

1 Abenicio Cisneros (SBN: 302765)
2 acisneros@capublicrecordslaw.com
3 Law Office of Abenicio Cisneros
4 2443 Fillmore St. #380-7379
5 San Francisco, CA 94115
6 707-653-0438

7 Sara B. Kohgadai (SBN: 319392)
8 legal@kohgadailaw.com
9 Law Office of Sara B. Kohgadai
10 P.O. Box 6201
11 Alameda, Ca 94501
12 (650) 636-7549

13 Attorneys for Petitioners and Plaintiffs
14 AARON SWARTZ DAY POLICE
15 SURVEILLANCE PROJECT and OPEN THE GOVERNMENT

16 **SUPERIOR COURT OF THE STATE OF CALIFORNIA**
17 **FOR THE COUNTY OF LOS ANGELES**

18 AARON SWARTZ DAY POLICE
19 SURVEILLANCE PROJECT, OPEN THE
20 GOVERNMENT
21
22 Petitioners and Plaintiffs,

23 vs.

24 CITY OF LONG BEACH POLICE
25 DEPARTMENT,
26
27 Respondent and Defendant.

) Case No.: **21STCP00627**
)
) **VERIFIED PETITION FOR WRIT OF**
) **MANDATE AND COMPLAINT FOR**
) **DECLARATORY RELIEF**
)
) **[California Constitution Article I § 3; Gov't**
) **Code § 6250, et seq.; Civ. Proc. Code §§ 1060,**
) **1085; Civ. Code § 3422; Civil Code §**
) **1670.9(c)]**
)
)
)

28 **INTRODUCTION**

1. Petitioners and Plaintiffs Aaron Swartz Day Police Surveillance Project (“ASDPSP”) and Open The Government (“OTG”) (hereinafter referred to together as “Petitioners”) hereby seek a

1 writ of mandate and declaratory relief to enforce the California Public Records Act (“CPRA”).

2 2. Petitioner OTG submitted one public records request on July 9, 2019 to City of Long
3 Beach Police Department (“Respondent,” “the City”) regarding Respondent’s solicitation,
4 acquisition, and use of facial recognition technology and software.

5 3. Petitioner ASDPSP submitted three public records requests, on December 26, 2018
6 and January 11, 2019, respectively, to the Respondent regarding Respondent’s use of (1) facial
7 recognition technology and software, (2) predictive algorithmic software packages designed to
8 anticipate criminal activities (“predictive policing”) and (3) cell phone interception devices (known
9 as “Stingrays”).¹

10 4. Respondent unlawfully claimed no documents existed in response to all of these
11 requests; Respondent claimed that it possessed no records responsive to any of Petitioners’ requests.
12 However, evidence indicates Respondent does, in fact, possess records related to its use of facial
13 recognition technology, Stingrays, and predictive policing. Whether Respondent refused to conduct
14 an adequate search for records, unreasonably misconstrued Petitioners’ requests, or intentionally
15 withheld responsive records, Respondent’s failure to provide responsive records in response to
16 Petitioner’s requests violated the CPRA.

17 5. The public has a significant interest in the disclosure of these records, which are
18 subject to the CPRA. Facial recognition technology, which identifies suspects by matching photos
19 with other databases such as driver’s license photos, implicates such serious privacy concerns its
20 use is banned already in major cities such as San Francisco, Portland, and Boston.² “Stingrays,” or
21 cell-site simulators, are cell phone surveillance devices that mimic cell phone towers and send out
22 signals to trick cell phones in the area into transmitting their locations and identifying information.³
23 Lastly, “predictive policing” is exactly what it sounds like: using computer systems to *predict* where
24 to deploy police or to identify individuals who are purportedly more likely to commit or be a victim
25 of a crime—before it happens.⁴ Respondent’s use of these technologies implicates serious

26 _____
27 ¹ Petitioner submitted other CPRA requests on or around that time which are not at issue in this Petition.

28 ² <https://nyti.ms/2ARmEqs>

³ <https://nyti.ms/2VG3Zr9>

⁴ <https://www.brennancenter.org/our-work/research-reports/predictive-policing-explained>

1 constitutional issues related to the scope of the public's right to privacy and limitations of the state's
2 ability to monitor and surveil members of the public. In essence, the CPRA was enacted to
3 empower the public to hold public agencies, like the Respondent, accountable against this kind of
4 abuse of power. Respondent is in clear violation of the law.

5 6. By this Petition and pursuant to the Code of Civil Procedure §§ 1085, *et seq.* and
6 Government Code §§ 6250, *et seq.*,⁵ Petitioners respectfully request from this Court: a writ of
7 mandate to command Respondent to immediately locate and disclose all non-exempt records
8 Petitioners requested and a declaration that the records Petitioners seek are non-exempt and subject
9 to mandatory disclosure.

JURISDICTION AND VENUE

10
11 7. This Court has jurisdiction under Gov't Code §§ 6258, 6259, Code of Civ. Proc.
12 § 1085, and Article VI, Section 10 of the California Constitution.

13 8. Venue is proper in this Court. The records in question, or some portion of them, are
14 situated in the County of Los Angeles, Gov't Code § 6259; the acts or omissions complained of
15 occurred in the County of Los Angeles, Code of Civ. Proc. § 393; and, Respondent is located in the
16 County of Los Angeles, Code of Civ. Proc. § 395.

PARTIES

17
18 9. Petitioner Aaron Swartz Day Police Surveillance Project ("ASDPSP"), is an
19 unincorporated association that regularly uses public records requests to collect and publish
20 information about the activity of law enforcement. In particular, ASDPSP works to ensure
21 transparency around what types of surveillance equipment law enforcement agencies maintain and
22 how that equipment is used. ASDPSP's previous public records requests have revealed important
23 information about law enforcement's use of surveillance equipment; for example, one request
24 revealed that the Sacramento Police Department shared data it collected from a license plate reader
25 with nearly 800 government agencies across the country, from the Federal Bureau of Investigations
26
27

28
⁵ Unless otherwise stated, all references to code sections are to the California Government Code.

1 (“FBI”) to Immigration and Customs Enforcement (“ICE”). ASDPS is a member of the public
2 within the meaning of §§ 6252(b)-(c).

3 10. Petitioner Open The Government (“OTG”) is a non-partisan nonprofit which focuses
4 on government transparency and accountability. Open The Government filed this CPRA request as
5 part of its project on facial recognition technology use by law enforcement. OTG is a member of the
6 public within the meaning of §§ 6252(b)-(c).

7 11. Respondent, the City of Long Beach Police Department, is a local public agency
8 within the meaning of §§ 6252(a), (d).

9
10 **FACTUAL ALLEGATIONS**

11 **Respondent Denied Access to Records by Incorrectly Claiming No Records Exist**
12 **Requests No. 1 and No. 2 – Facial Recognition Software Requests by ASDPSP and OTG**

13 12. On December 26, 2018, Petitioner ASDPSP sent a public records request for records
14 containing information related to the use and number, if any, of facial recognition software or facial
15 recognition-enabled equipment in place with Respondent. The scope of the request (“Request No.
16 1”) also included records reflecting:

- 17 a. whether any software has been purchased or if services are performed by outside
18 contractors for Respondent;
- 19 b. any pilot or testing programs and possible or planned acquisition of facial
20 recognition software packages, facial recognition-enabled equipment or service
21 agreements;
- 22 c. any existing or proposed usage policies regarding the use of facial recognition
23 software or facial recognition-enabled equipment, such as protocols, training
24 documents, data storage procedures and prohibited activities; and
- 25 d. any current or past litigation involving or referencing Respondent involving the
26 use of facial recognition software or facial recognition-enabled equipment.

1 13. The applicable period of Request No. 1 is January 1, 2015 to the date of the Request.
2 A true and accurate copy of this request is attached to this petition in *Exhibit A*.⁶

3 14. Respondent had an obligation under the CPRA to provide Petitioner a determination
4 of disclosability as to Request No. 1 within 10 days, approximately January 4, 2019. Respondent
5 did not meet this statutory deadline nor requested a timely extension to provide Respondent a
6 determination of disclosability.

7 15. On February 6, 2019, Respondent informed Petitioner that “it is not in possession of
8 records responsive to this request.” A true and accurate copy of this correspondence is attached to
9 this petition in *Exhibit A*.

10 16. On July 9, 2019, Petitioner OTG submitted a request to Respondent regarding its
11 solicitation, acquisition, and use of facial recognition technology (“Request No. 2”). The scope of
12 the search was limited to records produced from January 1, 2017 to the date of the request. A true
13 and accurate copy of this correspondence is attached to this petition in *Exhibit B*.

14 17. On July 12, 2019, Respondent responded to Request No. 2 in two emails. First,
15 Respondent acknowledged Petitioner OTG’s request and then in a separate email informed that it
16 “does not have any responsive records related to your inquiry.” A true and accurate copy of these
17 correspondence is attached to this petition in *Exhibit B*.

18 18. On July 18, 2019, Petitioner OTG sent a follow up email to the Respondent
19 regarding its determination that no responsive documents exist. Petitioner OTG requested that
20 another search be conducted. A true and accurate copy of this correspondence is attached to this
21 petition in *Exhibit B*.

22 19. Respondent’s claim that it does not have any responsive records is false and
23 improper. In October 2020, in response to another public records request⁷, Respondent made public
24 that it has been using the Los Angeles County Regional Identification System (“LACRIS”) facial
25 recognition program since 2010. In the applicable period for Requests No. 1 and No. 2 (2015-2019),
26

27 ⁶ All correspondence between the parties are obtained from Muckrock.com and are true and accurate copies. MuckRock
28 is a non-profit, collaborative news site that provides a repository of original materials and tools to aid journalists,
researchers, activists, and citizens in informing communities.

⁷ That request was made by a third-party and is not subject to this suit.

1 Respondent conducted 1077 facial recognition searches. A true and accurate copy of this
2 correspondence is attached to this petition in *Exhibit C*.

3 20. LACRIS developed a policy intended for “any authorized agency personnel
4 accessing the system.” A true and accurate copy of the policy is attached to this petition in *Exhibit*
5 *C*. The LACRIS policy specifically states that agencies outside of the LA County Sherriff’s office
6 may request a facial recognition search “only if the LACRIS Face Recognition Search Request
7 Form is completed.” A copy of the Search Request Form is included in the template policy offered
8 to agencies using the LACRIS system. (*See Facial Recognition Policy Template, Exhibit C* at p. 6).
9 The form can also be obtained by emailing lacrishd@lasd.org and, in order for a search to be
10 performed, requires the following information:

- 11 e. Requesting Agency;
- 12 f. Requester Name;
- 13 g. Requester Phone Number;
- 14 h. Requester Email;
- 15 i. Requester Signature;
- 16 j. Requester Date;
- 17 k. Reason for Search;
- 18 l. Case/File Number; and
- 19 m. Number of Images Submitted.

20 21. For Petitioners’ requests during the applicable period, there should be as many as
21 1077 responsive records with the above information, in addition to any other responsive records
22 with Respondent may possess.

23 **Request No. 3 – “Stingrays” Request by ASDPSP**

24 22. On January 11, 2019, Petitioner ASDPSP sent a public records request for records
25 containing information related to the use and number, if any, of IMSI-catcher or cell phone
26 interception devices (commonly called “Stingrays”) owned by or available for use by Respondent
27 via collaborative agreements, including the name of the department or agency that made Stingray
28 devices available. The scope of the request (“Request No. 3”) also included records reflecting:

- 1 a. any possible or planned acquisition of an IMSI-catcher device, any existing or
2 proposed usage policies regarding the use of cell phone interception technology
3 such as protocols, training documents and data storage procedures; and
4 b. any current or past litigation involving or referencing Respondent involving the
5 use of cell phone interception technology.

6 23. The applicable period for Request No. 3 is January 1, 2015 to the date of the
7 Request. A true and accurate copy of this request is attached to this petition in *Exhibit D*.

8 24. Respondent had an obligation under the CPRA to provide Petitioner a determination
9 of disclosability as to Request No. 3 within 10 days, approximately January 25, 2019. Respondent
10 did not meet this statutory deadline nor requested an extension to provide Respondent a
11 determination of disclosability.

12 25. On February 22, 2019, Respondent responded to Request No. 3, simply saying that
13 “it is not in possession of records responsive to this request.” A true and accurate copy of this
14 correspondence is attached to this petition in *Exhibit D*.

15 26. Despite Respondent’s claim that it is not in possession of records responsive to this
16 request, there is ample evidence that it does. For instance, Between October 2015 and
17 approximately November 2018, the City was involved in litigation regarding a CPRA request for,
18 among other things, agreements about Stingray products. *See Michelle Olson v. The City of Long*
19 *Beach et. al*, Los Angeles County Superior Court, Case No. BS158621 (2015). These records are
20 clearly responsive to Request No. 3, specifically ones reflecting “any current or past litigation
21 involving or referencing Respondent involving the use of cell phone interception technology.” *See*
22 *Exhibit D*.

23 27. In March 2016, Respondent created a draft policy related to its use of the Stingrays
24 called “Special Order: Cellular Communications Interception Technology.” Petitioner obtained this
25 draft copy from the City of Long Beach website.⁸ A true and accurate copy of this policy is attached
26 to this petition in *Exhibit E*.

27 _____
28 ⁸ <http://www.longbeach.gov/globalassets/police/media-library/documents/departments-and-bureaus/departments-and-bureaus/investigations-bureau/cell-site-simulator-policy--3-31-16-/>

1 **Request No. 4 – Predictive Policing Request by ASDPSP**

2 28. On January 11, 2019, Petitioner sent a public records request for records containing
3 information related to the use and number, if any, of Predictive Algorithmic software packages or
4 service agreements designed to anticipate criminal activities in place with Respondent’s agency.
5 The scope of the request (“Request No. 4”) also included records reflecting:

- 6 c. whether software has been purchased or if services are performed by outside
7 contractors for the Respondent;
- 8 d. any possible or planned acquisition of Predictive Algorithmic software packages
9 or service agreements, including any existing or proposed usage policies
10 regarding the use of Predictive Algorithmic software packages or service
11 agreements, such as protocols, training documents, data storage procedures and
12 prohibited activities; and
- 13 e. any current or past litigation involving or referencing Respondent involving the
14 use of Predictive Algorithmic Software Packages or Service Contractors.

15 29. The applicable period for Request No. 4 is January 1, 2015 to the date of the
16 Request. A true and accurate copy of this request is attached to this petition in *Exhibit F*.

17 30. Respondent had an obligation under the CPRA to provide Petitioner a determination
18 of disclosability as to Request No. 4 within 10 days, approximately January 25, 2019. Respondent
19 did not meet this statutory deadline nor requested an extension to provide Respondent a
20 determination of disclosability.

21 31. On February 8, 2019, Respondent informed Petitioner that “it is not in possession of
22 records responsive to this request.” A true and accurate copy of this correspondence is attached to
23 this petition in *Exhibit F*.

24 32. Respondent’s claim that it is not in possession of records responsive to this request is
25 objectively false. There is, in fact, evidence that Respondent entered into agreements in which
26 predictive policing “services are performed by outside contractors for the Respondent.” This means
27 Respondent was in possession of documents responsive to this request when it was made. For
28 instance, in February 2014, Respondent sought approval from the California Governor’s office to

1 continue its current contract with Systems Research and Application International
2 (“SRA”) for a professional Intelligence Analyst to evaluate and analyze criminal
3 intelligence information collected by the [Respondent] and collaborating agencies to
4 determine the credibility, reliability and pertinence of the information. Utilizing
5 SRA’s proprietary intelligence software, Orion, the Intelligence Analyst prepares
6 reports based on interpretation of intelligence information, participates in meetings
7 with Department personnel and other law enforcement agencies and assists in the
8 planning activities of the department’s intelligence section.”

9
10 33. The request specifies that it is “an ongoing, multi-year project that previously
11 received funding through the UASI 2011 grant program.” Respondent’s request, dated February 12,
12 2014, is for approval of a of \$202,500.00 budget paid at \$14,000.00 a month, which amounts to
13 approximately fifteen months. A true and accurate copy of this correspondence is attached to this
14 petition in *Exhibit G*.

15
16 34. In June 2019, Respondent submitted a “Vendor Selection Form” requesting purchase
17 authority to continue services with SRA International Inc. The form specifies that three analysts
18 “have been working with the Police Department for several years.” The analysts’ services include
19 compiling data which “assist officers and detectives in taking a strategic, targeted approach
20 essential to the criminal investigation and prosecution of possible suspects.” A true and accurate
21 copy of this form is attached to this petition in *Exhibit G*.

22
23 35. In August 2020, the City published a 112-page initial report regarding the City’s
24 “Racial Equity and Reconciliation Initiative.” On pages 36 and 56 of the report, regarding strategies
25 to “Redesign police tactics, training, retention, and accountability,” the City includes an action item
26 to “explore the *practice of facial recognition technology and other predictive policing models* and
27 their disproportionate impacts on people of color by reviewing evidence- based practices.”
28 (emphasis added). A true and correct excerpt of relevant pages of the 112-page report is attached to
this petition in *Exhibit G*.

FIRST CAUSE OF ACTION:
VIOLATION OF THE CALIFORNIA CONSTITUTION ARTICLE 1, § 3(b)

36. Petitioners incorporate herein by reference the allegations of paragraphs 1 through 36
above, as if set forth in full.

37. The California Constitution provides an independent right of access to government

1 records: “The people have the right of access to information concerning the conduct of the people’s
2 business, and, therefore, the meetings of public bodies and the writings of public officials and
3 agencies shall be open to public scrutiny.” Cal. Constitution, Art. 1 § 3(b)(1). This provision was
4 adopted by the voters in 2004 because, as the ballot argument supporting the measure states, when
5 Californians asked questions of their government, they increasingly found “that answers are hard to
6 get.” The constitutional provision is intended to reverse that trend.

7 38. Respondent’s denial of access to disclosable records in Respondent’s possession that
8 are responsive to Petitioners’ public records requests violated Article 1, Section 3(b) of the
9 California Constitution.

10 **SECOND CAUSE OF ACTION:**
11 **PETITION FOR WRIT OF MANDATE AND DECLARATORY RELIEF PURSUANT TO**
12 **THE CALIFORNIA PUBLIC RECORDS ACT, GOV’T CODE § 6250, et seq.**

13 39. Petitioners incorporate herein by reference the allegations of paragraphs 1 through 39
14 above, as if set forth in full.

15 **General Principles of the California Public Records Act**

16 40. Under the California Public Records Act, § 6250 *et seq.*, all records that are
17 prepared, owned, used, or retained by any public agency and that are not subject to the CPRA’s
18 statutory exemptions to disclosure must be made publicly available for inspection and copying upon
19 request. §§ 6253(a)-(b).

20 41. In enacting the CPRA, the legislature recognized that:

21 A requester, having no access to agency files, may be unable to
22 precisely identify the documents sought. Thus, writings may be
23 described by their content. The agency must then determine whether it
24 has such writings under its control and the applicability of any
25 exemption. An agency is thus obliged to search for records based on
26 criteria set forth in the search request.

27 *Cal. First Amend. Coalition v. Superior Court*, 67 Cal. App. 4th 159, 165-66 (1998); *see* § 6253(b).

28 42. When a member of the public submits a records request to an agency, the agency is
given ten days to determine whether the request seeks copies of disclosable public records in the
possession of the agency and must notify the requestor of such determination and the reasons

1 therefor. § 6253(c). The agency must make a reasonable effort to search for and locate requested
2 records. *See Comm. Youth Athletic Ctr. v. City of National City*, (2013) 220 Cal.App.4th
3 1385,1417–1418; *Cal. First Amend. Coalition v. Superior Court*, *supra*, 67 Cal.App.4th at 166.

4 43. The CPRA also requires the government to “assist the member of the public [to]
5 make a focused and effective request that reasonably describes an identifiable record or records” by
6 taking steps to “[a]ssist the member of the public to identify records and information that are
7 responsive to the request or to the purpose of the request, if stated.” § 6253.1. An agency that
8 receives a request must also “[p]rovide suggestions for overcoming any practical basis for denying
9 access to the records or information sought.” *Id.*

10 44. Whenever it is made to appear by verified petition to the Superior Court of the
11 county where the records or some part thereof are situated that certain public records are being
12 improperly withheld from a member of the public, the Court shall order the officer or person
13 charged with withholding the records to disclose the public record or show cause why he or she
14 should not do so. § 6259(a). That section authorizes litigation where a public agency employs
15 means to effectively deny all access to public records. *Galbiso v. Orosi Public Utility Dist.*, (2008)
16 167 Cal. App. 4th 1063, 1088. The Court shall decide the case after examining the record in camera
17 (if permitted by the Evidence Code), papers filed by the parties, and any oral argument and
18 additional evidence as the Court may allow. § 6259(a). If the Court finds that the failure to disclose
19 is not justified, it shall order the public official to make the record public. § 6259(b).

20 45. A petitioner prevails under the CPRA where the petitioner shows that an agency
21 unlawfully denied access to records. *Comm. Youth Athletic Ctr v. City of National City*, *supra*, 220
22 Cal.App.4th at 1446-1447. An agency is not protected from liability merely because the denial of
23 access was due to the agency’s internal logistical problems or general neglect of its duties. *Id.*

24 46. Public policy favors judicial enforcement of the CPRA. The CPRA contains a
25 mandatory attorney’s fee provision for the prevailing plaintiff. § 6259(d). The purpose of the
26 provision is to provide “protections and incentives for members of the public to seek judicial
27 enforcement of their right to inspect public records subject to disclosure.” *Filarsky v. Super. Ct.*, 28
28 Cal.4th 419, 427 (2002).

1 **Respondent Violated the CPRA by Improperly Withholding Responsive Records**

2 47. Respondent’s unlawful withholding of the requested public records violates the
3 CPRA. The CPRA expressly provides that “access to information concerning the conduct of the
4 people’s business is a fundamental and necessary right of every person in this state.” Gov. Code §
5 6250. The purpose is to “give the public access to information that enables them to monitor the
6 functioning of their government.” *CBS, Inc. v. Block* (1986) 42 Cal.3d 646, 651; *Times Mirror Co.*
7 *v. Superior Court* (1991) 53 Cal.3d 1325, 1350. Monitoring police use of facial recognition
8 software, cell site interceptors, and predictive policing falls squarely within the legislative purpose
9 of empowering the public to hold the government accountable.

10 48. Here, Respondent withheld access to responsive records by unlawfully and
11 improperly denying the *existence* of those records. Even where Petitioner OTG requested a
12 secondary, follow up search, Respondent ignored the request. This representation that no
13 responsive records exist is a clear violation of the statute.

14 49. Further, by incorrectly claiming no responsive records exist, Respondent interfered
15 with Petitioners’ right to seek relief through court intervention. Petitioners only recently obtained
16 documents verifying a violation of the CPRA, which prompted this suit. Delayed access to relief
17 makes Respondent’s incorrect response even more egregious; the public should be able to rely on
18 the agency’s word as to whether records exist. Instead, Respondent forced Petitioners to conduct its
19 own search in order to seek relief.

20 50. Respondent conducted over 1000 facial recognition searches yet claimed to have no
21 records related to its use of facial recognition technology. Respondent was named and involved in
22 litigation that lasted over two years regarding its use of Stingray technology and failed to disclose
23 any records related to that litigation. Respondent itself addressed its use of predictive policing in an
24 attempt to offer “Racial Equity and Reconciliation,” but denied that any records regarding its use of
25 such software existed at all. Thus, with no faith that Respondent can be trusted to provide
26 transparency, Petitioners seek judicial intervention to enforce its rights under the CPRA and to
27 ensure Respondent’s compliance with its statutory obligations.

28 51. In conclusion, Respondent’s unlawful denial of access to public records represents

1 the very reasons the legislature enacted the CPRA. By failing to produce even one of these records,
2 Respondent is maintaining a shroud of secrecy around records related to police use of surveillance
3 technology, which are subject to the CPRA. Respondent's complete denial of access violates not
4 only the letter of the CPRA, but also its spirit. The CPRA is predicated on the principle that:

5 Openness in government is essential to the functioning of democracy. Implicit in
6 the democratic process is the notion that government should be accountable for its
7 actions. In order to verify accountability, individuals must have access to
8 government files. Such access permits checks against the arbitrary exercise of
9 official power and secrecy in the political process.

10 *Int'l Fed. Of Professional and Technical Engineers, Local 21, AFL-CIO v. Super. Ct.*, 42 Cal.4th
11 319, 328-39 (2007) (internal quotations omitted). Respondent's refusal to comply with the CPRA
12 and its evasion of the law is incompatible with openness in government and government
13 accountability; instead, these are the very manifestations of "the arbitrary exercise of official
14 power" and of "secrecy in the political process" the CPRA is intended to protect against. By its
15 conduct, Respondent obstructs public access to vital information and withholds from the public any
16 opportunity to either verify government accountability or to check against the abusive exercise of
17 official power. Transparency and accountability are especially imperative when the requested
18 records implicate potential violations of one's right to privacy, surveillance, and unlawful search
19 and seizure in criminal cases. In so doing, Respondent frustrates the democratic process itself.

20 **A Writ of Mandate and Declaratory Relief are Appropriate**

21 52. Respondent has a clear, present, ministerial duty to comply with the California
22 Constitution and Government Code § 6250, *et seq.*

23 53. Petitioners are entitled to seek relief due to violations of the CPRA. § 6258.

24 54. Petitioners has performed all conditions precedent to filing this petition. There are no
25 administrative exhaustion requirements under Government Code § 6250, *et seq.*

26 55. An actual controversy exists between the parties concerning whether Respondent
27 engaged in conduct that violates the statutory requirements of the CPRA and the California
28 Constitution. A judicial determination to resolve this actual controversy is necessary and
appropriate as soon as possible.

1 56. Petitioners have no plain, speedy, adequate remedy in the ordinary course of law
2 other than the relief sought in this petition. *See* Code of Civil Procedure § 1086.

3 **PRAYER FOR RELIEF**

4 WHEREFORE, Petitioners pray for judgment as follows:

- 5 1. For issuance of a writ of mandate directing Respondent to immediately locate and
6 provide Petitioners with all requested records, except those records that the Court
7 determines may lawfully be withheld;
- 8 2. For a declaration that Petitioners' requests sought records subject to mandatory
9 disclosure; that Petitioners' requests imposed a duty upon Respondent to promptly
10 provide public, non-exempt records in response; and that Respondent failed that duty;
- 11 3. For Petitioners to be awarded reasonable attorneys' fees and costs; and
- 12 4. For such other and further relief as the Court deems proper and just.

13 Dated: February 15, 2021

14 Respectfully submitted,

15 

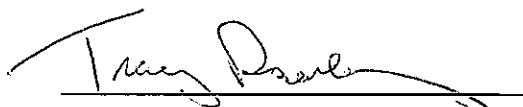
16
17 SARA B. KOHGADAI
18 Attorney for Petitioners and Plaintiffs

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

VERIFICATION

I, TRACY ROSENBERG, am a co-founder and member of the AARON SWARTZ DAY POLICE SURVEILLANCE PROJECT, a Petitioner and Plaintiff in this action. I have read the foregoing Petition for Writ of Mandate and Complaint for Declaratory Relief, and I know the contents thereof. The same is true of my own knowledge, except as to those matters which are therein alleged on information and belief, and, as to those matters, I also believe them to be true.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct. Executed on this the 16 day of February, 2021 in ALBANY, CALIFORNIA.



TRACY ROSENBERG
On behalf of AARON SWARTZ DAY
POLICE SURVEILLANCE PROJECT

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

VERIFICATION

I, LISA ROSENBERG, am the executive director of OPEN THE GOVERNMENT, a Petitioner and Plaintiff in this action. I have read the foregoing Petition for Writ of Mandate and Complaint for Declaratory Relief, and I know the contents thereof. The same is true of my own knowledge, except as to those matters which are therein alleged on information and belief, and, as to those matters, I also believe them to be true.

I declare under penalty of perjury under the laws of the State of California that the foregoing is true and correct. Executed on this the 25 day of February, 2021 in Washington DC.



LISA ROSENBERG
On behalf of OPEN THE GOVERNMENT

Exhibit A

From: Aaron Swartz Day Police Surveillance Project

12/28/2018

Subject: California Public Records Act Request: CALIFORNIA PUBLIC RECORDS REQUEST – FACIAL RECOGNITION SOFTWARE (Long Beach Police Department)

Portal

To Whom It May Concern:

Pursuant to the California Public Records Act, I hereby request the following records:

Per the California Public Records Act (Govt. Code 6250-6270), I am writing to request the following information from your office for the period January 1, 2015 to the date of this letter.

Number, if any, of Facial Recognition software or Facial Recognition-enabled equipment in place with this department or agency. Please specify if software has been purchased or if services are performed by outside contractors for the department or agency. Please include pilot or testing programs within the scope of this request

Any documents or correspondence during the period encompassing this request regarding possible or planned acquisition of Facial Recognition software packages, Facial Recognition-enabled equipment or service agreements.

Any existing or proposed usage policies regarding the use of Facial Recognition software or Facial Recognition-enabled equipment, including protocols, training documents, data storage procedures and prohibited activities.

Any current or past litigation involving or referencing this department or agency involving the use of Facial Recognition software or Facial Recognition-enabled equipment.

Please notify me when this information is available .

Thank you for your attention to this request and for your prompt reply within 10 days.

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 10 calendar days, as the statute requires.

Sincerely,

Aaron Swartz Day Police Surveillance Project

From: Long Beach Police Department

02/06/2019

Subject: [Records Center] PRA Request :: P001658-122818

Portal

--- Please respond above this line ---

Hello-
The Long Beach Police Department is not in possession of records responsive to this request.
Thank you,
Sergeant J. Brearley
Long Beach Police Department

Exhibit B

From: Freddy Martinez

07/09/2019

Subject: California Public Records Act Request: Facial Recognition - Long Beach (CA)

Portal

To Whom It May Concern:

Pursuant to the California Public Records Act, I hereby request the following records:

Records and materials related to the solicitation, acquisition, and use of face recognition technology and related software and services.

This software or services may be provided by Rekognition, Face++, and FaceFirst; this request is applicable to these and any other company providing facial recognition services under consideration or contract with this agency.

Responsive materials include but are not limited to:

- Agreements: contracts (including non-disclosure agreements), licensing agreements, nondisclosure agreements
- Bid records: Requests For Proposal (or equivalent calls for bids), sole source or limited source justification and approval documentation, documentation of selection, and other materials generated in the consideration and selection of the technology in question
- Company relations and communications: records related to meetings or follow-up actions with any vendors, companies, or other private entities marketing face recognition to this agency for immigration, intelligence, law enforcement, or other use.
- Financial records: purchase orders, invoices, and other memoranda and documentation.
- Marketing records: All marketing materials - unsolicited, requested, or otherwise - acquired from vendors of face recognition technology
- Policy records: any policy directives, guidance documents, memoranda, training materials, or similar records governing the use of face recognition technology for immigration, law enforcement, or other purposes. Any memoranda of understanding between this agency and other agencies to share data, access remote systems or other forms of information sharing with external agencies.
- Training records: training material governing the use, sharing, or access to any related data related to or collected by the face recognition software/technology, including the legal standard that is required before using the technology. Documents, should they exist, about training for bias in the use of facial recognition technology.
- Use and function records: Materials that describe the function of the software considered or in use by this agency, including emails, handouts, PowerPoint presentations, advertisements, or specification documents.
- Validation and accuracy: Records, reports, audits, and other documents sufficient to describe validation, accuracy, reliability, and policy compliance of the system.

Please limit the search to records produced from January 1, 2017 – present. Please include in your search as responsive records: communications, memorandums, background papers, meeting minutes, email exchanges, or presentation materials. If your office has questions about this request, please feel free to direct them to the address associated with this request or call the MuckRock office at 617-299-1832.

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 10 calendar days, as the statute requires.

From: Long Beach Police Department

02/24/2019

Subject: [Records Center] PRA Request :: P001723-011019

Portal

--- Please respond above this line ---

Hello,
The Long Beach Police Department does not have any responsive records to provide you relating to your public records request.
Thank you.

To monitor the progress or update this request please log into the Long Beach Police Department Records Center (https://u8387778.ct.sendgrid.net/wf/click?upn=xSfKPyHO1-2F4Mny2NCLJVuhdbZHEk-2Bsyll7bnblmbcqJ6vAS-2BVh-2FVnJ9-2FKr3pzcJ08SxgYyKxobhWdBnAbaa57eneR35YPo6Mfj3OvrS-2F1xK3nzcQU-2BaWOHNGLSvcxYVA_5WrN9CVaRxPioLigtDCsN0NP1CiG3jK0j5IKX-2BsdP2AGBMjak3Y1AP6h90GalJJD21090-2B2L-2Bs6yay2tiezqGBPS0Na9tLbW-2FOWytXaqBDEWkaNoZBDWoxwPTRd7XjqscbmmSedsSKuqXABuJHLcB-2FWNKK-2B5B3cxzePy-2FXj-2FjhwXPs4FryZKL-2Fz9HdjyYY1daLD1dWpYaUL4d2-2BZXx9OU3MD22UkKKuf5kHHz9MXCYkt3O4ZPuvBflSttgCQfWbIDB4xvW3fc9ckuLN5JKV0t-2FFLWSM7j8oMWMH2d3jwgnIOV3EbKa8OhaZk4yPgFQuWzAxkPn6T4twp-2B9Rlpp8oWNwUQ1tBRGeYtuhoX-2FPr7XlzxJacMNFUGm8Pq22FlqluFMmjEJVwldYbWdQrJWBia-3D-3D)

From: Freddy Martinez

07/18/2019

Subject: RE: California Public Records Act Request #P002601-070919

Mail

To Whom It May Concern:

I am appealing my records request that was sent on July 9, 2019 relating to the Long Beach Police Department's use and solicitation of facial recognition software. I do not believe that a reasonable search was conducted with regard to my request and would like for the search to be run again.

As stated in my last email, I am also looking for any communication regarding the potential implementation of facial recognition software. This includes any unsolicited proposals or marketing material from facial recognition companies to the Long Beach Police Department.

Thank you in advance for your anticipated cooperation in this matter.

Sincerely,
Freddy Martinez

Exhibit C



Sara B. Kohgadai Law Office <legal@kohgadailaw.com>

Fwd: [Records Center] PRA Request :: P005179-092820

Sara B. Kohgadai Law Office <legal@kohgadailaw.com> Sun, Jan 24, 2021 at 10:02 PM
To: "Sara B. Kohgadai Law Office" <legal@kohgadailaw.com>

From: Long Beach Police Department Public Records Center
<longbeachcapd@mycusthelp.net>
Subject: [Records Center] PRA Request :: P005179-092820
Date: October 21, 2020 at 3:42:26 PM PDT
To: "gdbuhl@gmail.com" <gdbuhl@gmail.com>

Attachments:
[vigilant_facesearch_dates-times.pdf](#)

--- Please respond above this line ---



Hello Mr. Buhl,

Please see below for the correspondence to the items being requested pertaining to the three facial recognition programs used by the Long Beach Police Department.

Showing the number of users.

LACRIS: LBPD has 38 trained and authorized users

Vigilant: Program is no longer in use and not authorized for use at this time; no current authorized users (26 users have made inquiries in this system prior to access being shut off)

Clearview: Program is not in use and is not a company we ever had a contract with so we do not have access to how many people have ever used the program. We have no current authorized users.

The timeframe of use.

LACRIS - 1/13/2010 – Present

Vigilant – 4/17/2018 – 9/28/2020

Clearview – Unknown

The number of inquiries or submitted photos.

LACRIS:

2010 78 searches

2011 62 searches

2012 17 searches

2013 65 searches

2014 12 searches

2015 50 searches

2016 126 searches

2017 185 searches

2018 94 searches

2019 622 searches

2020 2688 searches (as of 10/16/20)

Total Searches 3999

Vigilant:

2018 – 89 Searches

2019 – 53 Searches

2020 – 148 Searches

Clearview: Information not available and is not tracked

Number of inquiries where potential matches were made.

LACRIS, Vigilant and Clearview: unknown, this information is not tracked.

Any information you have regarding the number of matches returned per inquiry or accuracy percentages or**ratings.**

LACRIS: When conducting a facial recognition search, a candidate list of 243 images is returned for each search. Facial recognition only provides candidates for investigative leads. The templates returned are in a ranking order, not a percentage of likelihood.

Vigilant: Information is not tracked

Clearview: Unknown

The date of inquiries made, and the specific crimes being**Investigated.**

LACRIS: Not Available – LA County unable to provide and we cannot run a search in house. Type of Crime is not tracked.

Vigilant: Type of crime being investigated is not tracked. [See attached list for inquiry dates.](#)

Clearview: Unknown

Thank you.

To monitor the progress or update this request please log into the [Long Beach Police Department Records Center](#)





LACRIS
LOS ANGELES COUNTY
REGIONAL IDENTIFICATION SYSTEM

LACRIS Facial Recognition Policy

LACRIS Facial Recognition Policy

A. Preface

B. Purpose Statement

C. Digital Mugshot System

D. Authority

E. Training

F. Auditing

G. Accountability and Enforcement

H. Face Search Request

A. Preface

The Los Angeles County Regional Identification System (LACRIS) has developed a policy that shall be used as the foundation for those agencies that choose to utilize the LACRIS facial recognition system. LACRIS is responsible for the governance, oversight, and operation of its facial recognition system and program which it provides to the law enforcement community inside the county of Los Angeles. This policy is intended for LACRIS personnel and any authorized agency personnel accessing the system. Agencies are encouraged to implement their own policy which complements and does not contradict the LACRIS policy.

B. Purpose Statement

Facial recognition technology involves the ability to examine and compare significant characteristics of the human face. This technology can be a valuable tool to create investigative leads, reduce an imminent threat to health or safety, and help in the identification of deceased persons or persons unable to identify themselves. This facial recognition application supports the investigative efforts of law enforcement and public safety agencies within Los Angeles County resides in the County's Digital Mugshot System (DMS).

C. Digital Mugshot System

Established October 1, 2009, the DMS is the County's repository of all criminal mugshots. It only contains criminal mugshots which are supported by a fingerprint comparison conducted by the California Department of Justice (DOJ). Section 13150 of the California Penal Code requires at time of booking, a subject's fingerprints, photos, and arrest data to be collected, stored, and reported to the DOJ. This information is maintained in the DMS and used for investigative purposes by law enforcement personnel.

D. Authority

All deployments of the DMS facial recognition application are for official use only and considered law enforcement sensitive. The DMS is subject to the DOJ regulations placed on users and the dissemination of Criminal Offender Record Information (CORI).

The California Attorney General's Office issued Information Bulletin 13-04-CJIS, which provides guidance to law enforcement personnel on "right to know" and "need to know" access to CORI for investigative and official business purposes. This Bulletin, while not legally binding, references the relevant statutory codes (see below) that must be adhered to by users accessing the system.

Section 11075 of the California Penal Code (PC) defines CORI as "records and data compiled by criminal justice agencies for purposes of identifying criminal offenders and of maintaining as to each such offender a summary of arrests, pretrial proceedings, the nature and disposition of criminal charges, sentencing, incarceration, rehabilitation, and release."

Section 11105 of the PC identifies who has access to DOJ CORI and under what circumstances it may be released. Access is based upon the "right to know" and the "need to know." The "right to know" is defined as "authorized access to such records by statute" and the "need to know" is defined as "the information is required for the performance of official duties or functions." Title 11, sections 703 (d) and 707 (b) of the California Code of Regulations (CCR) require agencies to conduct record clearances on all personnel hired who have access to CORI. The unauthorized access and misuse of ACHS and CORI violates state statutes and may adversely affect an Individual's civil rights. Sections 11140 through 11144 of the PC prescribe penalties for misuse of state summary criminal history information, while PC sections 13301 through 13304 prescribe penalties for misuse of local summary criminal history information. Sections 6200 and 6201 of the Government Code prescribe the penalties for the misuse of various government records, which include CORI. Section 502 of the PC prescribes the penalties relating to computer crimes.

Title 11, section 707 (c) of the CCR requires each authorized agency to maintain, and make available for inspection, an audit trail for a period of three years from the date of release of CORI from an automated system. The audit trail must provide an agency with sufficient information to substantiate the "need to know."

Section 11078 of the PC requires each agency, holding or receiving CORI in a computerized system, to maintain a listing (audit trail) of the agencies to which it has released or communicated CORI. Also, pursuant to section 707 (c) of the CCR, this audit trail must be maintained for a period of three years and must include any routine releases.

All code sections, which may be amended from time to time, are current as of the time of the implementation of this policy.

E. Training

LACRIS provides training to those investigators who have requested and are authorized to access the facial recognition application for official use. Personnel who are authorized by their participating agency may utilize the facial recognition application *only* after they have been successfully trained by LACRIS personnel. Facial recognition Training provided by LACRIS meets the FBI's Criminal Justice Information Services (CJIS) minimum training criteria for usage of facial recognition systems.

F. Auditing

LACRIS will ensure that the DMS technology provided complies with the then current CJIS Security Policy in regard to audits. The DMS automatically audits user actions such as, logon time, date search, subject viewed, etc. LACRIS personnel will conduct random audits of users and report their findings directly to the user's agency. LACRIS audits user's search and activity compliance to include search reason, number of searches, subject status, watch list entries, etc. Audit report data will be compiled and stored at LACRIS for a minimum of three (3) years.

G. Accountability and Enforcement

LACRIS maintains several applications that must adhere to regulations and laws which includes user access. Through audits, if LACRIS determines there was misuse or a violation of these regulations and/or laws, it must take corrective action. Depending on the severity of the violation, LACRIS will hold those user(s) accountable for their actions. Penalties may include but are not limited to restricted access, revoked access, or prosecution. Users may also be subject to additional discipline from their respective agency, as well as other law enforcement agencies, including but not limited to State or Federal agencies.

H. Face Search Request

Outside agencies, or investigators from outside agencies, may request facial recognition searches to assist with investigations through LACRIS only if the LACRIS **Face Recognition Search Request Form** is completed. This form can be obtained through the LACRIS Help Desk at lacrishd@lasd.org and will require the following minimum information:

- Requesting Agency
- Requester Name Requester Phone Number
- Requester Email
- Requester Signature
- Requester Date
- Reason for Search
- Case/File Number
- Number of Images Submitted

LACRIS personnel will review each request prior to processing to ensure compliance with this policy. Users acknowledge the result of any facial recognition search provided by LACRIS shall be deemed only an investigative lead and **RESULTS ARE NOT TO BE CONSIDERED AS PROVIDING A POSITIVE IDENTIFICATION OF ANY SUBJECT**. Any possible connection or involvement of any subject to the investigation must be determined through further investigation and investigative resources.



LACRIS

LOS ANGELES COUNTY
REGIONAL IDENTIFICATION SYSTEM

Facial Recognition Policy Template

This template may be used by member agencies for creating policy and procedures that adhere to Federal and State laws pertaining to facial recognition use. This template adheres to current LACRIS policies and procedures regarding the use of facial recognition.

LACRIS will update and forward all new policy revisions when applicable.

XXX – PURPOSE AND SCOPE

The purpose of this policy is to establish procedures for the acceptable use of the images (probe and candidate), information and tools within the facial recognition system. Facial Recognition shall only be used when there is reasonable suspicion that such use will provide information relevant to an active investigation, imminent threat to health or safety (“at-risk”), or to help in the identification of deceased persons or persons unable to identify themselves. This policy applies to all law enforcement personnel who are granted direct access to the face recognition system as well as personnel who are permitted to request face recognition searches. Any outside agency, or personnel from an outside agency, requesting face recognition assistance with an investigation must also adhere to this policy, and must fill out a request form (samples at end of document), which indicates adherence to these policies.

XXX – DEFINITIONS & TERMS AS DEFINED BY LACRIS

Digital Mugshot System (DMS) – DMS is the repository of all criminal booking photos (mugshots) and includes a Facial Recognition application.

Facial Recognition – The automated searching of a facial image (probe) against a known database(s) resulting in a list of candidates ranked by computer-evaluated similarity score. This is commonly referred to as a one-to-many comparison.

Facial Reviewer- A person who successfully completed training by the FBI or LACRIS in facial comparison. (1) The review of a candidate list to identify possible matches. (2) One-to-one verification conducted in a high-throughput environment (e.g., stadium entrance).

Los Angeles County Regional Identification System (LACRIS) - The California Department of Justice’s CAL-ID program responsible for providing biometric identification services to Los Angeles County law enforcement agencies.

Probe- The facial image or template searched against a known mugshot database in a Facial Recognition System.

Surveillance- Lawful close watch kept over someone or something.

XXX - POLICY

This policy of the **[Insert agency name here]** is to solely utilize face recognition technology as an investigative tool during investigations, while recognizing the established privacy rights of the public.

XXX – PROHIBITIVE USES

1. Members shall not use face recognition to actively surveil members of the public through any camera or video device unless the person(s) are under an active criminal investigation or the surveillance is in response to an imminent threat of life.
2. Members shall not use face recognition on live stream video unless there is an imminent threat to life or involves at risk individuals.
3. Members shall not use facial recognition in connection with portable recorders (Penal Code 832.19. It should be noted 832.19 PC current sunset date of 01/01/2023).
4. Members shall not use facial recognition for predictive analysis.

XXX – FIRST AMENDMENT ACTIVITY

Facial recognition must be used in accordance with all federal and state laws, and all Departmental policies.

[Insert agency name here] and its personnel will not perform or request facial recognition searches about individuals or organizations that will violate the First, Fourth, and Fourteenth Amendments of the US Constitution and based solely on any of the following:

1. Their religious, political, or social views or activities.
2. Their participation in a particular noncriminal organization.
3. Their race, ethnicity, citizenship, place of origin, age, disability, gender, gender identification, sexual orientation, or other protected classification.

XXX – DATABASE AND DATA LIMITATIONS

1. **[Insert agency name here]** will not maintain, utilize, or keep any database to conduct facial recognition searches and shall only utilize the LACRIS DMS to conduct facial recognition searches. **(If your agency purchases or utilizes a separate commercial facial recognition system, (eg. Vigilant and Clearview) add a sentence that clearly states which facial recognition system other than the LACRIS DMS your agency will use or maintain; and ensure the clear separation between the LACRIS DMS and any other system(s)).**
2. **[Insert agency name here]** will only utilize the LACRIS DMS countywide facial recognition system to conduct facial recognition searches. **(If your agency uses more than the LACRIS Facial Recognition application, take out “only” and add the other system(s) you will be using. Ensuring the clear separation between the LACRIS DMS and any other system).**
3. No non-mugshot databases, such as the California driver’s license photo database, or open source photo databases, are linked to or accessible via the LACRIS DMS.
4. Potential matches returned by the facial recognition system are to be considered investigative leads only and cannot be used as the sole basis for an arrest or identification.

XXX – DOCUMENTATION

With any possible match where an investigative lead is generated on the facial recognition software, the face reviewer and/or investigator should write a detailed report on the information they have obtained.

XXX – INVESTIGATIVE SEARCHES

1. Probe images will only be used from legally obtained sources.
2. Face reviewers will determine if probe image(s) is suitable for facial recognition searches and may process images for the purpose of conducting a facial recognition search.

XXX – TRAINING

[Insert agency name here] personnel accessing the facial recognition system shall have successfully completed training provided by the Federal Bureau of Investigations (FBI) or LACRIS, which shall meet the Criminal Justice Information Services (CJIS) minimum training criteria for usage of facial recognition systems. Investigative searches shall only be conducted by trained face reviewers. Trained Face Reviewers are qualified to assess image quality and suitability for face recognition searches and to perform one-to-many and one-to-one face image comparisons.

XXX – AUDITS

The use of the LACRIS facial recognition system is controlled by state law pertaining to Criminal Offender Record Information (CORI). All use(s) of the LACRIS facial recognition system will be performed on a need to know and right to know basis per CORI regulations. All use(s) of the LACRIS facial recognition system and search requests are subject to audit by the Cal-DOJ, and LACRIS. In the event of an audit, the user will be required to provide appropriate justification for the use or request of a face recognition search.

Appropriate justification shall include a situation description and purpose for the search, including a detailed account of circumstances amounting to reasonable suspicion, a case/complaint number, and a file class/crime type, if available.

SAMPLE

Face Recognition Manual Search Request Form

Attention [Insert agency / unit name here] Staff:

Please assist our agency's investigation by conducting a facial recognition search of the attached images in the Los Angeles County Digital Mugshot Repository, as well as any repositories that are searchable through the California Facial Recognition Interconnect (CAFRI).

Our agency understands that any results are to be used as investigative leads only and shall not be considered a positive identification.

Requesting Agency:

Requester Name:

**Requester Phone
Number:**

Requester Email:

Case/File Number:

Reason for search:

**Number of Images
attached:**

Date:

Requester Signature

Printed Name

Approving Supervisor Signature

Printed Name

Insert Agency Logo here
is desired

UNCLASSIFIED//LAW ENFORCEMENT SENSITIVE
Cal-ID / Facial Recognition
Unit Manual Search Report

**THIS DOCUMENT IS NOT A POSITIVE IDENTIFICATION. IT IS AN INVESTIGATIVE TOOL ONLY
AND IS NOT PROBABLE CAUSE TO ARREST. FURTHER INVESTIGATION IS NEEDED TO
DEVELOP PROBABLE CAUSE TO ARREST.**

(Insert your Facial Recognition Case # here)	Submitted by:
Date Searched:	Investigating Agency:
Face Reviewer:	Agency Case Number:

Submitted Image	Investigative Lead
<i>Insert probe image here</i>	<i>Insert picture returned from facial recognition search here</i>

The above investigative lead is deemed viable for further investigation based on a facial recognition search and morphological comparison. See demographic information below:

Name: _____ Date of Birth: _____
CDL #: _____ MAIN #: _____
SID #: _____ Recent booking number: _____

Comments: *insert any pertinent info regarding recent arrest or contact locations here*

[Insert agency / unit name here] has determined that the image(s) provided did not result in a possible match in the digital mugshot repository at this time. If your agency wishes to provide additional images, a new facial recognition search request must be completed.

In the event LACRIS is notified to seal/destroy this record, it is your agency's responsible to destroy this information in compliance with California's Department of Justice Criminal Offender Record Information (Information Bulletin 13-04-CJIS).

This document is the property of [insert agency name here] and is prepared for the limited purpose of information sharing. This information is designated **U//LES and is shared in confidence**. This document contains Personally Identifiable Information (PII) and must be handled in accordance with the LACRIS Policy and FBI CJIS Security Policy. It may be shared with other LE agencies, but may not be posed within public view. This document must not be reclassified in any way, in whole or in part. Questions pertaining to this document can be directed to (insert email or phone number of your Facial Recognition unit).

Exhibit D

To Whom It May Concern:

Pursuant to the California Public Records Act, I hereby request the following records:

Per the California Public Records Act (Govt. Code 6250-6270), I am writing to request the following information from your office for the period January 1, 2015 to the date of this letter.

Number, if any, of IMSI-catcher or cell phone interception devices (commonly called stingrays or hailstorms) owned by this department or agency.

Number, if any, of IMSI-catcher or cell phone interception devices (commonly called stingrays or hailstorms) available for use by this department or agency via collaborative agreements that were utilized within the period encompassing this request. Please provide the name of the department or agency that made IMSI-catcher devices available to this department or agency for use.

Any documents or correspondence during the period encompassing this request regarding possible or planned acquisition of an IMSI-catcher device.

Any existing or proposed usage policies regarding the use of cell phone interception technology including protocols, training documents and data storage procedures.

Any current or past litigation involving or referencing this department or agency involving the use of cell phone interception technology.

Please notify me when this information is available.

Thank you for your attention to this request and for your prompt reply within 10 days.

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 10 calendar days, as the statute requires.

Sincerely,

Aaron Swartz Day Police Surveillance Project

From: Long Beach Police Department

02/22/2019

Subject: [Records Center] PRA Request :: P001725-011019

Portal

--- Please respond above this line ---

Hello Mr. Swartz,

The Long Beach Police Department does not have any responsive records to provide you relating to your public records request.

Thank you.

Exhibit E

Special Order
Cellular Communications Interception Technology

This Special Order policy will govern the use of the Long Beach Police Department's ("LBPD") cell site simulator (CSS) and is written to comply with Government Code section 53166, effective January 1, 2016.

The use of a CSS device provides valuable assistance in support of public safety objectives. Whether deployed as part of a search and rescue mission in a natural disaster, a terrorist event, fugitive apprehension, or to locate at-risk people or missing children, the CSS device fulfills a critical operational need. The CSS device saves countless hours of surveillance and investigative effort by helping detectives quickly locate and arrest suspects wanted for criminal offenses.

This policy shall serve to ensure that the CSS technology is used in a manner consistent with the requirements and protections of the U.S. Constitution, including the Fourth Amendment, and applicable statutory authorities. Moreover, any information obtained from the use of a CSS device must be handled in a way that is consistent with all applicable laws, regulations, and policies that guide law enforcement in how it may and may not collect, retain, and disclose data. As such, either a search warrant or exigent circumstances must exist prior to utilizing the CSS device.

In cases where the CSS device is deployed under exigent circumstances, by law, a search warrant must be obtained within three days of its use. The CSS operator will be responsible for ensuring that the proper legal paperwork is maintained.

The CSS computer, and any information obtained from it, shall only be utilized and accessed by authorized detectives in the Gang and Violent Crimes Division of the LBPD who have attended requisite training provided by the vendor.

Use of the CSS device must be approved by the Sergeant of the Career Criminal Apprehension Team (CCAT) or by his or her chain of command. Prior to approval, the CSS operator will ensure the use of the equipment will be in support of a public safety operation or criminal investigation and shall not be utilized unless the proper legal process has been followed, including either obtaining a search warrant or submitting an exigent request form with a telephone/telecommunications company. The CCAT sergeant is responsible for conducting periodic audits to ensure compliance with obtaining search warrants prior to using the CSS device, as well as auditing exigent circumstances to ensure search warrants are obtained within three days.

In all cases where the CSS is deployed, the authorized operator will complete a CSS deployment form. The form must be signed by the operator responsible for the operation and the CCAT Sergeant who approved the operation.

The form will be forwarded for review to the Lieutenant of the Crimes Against Persons

Section and the Commander of the Gang and Violent Crimes Division. After all review and signatures are obtained, the form will be returned to CCAT for retention in the CSS deployment file.

Any requests from another law enforcement agency to assist them with the use of the CSS device shall only be approved if it meets the criteria explained herein and LBPDP policies and procedures are followed during its deployment. No deployment will take place until the proper legal paperwork (i.e., search warrant or exigent request) has been provided to the LBPDP and has been reviewed to ensure it meets the legal requirements for use of the CSS device. If the request is approved, the CSS deployment form will be completed.

The CSS equipment will be secured and maintained in a locked LBPDP facility when not in the field. Access to the equipment will only be allowed to authorized personnel within the CCAT chain of command or those approved by the Gang and Violent Crimes Division Commander, or his or her designee.

The LBPDP is committed to ensuring that the collection and retention of data is lawful and appropriately respects the privacy interests of individuals. The LBPDP will not collect, retain, or disseminate any data except as authorized by this policy and by law. Consistent with applicable existing laws and requirements, including any duty to preserve exculpatory evidence, the Department's use of a CSS shall include the following privacy practices:

- When the equipment is used to locate a known cellular device, all data must be deleted as soon as that device is physically located and no less than once daily.
- When the equipment is used following a disaster, or in a search and rescue context, all data must be deleted as soon as the person(s) in need of assistance has been located, and no less than once every ten days.
- Prior to deploying the equipment for any mission, the CSS operator must verify that the equipment has been cleared of any previous operational data.
- When a suspect is known to have been in two separate geographically different areas, any data collected in an effort to identify the cellular device shall be deleted upon completion of the mission, unless the data collected is deemed to have evidentiary value.

Data collected by the device, which is retained for the investigation, shall only be shared with those involved within the investigation or when ordered produced as part of a legal compliance process.

The CCAT Sergeant shall conduct audits to ensure that the data is being deleted in compliance with the above manner. These audits shall take place no less than once every six months. The CCAT Sergeant will document these audits and submit them for review to the Lieutenant of the Crimes Against Persons Section. The audits will be

maintained in a file with the Crimes Against Persons Lieutenant and retained in compliance with the Department's business document retention policy.

Exhibit F

From: Aaron Swartz Day Police Surveillance Project

01/11/2019

Subject: California Public Records Act Request: CALIFORNIA PUBLIC RECORDS REQUEST – PREDICTIVE SOFTWARE (Long Beach Police Department)

Portal

To Whom It May Concern:

Pursuant to the California Public Records Act, I hereby request the following records:

Per the California Public Records Act (Govt. Code 6250-6270), I am writing to request the following information from your office for the period January 1, 2015 to the date of this letter.

Number, if any, of Predictive Algorithmic software packages or service agreements designed to anticipate criminal activities in place with this department or agency. Please specify if software has been purchased or if services are performed by outside contractors for the department or agency.

Any documents or correspondence during the period encompassing this request regarding possible or planned acquisition of Predictive Algorithmic software packages or service agreements.

Any existing or proposed usage policies regarding the use of Predictive Algorithmic software packages or service agreements. including protocols, training documents, data storage procedures and prohibited activities.

Any current or past litigation involving or referencing this department or agency involving the use of Predictive Algorithmic Software Packages or Service Contractors.

Please notify me when this information is available .

Thank you for your attention to this request and for your prompt reply within 10 days.

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 10 calendar days, as the statute requires.

Sincerely,

Aaron Swartz Day Police Surveillance Project

From: Long Beach Police Department

02/08/2019

Subject: PRA Request :: P001722-011019

Portal

Dear Aaron Swartz:

Thank you for your interest in public records of the Long Beach Police Department. Your request has been received and will be processed in the order it was received. Your request was received in this office on 1/10/2019 and given the reference number P001722-011019 for tracking purposes.

Records Requested: "To Whom It May Concern:

Pursuant to the California Public Records Act, I hereby request the following records:

Per the California Public Records Act (Govt. Code 6250-6270), I am writing to request the following information from your office for the period January 1, 2015 to the date of this letter.

Number, if any, of Predictive Algorithmic software packages or service agreements designed to anticipate criminal activities in place with this department or agency. Please specify if software has been purchased or if services are performed by outside contractors for the department or agency.

Any documents or correspondence during the period encompassing this request regarding possible or planned acquisition of Predictive Algorithmic software packages or service agreements.

Any existing or proposed usage policies regarding the use of Predictive Algorithmic software packages or service agreements. including protocols, training documents, data storage procedures and prohibited activities.

Any current or past litigation involving or referencing this department or agency involving the use of Predictive Algorithmic Software Packages or Service Contractors.

Please notify me when this information is available .

Thank you for your attention to this request and for your prompt reply within 10 days.

The requested documents will be made available to the general public, and this request is not being made for commercial purposes.

In the event that there are fees, I would be grateful if you would inform me of the total charges in advance of fulfilling my request. I would prefer the request filled electronically, by e-mail attachment if available or CD-ROM if not.

Thank you in advance for your anticipated cooperation in this matter. I look forward to receiving your response to this request within 10 calendar days, as the statute requires.

Sincerely,

Aaron Swartz Day Police Surveillance Project

From: Long Beach Police Department

02/08/2019

Subject: [Records Center] PRA Request :: P001722-011019

Portal

--- Please respond above this line ---

Hello Mr. Swartz,

This email is in response to your public records request where you requested documents related to "Predictive Algorithmic software packages or service agreements."

The Long Beach Police Department does not possess records responsive to your request.

Thank you

Exhibit G

CALIFORNIA GOVERNOR'S OFFICE OF EMERGENCY SERVICES

Homeland Security Grant Program FY 2013 Grant Number: 2013-00110 CalOES ID#: 037-95050

Subgrantee name: Los Angeles/Long Beach Urban Area Project: JRIC/LBPD Intelligence Analyst

REQUEST FOR SOLE SOURCE PROCUREMENT AUTHORIZATION

1. Project name: JRIC/LBPD Intelligence Analyst Project Budget: \$202,500
2. Describe the project and/or activity that will be provided by the proposed sole source vendor/contractor.

Equipment & Description	Cost	AEL number
Contract intelligence analyst services for information, investigation and intelligence sharing.	202,500	N/A-ORG

Approval of this sole source request will enable the Long Beach Police Department ("Department") to continue its current contract with Systems Research & Application International ("SRA") for a professional Intelligence Analyst to evaluate and analyze criminal intelligence information collected by the Department and collaborating agencies and to determine the credibility, reliability and pertinence of the information. Utilizing SRA's proprietary intelligence software, Orion, the Intelligence Analyst prepares reports based on interpretation of intelligence information, participates in meetings with Department personnel and other law enforcement agencies and assists in the planning activities of the Department's Criminal Intelligence Section (formerly known as the Officer of Counter Terrorism).

Note: This is an ongoing, multi-year project that previously received funding through the UASI 2011 grant program. Sole source approval was previously sought and granted. The previous sole source approval is attached for reference.

3. Describe your organization's standard procedures when sole source contracting is considered, including the conditions under which a sole source contract is allowed, and any other applicable criteria (i.e. approval requirements, monetary thresholds, etc.).

City of Long Beach Administrative Regulation 23-3, Subsection D:

When a planned purchase is expected to exceed \$5,000 and the requesting department determines that there is only one source for the equipment, materials or supplies sought, a sole source memorandum, which includes background and justification, must be prepared. For purchases between \$5,000 and \$50,000, the memo is submitted to the Purchasing Agent for approval.

For purchases in excess of \$50,000, the memo must be submitted to the City Manager for approval, and then sent to the Purchasing Agent. The Purchasing Agent will request the City Attorney to prepare the required Resolution for a sole source purchase. In this instance, the justification memo to the City Manager must include the following:

- (1) Identification of the sources with information on the type of services sought.
- (2) Number of those sources contacted.
- (3) Identification of the unique feature or emergency or reason it is impossible to advertise for bids.
- (4) Name of City employee who can testify regarding all of the above.

This memo will be forwarded to the City Attorney along with the request for a sole source Resolution.

4. Indicate which of the following circumstances resulted in your organization's need to enter into a sole source contract.
 - a. Item/service is only available from one source (Describe the process used to make that determination. Please provide details.)

ORION Intelligence Software is a SRA proprietary intelligence database used exclusively by the Department's Criminal Intelligence Section. ORION software allows intelligence analysts to aggregate and analyze data from disparate intelligence sources in both open source and classified information fields. The SRA Intelligence Analyst has extensive experience using the Department's database. As the sole manufacturer, distributor and service provider for the ORION database, only SRA's intelligence analysts are able to implement changes to refine and enhance the system to better meet the Department's needs.

5. Did your organization confirm that the contractor/vendor is not debarred or suspended?

Yes, the Department has validated that SRA International does not have active exclusions as reported on the Federal System for Awards Management website (See Sam.gov search results dated 2/10/2014, attached).

6. Will your organization be able to complete all activities associated with the sole source contract by the end of the grant performance period?

As stated above, this is an ongoing, multi-year project that previously received funding under the UASI program. The UASI 2011 funded portion of the Intelligence Analyst project will be fully expended before the grant end date. The Department may seek additional funding for this position in subsequent UASI grant periods.

7. Has your organization determined the costs are reasonable?

Yes. The Department believes the cost of the SRA Intelligence Analyst, \$14,000/mo., is reasonable. The Department has determined that the costs for SRA's professional services contract (\$79/hr.) is commensurate with the level of service and expertise provided by the Intelligence Analyst.

8. Please attach a copy of the cost benefit analysis prepared for this procurement.

Submitted by: Arlen Crabtree  Date: 02-12-14
(Name) (Signature)

Attachments:

- UASI 2011 Sole Source Approval
- Sam.gov Report, date 2/10/2014
- SRA International CBA



August 7, 2013

Alisa Finsten
Office of the Mayor
200 N. Spring Street, Room M175C
Los Angeles, Cal 90012

SUBJECT: APPROVAL OF SOLE SOURCE CONTRACT REQUEST
FY11 HOMELAND SECURITY GRANT PROGRAM (HSGP)
Grant #2011-0077, CalOES ID #037-95050

Dear Ms. Finsten:

The California Governor's Office of Emergency Services (Cal OES) has received, reviewed, and approved the your Sole Source contract request dated August 2, 2013, based on the information your office provided regarding the proposed purchase of:

- SRA Intelligence Analyst

If you have any questions about this letter, please contact your Program Representative, Casey Granados, at (916) 845-8436 or Casey.Granados@calema.ca.gov.

Thank you for your work in protecting California. We look forward to your continued collaboration towards our homeland security strategy and appreciate your cooperation and support.

Sincerely,

A handwritten signature in black ink that reads "Casey Granados". The signature is fluid and cursive, written over a horizontal line.

Casey Granados, Acting Unit Supervisor
Homeland Security Grant Unit

SAM Search Results
List of records matching your search for :

Search Term : "Systems Research & Application International*"
Record Status: Active

No Search Results

SRA International Cost Benefit Analysis

Long Beach Police Department
JRIC/LBPD Intelligence Analyst
UASI 2013, Project C-14-27

This is an ongoing, multi-year project that has been previously funded under the UASI program, FY 2008, 2009, 2010 and 2011. Sole source approval was sought and granted under each of the prior years.

Since first entering into contract with the City of Long Beach in 2010, the SRA Intelligence Analyst has integrated into the Long Beach Police Department's Criminal Intelligence Section (formerly known as the Office of Counter Terrorism), developing important extra-agency relationships and a crucial understanding of the Department's intelligence operation. Additionally, the SRA Intelligence Analyst is proficient in the use of SRA's proprietary ORION Intelligence Database, which is used exclusively by the Department, and holds all required security clearances necessary to perform the required job duties. Maintaining the continuity of personnel in this key position is critical to the effectiveness of the Department's intelligence program.

Cost:

The contract with SRA International for Intelligence Analyst carries an average monthly cost of \$14,000. The Department has determined that the costs for SRA's professional services contract (\$79/hr.) is commensurate with the level of service and expertise provided by the Intelligence Analyst.

Benefit:

The SRA Intelligence Analyst has attained an intimate understanding of the Department's organization, function and operations and how the Department collaborates with partnering intelligence agencies to identify and respond to potential threats. The SRA Intelligence Analyst has developed many extra-agency contacts, including personnel at the Los Angeles County Joint Regional Intelligence Center ("JRIC"), which have provided invaluable information concerning possible criminal terrorist activities. The SRA Intelligence Analyst has provided timely and relevant information at intelligence meetings, information shared with local and federal partners. A new analyst would not have the benefit of the intelligence community contacts and organizational awareness that SRA's Intelligence Analyst demonstrates. In the short term, the learning curve needed to successfully integrate into the Department processes and build contacts would be a detriment to the effectiveness of the position and the Department's intelligence operations. In the long term, there is no guarantee that a new analyst would be

able to provide the Department with the same level of expertise and service that the SRA Intelligence Analyst routinely delivers.

It is essential to the Department that any contractor assigned to this position be proficient in the use of SRA's proprietary ORION Intelligence Software. As an SRA employee, the SRA Intelligence Analyst has the access and ability required to implement changes to the ORION software to better meet the needs of the Department's intelligence operations. As Department needs change, the SRA Intelligence Analyst is be able to modify the software to meet those needs. This work is accomplished within the course of the Intelligence Analyst's day-to-day job responsibilities. Were the Department to seek out the services of a different firm/contractor to fill this position, this new analyst would not have the ability to modify the proprietary software's parameters. As a result, the Department would be forced to either (a) seek an additional contract with SRA to upgrade the ORION software platform as needed or (b) seek out a competing software solution. Either option would come at a significant incurred expense to the Department, both in terms of budget and time resources, to pay for software configuration and/or purchase new software and train Department personnel on a new platform. In comparison, Department personnel are already trained on the ORION platform and the SRA Intelligence Analyst's ability to modify the software as needed makes additional contracts for software configuration unnecessary.

Conclusion:

In summary, the SRA Intelligence Analyst is a proven asset to the Department's intelligence operations. Over the past few years, the SRA Intelligence Analyst has integrated into Department and the regional intelligence community and provided invaluable interpretation of intelligence data from multiple sources. Additionally, the SRA Intelligence Analyst has attained specific expertise in the use and improvement of the Department's ORION Software Platform. A rejection of this sole source request effectively nullifies the past investment in this position and removes a critical asset in the SRA Intelligence Analyst. By contrast, approving the sole source request allows the Department to continue under contract with SRA, thus leveraging the substantial investment that has already been made in continuing the Department's intelligence operations.

DEPARTMENT INFORMATION

PO NUMBER: _____ DEPARTMENT NAME: Police DATE: 6/17/19
 REQUESTOR: Leslie Bruce PHONE: 562-570-5391

VENDOR INFORMATION

NAME: SRA International Inc. VENDOR #: 5125
 DBA: _____ CONTACT: John Purdon
 ADDRESS: P.O. Box 742213, Atlanta, GA, 30374 EMAIL: John.Purdon@gdit.com
 PHONE: 609-335-1374 FAX: _____

MUNIS USER DEFINED FIELDS (UDFs)

PROCUREMENT PROCESS TYPE: Exception to Policy
 CHANGE ORDER REASON (IF APPLICABLE): _____
 INSURANCE: Yes No INSURANCE REASON (IF APPLICABLE): _____
 LABOR COMPLIANCE: Yes No TI EQUIPMENT: Yes No HOMELAND SECURITY GRANT: Yes No

DESCRIPTION OF PURCHASE

DESCRIPTION / JUSTIFICATION FOR PURCHASE / TIMING CONSIDERATIONS / SERVICE LEVEL IMPACT IF NOT APPROVED

The Police Department requests interim purchasing authority to continue services with SRA International, Inc. for three Intelligence Analysts. The three analysts have been working with the Police department for several years. They are assigned to the Criminal Intelligence Section, the Long Beach Common Operating Picture (LBCOP) program, and the Investigation Bureau's Gang Enforcement Section.

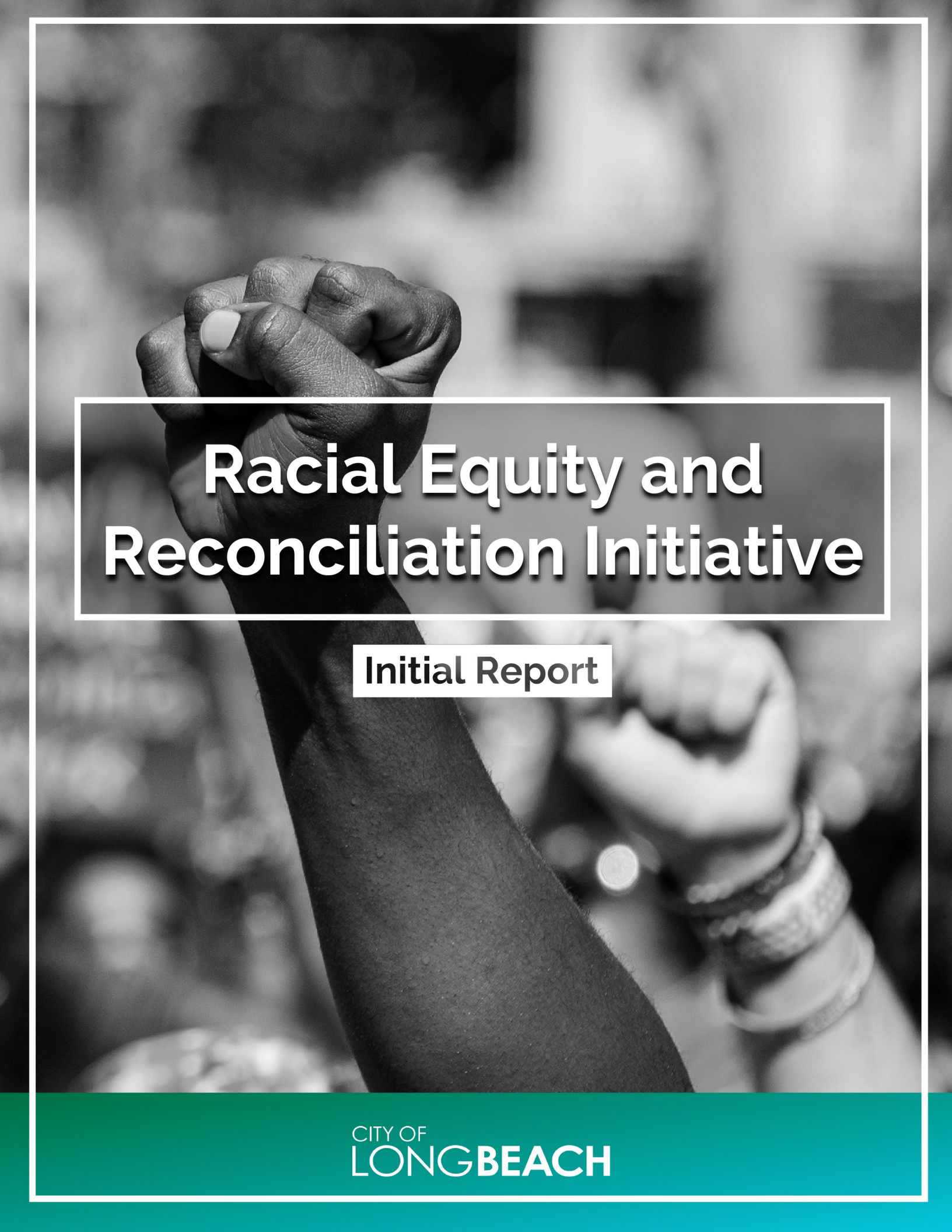
Cooperative contract agreements are being considered to provide a long-term solution to bring intelligence analysts to the Department.

Each analyst provides confidential services which include, but are not limited to: crime analysis, social media analysis, real time tips & leads, and suspect/location identification. They are also responsible for collecting information and providing tactical, strategic, and situational awareness to the Department. The compilation of this data, knowledge, and information assists officers and detectives in taking a strategic, targeted approach essential to their criminal investigations and prosecution of possible suspect(s). The analyst's tasks are confidential in nature and SRA fully understands privacy issues, rights of an individual/entity, and that any data and information gathered is intended for the sole use of the Police Department.

The skills provided by the contracted intelligence analysts are outside any descriptions currently offered by City of Long Beach job classifications. SRA specializes in providing analysts that pair IT expertise with analytical tools that allow Police Department leaders to make critical decisions, better and faster.

This project will be funded by the State COPS Grant, which does not require Los Angeles County sole source approval.

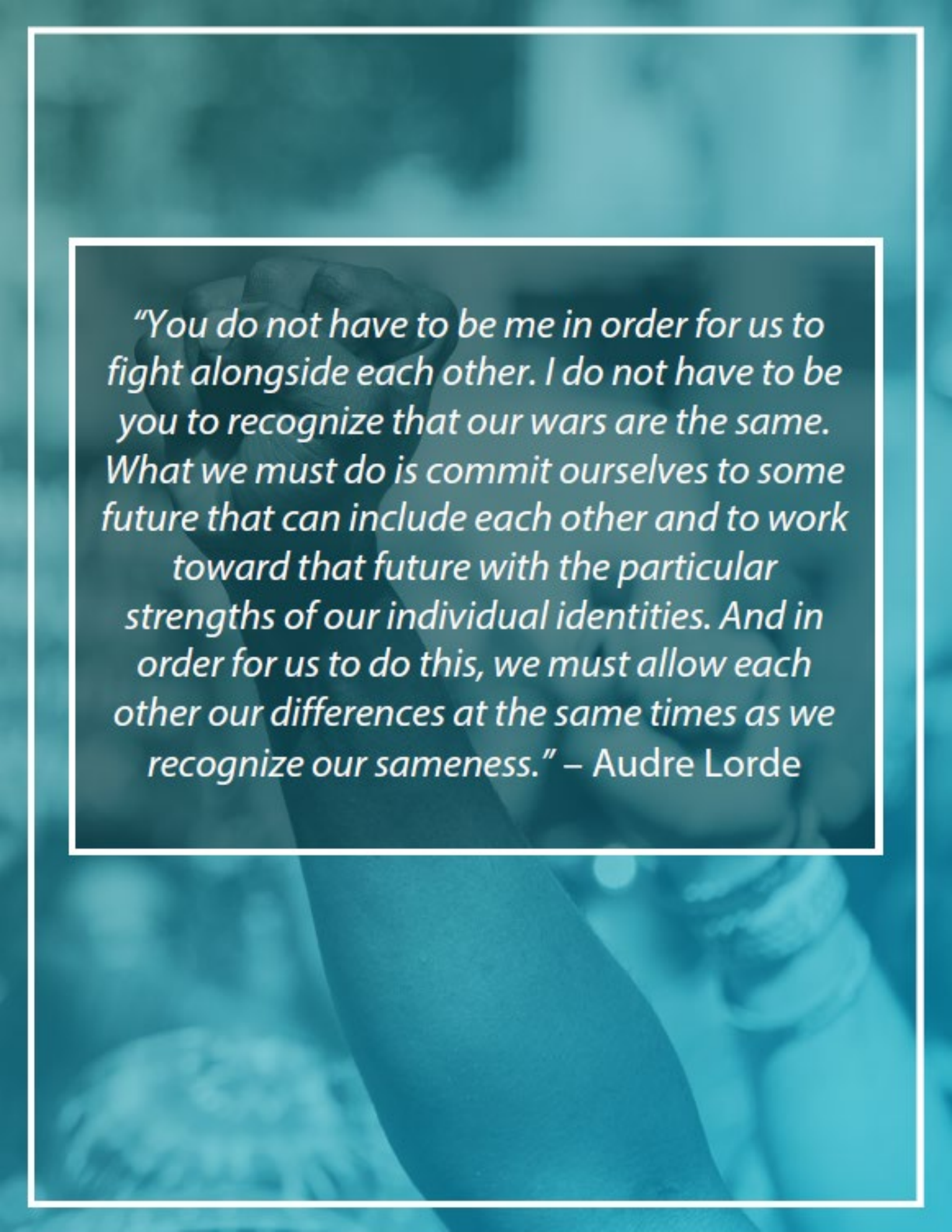
(Continued)



Racial Equity and Reconciliation Initiative

Initial Report

CITY OF
LONGBEACH



"You do not have to be me in order for us to fight alongside each other. I do not have to be you to recognize that our wars are the same. What we must do is commit ourselves to some future that can include each other and to work toward that future with the particular strengths of our individual identities. And in order for us to do this, we must allow each other our differences at the same times as we recognize our sameness." – Audre Lorde

Table of Contents

A Letter from City Health Officer Dr. Davis.....	4
Introduction.....	6
Reconciliation Framework.....	6
City Data.....	7
Community Listening and Engagement	8
General Approach.....	9
Participants.....	11
Key Findings.....	14
Equity Goals & Strategies.....	21
Community Stakeholder Response.....	46
Next Steps.....	62
Appendices.....	64
Appendix A: History of Violence Prevention Efforts.....	65
Appendix B: Summary of Outreach and Engagement.....	68
Appendix C: CSULB Data Analysis Report.....	73
Appendix D: Community & Staff Survey Analysis Report.....	94
Appendix E: Important Definitions.....	110
Appendix F: Acknowledgments/Contributors.....	112

Goal 3

Redesign police approach to community safety.

Strategy 3:	Potential Actions	Time Frame	Information Source
Redesign police tactics, training, retention and accountability.	A. Implement early intervention programs for problematic police employees to interrupt adverse patterns of behavior.	Short Term	
	B. Provide ongoing training on implicit bias, de-escalation techniques, procedural justice, systemic racism, trauma-informed response, racial sensitivity, mental health, and disabilities.	Immediate and On-Going	
	C. Review Civil Service hiring processes of police officers to better reflect community demographics and lived experiences. 1. Explore higher standards of education and/or experience for police officers at time of hire and methods to ensure there are not barriers to recruitment of diverse applicants. 2. Reexamine background checks, psychological assessments, and other screening mechanisms that disproportionately exclude Black people and people of color.	Immediate and On-Going	
	D. Review Civil Service Policy and standards of conduct to ensure zero tolerance of police officer activity with violent extremist groups.	Medium Term	
	E. Explore the practice of facial recognition technology and other predictive policing models and their disproportionate impacts on Black people and people of color by reviewing evidence-based practices.	Medium Term	
	F. Reexamine metrics currently used for Officer success and promotion.	Short Term	
	G. Explore the disproportionate policing of the Black community and communities of color. 1. Include a review of best practices of Internal Affairs structure and staffing. 2. Hold a public study session with the City Council to review police reporting metrics, how data is used, data transparency efforts, call for service data, and methods to improve transparency and accountability.	Immediate and On-Going	

Community Stakeholder Submission

Strategy 2: Redesign police oversight and accountability through improved complaint and discipline practices.

Action Items:

- A. Dissolve the CPCC in favor of a community oversight committee that has subpoena and disciplinary powers and is not housed or controlled by the police department
- B. Implement immediate short-term reforms to CPCC such as:
 - i. Direct the CPCC to institute and publish quarterly reports
 - ii. Institute commissioner trainings led by outside experts with community input on the selection process. the City Attorney's office.
 - iii. Provide officer compelled statements to the CPCC.
- C. Engage in a formal outside expert study, through a non-police community selection process, of the Citizen's Police Complaint Commission (CPCC), to identify necessary changes to its structure and explore creation of a new civilian police oversight body based on models from other California municipalities. Conduct further community outreach to ensure reforms and/or new oversight bodies meet community needs.
- D. Increase funding to CPCC to expand investigative capacity.
- E. Increases in funding to CPCC tied to expansion of oversight powers, including subpoena power to compel police officers and other witnesses to testify.

Strategy 3. Redesign police tactics, training, retention and accountability.

Action Items:

- A. Implement early intervention programs for problematic police employees to interrupt adverse patterns of behavior.
- B. Provide ongoing training on implicit bias and anti-racism, de-escalation techniques, procedural justice, systemic racism, trauma-informed response, racial sensitivity, mental health, and disabilities.
- C. Explore partnerships with CSULB, LBCC, other educational institutions, or community- based organizations to establish ethnic studies as part of Police training.
- D. Review Civil Service hiring processes of police officers to better reflect community demographics and lived experiences.
- E. Explore higher standards of education and/or experience for police officers at time of hire and methods to ensure there are not barriers to recruitment of diverse applicants.
 - i. Re-examine background checks, psychological assessments, and other screenings like racism, understanding of socio-economic and social justice, mechanisms that disproportionately exclude people of color.
- F. Review Civil Service Policy and standards of conduct to ensure zero tolerance of police officer activity with violent extremist groups.
- G. Explore the practice of facial recognition technology and other predictive policing models and their disproportionate impacts on people of color by reviewing evidence- based practices.
- H. Re-examine metrics currently used for Officer success and promotion.
- I. Explore the disproportionate policing of communities of color by examining the number of low-level arrests, and the number of patrols placed, time spent, resources spent (overtime, helicopters, number of single occupant police vehicles, etc.)