook County Sheriffs Office (IL)	Maywood	IL
Monroe County Sheriffs Office (GA)	Forsyth	GA
Webb Police Department (AL)	Webb	AL
Fillmore County Sheriffs Office (NE)	Geneva	NE
Florence Police Department (SC)	Florence	SC
Throop Police Department (PA)	Throop	PA
Cary Police Department (IL)	Cary	IL
York Police Department (NE)	York	NE

Branch County Sheriffs Office (MI)	Coldwater	MI
Inactive Tulsa County Sheriffs Office - Interdiction (OK)	Tulsa	OK
Perry Police Department (IA)	Perry	IA
Roma Police Department (TX)	Roma	TX
DEA Minneapolis (MN)	South Minneapolis	MN
Inactive Santa Ana Police Department (NM)	Santa Ana Pueblo	NM
Harrisburg Bureau of Police (PA)	Harrisburg	PA
Van Meter Police Department (IA)	Van Meter	IA
Inactive Lake Villa Police Department (IL)	Lake Villa	IL
Saginaw Police Department (MI)	Saginaw	MI
Inyo County Sheriffs Department (CA)	Independence	CA
Ford County Sheriffs Office (KS)	Dodge City	KS
Inactive San Augustine County Sheriffs Office (TX)	San Augustine	TX
Punta Gorda Police Department (FL)	PUNTA GORDA	FL
Camp Verde Marshals Office (AZ)	Camp Verde	AZ
Shellman Police Department (GA)	Shellman	GA
Goliad County Sheriffs Office (TX)	Goliad	TX
Vernal Police Department (UT)	Vernal	UT
Johnson City Police Department (NY)	Johnson City	NY
Meadville Police Department (PA)	Meadville	PA
Village of Clearview Police Department (WV)	Wheeling	WV
Penn Township Police Department (PA)	HANOVER	PA
Le Mars Police Department (IA)	Le Mars	IA
Hillsboro Police Department (TX)	Hillsboro	TX
Webb County Sheriffs Office (TX)	Laredo	TX
La Salle County Sheriff (TX)	Cotulla	TX
Ivins PD (UT)	Ivins	UT
Jackson County Sheriff (TX)	Edna	TX
Snowmass Village Police Department (CO)	Snowmass Village	CO
Manor Township Armstrong Co Police Department	McGrann	PA
Sunland Park Police Department (NM)	SUNLAND PARK	NM
Atlantic Police Department City of (IA)	Atlantic	IA
Clay County Sheriff Department (MS)	West Point	MS
Ellinwood Police Department (KS)	ELLINWOOD	KS
Ohio Department of Rehabilitation and Correction (OH)	Columbus	OH
Dodge City Police Department (KS)	Dodge City	KS

Starr County Sheriff (TX)	Rio Grande City	TX
Robstown Police Departement (TX)	Robstown	TX
Hempstead Police Department (NY)	Hempstead	NY
Yukon Police Department (OK)	YUKON	OK
North Carolina State Highway Patrol (NC)	Raleigh	NC
McMullen County Sheriffs Office (TX)	Tilden	TX
Waukesha Police Department (WI)	Waukesha	WI
Norton Police Department (VA)	Norton	VA
Lowell Police Department Town of (IN)	Lowell	IN
Stephen F. Austin University (TX)	NACOGDOCHES	TX
Juab County Sheriff Deptmartment (UT)	Nephi	UT
University of Wisconsin Superior (WI)	Superior	WI
Navarro Country District Attorney (TX)	Corsicana	TX
Inactive Grant County Sheriffs Department (AR)	Sheridan	AR
Lacy-Lakeview Police Department (TX)	Waco	TX
West New York Police Department (NJ)	West New York	NJ
China Grove Police Department (TX)	China Grove	TX
Palmyra Police Department (NY)	Palmrya	NY
Curry County Sheriffs Office (NM)	Clovis	NM
Inactive Wadena County Sheriffs Office (MN)	Wadena	MN
Coldwater Police Department (MS)	Coldwater	MS
Sarpy County Sheriffs Office (NE)	Papillion	NE
Strawberry Lane HOA (CA)_VME	N/A	N/A
Shawano County Sheriff Office (WI)	Shawano	WI
Case Western Reserve University Police Department (OH)	Cleveland	OH
Louisa County Sheriff Office (IA)	Wapello	IA
Balcones Heights Police Department (TX)	Balcones Heights	TX
Ruleville Police Department (MS)	Ruleville	MS
Beloit Police Department (KS)	Beloit	KS
La Grange Police Department (TX)	La Grange	TX
Stafford Police Department (TX)	Stafford	TX
McDowell County Sheriffs Office (WV)	Welch	WV
Monett Police Department (MO)	Monett	MO
Sunrise Beach Police Department (MO)	Sunrise Beach	MO

Hot List Sharing

The University of California Riverside Police Department (CA) Agency is sharing Hot List records with the following Agencys:

Agency:	Hot List(s):
Riverside Police Department	LEARN_University of California Riverside Police Department (CA)

Hot List Received

The University of California Riverside Police Department (CA) Agency is receiving Shared Hot List records from the following Agencys:

Agency:	Hot List(s):
Bradley County Sheriffs Office (TN)	LEARN_Bradley County Sheriffs Office (TN)
Burnet County TX Law Enforcement	BC F and M Warrants
Chula Vista Police Department	LEARN_Chula Vista Police Department
Flagler County Sheriffs Office	LEARN_Flagler County Sheriffs Office
Folsom Police Department	LEARN_Folsom Police Department
Grants Pass Police Department	LEARN_Grants Pass Department of Public Safety
La Mesa Police Department (CA)	LEARN_La Mesa Police Department
Lincoln Police Department (ND)	LEARN_Lincoln Police Department (ND)
Lowndes County Sheriffs Office (MS)	LEARN_Lowndes County Sheriffs Office (MS)
Merced Police Department CA	LEARN_Merced Police Department CA
Monroe County Sheriffs Office (MS)	LEARN_Monroe County Sheriffs Office (MS)
Petaluma Police Department (CA)	LEARN_Petaluma Police Department (CA)
Tewksbury Township Police Department (NJ)	LEARN_Tewksbury Township Police Department (NJ)

EXHIBIT "4"

From: elliscollective <elliscollective@proton.me>
To: Jeffrey.Talbott@ucr.edu, lorena.penaloza@ucr.edu
Cc: Jamie.lopez@ucr.edu, chancellor@ucr.edu, denise.woods@ucr.edu, charles.robinson@ucop.edu, president@ucop.edu
Date: Wed, 25 Mar 2026 01:39:44 +0000
Subject: Formal Notice of Non-Compliance
Attachments: Non-Compliance Letter.pdf

Dear Chancellor, Chief of Police, and Counsel,

Please see the attached letter regarding UCRPD’s non-compliance with California Civil Code section 1798.90.5 et seq. and deficiencies in the University’s response to our CPRA request.

As detailed in the attached correspondence, the records produced indicate that UCRPD shared ALPR data with out-of-state and federal agencies, and the University did not produce the requested external/network audit logs.

This email is to provide formal notice and to request a substantive written response within fifteen (15) calendar days of the date of the letter addressing the demands set out in the attachment.

Please confirm receipt.

Respectfully,Daniel Negrete

The Ellis Collective

The Ellis Collective

For belonging, civil rights
& equal access

elliscollective@proton.me
202.643.6306

March 24, 2026

Sent Via Email and Certified Mail

UC Riverside Police Department
Attn: Chief of Police
3500 Canyon Crest Drive
Riverside, CA 92521

UC Riverside Office of Legal Affairs
900 University Avenue
3148 Hinderaker Hall
Riverside, CA 92521

Re: Non-Compliance with California Civil Code § 1798.90.5 et seq. (SB 34)

Dear Chancellor, Chief of Police, and Counsel:

On February 17, 2026, the Ellis Collective submitted a request to the Office of Legal Affairs for records held by the University of California Police Department, Riverside ("UCRPD"). That request went unanswered, in violation of the California Public Records Act ("CPRA"), which requires agencies to make a determination within ten days[1]. Only after our organization sent a letter threatening legal action did UCRPD respond.

Based on the records subsequently produced, we write this letter to formally notify that the University of California, Riverside Police Department is in violation of University of California policy and California law governing the use and dissemination of Automated License Plate Recognition ("ALPR") data. Records reveal that UCRPD has shared ALPR data with no fewer than 121 out-of-state and federal law enforcement agencies, conduct that is expressly prohibited under California Civil Code section 1798.90.55(a)[2].

We further request that the University produce all materials responsive to the request. The request specifically sought both internal audit logs (searches conducted by UCRPD personnel) and external/network audit logs (searches conducted by outside agencies that queried or accessed UCRPD's ALPR data). The production included only internal search records. The external network audit logs, which would document the full scope of out-of-state and federal agency access to UCRPD's ALPR database, were not produced, and no exemption, privilege, or other legal justification was cited for their omission.

[1]Cal. Civ. Code § 7922.535(a)
[2]Cal. Civ. Code § 1798.90.55(a).

I. Statutory Framework

A. SB 34 — Prohibition on Out-of-State ALPR Data Sharing

Senate Bill 34, codified at California Civil Code sections 1798.90.5 through 1798.90.55, governs the collection, use, maintenance, sharing, and access of ALPR data by California public agencies. Section 1798.90.55(a) provides that a public agency "shall not sell, share, or transfer ALPR information, except to another public agency, and only as otherwise permitted by law."[3] The term "public agency" is defined exclusively as entities of *the state*—i.e., California state and local governmental bodies.[4] Out-of-state law enforcement agencies and federal agencies fall outside this definition. The Attorney General's Office has issued binding guidance confirming that SB 34 categorically bars the sharing of ALPR data with any non-California entity.[5]

B. SB 54 — The California Values Act

To the extent any of the 121 out-of-state or federal agency queries identified in the production were conducted in connection with immigration enforcement, UCRPD's facilitation of such access independently violates the California Values Act, Government Code section 7284 *et seq*. SB 54 prohibits California law enforcement agencies from using agency resources, including databases and personnel, to investigate, interrogate, detain, detect, or arrest persons for immigration enforcement purposes.[6] The Attorney General has reiterated this prohibition as recently as January 2025.[7] Providing out-of-state or federal agencies with access to UCRPD's ALPR network constitutes the use of agency resources in potential furtherance of immigration enforcement and is impermissible under SB 54.

C. ALPR Audit Log Obligations Under Civil Code §§ 1798.90.51–.53

California law imposes affirmative recordkeeping obligations on ALPR operators. Section 1798.90.52 requires that ALPR operators maintain a record of access that includes, at minimum, the date and time of access, the license plate or data element queried, and the username and organizational affiliation of the individual accessing the system.[8] Section 1798.90.51(b)(1) further mandates an annual audit of all end-user searches to determine compliance with the agency's usage and privacy policy.[9] The usage and privacy policy itself must include processes for periodic system audits and mechanisms to monitor compliance with applicable privacy laws.[10] These records are public records subject to disclosure under the CPRA.

---

[3] Cal. Civ. Code § 1798.90.55(a) ("A public agency shall not sell, share, or transfer ALPR information, except to another public agency, and only as otherwise permitted by law.").

[4] Cal. Civ. Code § 1798.90.5(f).

[5] Cal. Dep't of Justice, Information Bulletin No. 2023-DLE-06, supra note 3 ("SB 34 does not permit California [law enforcement agencies] to share ALPR information with private entities or out-of-state or federal agencies.").

[6] Gov. Code § 7284.6(a)(1).

[7] Updated Responsibilities of Law Enforcement Agencies Under the California Values Act, California TRUST Act, and the California Truth Act: Information Bulletin, Cal. Dep't of Justice (Jan. 17, 2025), https://oag.ca.gov/system/files/attachments/press-docs/2025-dle-03.pdf.

[8] Cal. Civ. Code § 1798.90.52.

[9] Cal. Civ. Code § 1798.90.51(b)(1).

[10] Cal. Civ. Code § 1798.90.53(a)(6).

II. UCRPD's Violations

A. Illegal Sharing of ALPR Data with Out-of-State and Federal Agencies

The CPRA production reveals that the following categories of agencies had access to UCRPD's ALPR system as of Febrary 26th, 2026: agencies from Texas, Louisiana, Alabama, Arizona, Mississippi, Kansas, Nebraska, New York, New Jersey, Pennsylvania, Michigan, West Virginia, Indiana, Utah, Colorado, Iowa, Oregon, South Carolina, North Carolina, Tennessee, South Dakota, North Dakota, New Mexico, Arkansas, Florida, Georgia, Wisconsin, Illinois, Kentucky, Nevada, Wyoming, Montana, and Virginia, as well as federal agencies including the Bureau of Indian Affairs, the Internal Revenue Service Criminal Investigations Division, Customs and Border Protection (CBP–NTC), the ATF (national account), the U.S. Postal Inspection Service, and Camp Pendleton Provost Marshal's Office.

In total, no fewer than 121 out-of-state and federal agencies appear in the audit logs produced. An additional entry for the El Cajon Police Department, a California agency that has blatantly violated several privacy laws, was listed in the sharing document. Several agencies were also designated as "inactive," including the Federal Bureau of Investigation, Pearl River County Sheriff's Office, Tooele City Police Department (UT), and Trinidad Police Department (CO), suggesting that access credentials were at some point provisioned to these entities.

Each instance of access by a non-California entity constitutes a separate violation of Civil Code section 1798.90.55(a).[11] The statute admits of no exception for "network" sharing through a third-party ALPR vendor platform. Regardless of whether access was provisioned directly by UCRPD or facilitated through a vendor such as Flock Safety, the obligation to restrict ALPR data sharing to California public agencies rests with UCRPD as the operating agency.[12]

B. Deficient CPRA Response — Failure to Produce External Network Audit Logs

The request submited to the Office of Legal Affairs was explicit and unambiguous in its scope, seeking:

> *"Part A: ALPR audit logs (internal + external/network) from January 1, 2024 through February 16, 2026. Include the fields available in your export such as timestamp/date, searching/requesting agency, user/account, search type, justification/reason, and search scope… (1) Searches/lookups performed by this agency's users/accounts; (2) Searches/lookups performed by external agencies that queried or included this agency's ALPR network/data (network audit logs)."*

UCRPD's production was limited to internal search logs only. The external/network audit logs were entirely omitted from the response. No accompanying correspondence identified this omission, invoked any statutory exemption, or otherwise justified the withholding of these records. Under the CPRA, an agency bears the affirmative burden of demonstrating that any withheld record is exempt under express provisions of law, or that the public interest in nondisclosure clearly outweighs the public interest in

[11] Cal. Civ. Code § 1798.90.55(a).
[12] Cal. Civ. Code § 1798.90.5(f).

disclosure.[13] Where records contain both exempt and non-exempt material, the agency must segregate and produce all reasonably segregable portions.[14]

UCRPD's failure to produce the requested network audit logs, or to articulate any lawful basis for withholding them, constitutes a violation of the CPRA. The undersigned reserves all rights and remedies available under law, including but not limited to seeking injunctive relief, a writ of mandate, and an award of attorney's fees and costs pursuant to Government Code section 7923.115(a).[15]

III. Demands

Accordingly, the undersigned hereby makes the following demands:

1. **Immediate production of all external/network ALPR audit logs** responsive to the original CPRA request, covering the period of January 1, 2024 through February 16, 2026, including all fields available in the system export (timestamp, querying agency, user/account, search type, justification/reason, and search scope). If any portion of these records is claimed to be exempt, UCRPD must identify the specific exemption relied upon and produce all reasonably segregable non-exempt portions.

2. **Immediate termination of all ALPR data-sharing arrangements** with out-of-state and federal law enforcement agencies, including but not limited to the revocation of any network access credentials, the removal of UCRPD data from any shared or federated ALPR platform accessible to non-California entities, and the disabling of any automated sharing protocols.

3. **A written accounting** identifying each out-of-state and federal agency that has been granted access to UCRPD's ALPR system or data at any time, the date access was first provisioned, the vendor platform(s) through which access was facilitated, and the current status of each agency's access.

4. **A comprehensive internal audit** conducted pursuant to Civil Code section 1798.90.51(b)(1) to assess the scope of non-compliant sharing and determine whether all searches of UCRPD's ALPR data during the relevant period were conducted in compliance with applicable law and the agency's usage and privacy policy.

5. **Adoption of corrective protocols** to ensure ongoing compliance with Civil Code sections 1798.90.5 through 1798.90.55 and Government Code section 7284 *et seq.*, including written policies governing vendor platform configurations, network sharing permissions, and periodic compliance reviews.

IV. Conclusion

The scope of non-compliant ALPR data sharing documented in UCRPD's own records is substantial and ongoing. The presence of 121 out-of-state and federal agencies in the audit logs, including federal immigration and border enforcement entities, raises serious concerns under both SB 34 and the

[13] Gov. Code § 7922.000.

[14] Gov. Code § 7922.525 ("Any reasonably segregable portion of a record shall be available for inspection by any person requesting the record after deletion of the portions that are exempted by law.").

[15] Gov. Code § 7923.115(a) (mandatory attorney's fees and costs to prevailing CPRA requester).

California Values Act. The incomplete CPRA response compounds these concerns by frustrating the public's ability to assess the full extent of unlawful data sharing.

This letter constitutes a final demand for compliance prior to the pursuit of available legal remedies. The undersigned requests a substantive written response within fifteen (15) calendar days of the date of this letter confirming the actions taken to address each of the demands enumerated above.[16]

Nothing in this letter shall be construed as a waiver of any right, remedy, or claim available under law, all of which are expressly reserved.

Respectfully,

Daniel Negrete

Daniel Negrete Gonzalez

cc:

UC Riverside Office of the Chancellor
UC Office of the President
UC Office of the General Counsel

[16]Gov. Code § 7923.000 (authorizing proceedings for injunctive or declaratory relief or writ of mandate).

EXHIBIT "5"

From: Lorena Penaloza <lorena.penaloza@ucr.edu>

To: elliscollective <elliscollective@proton.me>

Cc: "Jeffrey.Talbott@ucr.edu" <jeffrey.talbott@ucr.edu>, "Jamie.lopez@ucr.edu" <jamie.lopez@ucr.edu>, "chancellor@ucr.edu" <chancellor@ucr.edu>, "denise.woods@ucr.edu" <denise.woods@ucr.edu>, "charles.robinson@ucop.edu" <charles.robinson@ucop.edu>, "president@ucop.edu" <president@ucop.edu>

Date: Wed, 25 Mar 2026 08:43:26 -0700

Subject: Re: Formal Notice of Non-Compliance

Mr. Negate:

This email acknowledges receipt of your email and attached correspondence on behalf of UCR.

Lorena PeÑaloza

Chief Campus Counsel

UC Legal – UCR Office of Legal Affairs

On Tue, Mar 24, 2026 at 6:39 PM elliscollective <elliscollective@proton.me> wrote:

Dear Chancellor, Chief of Police, and Counsel,

Please see the attached letter regarding UCRPD's non-compliance with California Civil Code section 1798.90.5 et seq. and deficiencies in the University's response to our CPRA request.

As detailed in the attached correspondence, the records produced indicate that UCRPD shared ALPR data with out-of-state and federal agencies, and the University did not produce the requested external/network audit logs.

This email is to provide formal notice and to request a substantive written response within fifteen (15) calendar days of the date of the letter addressing the demands set out in the attachment.

Please confirm receipt.

Respectfully,Daniel Negrete

The Ellis Collective

From: Lorena Penaloza <lorena.penaloza@ucr.edu>
To: elliscollective <elliscollective@proton.me>
Cc: UCR Chancellor <chancellor@ucr.edu>, denise.woods@ucr.edu, charles.robinson@ucop.edu, president@ucop.edu, Jeffrey.Talbott@ucr.edu
Date: Tue, 07 Apr 2026 19:20:57 -0700
Subject: UCR Response to Notice of Alleged Non-Compliance
Attachments: Response to Ellis Collective Apr 7 2026.pdf

Dear Mr. Negrete:

Please see the attached response to your email and letter below.

Sincerely,

Lorena

Lorena PeÑaloza

Pronouns: Ella/She/Her

Chief Campus Counsel

UC Legal – UCR Office of Legal Affairs

900 University Avenue, Riverside, CA 92521

Hinderaker Hall, Suite 3148

951-827-2228(phone)

951-888-3074 (fax)

For scheduling, please contact Kristen Erving, Paralegal/Information Practices Coordinator, at kristen.erving@ucr.edu or (951) 827-5983

From: elliscollective <elliscollective@proton.me>

Sent: Tuesday, March 24, 2026 6:40 PM

To: Jeffrey.Talbott@ucr.edu; lorena.penaloza@ucr.edu

Cc: Jamie.lopez@ucr.edu; chancellor@ucr.edu; denise.woods@ucr.edu; charles.robinson@ucop.edu; president@ucop.edu

Subject: Formal Notice of Non-Compliance

Dear Chancellor, Chief of Police, and Counsel,

Please see the attached letter regarding UCRPD’s non-compliance with California Civil Code section 1798.90.5 et seq. and deficiencies in the University’s response to our CPRA request.

As detailed in the attached correspondence, the records produced indicate that UCRPD shared ALPR data with out-of-state and federal agencies, and the University did not produce the requested external/network audit logs.

This email is to provide formal notice and to request a substantive written response within fifteen (15) calendar days of the date of the letter addressing the demands set out in the attachment.

Please confirm receipt.

Respectfully,

Daniel Negrete

The Ellis Collective

Office of Legal Affairs
900 University Avenue
3148 Hinderaker Hall
Riverside, CA 92521

April 7, 2026

Sent via email (elliscollective@proton.me)

Ellis Collective
Attn: Daniel Negrete Gonzalez.

Re: Automated License Plate Recognition data

Dear Mr. Negrete:

I am writing in response to your letter dated March 24, 2026, alleging the University of California, Riverside (UCR) is out of compliance with California Civil Code Section 1798.90.5 et seq. We disagree with your interpretation of the information produced by UCR in response to your request and hope the details outlined in this letter will help provide some clarity.

1. Automated License Plate Readers (ALPR)

UCR neither owns or operates ALPR cameras or an ALPR system, nor does UCR maintain or control any stored data associated with them. UCR is an end user of the ALPR networks operated by Flock and Vigilant. As a result, UCR does not separately maintain its own ALPR database.

2. California Public Records Act (CPRA) Request Production

On or about February 17, 2026, your organization submitted a CPRA request for the following information:

> Part A: ALPR audit logs (internal + external/network) from January 1, 2024, through February 16, 2026. Include the fields available in your export such as timestamp/date, searching/requesting agency, user/account, search type, justification/reason, and search scope., STAC):
> 1. Searches/lookups performed by this agency's users/accounts;
> 2. Searches/lookups performed by external agencies that queried or included this agency's ALPR network/data (network audit logs).
>
> Part B: Lists of agencies and networks with Automated License Plate Reader (ALPR) sharing relationships (including, but not limited to fusion centers such as ARJIS, JRIC, NCRIC, OCIAC, STAC)
> 3. The names of agencies and organizations with which this agency shares ALPR data;
> 4. The names of agencies and organizations from which this agency receives ALPR data;

5. The names of agencies and organizations with which this agency shares "hot list" information;
6. The names of agencies and organizations from which this agency receives "hot list" information;

Part C: Current ALPR sharing settings/configuration, STAC):
7. Records sufficient to show the current ALPR sharing configuration, including whether each partner listed in Part A has query/search access to this agency's ALPR data and whether access is full vs hit-only vs hotlist-only (screenshots or configuration export acceptable)

You also provided a link[1] with instructions on how to conduct the search for the various pieces of information you requested.

After conducting a reasonable search, including following the instructions you provided, UCR produced all the documents that were reasonably responsive to the request, which included:

- the internal audit logs for both Flock and Vigilant (over 500 pages)
- the device configuration, which shows the configuration with the eight (8) applicable local agencies
- the data sharing report, which shows "detection" information, which is incomplete/partial information that is inputted into the Flock and Vigilant systems for a finite period of time.

The balance of the documents requested – Part A.2, Part B.3, 5 and 6 - were not produced because, I am informed, they do not exist because we do not own an ALPR database or system.

UCR has reviewed the demands submitted on behalf of the Ellis Collective. We believe this letter responds to demands one and three. The balance of the demands are being reviewed and considered, including improving its protective protocols. UCR appreciates the interest of the Ellis Collective in this important matter.

Sincerely,

Lorena Peñaloza
Chief Campus Counsel

ec: UC Office of the President
Jack S. Hu, Chancellor
Charles F. Robinson, General Counsel and Senior Vice President
Dr. Denise Woods, Vice Chancellor, Health, Well-being and Safety
Jeffrey Talbott, Chief of Police

[1] https://drive.proton.me/urls/JFC930F0G4#BVewJLnWPNEr

EXHIBIT "6"

From: elliscollective <elliscollective@proton.me>

To: Lorena Penaloza <lorena.penaloza@ucr.edu>

Cc: UCR Chancellor <chancellor@ucr.edu>, denise.woods@ucr.edu, charles.robinson@ucop.edu, president@ucop.edu, Jeffrey.Talbott@ucr.edu

Date: Wed, 06 May 2026 04:22:33 +0000

Subject: Re: UCR Response to Notice of Alleged Non-Compliance

---

Dear Ms. Peñaloza,

I am writing to clarify a detail in my previous email sent earlier today. Due to administrative timelines regarding next steps in this matter, I have moved the deadline for a substantive response forward to 9:00 AM this Friday, May 8, 2026.

I look forward to receiving the confirmation requested by that time.

Best,

Daniel Negrete

-------- Original Message --------

On Tuesday, 05/05/26 at 18:24 elliscollective <elliscollective@proton.me> wrote:

Dear Ms. Lorena,

The University's response is legally insufficient. It ignores the primary issue raised in the letter of non-compliance: UC Riverside's illegal sharing of ALPR data with out-of-state and federal agencies.

Furthermore, your assertion that records were not produced because UC Riverside does not "own" the system is a bad-faith interpretation of the law. SB 34 (Civil Code § 1798.90.5) applies to any agency that "accesses or uses" an ALPR system; ownership of the hardware is irrelevant. Additionally, records held by third-party vendors for University business are public records under the CPRA.

UC Riverside has had over a month to move beyond "reviewing and considering" these clear statutory requirements. I have provided every reasonable opportunity to resolve this matter voluntarily. I will now wait until 5 p.m. on May 8th, 2026, for a substantive response confirming that:

UC Riverside has disabled all ALPR data-sharing with out-of-state and federal agencies, as requested in Demand #2.

The University will produce the records requested in Part A.2 and Part B.3, 5, and 6 by a date certain, regardless of third-party hosting.

Please be advised that if I do not receive this confirmation by the deadline, I will treat your silence as a formal refusal to comply with California law. Your choice to ignore these violations after being put on notice will be presented to the court as evidence of willful non-compliance, which warrants statutory damages and attorney’s fees.

Best,

Daniel Negrete

On Tuesday, 7 April 2026 at 7:21 PM, Lorena Penaloza <lorena.penaloza@ucr.edu> wrote:

Dear Mr. Negrete:

Please see the attached response to your email and letter below.

Sincerely,

Lorena

Lorena PeÑaloza

Pronouns: Ella/She/Her

Chief Campus Counsel

UC Legal – UCR Office of Legal Affairs

900 University Avenue, Riverside, CA 92521

Hinderaker Hall, Suite 3148

951-827-2228(phone)

951-888-3074 (fax)

For scheduling, please contact Kristen Erving, Paralegal/Information Practices Coordinator, at kristen.erving@ucr.edu or (951) 827-5983

From: elliscollective <elliscollective@proton.me>

Sent: Tuesday, March 24, 2026 6:40 PM

To: Jeffrey.Talbott@ucr.edu; lorena.penaloza@ucr.edu

Cc: Jamie.lopez@ucr.edu; chancellor@ucr.edu; denise.woods@ucr.edu; charles.robinson@ucop.edu; president@ucop.edu

Subject: Formal Notice of Non-Compliance

Dear Chancellor, Chief of Police, and Counsel,

Please see the attached letter regarding UCRPD’s non-compliance with California Civil Code section 1798.90.5 et seq. and deficiencies in the University’s response to our CPRA request.

As detailed in the attached correspondence, the records produced indicate that UCRPD shared ALPR data with out-of-state and federal agencies, and the University did not produce the requested external/network audit logs.

This email is to provide formal notice and to request a substantive written response within fifteen (15) calendar days of the date of the letter addressing the demands set out in the attachment.

Please confirm receipt.

Respectfully,

Daniel Negrete

The Ellis Collective

EXHIBIT "7"

From: Lorena Penaloza <lorena.penaloza@ucr.edu>
To: elliscollective <elliscollective@proton.me>
Cc: UCR Chancellor <chancellor@ucr.edu>, denise.woods@ucr.edu, charles.robinson@ucop.edu, president@ucop.edu, Jeffrey.Talbott@ucr.edu
Date: Mon, 11 May 2026 13:24:17 -0700
Subject: RE: UCR Response to Notice of Alleged Non-Compliance
Attachments: Shared Data Report.pdf

Dear Mr. Negrete:

I apologize for the delay in my response.

There appears to be a misunderstanding and some ongoing confusion about UCR's response. As indicated in UCR's response, UCR is an end-user as defined in Civil Code section 1798.90.5(a) and not an owner of ALPR cameras or systems as defined by Civil Code section 1798.90.5(d): "'Automated license plate recognition system' or 'ALPR system' means a searchable computerized database resulting from the operation of one or more mobile or fixed cameras combined with computer algorithms to read and convert images of registration plates and the characters they contain into computer-readable data." UCR's obligations as an end-user are set out in Civil Code section 1798.90.53.

I am informed that UCR does not share its data with out-of-state law enforcement agencies or federal agencies. I am further information that UCR recently reached out to its ALPR system vendors and confirmed this information; whereby the data sharing report was updated (see attached).

I am told that the documents you requested in Part A.2, and Part B.3, 5 and 6, do not exist for UCR.

Lorena PeÑaloza

Pronouns: Ella/She/Her

Chief Campus Counsel

UC Legal – UCR Office of Legal Affairs

900 University Avenue, Riverside, CA 92521

Hinderaker Hall, Suite 3148

951-827-2228(phone)

951-888-3074 (fax)

For scheduling, please contact Kristen Erving, Paralegal/Information Practices Coordinator, at kristen.erving@ucr.edu or (951) 827-5983

From: elliscollective <elliscollective@proton.me>

Sent: Tuesday, May 5, 2026 9:23 PM

To: Lorena Penaloza <lorena.penaloza@ucr.edu>

Cc: UCR Chancellor <chancellor@ucr.edu>; denise.woods@ucr.edu; charles.robinson@ucop.edu; president@ucop.edu; Jeffrey.Talbott@ucr.edu

Subject: Re: UCR Response to Notice of Alleged Non-Compliance

Dear Ms. Peñaloza,

I am writing to clarify a detail in my previous email sent earlier today. Due to administrative timelines regarding next steps in this matter, I have moved the deadline for a substantive response forward to 9:00 AM this Friday, May 8, 2026.

I look forward to receiving the confirmation requested by that time.

Best,

Daniel Negrete

-------- Original Message --------

On Tuesday, 05/05/26 at 18:24 elliscollective <elliscollective@proton.me> wrote:

Dear Ms. Lorena,

The University's response is legally insufficient. It ignores the primary issue raised in the letter of non-compliance: UC Riverside's illegal sharing of ALPR data with out-of-state and federal agencies.

Furthermore, your assertion that records were not produced because UC Riverside does not "own" the system is a bad-faith interpretation of the law. SB 34 (Civil Code § 1798.90.5) applies to any agency that "accesses or uses" an ALPR system; ownership of the hardware is irrelevant. Additionally, records held by third-party vendors for University business are public records under the CPRA.

UC Riverside has had over a month to move beyond "reviewing and considering" these clear statutory requirements. I have provided every reasonable opportunity to resolve this matter voluntarily. I will now wait until 5 p.m. on May 8th, 2026, for a substantive response confirming that:

UC Riverside has disabled all ALPR data-sharing with out-of-state and federal agencies, as requested in Demand #2.

The University will produce the records requested in Part A.2 and Part B.3, 5, and 6 by a date certain, regardless of third-party hosting.

Please be advised that if I do not receive this confirmation by the deadline, I will treat your silence as a formal refusal to comply with California law. Your choice to ignore these violations after being put on notice will be presented to the court as evidence of willful non-compliance, which warrants statutory damages and attorney's fees.

Best,

Daniel Negrete

On Tuesday, 7 April 2026 at 7:21 PM, Lorena Penaloza <lorena.penaloza@ucr.edu> wrote:

Dear Mr. Negrete:

Please see the attached response to your email and letter below.

Sincerely,

Lorena

Lorena PeÑaloza

Pronouns: Ella/She/Her

Chief Campus Counsel

UC Legal – UCR Office of Legal Affairs

900 University Avenue, Riverside, CA 92521

Hinderaker Hall, Suite 3148

951-827-2228(phone)

951-888-3074 (fax)

For scheduling, please contact Kristen Erving, Paralegal/Information Practices Coordinator, at kristen.erving@ucr.edu or (951) 827-5983

From: elliscollective <elliscollective@proton.me>

Sent: Tuesday, March 24, 2026 6:40 PM

To: Jeffrey.Talbott@ucr.edu; lorena.penaloza@ucr.edu

Cc: Jamie.lopez@ucr.edu; chancellor@ucr.edu; denise.woods@ucr.edu; charles.robinson@ucop.edu; president@ucop.edu

Subject: Formal Notice of Non-Compliance

Dear Chancellor, Chief of Police, and Counsel,

Please see the attached letter regarding UCRPD's non-compliance with California Civil Code section 1798.90.5 et seq. and deficiencies in the University's response to our CPRA request.

As detailed in the attached correspondence, the records produced indicate that UCRPD shared ALPR data with out-of-state and federal agencies, and the University did not produce the requested external/network audit logs.

This email is to provide formal notice and to request a substantive written response within fifteen (15) calendar days of the date of the letter addressing the demands set out in the attachment.

Please confirm receipt.

Respectfully,

Daniel Negrete

The Ellis Collective

EXHIBIT "8"

Detections Shared

The University of California Riverside Police Department (CA) Agency is Sharing its Detection data with the following Agencies:

None

Detections Received

The University of California Riverside Police Department (CA) Agency is receiving Detection data from the following Agencies:

Agency	City	State
Grand Junction Police Department (CO)	Grand Junction	CO
Coweta County Sheriffs Office	Newnan	GA
Coral Springs Police Department	Coral Springs	FL
Galveston Auto Theft Task Force	Dickinson	TX
Riverside Police Department	Riverside	CA
Vigilant Solutions Sales	Chicago	IL
Skokie Police Department	Skokie	IL
Santa Ana Police Department	Santa Ana	CA
Orange County Sheriffs Department	Aliso Viejo	CA
Anaheim Police Department	Anaheim	CA
Orange Police Department	Orange	CA
Tustin Police Department	Tustin	CA
Westminster Police Department	Westminster	CA
Laguna Beach Police Department	Laguna Beach	CA
Kemah Police Department	Kemah	TX
Seal Beach Police Department	Seal Beach	CA
Brea Police Department	Brea	CA
UC Irvine Police Department	Irvine	CA
La Habra Police Department	La Habra	CA
Irvine Police Department (CA)	Irvine	CA
Newport Beach Police Department	Newport Beach	CA
Palm Beach County Sheriffs	West Palm Beach	FL
Frisco Police Department	Frisco	TX
Sacramento Police Department	Sacramento	CA
Corona Police Department	Corona	CA
Sikeston Police Department	Sikeston	MO
Springfield MO Police Department	Springfield	MO

EXHIBIT "9"

Automated License Plate Readers (ALPRs)

468.1 PURPOSE AND SCOPE

The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of Automated License Plate Reader (ALPR) technology.

468.2 POLICY

The policy of the UC Riverside Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

468.3 ADMINISTRATION

The ALPR technology, also known as License Plate Recognition (LPR), allows for the automated detection of license plates. It is used by the UC Riverside Police Department to convert data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates and missing persons. It may also be used to gather information related to active warrants, homeland security, electronic surveillance, suspect interdiction and stolen property recovery.

All installation and maintenance of ALPR equipment, as well as ALPR data retention and access, shall be managed by the Support Services Division Commander. The Support Services Division Commander will assign members under his/her command to administer the day-to-day operation of the ALPR equipment and data.

468.3.1 ALPR ADMINISTRATOR

The Support Services Division Commander shall be responsible for developing guidelines and procedures to comply with the requirements of Civil Code § 1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

(a) A description of the job title or other designation of the members and independent contractors who are authorized to use or access the ALPR system or to collect ALPR information.

(b) Training requirements for authorized users.

(c) A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.

(d) Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52.

(e) The title and name of the current designee in overseeing the ALPR operation.

(f) Working with the Custodian of Records on the retention and destruction of ALPR data.

(g) Ensuring this policy and related procedures are conspicuously posted on the department's website.

468.4 OPERATIONS

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

(a) An ALPR shall only be used for official law enforcement business.

(b) An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR.

(c) While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

(d) No member of this department shall operate ALPR equipment or access ALPR data without first completing department-approved training.

(e) No ALPR operator may access department, state or federal data unless otherwise authorized to do so.

(f) If practicable, the officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert.

468.5 DATA COLLECTION AND RETENTION

The Support Services Division Commander is responsible for ensuring systems and processes are in place for the proper collection and retention of ALPR data. Data will be transferred from vehicles to the designated storage in accordance with department procedures.

All ALPR data downloaded to the server should be stored for a minimum of one year and in accordance with the established records retention schedule. Thereafter, ALPR data should be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a discovery request or other lawful action to produce records. In those circumstances the applicable data should be downloaded from the server onto portable media and booked into evidence.

468.6 ACCOUNTABILITY

All data will be closely safeguarded and protected by both procedural and technological means. The UC Riverside Police Department will observe the following safeguards regarding access to and use of stored data (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

(a) All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52).

(b) Members approved to access ALPR data under these guidelines are permitted to access the data for legitimate law enforcement purposes only, such as when the data relate to a specific criminal investigation or department-related civil or administrative action.

(c) ALPR system audits should be conducted on a regular basis.

For security or data breaches, see the Records Release and Maintenance Policy.

468.7 RELEASING ALPR DATA

The ALPR data may be shared only with other law enforcement or prosecutorial agencies for official law enforcement purposes or as otherwise permitted by law, using the following procedures:

(a) The agency makes a written request for the ALPR data that includes:

1. The name of the agency.
2. The name of the person requesting.
3. The intended purpose of obtaining the information.

(b) The request is reviewed by the Support Services Division Commander or the authorized designee and approved before the request is fulfilled.

(c) The approved request is retained on file.

Requests for ALPR data by non-law enforcement or non-prosecutorial agencies will be processed as provided in the Records Maintenance and Release Policy (Civil Code § 1798.90.55).

468.8 TRAINING

The Training Sergeant should ensure that members receive department-approved training for those authorized to use or access the ALPR system (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

EXHIBIT "10"

FAQ

Managing your LPR data

Frequently asked questions

Motorola Solutions hosted environment presents a great convenience to customers wishing to deploy license plate recognition (LPR) in a scalable fashion without concern of servers, storage space, database maintenance or software updates. Using a hosted environment benefits agencies in many ways, but it does present some questions for those not familiar with hosting data in the cloud.

Q. How does data sharing work?

A. Motorola Solutions maintains three distinct license plate recognition (LPR) platforms, VehicleManager, VehicleManager Enterprise and ClientPortal. All data collected by Motorola's customers, whether in VehicleManager, VehicleManager Enterprise or ClientPortal, is the property of the respective customer, and Motorola has no rights or ownership to any of this data. All customers manage and control all access to their LPR data as well as maintain their own data retention period, even on shared data.

VehicleManager is a hosted solution made available exclusively to law enforcement (LE) customers. The VehicleManager software and database, the data center housing VehicleManager, and the people and processes governing VehicleManager are compliant with all relevant aspects of the FBI-CJIS Security Policy. Law enforcement agencies may choose (at their sole discretion) to share their data to other law enforcement agencies within the VehicleManager platform, but there is no mechanism to share this data outside of VehicleManager.

VehicleManager Enterprise and **ClientPortal** are hosted solutions, similar to VehicleManager, made available to all enterprise customers. These customers consist of parking enforcement entities, parking management companies, property management and retail facilities, homeowners associations, casinos and many other types of enterprises.

As with law enforcement agencies in VehicleManager, VehicleManager Enterprise and ClientPortal customers may choose to share (at their sole discretion) their data to other VehicleManager Enterprise and ClientPortal customers. Unlike VehicleManager however, they also have the ability to share their data to law enforcement customers via a one-way sharing mechanism from VehicleManager Enterprise and ClientPortal to VehicleManager. To prevent the inadvertent sharing of data from law enforcement accounts, Motorola has physically separated Law Enforcement data within Azure Gov and enterprise data in Azure Commercial. This physical segmentation of networks blocks the data passing from VehicleManager (LE) data into our enterprise environments.

Q. What is "commercial data"?

A. We maintain a separate database of commercial LPR data. This data is collected by repossession vehicles. This data is not commingled with law enforcement or enterprise data, nor is law enforcement or enterprise data ever accessible to commercial entities. This is part of meeting CJIS compliance requirements for data access for our law enforcement customers. We provide our law enforcement and enterprise customers access to this commercial dataset to generate improved vehicle location insights with a greater quantity of data points.

Q. How long is my data stored?

A. As the data is your property, it is held according to the retention policy set forth by you. Retention policies may be adjusted by the Agency or Site Manager at any time, and different retention policies may be set for "detections" and "hits" to allow for consistency with any policy in place and/or legislation. Even if you choose to share data with specific law enforcement agencies, the data retention policies set on your data by you, still apply. Data is automatically deleted from the system based on the retention policy, and Motorola Solutions keeps no record of data after deletion unless metadata archival and classification is requested by the agency.

Q. How secure is my data?

A. Your data resides in a data center featuring redundant power sources, redundant fiber connectivity, redundant disk arrays, environmental monitoring, secure access control, physical escorts for on-site visitors, multiple diesel fuel backup generators, active fire prevention and suppression, and on-site system administrators and engineers. For our law enforcement customers, our systems are completely CJIS compliant, not only compliant because they are "Hosted in a CJIS Compliant Cloud." To meet CJIS compliance vendors must address:

- Data encryption from the edge to the cloud.
- Data can only be accessed by approved personnel.
- Data access is restricted, including to the vendor, and is totally managed by the agency.
- Criminal background checks of vendor personnel that have access to the data.
- Physical security safeguards at data center and critical infrastructure locations.
- Robust audits and accountability based on users, search parameters etc.
- System IP address logging for accountability of access.
- Multi-factor authentication for access to the data that can be coupled with optional secure single sign-on.
- Mandatory user logout after inactivity.
- Configured and managed user accounts to restrict or limit access based on roles.
- Printable audit reports for record management and challenges.

Additional safeguards

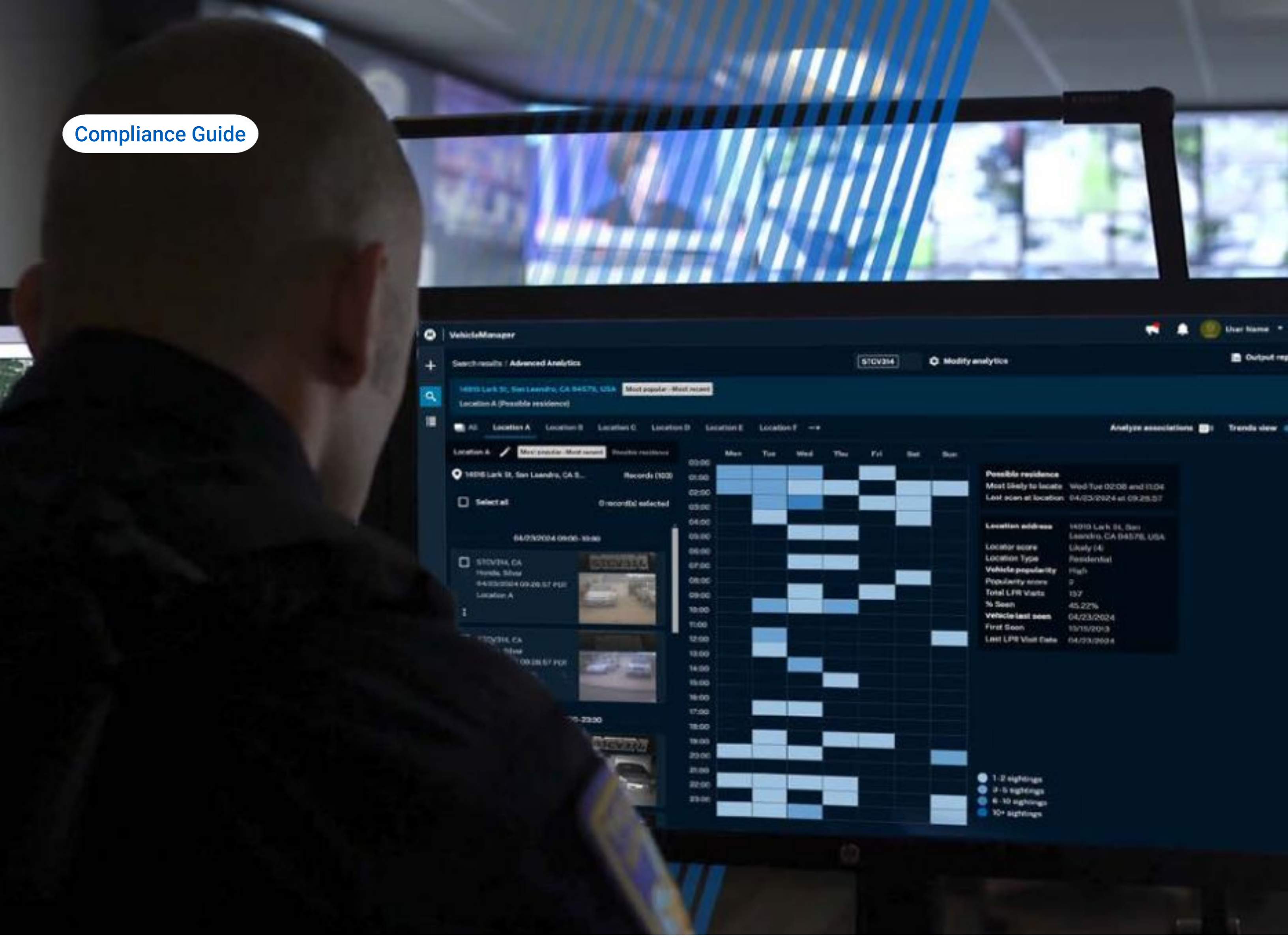
Built-in scheduled health and maintenance checks of systems and cameras.

- Report on every system and every camera.- Mobile health reports can report on your parameters – weekly, monthly, etc.
- Maintain easy accountability and proper use.
- Data retention is managed by the agency and can apply a custom required policy on both detections and open cases.
- Full auditing capability, including ANY users from a shared agency querying the data.
- Digital evidentiary data can be easily preserved for court (not a copy, but the raw data).
- Required reasoning notation to query the LPR database is mandatory.

See the full security briefing and compliance guide here.

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. motorolasolutions.com

EXHIBIT "11"



VehicleManager CJIS security compliance guide

Protecting license plate recognition data

MOTOROLA SOLUTIONS

Overview

Motorola Solutions offers its law enforcement clients a hosted analytics solution called VehicleManager.

Unless on-premise deployment is required by the customer, all IT assets and software applications are hosted in colocation, Infrastructure as a Service, and Software as a Service configurations with Motorola Solutions' owned IT assets. Assets are located within Motorola Solutions' contracted data center. Physical and environmental security controls are managed by Microsoft Azure. Information about the data center can be found at this link: Microsoft Azure Data Center. Plate images are stored separately at Amazon Web Services in Ashburn, VA.

Microsoft is a worldwide leader that provides hosted services and top-notch information security. Microsoft is certified to ISO 9001:2015, the internationally recognized standard for Quality Management Systems, and has been independently audited and verified for compliance under Statement on Auditing Standards No. 70 [SOC 2 Report]. The SOC 2 report is available under a Non-Disclosure Agreement. The public SOC 3 can be found here: SOC 3

The physical and network security measures employed at the Motorola Solutions data center are comprehensive.

The Microsoft Azure Data Center has also been certified to meet FedRAMP High security controls and granted an ATO by DHS. While license plate reader data inherently contains no personal information, it can be linked to other sources or free-text fields that may allow the end user to enter data that could be viewed as personally identifiable information (PII) or Criminal Justice Information (CJI), which is beyond our control. Of greater relevance, law enforcement hot list information, such as NCIC, is managed by Motorola Solutions law enforcement customers and may potentially contain CJI as defined in 4.1 of the CJIS Security Policy. For these reasons, Motorola Solutions has voluntarily implemented security controls we believe are necessary to comply with the relevant sections. The current version of the FBI-CJIS Security Policy is available here.

Relevant Sections of FBI-CJIS Security Policy

Within the scope of this document and as it pertains to the FBI-CJIS Security Policy, Motorola Solutions is a private contractor, as defined in that policy. Going beyond the minimum requirements, the following table highlights those sections of the FBI-CJIS Security Policy that are believed to apply to the Motorola Solutions-hosted solution:

Access Control (AC)

AC-2

VehicleManager enables customer-controlled, role-based access through customizable user profiles and permissions, so that users have only the minimum privileges necessary for their roles. The system employs Access Control Lists (ACLs) to secure critical components, enforces password policies consistent with FBI Security Policy, and logs privilege changes indefinitely for auditing purposes. Inactive accounts are automatically inactivated after 60 days and disabled after 90 days, requiring Agency Manager reactivation to maintain strict access control.

AC-3

VehicleManager implements Access Control Lists (ACLs) to secure database servers, firewalls, VPNs, and software applications, while also providing customer-controlled resource restrictions and role-based user management, with customizable permission sets and password policies, in compliance with the FBI Security Policy.

AC-4

Secure HTTP (HTTPS) with TLS 1.2+ is used to protect data in transit, ensuring secure communication over networks. Additionally, the system employs all four types of data partitioning, separating components such as the web server, database server, and user information to maintain robust data isolation and security.

AC-5

Customer-controlled, tiered role-based access in VehicleManager allows agencies to create user profiles with extensive, customizable permissions and access controls, so users have only the necessary rights for their roles. Changes to user rights and privileges are logged indefinitely and available in audit records. The system also employs Access Control Lists (ACLs) to secure critical components such as database servers, firewalls, VPNs, and applications, while providing resource restrictions and FIPS 140-3 certified encryption for both data at rest and data in transit. Additionally, agencies can manage password policies, including character complexity and change requirements, in compliance with the FBI Security Policy.

AC-6

Windows tracking on the virtual machines enforces account lockouts after five unsuccessful login attempts, while all user logins and activities are logged to ensure accountability. Tiered role-based access with customizable user profiles allows agencies to assign only the necessary permissions, with changes to rights and privileges logged indefinitely for audit purposes. Access Control Lists (ACLs) secure critical components such as database servers, firewalls, and VPNs, while customer-controlled resource restrictions and FIPS 140-3 certified encryption protect data at rest and in transit via HTTPS. Additional safeguards include password policy management consistent with FBI CJIS Security Policy and advanced threat protection through Microsoft System Defender, BigFix, and Palo Alto Cortex XDR.

AC-7

Accounts are locked for 2 hours after 5 consecutive unsuccessful login attempts, ensuring compliance with CJIS requirements and mitigating the risk of unauthorized access from repeated attempts. The portion of the control requiring administrator release of the lock will be remediated by mid Q2 2026.

AC-8

Before access is granted, VehicleManager displays a mandatory acknowledgment banner that users must accept to ensure they are aware of system policies and expectations. The acknowledgment is logged automatically, recording the date, time, and activity performed, and the banner cannot be bypassed, in compliance with CJIS requirements.

AC-11

VehicleManager requires users to affirmatively acknowledge a pop-up banner before access is granted, with the acknowledgment logged by tracking the date, time, and activity performed. The banner cannot be bypassed, promoting user accountability. Additionally, session locks are automatically engaged after 25 minutes of inactivity, requiring users to re-enter their credentials to regain access, further securing system resources.

AC-17

Windows tracking enforces account lockouts after five unsuccessful login attempts, while all user logins and activities are logged, including IP tracking for each user to ensure accountability. Data is secured with a minimum of 256-bit encryption and FIPS 140-3 certification for both data at rest and in transit, with certificates available upon request to meet compliance requirements.

AC-19

Motorola Solutions' mobile device usage can be configured to align with agency policies by utilizing the same user profiles configured within VehicleManager. This ensures consistent access control and auditing across both the web application and the mobile platform, maintaining compliance with CJIS standards.

Audit and Accountability (AU)

AU-2

Windows and application tracking logs all user log-on events, including unsuccessful login attempts, and locks accounts after five failed attempts. These activities are recorded to ensure accountability and support compliance with CJIS auditing requirements. The general approach to audit logging is to capture events and content associated with all authentication, file use, user/group management, events sufficient to establish what occurred, the sources of events, outcomes of events, and operational transactions.

AU-3

VehicleManager captures all system actions in a comprehensive, auditable format, enabling robust tracking of user activity. For every transaction, whether successful or unsuccessful, from initial authentication through session termination, Agency Managers can monitor the originating IP address, the specific activity performed, and the precise timing of each event, maintaining accountability and supporting CJIS compliance requirements. All events and content specified in AU-3 and AU-3(1) with the exception of bytes sent and received are captured and available to the end user auditor in the audit module. Research and investigation are being conducted to determine the level of effort and timeline to provide the byte content.

AU-4

Audit records are retained for a minimum of one year, with the option for longer retention based on customer specifications. VehicleManager follows retention routines established by the data owner, and metadata for transaction activity is preserved to support system integrity and compliance audits.

AU-5

VehicleManager retains audit records for a minimum of one year, unless the customer specifies otherwise. Retention routines are executed as established by the data owner, and metadata for transaction activity is preserved to support compliance and integrity audits, to help ensure that audit processing failures do not result in data loss or non-compliance.

AU-6

VehicleManager enables agencies to monitor, analyze, and report audit logs through built-in auditing tools and a report scheduler in VehicleManager. Agencies can review logs weekly to identify inappropriate or unusual activity, and VehicleManager assists clients in obtaining necessary audit data. Additionally, Motorola Solutions audits its authorized staff with access to software applications and data, to facilitate compliance with CJIS requirements.

AU-7

VehicleManager's auditing tools and report scheduler provide agencies with the ability to generate detailed, customizable reports. These tools can streamline the analysis of audit logs and reduce the complexity of auditing processes while maintaining compliance with CJIS requirements.

AU-9

Audit records in VehicleManager are safeguarded through retention of at least one year (unless specified otherwise by the customer) and protected by customer-controlled access restrictions and FIPS 140-3 certified encryption for data at rest and in transit. This facilitates the availability of audit information and is secure for compliance and investigative purposes.

Configuration Management (CM)

CM-3

Motorola Solutions employs a centralized Change Management Plan for software patches and updates on its data center, and Kubernetes assets. This process includes rigorous testing, ample preparation, and rollback plans to ensure that configuration changes do not disrupt operations or compromise security.

CM-4

All software patches and updates are subject to a thorough security impact analysis before deployment. Motorola Solutions' centralized patch management process includes testing and rollback plans to assess and mitigate potential risks.

CM-8

Motorola Solutions maintains a centralized management system for its data center assets, ensuring an accurate inventory of all components. This supports compliance, security, and effective configuration management.

Identification and Authorization (IA)

IA-2

VehicleManager supports identification and authentication through robust password policies in compliance with CJIS Security Policy, including complexity and change requirements. Accounts are automatically inactivated after 60 days of inactivity and disabled after 90 days, requiring reactivation by an Agency Manager.

IA-3

VehicleManager employs Secure HTTP (HTTPS) with TLS encryption to authenticate and protect data in transit, so that devices accessing the system are securely identified and authorized.

IA-4

User identifiers are managed in compliance with CJIS standards. VehicleManager inactivates user accounts after 60 days of inactivity and disables them after 90 days, with automated warnings sent to users and Agency Managers before deactivation. Reactivation requires Agency Manager approval to maintain strict identifier control.

IA-5

VehicleManager enforces password policies that comply with CJIS requirements, including complexity standards and mandatory change intervals. To prevent unauthorized access, accounts are automatically inactivated after 60 days without a password update and fully disabled after 90 days. For enhanced security, the system requires AAL2 Multi-Factor Authentication (MFA) and supports integration with customer-owned identity solutions, such as SAML or OAuth.

IA-7

VehicleManager uses FIPS 140-3 certified cryptographic modules in its deployments sothat all randomly generated numbers in use when authenticating are compliant and sufficiently secure for their purpose.

IA-8

Identification and authentication for non-organizational users are managed through agency-controlled access and user profiles within VehicleManager, ensuring compliance with CJIS policies on external user access.

System and Communication Protection (SC)

SC-2

Motorola Solutions uses data partitioning to ensure secure separation of resources, including the web server, database server, user information, and other critical components. All four types of partitioning specified by CJIS are implemented.

SC-4

Data partitioning within VehicleManager ensures secure separation of customer data, including information stored on the web server, database server, and other system components. This protects shared resources from unauthorized access.

SC-5

Denial of Service (DoS) protection is implemented through a combination of industry-standard Cisco packet inspection, Azure Load Balancers, and a Web Application Firewall (WAF). These tools provide robust network monitoring, traffic management, and filtering to prevent service disruptions and unauthorized access. Together, they ensure network availability and the secure handling of Criminal Justice Information (CJI), even during potential attack scenarios.

SC-7

Boundary protection is ensured through the use of industry-standard Cisco packet inspection, and a Web Application Firewall (WAF). These mechanisms monitor and control incoming and outgoing network traffic, preventing unauthorized access and promotingdata security. By leveraging these tools, along with secure HTTPS and TLS encryption for data in transit, Motorola Solutions protects system boundaries and maintains the confidentiality and integrity of Criminal Justice Information (CJI).

SC-8

VehicleManager employs Secure HTTP (HTTPS) with TLS 1.3 encryption currently in place to ensure the confidentiality and integrity of data transmitted across public networks, meeting CJIS requirements for secure communication.

SC-10

VehicleManager facilitates the immediate termination of network connections upon session conclusion, ensuring that the link is severed immediately whether the disconnect is user-initiated or forced.This control maintains system integrity by preventing unauthorized session persistence and supporting CJIS compliance for secure session management.

SC-12

FIPS 140-3 certified encryption ensures secure cryptographic key management for data at rest and in transit. Certificates are available upon request to demonstrate compliance with CJIS requirements.

SC-13

Motorola Solutions complies with FBI-CJIS encryption standards by utilizing FIPS 140-3 certified cryptographic methods, meeting the minimum requirement of 256-bit encryption for both data at rest and data in transit for the secure storage and transfer of CJI.

SC-28

Data at rest is secured with FIPS 140-3 certified encryption using a minimum of 256-bit encryption, in compliance with CJIS requirements for protecting stored CJI.

System and Information (SI)

SI-2

Motorola Solutions employs a centralized patch management process for its data center assets, which includes a Change Management Plan, thorough testing, and rollback procedures to remediate software flaws effectively.

SC-3

Malware protection is provided through Microsoft System Defender and PaloAlto Cortex XDR, ensuring systems are safeguarded against malicious code and unauthorized software.

SI-4

Automated system monitoring is conducted using Cisco intrusion detection tools and techniques, as well as PaloAlto Cortex XDR, for real-time detection and response to potential security threats.

SI-5

Motorola Solutions delivers security alerts and advisories through agency notifications and manager emails. Microsoft Azure's Security Advisory system notifies key IT personnel, including the VP of IT, during significant security events.

SI-7

Motorola Solutions promotes the integrity of software, firmware, and information through automated monitoring and inspection tools, including PaloAlto Cortex and other industry-standard solutions. These tools detect, report, and mitigate any integrity violations.

SI-11

Error handling and incident notification mechanisms are in place, including automated alerts and advisories sent to agency managers and IT personnel. These systems help to ensure that errors are promptly addressed and that agencies remain informed of system status.

Narrative on FBI-CJIS security policy

Motorola Solutions' VehicleManager web-based solutions are exclusively available to law enforcement. All Motorola Solutions agencies are ORI-vetted police agencies that manage the users they authorize. The data an agency collects can be shared with specific law enforcement agencies via an MOU, shared with Motorola Solutions' national law enforcement database, or exclusively retained for that client agency's use only. This is accomplished by the Agency Manager employing configurable resource restrictions and role-based access privileges.

As a company, Motorola Solutions specifies in several places, including on its website and in its Master Customer Agreement—which is agreed to and signed prior to purchasing Motorola Solutions products and/or services—that the VehicleManager data collected or contributed by law enforcement remains the property of the agency, and Motorola Solutions has no rights to that data. That information is shared in accordance with the data owner's sharing rules. Motorola Solutions further classifies all this information internally as Criminal Justice Data and has strong policies for handling, storage, and destruction of this information.

Motorola Solutions does not share, sell, or make use of law enforcement-generated Criminal Justice Data in any way. Furthermore, any data retention policy or the sharing of an agency's data is entirely under the agency's control. Many federal, state, county, and municipal jurisdictions have legislation or guidance on appropriate legal or privacy rules.

The VehicleManager client application allows for the Agency Manager role, within the customer agency, to make the necessary changes to data sharing and retention rules. However, it is the sole responsibility of the data owner to ensure that the data submitted, entered, or shared is done so in recognition of and in accordance with the customer agencies' governing laws, regulations, and policies. The data owner is responsible for establishing the sharing rules, retention policies, appropriate data entry rules, and the accuracy and timeliness of the data.

Motorola Solutions uses technical controls and mechanisms within its suite of products to facilitate privacy controls over data and restrict access to only those granted access by the agency. Motorola Solutions only allows staff to access data when performing customer support duties authorized by the customer. Remote access sessions to customer systems to assist a client are intended to be granted access and monitored (virtual escorting) during the customer support session by the customer, through the mechanism agreed upon.

Those technical controls include configurable access rights, agency-controlled information sharing, logging user activity and access, account inactivation for periods of inactivity, session locks, strong password criteria for system access, encrypted data transport, and data storage at a facility that meets FBI-CJIS Security Policy Physically Secure Location criteria.

Even though Motorola Solutions has built-in tools to facilitate audit and accountability controls consistent with the FBI-CJIS Security Policy, it is the client agency's responsibility to perform the audit processes using the Motorola Solutions product tools provided. Motorola Solutions internally monitors system availability, unauthorized access, and system and data integrity.

Motorola Solutions internally monitors system availability, unauthorized access, and system and data integrity. If the customer deems that additional events and content logging are required, we will work with customers to remediate any perceived gaps.

Below are high-level descriptions of Motorola Solutions enterprise efforts to address FBI-CJIS Security Policy areas.

Personnel security

In an effort to maintain the integrity of Motorola Solutions' business relationships with clients and their data, as well as its own purposes, Motorola Solutions performs commercial name-based background screening on all of its employees prior to employment.

When required by a client, all Motorola Solutions staff directly supporting its agencies that may have access are subject to FBI-CJIS Security Policy Personnel Security procedures.

Motorola Solutions cannot, by federal law, independently perform fingerprint-based background check screening. Accordingly, it is within the jurisdiction and responsibility of the client agency to perform that screening if they believe it is required based on the existence of Criminal Justice Information or for access to agency on-premise environments that may contain Criminal Justice Information provided by FBI-CJIS.

Motorola Solutions staff has, however, successfully completed FBI fingerprint-based background check screening by the FBI-CJIS System Agency in several states that require the fingerprint-based background checks. Only those employees that have passed the personnel screening process are allowed to provide technical system support or access the system in support of client agencies requests. If Motorola Solutions becomes aware of any prohibiting activity, those employees' access rights to VehicleManager or customer systems are suspended pending final resolution by the courts. In those states requiring CJIS screening, those CJIS System Agencies and clients are notified of activity and suspension of access.

These employees, in addition to others, have executed and will upon request, execute the FBI-CJIS Security Addendum. Copies are retained by Motorola Solutions FBI-CJIS ISO along with records of Security Awareness Training that included topics on privacy, confidentiality and data security. Motorola Solutions staff performs security awareness training through CJIS Online, which has been accepted by all states requiring the CJIS Security Awareness Training. Security addenda are also posted there.

Incident response planning

With the intention of meeting or exceeding the relevant aspects of the FBI-CJIS Security Policy, Motorola Solutions has several administrative and technical controls to adhere to those criteria in response to and subsequent reporting for cyber security events within its control. Motorola Solutions employs and manages malware and virus protection, patch management policies, intrusion detection and intrusion prevention systems to protect the customer-owned data in VehicleManager. Motorola Solutions uses tools and processes to monitor for malicious activity and address any data breaches.

Motorola Solutions has a Global incident Response Plan (shared upon request) consistent with the FBI-CJIS Security Policy. A component of that plan is to communicate to impacted parties, in the event of any physical or technical breach causing customer data loss, unauthorized access or misuse of data or systems through an incident reporting process.

Azure GovCloud has been evaluated in the 49 states for their incident response plan and meets FedRAMP High certification. MSI and Microsoft will agree to report breaches of the provider boundary or internal network access controls to the affected customer's Local Agency Security Officer (LASO) once verified.

Physical security

The physical protection mechanisms at the Microsoft Azure Government facility are consistent with, or greater than, the FBI-CJIS Physically Secure Location criteria. Microsoft also undergoes auditing by an independent third-party auditor for SOC 2 and FedRAMP.

Microsoft data centers have FedRAMP High certification approved by DHS. Motorola Solutions is responsible for the security, confidentiality, and privacy of the data in its custody; accomplished through technical controls, consistent with the FBI-CJIS Security Policy, for the systems and data Motorola Solutions hosts for client agencies.

Microsoft provides physical security for the facility, communications infrastructure, firewalls, reliable internet, power conditioning, and HVAC, and is responsible for the confidentiality and privacy based on those physical security controls.

Microsoft Azure staff have no authorized logical access (GUI) to VehicleManager applications or physical/logical access to the unencrypted data. Motorola Solutions has Motorola Solutions managed encryption keys.

Auditing and accountability

Motorola Solutions' VehicleManager applications include built-in audit functions that allow an agency to view and audit user and transactional activity. The customer-available audit functionality is consistent with those identified in the FBI-CJIS Security Policy. It was designed to enable integrity audits to increase the probability that authorized users will conform to a prescribed pattern of behavior. It focuses on "events" and "content" as specified in Section Audit and Accountability controls AU-2, AU-3 and AU-3(1).

Motorola Solutions audits its staff activity to verify adherence to our acceptable use standards.

Auditing of the data center facilities, processes, policies, and procedures is accomplished by third-party auditing firms and represented in SOC 2 and FedRAMP ATO documentation is managed by Microsoft as a trusted cloud service provider partner of Motorola Solutions.

Note: SOC 2 reports are not an acceptable equivalent for the FBI-CJIS audit. Even though they provide valuable insight into security controls, they are not accepted in lieu of an audit by a CJIS agency.

The Microsoft Azure Data Center has undertaken the required third-party attestation for FedRAMP High certification issued by DHS. This rigorous assessment process is based upon NIST 800-53 controls.

Evaluation of compliance

Per the FBI-CJIS Security Policy, the responsibility for facility and product compliance evaluation lies with the contracting government agency. Motorola Solutions firmly believes that the Microsoft Azure Data Center meets the physical security controls criteria and satisfies compliance with the FBI-CJIS Security Policy. This belief is supported by several independent third-party reviews.

Motorola Solutions also develops and designs its applications and hardware offerings to be in compliance with the FBI-CJIS Security Policy. Motorola Solutions will agree to remediate any CJIS Security Policy related findings and develop a POAM to resolution.

Motorola Solutions, complements our process with its own rigorous information security requirements through a Market Readiness Assessment and Product Security Review during the design and deployment phases of product development which further enhances Motorola Solutions' products and achieving our goals of secure design and compliance.

FBI-CJIS certification vs. compliance

Motorola Solutions often receives the question: Are you CJIS Certified? The answer to that question is there is no certification body that can provide that designation. That is because different state, local, and federal agencies can have additional requirements or similar but different interpretations of security controls that can occur for each of their contract relationships, e.g., storing investigative, CHRI data vs. VehicleManager and data. The numerous variations of those circumstances would not enable any cloud service provider or SaaS offering to indicate that they are FBI-CJIS Security Policy compliant nationally.

When a contracting government agency (law enforcement or criminal justice agency) has a desire to enter into the contracted government relationship for particular government services involving CJI, such as using cloud services or SaaS applications, the providers cited—including Motorola Solutions—can only provide the government entity documentation related to the administrative, technical, physical and personnel policy controls to demonstrate the controls are in place.

This information then needs to be evaluated and validated by the government entity to determine whether what a service provider states meets compliance requirements and will withstand an FBI-CJIS Security Policy compliance audit. This analysis often occurs if CJI is within the scope of the project, with assistance from the FBI-CJIS Information Security Officer staff or state CJIS System Agency ISO to enable meeting the FBI-CJIS Security Policy compliance criteria. In this case, compliance would be required for the storage and access of VehicleManager and data, and to first determine whether the information is considered FBI-CJIS Security Policy-defined Criminal Justice Information. Then, determine what parts of the CJIS Security Policy apply – all or some.

The best way to resolve compliance is the evaluation of documentation, clear contracts and agreements that set expectations, vendor reputation, and trust are ultimately how information security control compliance is achieved, regardless of the standard body that sets the requirements. You need a vendor you can develop and sustain a trusted relationship with.

Encryption

All VehicleManager "Notes" or free-text fields stored "at rest" on VehicleManager servers are encrypted in accordance with FIPS 140-3. All data "in transit" transmitted is encrypted as well using Microsoft Server 2019 FIPS 140-3 certificates.

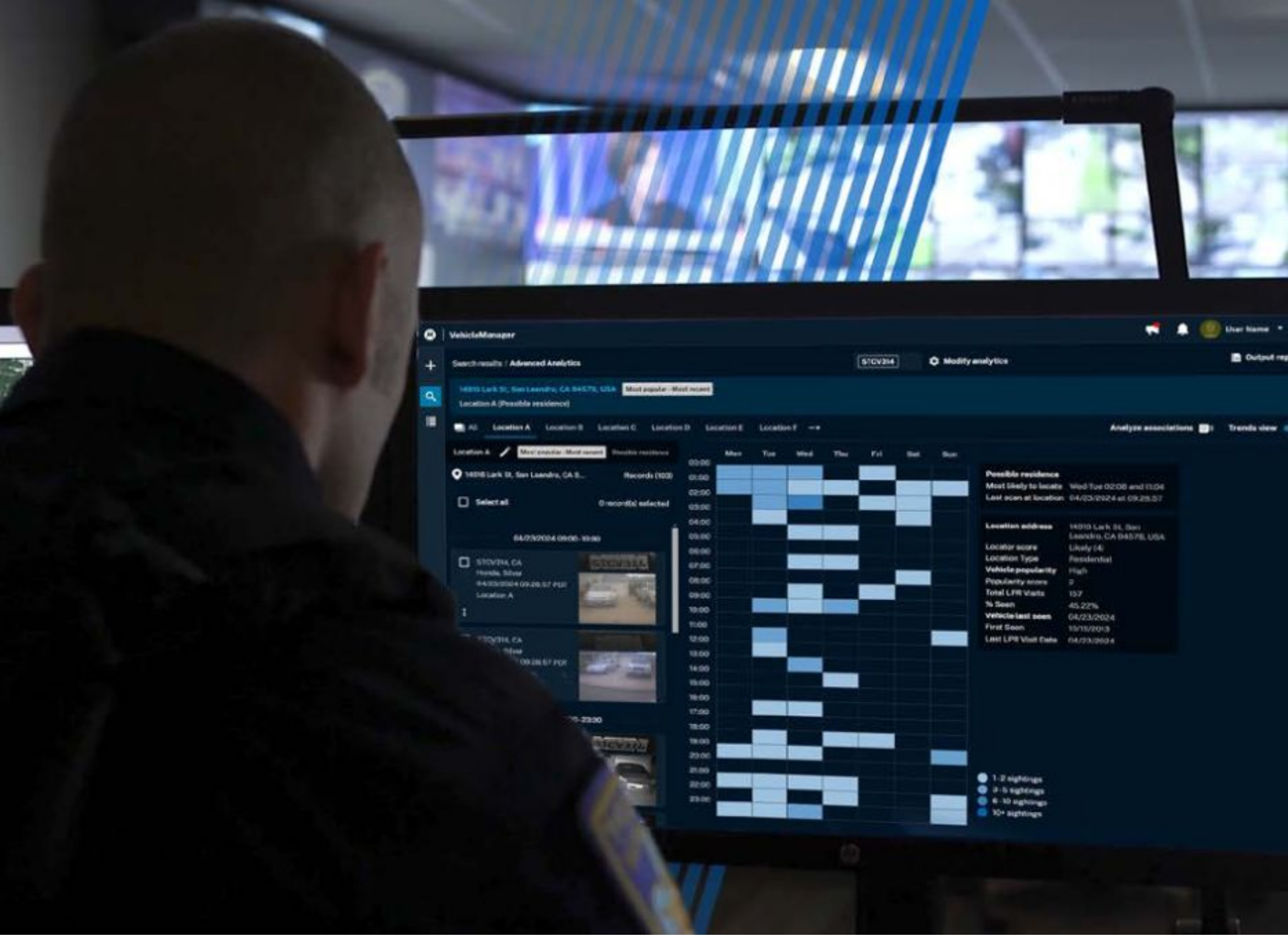
Within the system, there are several encryption modes. From the initial detection prior to the data being sent via https, the data is not encrypted. While the data is in transit https protocols are used; Motorola Solutions uses encryption for transmitted data to and from servers, deploying Secure Socket Layer/Transport Layer Security protocols.

That encryption protocol encrypts all data when it leaves the Car Detector Mobile software application VehicleManager software application. The VehicleManager application encrypts all responses sent to the end user and communicates over the Internet with a Motorola Solutions-managed Microsoft Azure Government Platform. The Microsoft Server employs FIPS 140-3-certified algorithms during data transit and at rest. The server(s) are used to manage traffic and to store and process data transactions on servers located in the Microsoft Azure Data Center.

Motorola Solutions uses Microsoft Windows Server 2019 and the Internet Information Services application module to enable the use of available encryption algorithms.

When a detection is matched to a hot-listed vehicle in the VehicleManager server (the hot list could be supplied by the client agency via SFTP), the data leaves the VehicleManager cloud environment and traverses via https back to the patrol vehicle that made the detection, which would then see the alert. As per the FBI-CJIS Security Policy, the patrol vehicle is considered a physically secure location and does not require encryption. However, the end user's free-text field, which could contain sensitive information, is encrypted to the CJIS FIPS standard.

Additional questions can be referred to your Motorola Solutions representative.



Questions?

Visit www.motorolasolutions.com/en_us/support or contact our 24-hour support staff at:

Web: customerhub.motorolasolutions.com

Phone: 1-800-MSI-HELP

For free online VehicleManager training, visit: learningcenter.motorolasolutions.com

For assistance with the topics covered in this guide or other Motorola Solutions Vehicle Intelligence products, please contact the Vehicle Image & Intelligence training group:
VIITraining@motorolasolutions.com

MOTOROLA SOLUTIONS

Motorola Solutions, Inc. 500 West Monroe Street, Chicago, IL 60661 U.S.A. motorolasolutions.com