AGENDA

Public Safety, Courts and Civil Service Policy Committee

Thursday, September 11, 2025, 9:00 a.m.

Aurora Room

15151 E. Alameda Parkway

Aurora, CO 80012

Council Member Danielle Jurinsky, Chair
Council Member Stephanie Hancock, Vice Chair
Council Member Amsalu Kassaw, Member

Public participant dialing instructions
Join the meeting LIVE here
Dial 720-388-8447 Meeting ID: 130 756 273#

Council Goal: Assure a safe community for people
This meeting will uploaded on the city's YouTube channel. Watch at YouTube.com/TheAuroraChannel.

DRAFT – SUBJECT TO APPROVAL

Public Safety, Courts and Civil Service Committee

August 14, 2025

Members Present	Danielle Jurinsky, Chair Stephanie Hancock, Vice-Chair Amsalu Kassaw, Member
Others Present	M. MacDonald, C. Atkinson, M. Crawford, A. Heider, E. Cadiz, L. Battan, M. Platt, S. Griffin, D. Exstrom, L. Rehwalt, D. Small, A. Donadio, A. Robnett, R. Weber, A. Garcia, H. Hackbarth, Y. Emeson, J. Schneebeck, J. Pearce, M. Hanifin, M. Chapman, J. Bajorek, M. Gaskill, E. Adams, A. Morris, D. Carrel, D. Stafford, S. Vanburen, J. Soules, J. Batchelor, T. Bunetta, M. Hays, P. Schulte, S. Day, H. Hackbarth, L. Callanen, M. Hildebrand

---

1. Call to Order

The meeting was called to order at 9:00 a.m.

2. Approval of Minutes

The July 10, 2025 minutes were approved.

3. Consent Items

3.a Aurora911 Retention Update - August 2025

3.b Motor Vehicle Theft Recovery Voucher Program Update

3.c Police Retention Update - August 2025

3.d Special Operations Crime Suppression Update – August 2025

3.e Aurora Fire Rescue Retention Update - August 2025

4. General Business

4.a Ordinance to Amend the City Code Pertaining to Automated Vehicle Identification System Penalty Notices

Mandy MacDonald, Police Legal Advisor, explained this ordinance is based upon changes to Colorado law that now allows the City to operate photo speed enforcement vehicles without a city employee operator inside, so the City has engaged a vendor to issue these penalty assessments.

J. Batchelor added that one of the biggest changes is the old ordinance said it had to be manned, but the change in state law no longer requires that. He noted this was one of the big things driving our negative financial performance.

CM Jurinsky asked if they are back to getting bids.

J. Batchelor responded that they had bids and selected the vendor. He said they are also working through equipment procurement and a rollout plan right now.

P. Schulte asked if there were any objection with moving this forward.

There were no objections.

4.b Public Safety Action Plan Update

Current Staffing

J. Batchelor reported on staffing and training numbers.

M. Hildebrand stated that right now that they have an FTEP that will come out in Octboer with around 35 people. He said they are experiencing the lowest attrition that he has seen in a long time, and are starting a class in September with around 35 people as well. He noted that they are aiming for 30 to 35 people per Academy class and they are getting a lot of lateral requests across the state right now.

CM Jurinsky shared some of the feedback she is getting from laterals, which is they love the fast track and the lateral bonus.

P. Schulte appreciated Council's support in changing he hiring process, as it has been very beneficial.

M. Hildebrand said that in some of the lateral interviews, they were excited about some of the policy changes in going after offenders and being police again.

CM Jurinsky commented that before Chief Chamberlain got there, there was no police work going on in this department for who knows how long, and they are on the right track right now. She voiced that officers are calling her from all kinds of different departments saying they want to come to Aurora after hearing the culture has changed and there is a nice bonus.

CM Hancock expressed that she did a ride along last week and pretty much covered the Ward 4 area and up and down the Colfax corridor, and did a survey in terms of how the officers were feeling in terms of support, activity, training, and all the changes. She stated that you could feel down to the troops the feeling of they are actually fighting crime now, the atmosphere on the street has changed, and they had high praise for the chief.

Crime Rates

J. Batchelor went over the crime rate numbers, showing significant decreases year to date across the crime categories. He said they had a little pop up on the prior four weeks.

M. Hildebrand added that July is a bigger time of year, so some of that increase is seen there, but he looks at the year to date. He said he is really in tune with their fatal and nonfatal shootings, and they are 17 fatal shootings down over a year. He explained that seeing a plus is concerning, but they are also going to trend that over some time. However, if they continue to see those pluses, that is very concerning. He mentioned that they are seeing things with popup parties and house parties and Denver is seeing the same trends. He stated that these parties are attracting the wrong people, with a mixture of criminals and kids that just go to attend a party, which makes a large group that inevitably ends with a shooting, a fight, or

something else. He shared they are taking a much more proactive stance on those and have worked with Aurora 911 to create a new call called House Party and hopefully they can identify who is hosting the parties, hold them accountable, and disperse these parties to prevent shootings, as five of their shooting homicides this year were directly connected to house parties.

CM Jurinsky praised 911 for an incident she had to call about. She explained that she had to call them because a homeless man showed up on her patio at JJ's, who had a blow torch for his foilies and dumped his bag out all over the patio. She went out to confront him and he had a gun on the patio, so she called 911. The 911 operator started in with questions, but she told her there was a man with a gun on her patio and the operator stopped with the questions and said they were en route and the police got there immediately.

CM Kassaw shared that there was another homeless person found dead of an overdose yesterday in a small business parking lot.

T. Bunetta thanked CM Jurinsky for the feedback and said she would pass that on to the team. She said questions will always remain, but the great thing about protocol now is that they have the ability to fast track and immediately deploy.

CM Hancock commented it was good to know they have the flexibility to do that.

Youth Violence

L. Battan reported that in July, they had success with 11 of their saved candidates, including 5 for 5 last night. She said they are gearing up for the next call-in in September for juvenile only, which is the first time they are doing that for SAVE.

CM Jurinsky asked if they are working closely with The Road Called Straight on this.

L. Battan responded yes, they are their partners.

J. Batchelor added that is one of the great things about the stories, is they talk about the work of our partners.

CM Hancock asked when they are going to be compelled to come.

L. Battan answered that they already have that in place with the 18th, where they are court-ordering people to attend. She said they have not implemented the 17th yet, but look forward to working with our 18th partners to show the 17th partners the work we do and what it is working.

Crisis Response Team

L. Battan voiced that they had 500 calls for service between AMRT and CRT, and they stood up their third AMRT unit. She said their Targeted Violence Prevention team really engaged with all different levels of government in getting people help that needed it who are threatening mass violence. She said case management is a crucial part in getting people connected to resources, which will hopefully interrupt some of the high utilization cycle.

CM Jurinsky asked if they have seen any violence towards their clinicians.

L. Battan answered not that she is aware of lately.

CM Hancock voiced that it is great to have three now.

L. Battan added that they are hiring for a Targeted Violence Prevention clinician and case manager right now.

J. Batchelor noted there are writeups and stories in the packet on these to help citizens understand the type of work they are doing.

Homeless Encampment

J. Batchelor discussed the number of abatements, referrals, and year to date numbers regarding the homeless. He pointed out a little uptick in 2025, which shows that we are getting out and doing more abatements.

CM Jurinsky asked if we are still billing the state on the CDOT related ones.

J. Batchelor answered yes, that there is an IGA with CDOT, and when we are taking care of things on CDOT property, our abatement contractor takes care of that and then we bill them. He broke down the numbers by ward as well, and said J. Prosser and her team are doing a good job coordinating and they have a good feel for where the hot spots are.

CM Jurinsky inquired if the HART team included police officers.

J. Batchelor responded yes.

CM Jurinsky noted that a lot of the homeless have weapons on them, so she was glad police were a part of these.

4.c Domestic Violence Update August 2025

C. Atkinson updated that the stats of July 30th, which are 2,358 open DV cases, 2 new DV cases in the last 30 days, 1,028 active DV warrants, and 354 DV cases on probation.

P. Schulte noted that the two new DV cases were the two that occurred on June 30th.

CM Jurinsky asked the chief if there were going to do anything about the active warrants.

P. Schulte expressed that his office was reviewing the cases that have active warrants and a substantial number of them were getting dismissed because they have been just sitting there.

C. Atkinson added they are sending a report to the prosecutor's office on ones that are expiring every month for them to be reviewed instead of automatically renewing them at the 7 year mark.

CM Jurinsky voiced interest in seeing the active warrants within the past two years and seeing what they can do with the police department to put a team together quickly to try and clear some of these warrants and catch some of these people.

M. Hildebrand responded that if they can develop a list and push it out and dedicate a couple units to warrant pickups, they could probably scrub that list pretty quickly as long as they are pretty recent.

CM Jurinsky recommended putting an emphasis on taking 30 days and trying to clear some of these warrants.

M. Hildebrand said he would work on that.

C. Atkinson discussed open DV cases by county, by year, and age by year filed. She also went over the time between filing and disposition, with many dispositions occurring 90 days after the incident date. She talked about DV cases filed by month, DV statistics by the last 5 years, and active DV dispositions. She asked how often they want updates and what would they like to see.

CM Jurinsky answered that she would like to see the numbers go down and get out of our court.

P. Schulte stated that they have the Speedy Trial Act that requires them to get rid of these in 90 days, which is why they are seeing these numbers, so it will really be telling in December. He asked if they wanted to wait until December to have another update.

CM Jurinsky voiced that they will not have a meeting in December, and asked if they could do it in November.

P. Schulte answered yes.

CM Jurinsky requested for them to try not to dismiss any involving an assault unless it is very old.

P. Schulte responded there is a very specific criteria they talked about, which are the ones that have good probable cause, witnesses, and the police officers still here to keep those active.

CM Jurinsky said she would like to see how many active cases we still have in our court, how many active warrants, and how many are still on probation in November.

C. Atkinson shared they did not replace some probation officers that left because they were unwinding them, and right now they have a very high caseload between 120 to 130 per PO, which is really high, but expects that to go down by December.

5. Miscellaneous Matters for Consideration

S. Day asked the Committee if they were okay with them presenting on the court hours for 2026 at Study Session scheduled for September 11th.

CM Jurinsky answered yes. She asked if the police were working four 10's.

M. Hildebrand answered yes.

T. Bunetta introduced Allison Heider, Aurora 911's Senior Communications Strategist, who helped them establish their public engagement and community engagement platforms and is doing an exceptional job of making connections. She said she was looking forward to building bridges with many different areas.

J. Batchelor explained that T. Bunetta and her team have come to some of the board meetings and presented and got really positive feedback, and she decided that they should be doing more of that by having dedicated resource to help tell the 911 story to our citizens and help them understand the process.

CM Jurinsky expressed she did a jail shift a couple weeks ago and loved the new device on deciphering types of drugs, and she was trained on it. She said in talking with detention staff and officers from all three districts coming in, and morale is definitely up. She shared that there are several seasoned officers coming in to help officers expedite the process with paperwork and computer input, but she would

still like to see it go a little bit faster so officers can get back on the road sooner. She also wanted to see the upstairs of the jail reopened and was not happy to hear that our 72-hour holds are being sent to the county.

C. Atkinson responded they had some facility issues with electrical and plumbing, and the plan was to open on the 18th, but they had to delay it by a week.

M. Hildebrand voiced that over the last few years, they have looked at efficiencies in trying to reduce the process, but they can take another look at that. He noted that some of it our process, some of it is the jail intake process, and some of it is the requirement of the counties. He said that DV stuff also adds time because they have to do affidavits. However, this is the fastest that it has even been.

CM Hancock asked if there could be some process improvement in how the forms are or if there are some things that can be filled in automatically that are on every form to help speed it up a little bit.

M. Hildebrand responded that some of the information they have to input is how they flag certain things and collect data, and they are required to do certain things that they cannot get around, which causes the process to be what it is. However, they will take another look at the Versadex system and see if there are any other places they can try to streamline it.

CM Jurinsky pointed out that some of the homeless people are coming in with bundles of stuff, so maybe having a second property intake station could help speed up some things. She believed that some of it is because they are policing again and she was there on a Friday night shift, which is very busy.

P. Schulte added what takes the longest is for the court process, as they make the officers sit there at the jail and do all the probable cause statements, instead of just dropping them off, which is what takes the most time. He recommended not changing that, because he wants the officers to be completely done with all the court paperwork when they go back out.

CM Jurinsky appreciated seeing more seasoned officers giving their time to helping, but suggested maybe looking into injured officers or those that need to be on light duty to help with that.

M. Hildebrand stated that light duty fluctuates and they would want somebody who is going to be on light duty for a period of time so they can go in there, learn the processes, and be a help and not hold things up. He said they have done it on overtime. He added the longer the officers are with the people going to jail, they more opportunities there are for them to get agitated and be conflict between them and our officers, as they spend a long period of time in handcuffs.

CM Jurinsky reiterated that a big delay was property and how much stuff people are coming into the jail with, and having just one property station was not very efficient. She recommended getting officers on light duty to help, utilizing the space at the jail when waiting, and seeing what it would take to put in a second camera for property intake. She said ultimately, morale was up with detention staff and officers, she loved seeing the machine so officers do have to expose themselves to the drugs, and it was very positive apart from the waiting time issue. She asked if the City was getting money from the phones in the holding cells that are being used, because it was being used all night long.

C. Atkinson believed there was a charge for that, but said she will look into it. She felt they were probably getting a portion back on that, as they have a vendor it goes through, but did not know how much. She added that other council members are also welcome to come to the jail any time.

P. Schulte voiced he would look to see what they could do legally regarding that.

6. Confirm Next Meeting

CM Jurinsky stated the next meeting is September 11, 2025, at 9 a.m.

7. Adjournment

APPROVED: _____

Danielle Jurinsky, Chair

CITY OF AURORA
Council Agenda Commentary

Item Title: Police Retention Update
Item Initiator: Danelle Carrel, Executive Support Manager
Staff Source/Legal Source: John Schneebeck, Business Services Manager / Mandy MacDonald, Assistant City Attorney
Outside Speaker: N/A
Council Goal: 2012: 1.0--Assure a safe community for people

COUNCIL MEETING DATES:

Study Session: N/A

Regular Meeting: N/A

ITEM DETAILS *(Click in highlighted area below bullet point list to enter applicable information.)*

John Schneebeck, Business Services Manager / Mandy MacDonald, Assistant City Attorney

ACTIONS(S) PROPOSED *(Check all appropriate actions)*

☐ Approve Item and Move Forward to Study Session

☐ Approve Item as proposed at Study Session

☐ Approve Item and Move Forward to Regular Meeting

☐ Approve Item as proposed at Regular Meeting

☒ Information Only

☐ Approve Item with Waiver of Reconsideration
Reason for waiver is described in the Item Details field.

PREVIOUS ACTIONS OR REVIEWS:

Policy Committee Name: N/A

Policy Committee Date: N/A

Action Taken/Follow-up: ***(Check all that apply)***

☐ Recommends Approval

☐ Does Not Recommend Approval

☐ Forwarded Without Recommendation

☐ Recommendation Report Attached

☐ Minutes Attached

☐ Minutes Not Available

HISTORY *(Dates reviewed by City council, Policy Committees, Boards and Commissions, or Staff. Summarize pertinent comments. ATTACH MINUTES OF COUNCIL MEETINGS, POLICY COMMITTEES AND BOARDS AND COMMISSIONS.)*

N/A

ITEM SUMMARY *(Brief description of item, discussion, key points, recommendations, etc.)*

Monthly update on Police Retention.

FISCAL IMPACT

Select all that apply. (If no fiscal impact, click that box and skip to "Questions for Council")

☐ Revenue Impact ☐ Budgeted Expenditure Impact ☐ Non-Budgeted Expenditure Impact
☐ Workload Impact ☒ No Fiscal Impact

REVENUE IMPACT
Provide the revenue impact or N/A if no impact. (What is the estimated impact on revenue? What funds would be impacted? Provide additional detail as necessary.)

BUDGETED EXPENDITURE IMPACT
Provide the budgeted expenditure impact or N/A if no impact. (List Org/Account # and fund. What is the amount of budget to be used? Does this shift existing budget away from existing programs/services? Provide additional detail as necessary.)

NON-BUDGETED EXPENDITURE IMPACT
Provide the non-budgeted expenditure impact or N/A if no impact. (Provide information on non-budgeted costs. Include Personal Services, Supplies and Services, Interfund Charges, and Capital needs. Provide additional detail as necessary.)

WORKLOAD IMPACT
Provide the workload impact or N/A if no impact. (Will more staff be needed or is the change absorbable? If new FTE(s) are needed, provide numbers and types of positions, and a duty summary. Provide additional detail as necessary.)

QUESTIONS FOR COUNCIL

Information Only

LEGAL COMMENTS

The City Manager shall be responsible to the council for the proper administration of all affairs of the City placed in his charge and, to that end, he shall have the power and duty to make written or verbal reports to the Council concerning the affairs of the city under his supervision. (City Charter §7-4(e)). (MacDonald)

Aurora Police Department

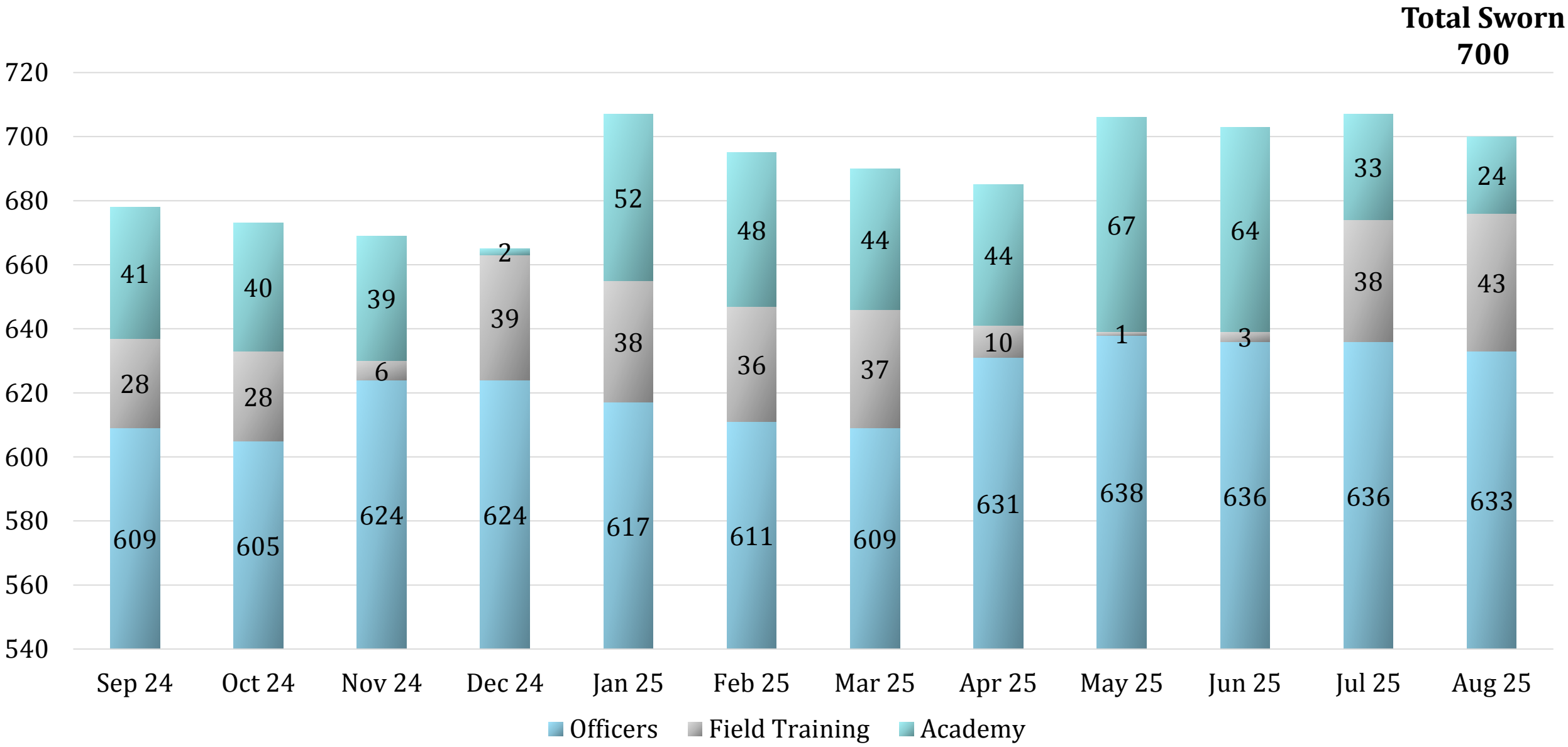
Mission: Partnering with our community to make Aurora safer every day

Vision: APD will continually evolve as an innovative agency

Business Services Division

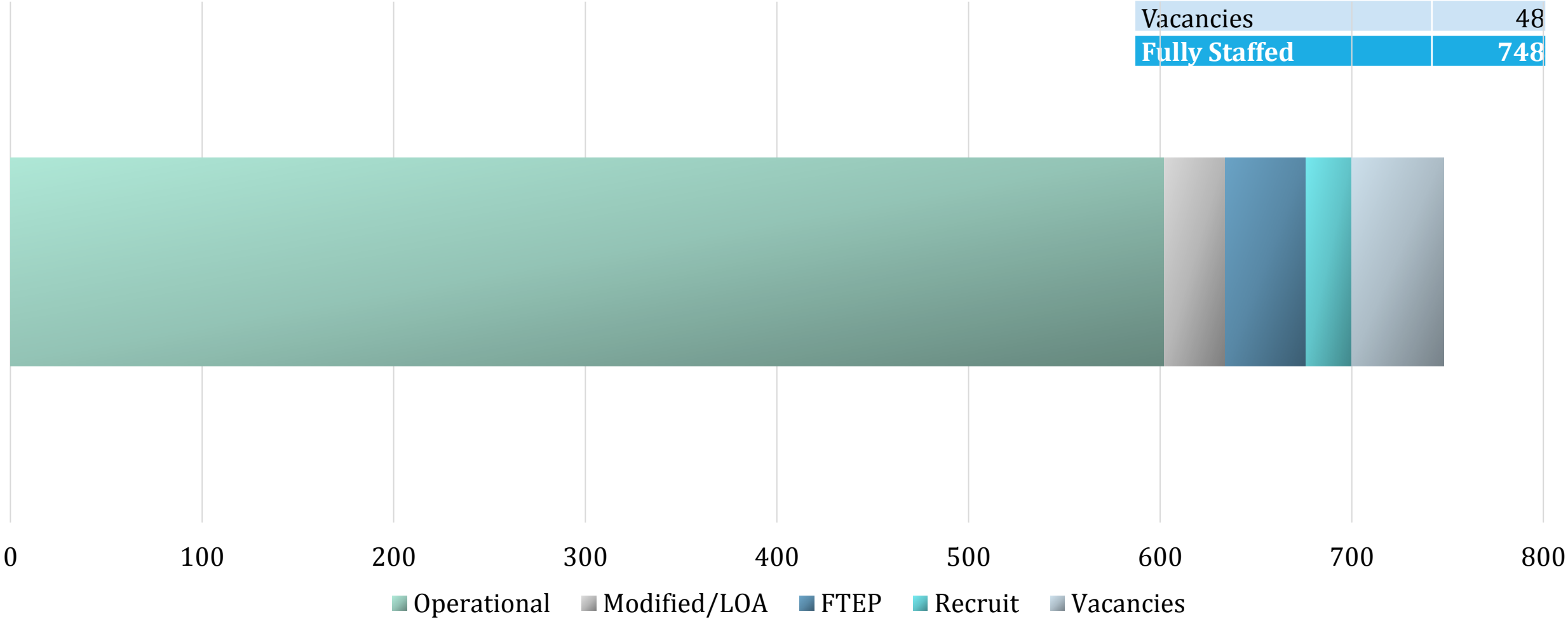
MONTHLY RETENTION REVIEW

Sworn Staffing



Sworn Staffing Status

Status	Total
Operational	601
Modified/LOA	32
FTEP	43
Recruit	24
Vacancies	48
Fully Staffed	**748**



2025 Sworn Staffing

Additions:

76 Basics (2025-1B 49, 2025-2B 27)
10 Laterals (2025-1L 4, 2025-2L 6)
6 Reinstatements
92 Total Adds

Losses as of 8/31/25:

39 Resignations (13 commissioned, 8 FTEP, 18 recruits)
13 Retirements
3 Transfers (1 commissioned, 2 FTEP)
1 Death (1 commissioned)
1 Termination (1 commissioned)
57 Total Losses

35 Net Additions

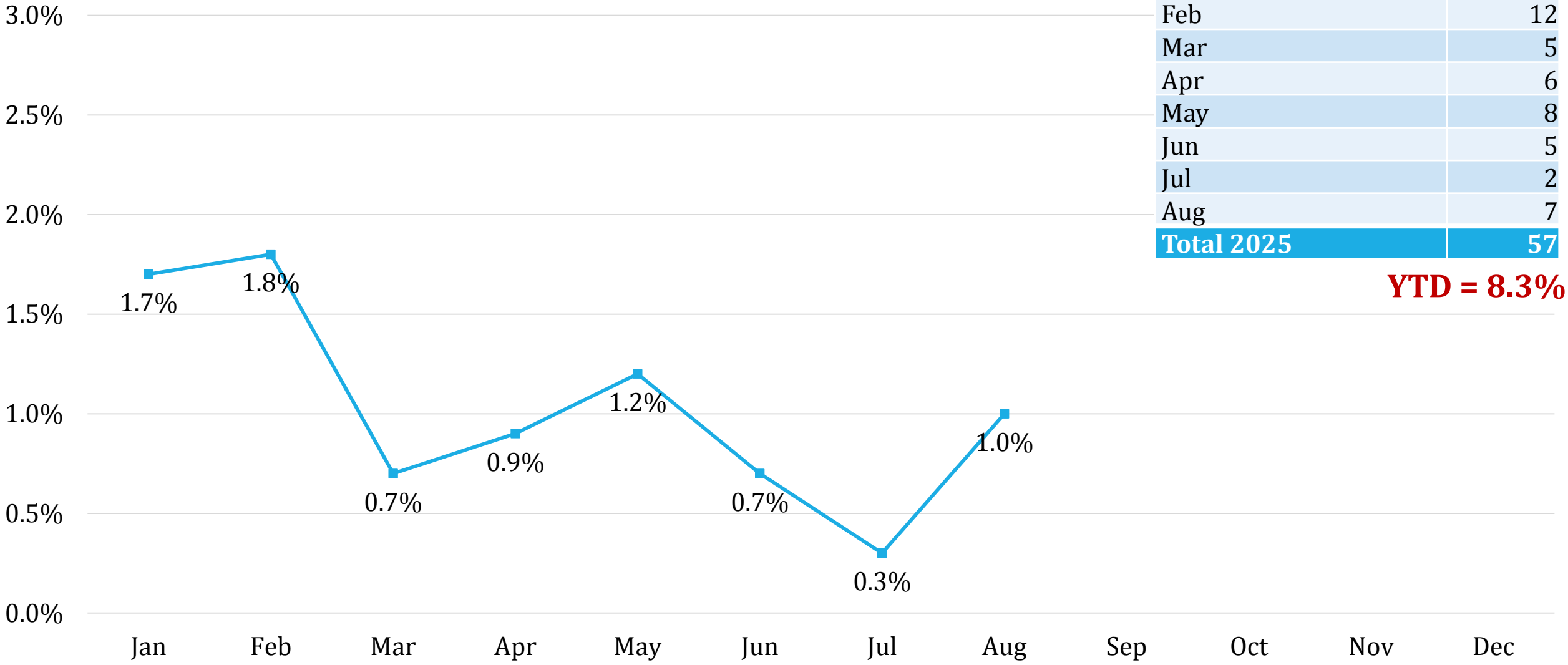
August FTEP/Recruit Numbers

Class	Count	FTEP Completion
Reinstatements	1	4-8 weeks
2024-2B (6/17/24) deferred to 2025-1B FTEP	1	10/24/25
2024-2B (6/17/24) deferred to 2025-2B	1	2/27/26
2025-1B (1/13/25) FTEP	35	10/24/25
2025-1B (1/13/25) deferred	4	2/27/26
2025-2B (5/19/25)	19	2/27/26
2025-2L (7/29/25) FTEP	6	10/10/25
Total	**67**	

Police Turnover Percent

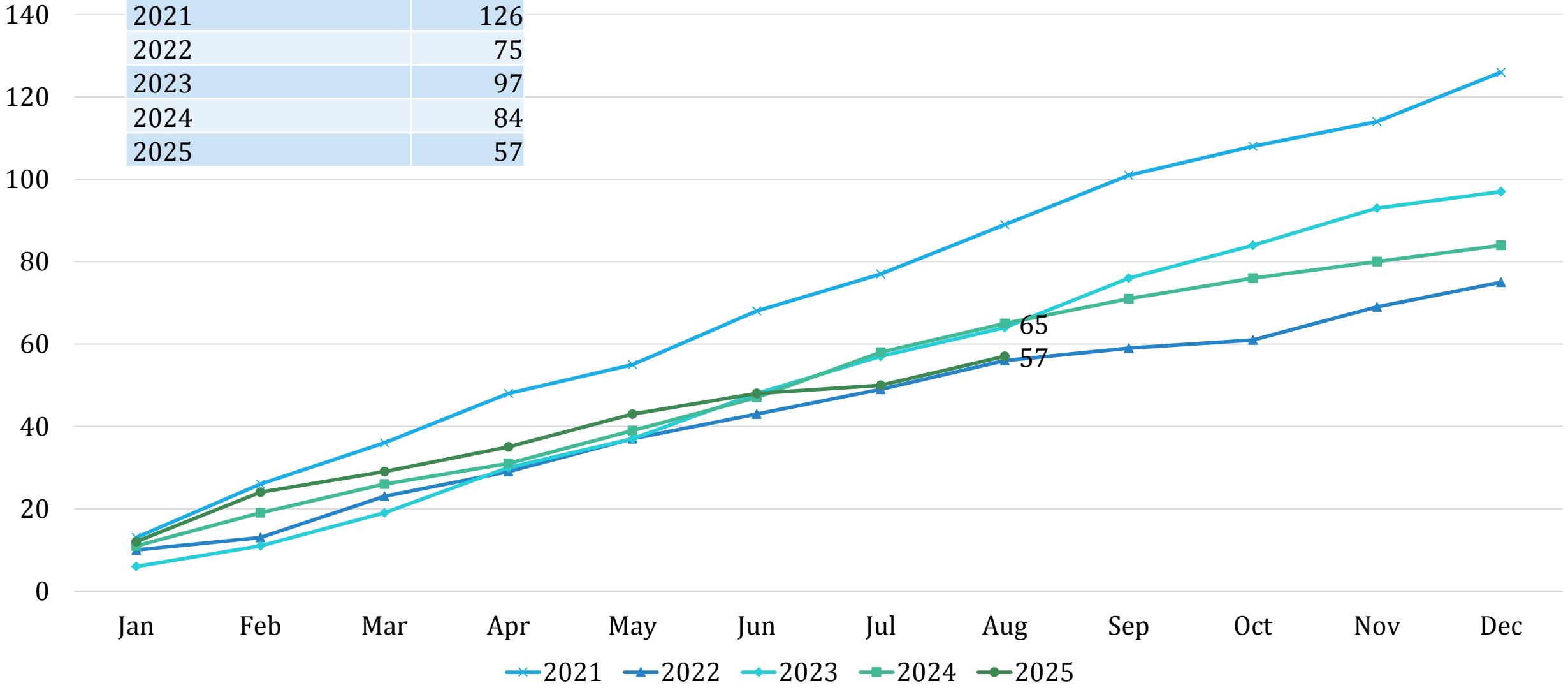
Month	Total
Jan	12
Feb	12
Mar	5
Apr	6
May	8
Jun	5
Jul	2
Aug	7
Total 2025	**57**

YTD = 8.3%



Attrition Review

Year	Total
2021	126
2022	75
2023	97
2024	84
2025	57



August Sworn Separations Detail

6 Resignations (3 commissioned, 3 recruits)
1 Retirement
7 Total Losses

Category	Count
Personal Reasons	4
Move from Area	2
Retirement	1
Total	**7**

Assignment	Count
Recruit	3
Investigations	2
Patrol	2
Total	**7**

CITY OF AURORA
Council Agenda Commentary

Item Title: Motor Vehicle Theft Recovery Voucher Program Update
Item Initiator: Danelle Carrel, Executive Support Manager
Staff Source/Legal Source: John Schneebeck, Business Services Manager / Mandy MacDonald, Assistant City Attorney
Outside Speaker: N/A
Council Goal: 2012: 1.0--Assure a safe community for people

COUNCIL MEETING DATES:

Study Session: N/A

Regular Meeting: N/A

ITEM DETAILS *(Click in highlighted area below bullet point list to enter applicable information.)*

John Schneebeck, Business Services Manager / Mandy MacDonald, Assistant City Attorney

ACTIONS(S) PROPOSED *(Check all appropriate actions)*

☐ Approve Item and Move Forward to Study Session

☐ Approve Item as proposed at Study Session

☐ Approve Item and Move Forward to Regular Meeting

☐ Approve Item as proposed at Regular Meeting

☒ Information Only

☐ Approve Item with Waiver of Reconsideration
Reason for waiver is described in the Item Details field.

PREVIOUS ACTIONS OR REVIEWS:

Policy Committee Name: N/A

Policy Committee Date: N/A

Action Taken/Follow-up: ***(Check all that apply)***

☐ Recommends Approval

☐ Does Not Recommend Approval

☐ Forwarded Without Recommendation

☐ Recommendation Report Attached

☐ Minutes Attached

☐ Minutes Not Available

HISTORY *(Dates reviewed by City council, Policy Committees, Boards and Commissions, or Staff. Summarize pertinent comments. ATTACH MINUTES OF COUNCIL MEETINGS, POLICY COMMITTEES AND BOARDS AND COMMISSIONS.)*

N/A

ITEM SUMMARY *(Brief description of item, discussion, key points, recommendations, etc.)*

Monthly update on the Motor Vehicle Theft Recovery Program.

FISCAL IMPACT

Select all that apply. (If no fiscal impact, click that box and skip to "Questions for Council")

☐ Revenue Impact ☐ Budgeted Expenditure Impact ☐ Non-Budgeted Expenditure Impact
☐ Workload Impact ☒ No Fiscal Impact

REVENUE IMPACT
Provide the revenue impact or N/A if no impact. (What is the estimated impact on revenue? What funds would be impacted? Provide additional detail as necessary.)

N/A

BUDGETED EXPENDITURE IMPACT
Provide the budgeted expenditure impact or N/A if no impact. (List Org/Account # and fund. What is the amount of budget to be used? Does this shift existing budget away from existing programs/services? Provide additional detail as necessary.)

N/A

NON-BUDGETED EXPENDITURE IMPACT
Provide the non-budgeted expenditure impact or N/A if no impact. (Provide information on non-budgeted costs. Include Personal Services, Supplies and Services, Interfund Charges, and Capital needs. Provide additional detail as necessary.)

N/A

WORKLOAD IMPACT
Provide the workload impact or N/A if no impact. (Will more staff be needed or is the change absorbable? If new FTE(s) are needed, provide numbers and types of positions, and a duty summary. Provide additional detail as necessary.)

N/A

QUESTIONS FOR COUNCIL

N/A

LEGAL COMMENTS

The City Manager shall be responsible to the council for the proper administration of all affairs of the City placed in his charge and, to that end, he shall have the power and duty to make written or verbal reports to the Council concerning the affairs of the city under his supervision. (City Charter §7-4(e). (MacDonald)

CITY MVTR VOUCHER PROGRAM
City Of Aurora
August 2025

DATE	AMOUNT ISSUED	AMOUNT REDEEMED
8/1/2025	$1,470.00	$1,470.00
8/2/2025	$840.00	$840.00
8/4/2025	$755.00	$755.00
8/5/2025	$595.00	$595.00
8/6/2025	$715.00	$715.00
8/7/2025	$795.00	$795.00
8/8/2025	$1,310.00	$995.00
8/9/2025	$935.00	$935.00
8/11/2025	$515.00	$795.00
8/12/2025	$560.00	$560.00
8/13/2025	$200.00	$200.00
8/14/2025	$715.00	$680.00
8/15/2025	$1,825.00	$1,825.00
8/16/2025	$915.00	$915.00
8/18/2025	$400.00	$400.00
8/19/2025	$1,500.00	$1,500.00
8/20/2025	$400.00	$400.00
8/21/2025	$835.00	$835.00
8/22/2025	$835.00	$830.00
8/23/2025	$0.00	$0.00
8/25/2025	$795.00	$795.00
8/26/2025	$1,400.00	$1,400.00
8/27/2025	$955.00	$955.00
8/28/2025	$1,127.00	$1,092.00
8/29/2025	$0.00	$0.00
8/30/2025	$240.00	$240.00
August Total	**$20,632.00**	**$20,522.00**
YTD Total	**$163,487.10**	**$162,122.10**
Program Grand Total		**$1,002,917.45**

CITY OF AURORA
Council Agenda Commentary

Item Title: Special Operations Crime Suppression Update
Item Initiator: Danelle Carrel, Executive Support Manager
Staff Source/Legal Source: Matt Brukbacher, Police Commander / Mandy MacDonald, Assistant City Attorney
Outside Speaker: N/A
Council Goal: 2012: 1.0--Assure a safe community for people

COUNCIL MEETING DATES:

Study Session: N/A

Regular Meeting: N/A

ITEM DETAILS *(Click in highlighted area below bullet point list to enter applicable information.)*

Matt Brukbacher, Police Commander / Mandy MacDonald, Assistant City Attorney

ACTIONS(S) PROPOSED *(Check all appropriate actions)*

☐ Approve Item and Move Forward to Study Session

☐ Approve Item as proposed at Study Session

☐ Approve Item and Move Forward to Regular Meeting

☐ Approve Item as proposed at Regular Meeting

☒ Information Only

☐ Approve Item with Waiver of Reconsideration
Reason for waiver is described in the Item Details field.

PREVIOUS ACTIONS OR REVIEWS:

Policy Committee Name: N/A

Policy Committee Date: N/A

Action Taken/Follow-up: ***(Check all that apply)***

☐ Recommends Approval

☐ Does Not Recommend Approval

☐ Forwarded Without Recommendation

☐ Recommendation Report Attached

☐ Minutes Attached

☐ Minutes Not Available

HISTORY *(Dates reviewed by City council, Policy Committees, Boards and Commissions, or Staff. Summarize pertinent comments. ATTACH MINUTES OF COUNCIL MEETINGS, POLICY COMMITTEES AND BOARDS AND COMMISSIONS.)*

N/A

ITEM SUMMARY *(Brief description of item, discussion, key points, recommendations, etc.)*

Monthly update to account for proactive activities by the Speciality Units within the Special Operations Bureau. The attached documents will cover the activities of the Traffic Bureau, the Operations Support Section (Swat, Fugitive, and Safe Streets Task Force), and the Investigative Support Section (Gang Unit, DART Unit, Narcotics Unit, and the GRIT Unit).

FISCAL IMPACT

Select all that apply. (If no fiscal impact, click that box and skip to "Questions for Council")

☐ Revenue Impact ☐ Budgeted Expenditure Impact ☐ Non-Budgeted Expenditure Impact
☐ Workload Impact ☒ No Fiscal Impact

REVENUE IMPACT
Provide the revenue impact or N/A if no impact. (What is the estimated impact on revenue? What funds would be impacted? Provide additional detail as necessary.)

BUDGETED EXPENDITURE IMPACT
Provide the budgeted expenditure impact or N/A if no impact. (List Org/Account # and fund. What is the amount of budget to be used? Does this shift existing budget away from existing programs/services? Provide additional detail as necessary.)

NON-BUDGETED EXPENDITURE IMPACT
Provide the non-budgeted expenditure impact or N/A if no impact. (Provide information on non-budgeted costs. Include Personal Services, Supplies and Services, Interfund Charges, and Capital needs. Provide additional detail as necessary.)

WORKLOAD IMPACT
Provide the workload impact or N/A if no impact. (Will more staff be needed or is the change absorbable? If new FTE(s) are needed, provide numbers and types of positions, and a duty summary. Provide additional detail as necessary.)

QUESTIONS FOR COUNCIL

Information Only

LEGAL COMMENTS

The City Manager shall be responsible to the council for the proper administration of all affairs of the City placed in his charge and, to that end, he shall have the power and duty to make written or verbal reports to the Council concerning the affairs of the city under his supervision. (City Charter §7-4(e)). (MacDonald)

Public Safety and Courts
APD Special Operations Bureau
Crime Suppression
September 2025
2024/2025 YTD
August 3 thru August 30 stats

Citywide Weekly Crime Summary

Aurora Police Department - PACT Statistics — District: ALL

*Trend crimes are measured by a count of **incidents** that **occurred** during the data periods*	Wk 31	Wk 32	Wk 33	Wk 34	*(52 Week) Weekly Avg*	4 Week Prior	4 Week Current	4 Week Difference	4 Week % Chg	*(3 Year) 4 Week Avg*	Y -T- D Last Year	Y -T- D Current Year	Y-T-D Difference	Y-T-D % Chg	*(5 Year) Y-T-D Avg*
Current Wk 35: 08/25/25 - 08/31/25						06/30 - 07/27	07/28 - 08/24	+ or -	% chg	*avg*	01/01 - 08/24		+ or -	% chg	*avg*
Major Crimes															
Murder	**1**	**1**	**0**	**0**	***1***	**4**	**2**	**-2**	**(50.0%)**	***5***	**28**	**22**	**-6**	**(21.4%)**	***26***
Sex Assault	**4**	**3**	**3**	**5**	***5***	**26**	**15**	**-11**	**(42.3%)**	***29***	**196**	**170**	**-26**	**(13.3%)**	***221***
Aggravated Assault	**36**	**33**	**45**	**43**	***39***	**155**	**157**	**+2**	**1.3%**	***181***	**1,367**	**1,225**	**-142**	**(10.4%)**	***1,315***
All Gang Involved Activity	8	5	5	4	*5*	14	22	+8	57.1%	*29*	214	175	-39	(18.2%)	*389*
All Shootings (bullet hit flesh)	1	1	2	1	*1*	5	5	+0	0.0%	*12*	68	41	-27	(39.7%)	*84*
Robbery	**17**	**7**	**9**	**13**	***8***	**34**	**46**	**+12**	**35.3%**	***57***	**349**	**239**	**-110**	**(31.5%)**	***465***
Robbery Commercial	6	1	0	3	*2*	6	10	+4	66.7%	*15*	96	49	-47	(49.0%)	*146*
Robbery Individual	11	6	9	10	*6*	28	36	+8	28.6%	*43*	253	190	-63	(24.9%)	*319*
Robbery Street	10	4	8	9	*6*	26	31	+5	19.2%	*37*	221	164	-57	(25.8%)	*270*
Robbery Residential	1	2	1	1	*1*	2	5	+3	150.0%	*6*	32	26	-6	(18.8%)	*49*
Burglary	**12**	**17**	**19**	**22**	***21***	**72**	**70**	**-2**	**(2.8%)**	***101***	**876**	**600**	**-276**	**(31.5%)**	***1,060***
Burglary Residential	5	11	6	9	*9*	34	31	-3	(8.8%)	*41*	314	276	-38	(12.1%)	*404*
Burglary Commercial	7	6	13	13	*12*	38	39	+1	2.6%	*60*	562	324	-238	(42.3%)	*656*
Motor Vehicle Theft	**34**	**44**	**45**	**31**	***49***	**160**	**154**	**-6**	**(3.8%)**	***360***	**2,404**	**1,417**	**-987**	**(41.1%)**	***3,206***
MVT	34	44	45	31	*49*	160	154	-6	(3.8%)	*356*	2,304	1,417	-887	(38.5%)	*3,023*
MVT Puffer	2	0	0	2	*2*	1	4	+3	300.0%	*6*	119	57	-62	(52.1%)	*187*
Local MVT/Local Recovery	6	8	8	6	*8*	26	28	+2	7.7%	*64*	423	228	-195	(46.1%)	*583*
Local MVT/Outside Recovery	12	9	8	7	*17*	48	36	-12	(25.0%)	*129*	870	439	-431	(49.5%)	*1,261*
Outside MVT/Local Recovery	20	27	23	13	*21*	68	83	+15	22.1%	*167*	958	643	-315	(32.9%)	*1,421*
Larceny	**111**	**115**	**105**	**96**	***129***	**492**	**427**	**-65**	**(13.2%)**	***563***	**4,641**	**3,966**	**-675**	**(14.5%)**	***5,024***
Larceny from Motor Vehicle	40	34	27	31	*44*	152	132	-20	(13.2%)	*167*	1,396	1,327	-69	(4.9%)	*1,612*
Larceny Shoplift	34	34	40	29	*42*	160	137	-23	(14.4%)	*124*	1,321	1,248	-73	(5.5%)	*963*
Major Index Crimes Occurred	***215***	***220***	***226***	***210***	***252***	***943***	***871***	***-72***	***(7.6%)***	***1,296***	***9,861***	***7,639***	***-2,222***	***(22.5%)***	***11,317***

Ran: 9/2/2025 12:49:31 PM

Tactical Response Section – Lt. Dan Baginski
SWAT and K9

SWAT	August 2024	August 2025	YTD 2024	YTD 2025
Total Deployments:	18	19	194	124
Barricades:	1	0	11	5
Call-outs: Full	0	0	4	4
Call-outs: Part	-	2	-	2
Fugitive Operations w/arrests made:	4	5	67	52
Total arrests:	8	10	140	103
Planned search warrants:	12	6	64	45
Narcotics Assists (buy/bust or flush):	2	3	20	22
Hostage Calls:	0	0	1	0
Trained Intra or Outside Agency:	1	3	33	49
Community Events:	0	0	1	7

K9	August 2024	August 2025	YTD 2024	YTD 2025
Dog Deployments:	83	117	856	699
Patrol Assists:	142	208	1,107	768
Bites:	0	0	3	3
Surrenders:	9	20	45	65
Explosive Searches:	7	7	31	30
Firearms Searches:	15	24	129	109
Narcotics Searches:	0	0	5	3
Guns Located:	1	0	4	4
Casings/Ammunition Located:	4	3	143	89
Community Events:	0	6	1	21
Call Outs	9	7	12	16

Strategic Enforcement Section – Lt. Jason Paulovich
GANGS and FANU

GANGS	August		YTD	
	2024	2025	2024	2025
Felony Arrests:	17	8	49	61
Misdemeanor Arrests:	6	2	40	32
Guns Recovered:	8	5	31	72
Gang Contacts	-	32	-	193
Field Interview (FI)	-	41	-	74

FANU	August		YTD	
	2024	2025	2024	2025
Felony Arrests:	13	24	85	212
Misdemeanor Arrests:	4	0	26	0
Guns Seized:	9	3	47	61
Search Warrants	2	32	18	190
Methamphetamine:	754.5	0	6355.7	73473.83
Heroin:	20.30	0	361.6	3601.59
Cocaine/Crack:	198.80	6.6	1529.4	1040.25
Fentanyl:	0	8.5	14821.1	21494.04
Fentanyl Pills:	1686.90	0	1686.90	2903.14
Marijuana:	0	0	4014.7	16.3
Other Drugs:	33.2	0	491.20	609.7
Money seized:	$27,646.00	0	$87,656.09	$40,817.11

All weights are in ggw

Traffic Section – Lt. Chris Amsler

TRAFFIC	August		YTD	
	2024	2025	2024	2025
Traffic summons issued (Total):	687	796	7,468	6,587
State Summons	93	57	801	861
Muni Traffic	251	245	2,539	2,040
Muni Speeding	343	494	4,128	3,686
Crash reports (Total):	283	326	2,662	2,529
Sworn:	115	32	1,281	479
CSR:	168	294	1,381	2,050
DUI's Total for agency:	35	64	386	508
Traffic DUI's (included above)	0	0	15	14
Fatals:	0	5	32	30
Hit and Runs Total Agency:	138	128	1,460	1,016
Traffic Investigated:	66	44	741	469
Citywide Registration Violations	208	378	1,657	3,913

CITY OF AURORA
Council Agenda Commentary

Item Title: Aurora Police and Aurora Public Schools Memoradum of Understanding
Item Initiator: Danelle Carrel, Executive Support Manager
Staff Source/Legal Source: Michael Hanifin, Commander / Mandy MacDonald, Assistant City Attorney
Outside Speaker: N/A
Strategic Outcome: Safe: Promoting safety in our built environment through effective administration of city codes and ordinances and responding to emergencies appropriately to preserve and enhance the community's sense of security and well-being.

COUNCIL MEETING DATES:

Study Session: 10/6/2025

Regular Meeting: 10/20/2025

2nd Regular Meeting (if applicable): N/A

Item requires a Public Hearing: ☐ Yes ☐ No

ITEM DETAILS *(Click in highlighted area below bullet point list to enter applicable information.)*

- Waiver of reconsideration requested, and if so, why
- Sponsor name
- Staff source name and title / Legal source name and title
- Outside speaker name and organization
- Estimated time: (For Study Session items only indicate combined time needed for presentation and discussion)

Staff Source: Michael Hanifin, Police Commander
Legal Source: Mandy MacDonald, Assistant City Attorney
Estimated Time: 5 minutes

ACTIONS(S) PROPOSED *(Check all appropriate actions)*

☒ Approve Item and Move Forward to Study Session

☐ Approve Item and Move Forward to Regular Meeting

☐ Information Only

☐ Approve Item with Waiver of Reconsideration
Reason for waiver is described in the Item Details field above.

☐ Approve Item as Proposed at Policy Committee

☐ Approve Item as Proposed at Study Session

☐ Approve Item as Proposed at Regular Meeting

PREVIOUS ACTIONS OR REVIEWS:

Policy Committee Name: N/A

Policy Committee Date: N/A

Action Taken/Follow-up: ***(Check all that apply)***

☐ Recommends Approval ☐ Does Not Recommend Approval

☐ Forwarded Without Recommendation ☐ Minutes Not Available

☐ Minutes Attached

HISTORY *(Dates reviewed by City council, Policy Committees, Boards and Commissions, or Staff. Summarize pertinent comments. ATTACH MINUTES OF COUNCIL MEETINGS, POLICY COMMITTEES AND BOARDS AND COMMISSIONS.)*

N/A

ITEM SUMMARY *(Brief description of item, discussion, key points, recommendations, etc.)*

Memorandum of Understanding between Aurora Police Department and Aurora Public Schools to provide for the health, safety, and welfare of the Aurora Public Schools students and staff by providing for partnership programs to high schools.

FISCAL IMPACT

Select all that apply. (If no fiscal impact, click that box and skip to "Questions for Council")

☐ Revenue Impact ☒ Budgeted Expenditure Impact ☐ Non-Budgeted Expenditure Impact
☐ Workload Impact ☐ No Fiscal Impact

REVENUE IMPACT
Provide the revenue impact or N/A if no impact. (What is the estimated impact on revenue? What funds would be impacted? Provide additional detail as necessary.)

Money received for training

BUDGETED EXPENDITURE IMPACT
Provide the budgeted expenditure impact or N/A if no impact. (List Org/Account # and fund. What is the amount of budget to be used? Does this shift existing budget away from existing programs/services? Provide additional detail as necessary.)

Budget is established for the School Resource Officer program and staffed by the authorized number of officers from the department.

NON-BUDGETED EXPENDITURE IMPACT
Provide the non-budgeted expenditure impact or N/A if no impact. (Provide information on non-budgeted costs. Include Personal Services, Supplies and Services, Interfund Charges, and Capital needs. Provide additional detail as necessary.)

N/A

WORKLOAD IMPACT
Provide the workload impact or N/A if no impact. (Will more staff be needed or is the change absorbable? If new FTE(s) are needed, provide numbers and types of positions, and a duty summary. Provide additional detail as necessary.)

N/A

QUESTIONS FOR COUNCIL

Does the Committee approve this MOU to move forward for consideration by full council?

LEGAL COMMENTS

Governments may cooperate or contract with one another to provide any function, service, or facility lawfully authorized to each of the cooperating or contracting units only if such cooperation or contracts are authorized by each party thereto with the approval of its legislative body or other authority having the power to so approve. (Colo. Rev. Stat. §29-1-203(1)). City Council may, by resolution, enter into Intergovernmental Agreements with other governmental units or special districts for the joint use of buildings, equipment or facilities, and for furnishing or receiving commodities or services. (City Charter §10-12). (MacDonald)

AURORA POLICE DEPARTMENT AND AURORA PUBLIC SCHOOLS

SCHOOL RESOURCE OFFICER MEMORANDUM OF UNDERSTANDING

This Memorandum of Understanding, dated as hereinafter set forth, is made, by and between the ADAMS/ARAPAHOE 28J SCHOOL DISTRICT (hereinafter "Aurora Public Schools" and/or the "School District"), and the CITY OF AURORA POLICE DEPARTMENT (hereinafter "Aurora Police Department and/or "Police Department")

PURPOSE: The purpose of this Agreement is to provide for the health, safety and welfare of Aurora Public School students and staff by providing for partnership programs to high schools.

WHEREAS, the Aurora Police Department agrees to provide the Aurora Public Schools a School Resources Officer (SRO) Program in the School District to provide for the health, safety and welfare of Aurora Public School students and staff, and;

WHEREAS, the Aurora Public Schools and the Aurora Police Department desire to set forth in this SRO Agreement the specific terms and conditions of the services to be performed and provided by the SROs in the School District;

1. **Financial Agreements, Equipment and Facilities.**

A. Aurora Public Schools will provide appropriate office space and equipment for the officer(s) assigned to each school location. The space will allow for confidential discussions as well as uninterrupted interviews between officers, students, parents, and staff.

B. The cost of the SRO Program shall be paid by the Aurora Police Department, however, when appropriate, representatives from the School District or the individual school administration and the Police Department may discuss financial arrangements for additional equipment, training, or other programs that would be mutually beneficial for all organizations.

2. **Employment of School Resource Officers.**

A. The SROs shall be employees of the Police Department and shall be subject to the administration, supervision and control of the Police Department.

B. The SROs shall be subject to all personnel policies and practices of the Police Department except as such policies or practices may be modified by the terms and conditions of this Agreement.

C. The Police Department, in its sole discretion, shall have the power and authority to hire, discharge, and discipline SROs.

D. Selections for SRO positions shall be made exclusively by the Aurora Police Department. If a principal or designated administrator is dissatisfied with an SRO who has been assigned to that principal's school, then that principal may discuss concerns and alternatives with Commander of the SRO program up to and including requesting that a different SRO officer be assigned to the designated area. APD shall take reasonable actions to address the principal's concerns up to and including assigning a new SRO to the designated area.

E. Aurora public schools request that two SROs be assigned to the following schools:

-Aurora Central High School

-Hinkley High School

-Aurora West Prep Academy

-Vista Peak Preparatory

-Gateway High School

-Rangeview High School

The Aurora Police Department will have a minimum of 2 officers assigned to 4 of the above High Schools. The Aurora Police Department shall have the ability to make staffing changes as necessary to accommodate departmental needs.

3. **Duty Hours.**

A. Whenever possible, it is the intent of the parties that the SRO's duty hours shall conform to the school day.

B. It is understood and agreed that time spent by SROs attending municipal court, juvenile court, and/or criminal cases arising from and/or out of their employment as an SRO shall be considered as hours worked under this Agreement.

C. In the event of an emergency, if one or more SROs are ordered by the Police Department to leave their school during normal duty hours as described above and to perform other services for the Police Department, then the time spent shall not be considered hours worked under this Agreement.

D. In the event an SRO is absent from work, the SRO shall notify his or her supervisor in the Police Department. The Police Department will assign another qualified officer, if available, to substitute for the SRO who is absent. In the event additional officers are unavailable, the Aurora Police Department will inform school administration of the unavailability as soon as practicable.

4. **Term of Agreement.**

A. The initial term of this Agreement is three years commencing on the ___ day of _____, , and ending on the ____ day of _____,, however, should either party encounter budgetary or personnel constraints that make the continuation of this agreement impractical, then either party may cancel this agreement upon sixty days notice to the other.

B. This Agreement shall be automatically renewed for successive one-year periods unless either party requests termination or modification of this agreement after one year. Requests for termination or modifications will be made in writing and signed by both parties with 60 days' notice. This Agreement will remain in effect until either party terminates this agreement.

5. **Duties of School Resource Officers.**

The SRO's duties will include, but not be limited to, the following:

A. To be an extension of the principal's office for assignments consistent with this Agreement.

B. To be a visible, active law enforcement figure on campus dealing with law enforcement matters and originating on the assigned campus. SRO's will not be responsible for discipline or involved in school code violations.

C. To provide a classroom resource for law education using approved materials.

D. To be a resource and partner to APS Security and provide guidance and training to Principals and school staff on crisis management protocols and scenarios.

E. To be a resource for students which will enable them to be associated with a law enforcement figure and role model in the students' environment.

F. To be a resource for teachers, parents and students for conferences on an individual basis dealing with individual problems or questions, particularly in the area of substance control.

G. To make appearances before site councils, parent groups, and other groups associated with the campus and as a speaker on a variety of requested topics, particularly drug and alcohol abuse.

H. To document activities of all SROs on and off campus and as a compiler of a monthly report to be provided to the SRO Sergeant, to the principal of the assigned school and to the APS Director of Security.

I. It will be the responsibility of the SRO to report all crimes originating on campus. Information on cases that are worked off-campus by the Police Department or other agencies involving students on a campus served by an SRO will be provided to the SRO. As a courtesy, APD will inform school administration of the existence of investigations involving off campus activities of students.

K. The SRO will share information with the administrator about persons and conditions that pertain to campus safety concerns.

L. The SRO will be familiar with helpful community agencies, such as mental health clinics, drug treatment centers, etc., that offer assistance to dependency- and delinquency-prone youths and their families. Referrals will be made when necessary.

M. The SRO and the principal will develop plans and strategies to prevent and/or minimize dangerous situations which might result in student unrest with the understanding that disciplining students is a School District responsibility. SROs shall not be utilized to enforce school code violations.

N. The SRO will coordinate all of his/her activities with the principal and staff members concerned and will seek permission, guidance, and advice prior to enacting any programs within the school.

O. The SRO may be asked to provide community wide crime prevention presentations that include, but are not limited to:

1. Drugs and the law – Adult and juvenile;
2. Alcohol and the law – Adult and juvenile;
3. Sexual assault prevention;
4. Safety programs – Adult and juvenile;
5. Assistance in other crime prevention programs as assigned.

P. The SROs will wear their department authorized duty weapons and uniform in accordance with APD policy.

Q. SRO's will wear and operate Body Worn Cameras in accordance with APD policy.

R. The Police Department will furnish LPR (License Plate Reader) cameras at high schools for two years at no cost to the school district. Their effectiveness will be re-evaluated after two years, and determination will be made to continue or discontinue their use. FLOCK, the supplier of the equipment, will handle maintenance and installation.

6. **Chain of Command.**

A. As employees of the Police Department, SROs will be subject to the chain of command of the Police Department.

B. In the performance of their duties, SROs shall coordinate and communicate with the principal or the principals' designee of the school to which they are assigned.

7. **Transporting Students Off Campus**

A. SROs shall not transport students in Police Department vehicles except when the students are victims of a crime, under arrest, or some other emergency circumstances exist.

B. SROs shall notify school personnel upon removing a student from campus for any of the reasons listed above.

8. **Access to Education Records.**

A. School officials shall allow SROs to inspect and copy any public records maintained by the school to the extent permitted by law. The Parties specifically acknowledge that the sharing of directory information of a student is authorized by law. The Parties further recognize and reaffirm the Memorandum of Understanding between the Parties dated January 28, 2015 and attached as Exhibit A, which allows the sharing of disciplinary and truancy information during the investigation of a criminal matter.

B. If some information in a student's record is needed in an emergency to protect the health or safety of the student or other individuals, school officials shall disclose to the SRO that information which is needed to respond to the emergency situation based on the seriousness of the threat to someone's health or safety; the need of the information to meet the emergency situation and the extent to which time is of the essence.

C. If confidential student record information is needed by an SRO, but no emergency situation exists, the information may be released only as permitted by law.

D. All APD Records will be maintained by the Aurora Police Department. All requests for APD Records shall be referred to the APD Records Department.

9. Access to Aurora Public School Facilities

A. All sworn police officers will have access to Aurora Public School facilities through district access card system using the officer's APD department issued building pass.

B. SRO leadership will notify APS dispatch immediately in the event a sworn officer has left the department to ensure that officer no longer has access to the district.

C. At a minimum The Aurora Police Department will send bi-weekly updates to APS dispatch to notify of recent hires to the department and those who have left the department.

D. The SRO lieutenant will be responsible for training and notifications relating to APS building access.

10. **Governmental Immunity.**

A. With regard to legal issues or contingencies, each signatory to this agreement acknowledges that they, and the other signatory, are subject to, and controlled by the

provisions of the Colorado Governmental Immunity Act, Section 24-10-101 et. Seq., Colorado Revised Statutes.

11. All notices required hereunder shall be given to:

Aurora Public Schools
Superintendent of Schools
15701 E. 1st Drive
Aurora, CO 80011
General Counsel for APS
15701 E 1st Drive
Aurora, CO 80011

Aurora Police Department
Attn: Chief Todd Chamberlain
15001 E. Alameda Ave.
Aurora, CO 80012
Aurora City Attorney's Office
15151 E. Alameda Pkwy, Suite 5300
Aurora, CO 80012

All notices so given in writing shall be effective upon receipt when hand delivered, or upon mailing if notice is given by first class mail.

IN WITNESS WHEREOF, the parties hereto have caused this Agreement to be executed the day and year first written above.

Aurora Public Schools

Michael Giles, Jr.
APS Superintendent

APPROVED AS TO FORM:

Brandon Eyre
General Council Aurora Public Schools

Aurora Police Department

Chief Todd Chamberlain

ATTEST:

APPROVED AS TO FORM:

Megan Platt

Megan Platt
Aurora Police Department Legal Advisor

RESOLUTION NO. R2025- ____

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF AURORA, COLORADO, APPROVING THE MEMORANDUM OF UNDERSTANDING BETWEEN THE AURORA POLICE DEPARTMENT AND AURORA PUBLIC SCHOOLS RELATED TO SCHOOL RESOURCE OFFICERS

WHEREAS, Section 10-12 of the City Charter authorizes the City Council, by resolution, to enter into contracts or agreements with other governmental units or special districts for the joint use of buildings, equipment, or facilities, and for the furnishing or receiving of services; and

WHEREAS, the Aurora Police Department agrees to provide school resource officers (SROs) to Aurora Public Schools (APS); and

WHEREAS, SROs support the health, safety, and welfare of APS students and staff by providing for partnership programs to high schools; and

WHEREAS, this Memorandum of Understanding sets forth the terms and conditions of the services to be performed by the SROs provided by the Aurora Police Department.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF AURORA, COLORADO, THAT:

Section 1. The Memorandum of Understanding between the Aurora Police Department and Aurora Public Schools regarding school resource officers is hereby approved.

Section 2. The Mayor and City Clerk are hereby authorized to execute the attached agreement in substantially the form presented at this meeting with such technical additions, deletions, and variations as may be deemed necessary or appropriate by the City Attorney.

Section 3. All resolutions or parts of resolutions of the City in conflict herewith are hereby rescinded.

RESOLVED AND PASSED this _____ day of _____ 2025.

_____
MIKE COFFMAN, Mayor

ATTEST:

_____
KADEE RODRIGUEZ, City Clerk

APPROVED AS TO FORM:

PETER A. SCHULTE, CITY ATTORNEY

By: Amanda MacDonald RLA
AMANDA MACDONALD, Assistant City Attorney

CITY OF AURORA
Council Agenda Commentary

Item Title: Aurora Police and ATF MOU
Item Initiator: Danelle Carrel, Executive Support Manager
Staff Source/Legal Source: DJ Tisdale, Lieutenant / Mandy MacDonald, Assistant City Attorney
Outside Speaker: N/A
Strategic Outcome: Safe: Promoting safety in our built environment through effective administration of city codes and ordinances and responding to emergencies appropriately to preserve and enhance the community's sense of security and well-being.

COUNCIL MEETING DATES:

Study Session: 10/6/2025

Regular Meeting: 10/20/2025

2nd Regular Meeting (if applicable): N/A

Item requires a Public Hearing: ☐ Yes ☐ No

ITEM DETAILS *(Click in highlighted area below bullet point list to enter applicable information.)*

- Waiver of reconsideration requested, and if so, why
- Sponsor name
- Staff source name and title / Legal source name and title
- Outside speaker name and organization
- Estimated time: (For Study Session items only indicate combined time needed for presentation and discussion)

Staff Source: DJ Tisdale, Lieutenant
Legal Source: Mandy MacDonald, Assistant City Attorney

ACTIONS(S) PROPOSED *(Check all appropriate actions)*

☒ Approve Item and Move Forward to Study Session

☐ Approve Item and Move Forward to Regular Meeting

☐ Information Only

☐ Approve Item with Waiver of Reconsideration
Reason for waiver is described in the Item Details field above.

☐ Approve Item as Proposed at Policy Committee

☐ Approve Item as Proposed at Study Session

☐ Approve Item as Proposed at Regular Meeting

PREVIOUS ACTIONS OR REVIEWS:

Policy Committee Name: N/A

Policy Committee Date: N/A

Action Taken/Follow-up: ***(Check all that apply)***

☐ Recommends Approval ☐ Does Not Recommend Approval

☐ Forwarded Without Recommendation ☐ Minutes Not Available

☐ Minutes Attached

HISTORY *(Dates reviewed by City council, Policy Committees, Boards and Commissions, or Staff. Summarize pertinent comments. ATTACH MINUTES OF COUNCIL MEETINGS, POLICY COMMITTEES AND BOARDS AND COMMISSIONS.)*

N/A

ITEM SUMMARY *(Brief description of item, discussion, key points, recommendations, etc.)*

This MOA establishes the procedures and responsibilities of both the Aurora Police Department and ATF for the reimbursement of certain overtime and other pre-approved expenses incurred pursuant to the authority in Section II.

FISCAL IMPACT

Select all that apply. (If no fiscal impact, click that box and skip to "Questions for Council")

☐ Revenue Impact ☐ Budgeted Expenditure Impact ☐ Non-Budgeted Expenditure Impact
☐ Workload Impact ☒ No Fiscal Impact

REVENUE IMPACT
Provide the revenue impact or N/A if no impact. (What is the estimated impact on revenue? What funds would be impacted? Provide additional detail as necessary.)

BUDGETED EXPENDITURE IMPACT
Provide the budgeted expenditure impact or N/A if no impact. (List Org/Account # and fund. What is the amount of budget to be used? Does this shift existing budget away from existing programs/services? Provide additional detail as necessary.)

NON-BUDGETED EXPENDITURE IMPACT
Provide the non-budgeted expenditure impact or N/A if no impact. (Provide information on non-budgeted costs. Include Personal Services, Supplies and Services, Interfund Charges, and Capital needs. Provide additional detail as necessary.)

WORKLOAD IMPACT
Provide the workload impact or N/A if no impact. (Will more staff be needed or is the change absorbable? If new FTE(s) are needed, provide numbers and types of positions, and a duty summary. Provide additional detail as necessary.)

QUESTIONS FOR COUNCIL

Does the Committee approve to move this item to Study Session for full council?

LEGAL COMMENTS

Governments may cooperate or contract with one another to provide any function, service, or facility lawfully authorized to each of the cooperating or contracting units only if such cooperation or contracts are authorized by each party thereto with the approval of its legislative body or other authority having the power to so approve. (Colo. Rev. Stat. §29-1-203(1)). City Council may, by resolution, enter into Intergovernmental Agreements with other governmental units or special districts for the joint use of buildings, equipment or facilities, and for furnishing or receiving commodities or services. (City Charter §10-12) (MacDonald)

U.S. Department of Justice

Bureau of Alcohol, Tobacco,
Firearms and Explosives

Washington, DC 20226
www.atf.gov

MEMORANDUM OF AGREEMENT

Between the
Bureau of Alcohol, Tobacco, Firearms and Explosives

And

Aurora Police Department

for
Reimbursement of Overtime Salary Costs
associated with
ATF TASK FORCE

****

This Memorandum of Agreement (MOA) is entered into by the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), headquartered in Washington, D.C., and the Aurora Police Department, headquartered in Aurora,CO, for the purpose of reimbursement of overtime salary costs and other costs, with prior ATF approval, including but not limited to travel, fuel, training, and equipment, incurred by the Aurora Police Department in providing resources to assist ATF.

Payments may be made to the extent they are included in ATF's Fiscal Year Plan and the monies are available to satisfy the request(s) for reimbursable overtime expenses.

I. DURATION OF THIS MEMORANDUM OF AGREEMENT

This MOA is effective with the signatures of all parties, and if signed on different dates the later date. This MOA terminates at the close of business on August 31, 2030, subject to Section VII of the MOA.

II. AUTHORITY

This MOA is established pursuant to the following provisions:

A. Title 28, U.S.C., Section 524(c), the Department of Justice, Assets Forfeiture Fund, which provides for the payment of overtime salaries, travel, fuel, training, equipment and other similar costs of State and local law enforcement officers that

are incurred in a joint asset forfeiture law enforcement operation with a Federal law enforcement agency participating in the Assets Forfeiture Fund initiative.

B. Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations Bill, which provides for the reimbursement of overtime salary costs of local, county, or State law enforcement agencies incurred while assisting ATF in joint law enforcement operations.

C. Title 28, U.S.C., Section 530C, which provides that the activities of the Department of Justice (including any bureau, office, etc.) may be carried out through any means, including through contracts, grants, or cooperative agreements with non-Federal parties.

This Memorandum of Agreement (MOA) is not a funding allocation document.

III. PURPOSE OF THIS MEMORANDUM OF AGREEMENT

This MOA establishes the procedures and responsibilities of both the Aurora Police Department and ATF for the reimbursement of certain overtime and other pre-approved expenses incurred pursuant to the authority in Section II.

IV. NAME OF JOINT OPERATION/TASK FORCE (if applicable)

The name of this joint operation/task force: ATF TASK FORCE

V. CONDITIONS AND PROCEDURES

A. The Aurora Police Department shall assign officer(s) to assist ATF in investigations of Federal, state, and local laws. To the maximum extent possible, the officer(s) will be assigned on a dedicated, rather than rotational basis. The Aurora Police Department shall provide ATF with the name(s), title(s), and employee identification number(s) of the officer(s) assigned to the investigation.

B. The Aurora Police Department shall provide ATF, within ten (10) calendar days of the signing of this MOA, with a contact name, title, telephone number and address. The Aurora Police Department shall also provide the name of the official responsible for providing audit information under paragraph VI of this MOA, and the name of the official authorized to submit an invoice to ATF under paragraph V, subparagraph E.

C. The Aurora Police Department shall provide ATF, within ten (10) calendar days of the signing of this agreement, with the financial institution where the law

enforcement agency wants the Electronic Funds Transfer (EFT) payment deposited for reimbursement. The mechanism for this is the Unified Financial Management System (UFMS) Vendor Request Form. Within the UFMS Vendor Request form, the DUNS Number should be provided (DUNS – Data Universal Numbering System, identifies business entities on a location-specific basis) under section 12. When completed, forward this form to the appropriate ATF field office address:

ATF, ATTN: GS Jason Cole, 950 17th Street, Ste 1800, Denver, CO 80202, Jason.Cole@atf.gov

D. The Aurora Police Department may request reimbursement for payment of overtime expenses and other costs with prior ATF approval, including but not limited to travel, fuel, training, and equipment, directly related to work performed by its officer(s) assigned as members of a joint operation/task force with ATF for the purpose of conducting an official investigation.

E. Invoices submitted to ATF for the payment of expenses must be submitted on the appropriate forms as provided by ATF. The invoice shall be signed by an authorized representative of the Aurora Police Department and submitted to ATF field office for signature and verification of the invoice.

F. The Aurora Police Department will submit all requests for reimbursable payments, together with the appropriate documentation, to ATF by the 10th day of each subsequent month that the agency is seeking reimbursement.

(1). If the reimbursement request is not received by the ATF field office by the 10th of the subsequent month, the ATF field office will advise the agency, in writing, that the reimbursement request is late, and if the reimbursement request is not received within the next 10 working days, the overtime costs will not be reimbursed.

(2). No waivers or extensions will be granted or honored. The Aurora Police Department will submit the request for reimbursement email to the following address:

ATF, ATTN: GS Jason Cole, 950 17th Street, Ste 1800, Denver, CO 80202, Jason.Cole@atf.gov

G. The ATF Supervisor shall be responsible for certifying that the request is for overtime expenses incurred by the Aurora Police Department for participation

with ATF during the joint operation/task force. The responsible State or local official shall also certify that requests for reimbursement of expenses have not been made to other Federal law enforcement agencies.

H. The Aurora Police Department acknowledges that they remain fully responsible for their obligations as the employer of the officer(s) assigned to the joint operation/task force and are responsible for the payment of the overtime earnings, withholdings, insurance coverage, and all other requirements by law, regulations, ordinance or contract regardless of the reimbursable overtime charges incurred.

I. All reimbursable hours of overtime work covered under this MOA must be approved in advance by the ATF supervisor.

J. All sworn State, county and local law enforcement officers cannot exceed the fiscal year reimbursement cap, which is the equivalent of 25 percent of a GS-12, Step-1 salary. Sworn law enforcement officers in the State, county or local law enforcement agency assigned to cover when a TFO or other sworn law enforcement officer, has been called away on an ATF matter, shall not be reimbursed with SLOT funds.

K. Any Sworn State, county and local law enforcement officer receiving funding from multiple sources, such as Organized Crime Drug Enforcement Task Force (OCDETF) or High Intensity Drug Trafficking Area (HIDTA), cannot exceed the fiscal year salary cap when all funding is combined; it is the RAC/GS's responsibility to ensure that the officer does not receive double funding in excess of the fiscal year cap.

L. The ATF supervisor will forward all approved reimbursement requests to the Field Operations, Resource Management Branch for payment.

M. **This document (MOA) does not obligate funds.** Funding authority, with maximum reimbursement costs to any one law enforcement officer during the fiscal year (October 1 – September 30); will be provided through other documents. The agency will receive an allocation confirmation from the field division.

If available, the funding is contingent upon annual appropriation laws, Title 28, U.S.C., Section 524(c), annual appropriations, and Title 31, U.S.C., Section 332.

If available, funding allocations for reimbursement of expenses will be transmitted through a separate document.

VI. PROGRAM AUDIT

This MOA and its procedures are subject to audit by ATF, the Department of Justice, Office of Inspector General, the Government Accountability Office, and other auditors authorized by the Federal government. The Aurora Police Department agrees to permit such audits and agrees to maintain all records relating to these transactions for a period of not less than three years; and in the event of an on-going audit, until such time as the audit is completed.

These audits include reviews of any and all records, documents, reports, accounts, invoices, receipts, or expenditures relating to this agreement; as well as the interview of any and all personnel involved in these transactions.

VII. REVISIONS

The terms of this MOA may be amended upon written approval by the original parties, or their designated representatives. Any amendment to this MOA becomes effective upon the date of approval as stated in the amendment. Either party can cancel this MOA upon 60-calendar day's written notice to the other party. The ATF will only process request for overtime for overtime incurred before the date of cancellation, absent a specific written agreement to the contrary.

VIII. NO PRIVATE RIGHT CREATED

This is an internal Government agreement between ATF and the Aurora Police Department and is not intended to confer any right or benefit to any private person or party.

IX. LIMITATIONS

A. The relationship between the Parties to this Agreement is and shall remain that of independent departments and agencies. Nothing herein shall be construed to imply either Party's employees are employees of the other.

B. A determination that any term of this MOA is invalid for any reason shall not affect the validity of the remaining terms.

C. The obligations in this MOA are subject to the availability of the necessary resources to the Parties. No provision of this MOA shall be interpreted to require obligation or payment of funds in violation of the Anti-deficiency Act, 31 U.S.C. Section 1341, or other applicable laws.

D. Each Party shall assume the responsibility and liability for the acts and omissions of its own employees or agents in connection with the performance of their obligations under this Agreement that are executed within the scope of their employment, including claims for injury, loss or damage to personal property or death, except in the case of the federal Government, liability shall be determined pursuant to the Federal Tort Claim Act (FTCA – 28 U.S.C. Section 1346).

E. The mutual covenants and terms, and any applicable MOUs, represent the entire Agreement and understanding of the Parties with respect to the subject matter hereof, and supersede all prior and contemporaneous agreements and understandings relative to such subject matters. No representations or statements of any kind made by either Party, which are not expressly stated herein, shall be binding on such Party.

F. Failure or delay on the part of any Party to exercise any right, remedy, power or privilege hereunder shall not operate as a waiver thereof. A waiver, to be effective, must be in writing and signed by the Party making the waiver. A written waiver of a default shall not operate as a waiver of any other default or of the same type default on a future occasion.

G. The terms and provisions in this Agreement shall be construed under the applicable federal statutes and regulations.

X. SIGNATURES AND ACKNOWLEDGEMENT

A. By subscription of their signatures below, the Parties represent and warrant that they are duly authorized to enter into this MOA on behalf of ATF and Aurora Police Department respectively. By subscription of their signatures below, the Parties acknowledge that they have read, understand, and intend to abide by the terms of this MOA.

APRIL MCILWAIN Digitally signed by APRIL MCILWAIN Date: 2025.08.12 14:34:23 -04'00'

April McIlwain
Deputy Chief Financial Officer
Office of Management
ATF
Date: _____

Brent Beavers
Special Agent in Charge
Denver Field Division
ATF
Date: _____

Todd Chamberlain
Chief of Police
Aurora Police Department
Date: _____

RESOLUTION NO. R2025- ____

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF AURORA, COLORADO, APPROVING THE INTERGOVERNMENTAL AGREEMENT BETWEEN THE BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES ("ATF") AND THE AURORA POLICE DEPARTMENT RELATED TO REIMBURSEMENT FOR OVERTIME SALARY COSTS ASSOCIATED WITH THE ATF TASK FORCE

WHEREAS, the City is constitutionally and statutorily empowered pursuant to Colo. Const., Article XIV, §18 and Sections 29-1-201, *et seq*., C.R.S. to cooperate or contract via intergovernmental agreement with one another to provide functions, services or facilities authorized to each cooperating government; and

WHEREAS, Section 10-12 of the City Charter authorizes the City Council, by resolution, to enter into contracts or agreements with other governmental units or special districts for the joint use of buildings, equipment, or facilities, and for the furnishing or receiving of services; and

WHEREAS, Title 28, U.S.C., Section 530C, provides that the activities of the Department of Justice (including any bureau, office, etc.) may be carried out through any means, including through contracts, grants, or cooperative agreements with non-federal parties, such as the City of Aurora; and

WHEREAS, pursuant to the Agreement, the Aurora Police Department will assign officers to assist the ATF in investigations of federal, state, and local laws; and

WHEREAS, this Agreement establishes the procedures and responsibilities of both the Aurora Police Department and the ATF for the reimbursement of certain overtime and other pre-approved expenses incurred by the Aurora Police Department in providing resources to assist the ATF in investigations of federal, state, and local laws.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF AURORA, COLORADO, THAT:

Section 1. The Intergovernmental Agreement between the Aurora Police Department and the Bureau of Alcohol, Tobacco, Firearms, and Explosives regarding reimbursement of overtime salary costs is hereby approved.

Section 2. The Mayor and City Clerk are hereby authorized to execute the attached agreement in substantially the form presented at this meeting with such technical additions, deletions, and variations as may be deemed necessary or appropriate by the City Attorney.

Section 3. All resolutions or parts of resolutions of the City in conflict herewith are hereby rescinded.

RESOLVED AND PASSED this _____ day of _____ 2025.

_____
MIKE COFFMAN, Mayor

ATTEST:

_____
KADEE RODRIGUEZ, City Clerk

APPROVED AS TO FORM:

PETER A. SCHULTE, CITY ATTORNEY

By: Amanda MacDonald RLA
AMANDA MACDONALD, Assistant City Attorney

CITY OF AURORA
Council Agenda Commentary

Item Title: Adult Protective Services Cooperative Agreement
Item Initiator: Danelle Carrel, Executive Support Manager
Staff Source/Legal Source: Mark Hildebrand, Deputy Chief / Mandy MacDonald, Assistant City Attorney
Outside Speaker: N/A
Strategic Outcome: Safe: Promoting safety in our built environment through effective administration of city codes and ordinances and responding to emergencies appropriately to preserve and enhance the community's sense of security and well-being.

COUNCIL MEETING DATES:

Study Session: 10/6/2025

Regular Meeting: 10/20/2025

2nd Regular Meeting (if applicable): N/A

Item requires a Public Hearing: ☐ Yes ☐ No

ITEM DETAILS *(Click in highlighted area below bullet point list to enter applicable information.)*

- Waiver of reconsideration requested, and if so, why
- Sponsor name
- Staff source name and title / Legal source name and title
- Outside speaker name and organization
- Estimated time: (For Study Session items only indicate combined time needed for presentation and discussion)

Staff Source: Mark Hildebrand, Deputy Chief
Legal Source: Mandy MacDonald, Assistant City Attorney
Estimated Time: 5 mins

ACTIONS(S) PROPOSED *(Check all appropriate actions)*

☒ Approve Item and Move Forward to Study Session

☐ Approve Item and Move Forward to Regular Meeting

☐ Information Only

☐ Approve Item with Waiver of Reconsideration
Reason for waiver is described in the Item Details field above.

☐ Approve Item as Proposed at Policy Committee

☐ Approve Item as Proposed at Study Session

☐ Approve Item as Proposed at Regular Meeting

PREVIOUS ACTIONS OR REVIEWS:

Policy Committee Name: N/A

Policy Committee Date: N/A

Action Taken/Follow-up: ***(Check all that apply)***

☐ Recommends Approval ☐ Does Not Recommend Approval

☐ Forwarded Without Recommendation ☐ Minutes Not Available

☐ Minutes Attached

HISTORY *(Dates reviewed by City council, Policy Committees, Boards and Commissions, or Staff. Summarize pertinent comments. ATTACH MINUTES OF COUNCIL MEETINGS, POLICY COMMITTEES AND BOARDS AND COMMISSIONS.)*

N/A

ITEM SUMMARY *(Brief description of item, discussion, key points, recommendations, etc.)*

Multi-Agency Cooperative Agreement to clarify the coordinated duties and responsibilities of agencies involved in reporting, responding, and investigating reports regarding the abuse, caretaker neglect, and exploitation (mistreatment), and self-neglect of at-risk adults; and (2) to ensure coordinated response during all hours, provide for special requests for assistance from one party to another, and arrange for joint investigation(s) when needed to maximize the effectiveness of the civil and criminal investigative processes.

FISCAL IMPACT

Select all that apply. (If no fiscal impact, click that box and skip to "Questions for Council")

☐ Revenue Impact ☐ Budgeted Expenditure Impact ☐ Non-Budgeted Expenditure Impact
☐ Workload Impact ☒ No Fiscal Impact

REVENUE IMPACT
Provide the revenue impact or N/A if no impact. (What is the estimated impact on revenue? What funds would be impacted? Provide additional detail as necessary.)

BUDGETED EXPENDITURE IMPACT
Provide the budgeted expenditure impact or N/A if no impact. (List Org/Account # and fund. What is the amount of budget to be used? Does this shift existing budget away from existing programs/services? Provide additional detail as necessary.)

NON-BUDGETED EXPENDITURE IMPACT
Provide the non-budgeted expenditure impact or N/A if no impact. (Provide information on non-budgeted costs. Include Personal Services, Supplies and Services, Interfund Charges, and Capital needs. Provide additional detail as necessary.)

WORKLOAD IMPACT
Provide the workload impact or N/A if no impact. (Will more staff be needed or is the change absorbable? If new FTE(s) are needed, provide numbers and types of positions, and a duty summary. Provide additional detail as necessary.)

QUESTIONS FOR COUNCIL

Does the Committee approve to move forward to Study Session for full council?

LEGAL COMMENTS

Governments may cooperate or contract with one another to provide any function, service, or facility lawfully authorized to each of the cooperating or contracting units only if such cooperation or contracts are authorized by each party thereto with the approval of its legislative body or other authority having the power to so approve. (Colo. Rev. Stat. §29-1-203(1)). (MacDonald)

City Council may, by resolution, enter into Intergovernmental Agreements with other governmental units or special districts for the joint use of buildings, equipment or facilities, and for furnishing or receiving commodities or services. (City Charter §10-12). (MacDonald)

Pursuant to C.R.S. 26-3.1-103(2), each county department, law enforcement agency, district attorney's office, and other agency responsible under federal law or the laws of this state to investigate mistreatment or self-neglect of at-risk adults shall develop and implement cooperative agreements to coordinate the investigative duties of such agencies. The focus of such agreements is to ensure the best protection for at-risk adults. The agreements must provide for special requests by one agency for assistance from another agency and for joint investigations. The agreements must further provide that each agency maintain the confidentiality of the information exchanged pursuant to such joint investigations. This Agreement fulfills the Aurora Police Department’s obligation under state law. (MacDonald)

Adult Protective Services Cooperative Agreement

I. PARTIES: This Adult Protective Services Cooperative Agreement (the "Agreement") is entered into by and between the following parties: (1) the Arapahoe County Department of Human Services; (2) the Arapahoe County Attorney's Office; (3) the District Attorney, 18th Judicial District; (4) Arapahoe County Sheriff's Office; (5) Aurora Police Department; (6) Town of Bow Mar Police Department; (7) Town of Centennial Police Department; (8) Cherry Hills Village Police Department; (9) Englewood Police Department; (10) Glendale Police Department; (11) Columbine Valley Police Department; (12) Greenwood Village Police Department; (13) Littleton Police Department; (14) Sheridan Police Department; (15) Colorado State Highway Patrol's Office; and (16) Arapahoe County Community College Police Department.

II. SUBJECT: Arapahoe County Adult Protective Services Cooperative Agreement for investigation of reports involving possible mistreatment or self-neglect of at-risk adults with Intellectual and Developmental Disabilities (IDD).

III. PURPOSE: In accordance with statute 26-3.1-103 (2), C.R.S., this Agreement is made (1) to clarify the coordinated duties and responsibilities of agencies involved in reporting, responding, and investigating reports regarding the abuse, caretaker neglect, and exploitation (mistreatment), and self-neglect of at-risk adults; and (2) to ensure coordinated response during all hours, provide for special requests for assistance from one party to another, and arrange for joint investigation(s) when needed to maximize the effectiveness of the civil and criminal investigative processes.

IV. TERM OF AGREEMENT: This Agreement will commence upon the date of the final signature and will be in effect for five (5) years. Changes in or termination of in the Agreement may be made at any time by mutual consent of APS and the above-mentioned entities.

V. BACKGROUND AND BASIS FOR THE AGREEMENT: Colorado Revised Statute, Section 26-3.1-103 (2) states: In each county department, law enforcement agency, district attorney's office, other agency responsible under federal law or the laws of this state to investigate mistreatment, self-neglect or exploitation of at-risk adults shall develop and implement cooperative agreements to coordinate the investigative duties of such agencies. The focus of such agreement shall be to ensure the best protection for at-risk adults. The agreements shall provide for special requests by one agency for assistance from another agency and for joint investigations. The agreement shall further provide that each agency shall maintain the confidentiality of the information exchanged pursuant to such joint investigation.

VI. DEFINITIONS: The following terms, as used in this Agreement, shall have the ascribed to them in the statutes set forth below:

1. Abuse (as defined in §26-3.1-101(1), C.R.S.);
2. At-risk adult (as defined in §26-3.1-101(1.5), C.R.S.);
3. At-risk adult with IDD (as defined in §18-65-102(2.5), C.R.S.);
4. At-risk elder (as defined in §18-65-102(3), C.R.S.);

5. Caretaker (as defined in §26-3.1-101(2), C.R.S.);
6. Caretaker Neglect (as defined in §26-3.1-101(2.3), C.R.S.);
7. Employer (as defined in §26-3.1-111(2)(b), C.R.S.);
8. Exploitation (as defined in §26-3.1-101(4), C.R.S.);
9. Mistreatment (as defined in §26-3.1-101(7), C.R.S.); and
10. Self-neglect (as defined in §26-3.1-101(10), C.R.S.);

VII. PRINCIPLES OF THE AGREEMENT: In accordance with C.R.S. 26-3.1 – 103, this agreement is made to ensure coordinated response during all hours, to provide for special requests for assistance from one agency to another, and to arrange for joint investigation(s) when needed to maximize the effectiveness of the civil and criminal investigative processes.

It is understood that joint investigations may be used as a means to coordinate the efforts of the involved agencies, and that each individual agency remains accountable to its own rules, policies, and statutes. Nothing in this Agreement shall substitute or represent a change in any party's legally mandated responsibilities.

It is understood that all parties to this Agreement shall accept reports of known or suspected mistreatment or self-neglect of at-risk adults and share those reports with the parties to this agreement as described below.

VIII. BUSINESS AND NON-BUSINESS HOUR PROCESSES: Arapahoe County Adult Protective Services("APS") are required by APS program rule to have an established process to receive reports during business and non-business hours.

The Arapahoe County Department of Human Services, herein known as Adult Protective Services (APS), receives reports during business hours at (303) 636-1750. Business hours are 8:00 AM – 4:30 PM, Monday – Friday.

Calls of reports should be made to (303) 636-1750 24 hours a day, 7 days a week. All reports should be made immediately to APS, regardless of the time of day. APS does not accept reports made by fax or email. Reports made during county observed holidays are received by Arapahoe County Sheriff Office Dispatch/Communications, and ACSO is responsible for contacting the on-call Arapahoe County Department employee.

IX. DISPOSITION OF REPORTS: A copy of all reports of made to APS shall be forwarded to the appropriate law enforcement agency within twenty-four hours of receipt of the report, excluding weekends, holidays, or days the county is closed. When applicable, reports should be forwarded the next business day.

A copy of all reports of mistreatment and self-neglect made to law enforcement and the district attorney's office shall be forwarded to APS within twenty four of receipt of the report.

The report shall include: the name, age, and address of the at-risk adult; the name and address of the at-risk adult's caretaker, if any; the suspected nature and extent of the at-risk adult's

injury, if any; the nature and extent of the condition that will reasonably result in mistreatment or self-neglect; and other pertinent information.

Reports involving criminal allegations of mistreatment, including caretaker neglect shall be immediately referred to local law enforcement. When criminal allegations are not initially apparent, the caseworker shall refer to the appropriate law enforcement office as soon as there are reasonable suspicions that a crime has been committed.

Reports of abuse, caretaker neglect, and/or exploitation of at-risk elders, 70 years of age or older, must be reported to law enforcement. Law enforcement will forward all reports of abuse, caretaker neglect, or exploitation of at-risk elders to APS within 24 hours. APS will review and evaluate each report to determine if the at-risk elder meets the statutory requirements of an at-risk adult pursuant to C.R.S. 26-3.1-101 (1) before protective services are rendered.

If a report is made to APS and it is later discovered that the person is 70 years of age or older, APS will notify law enforcement immediately. These are cases when the reporting party is not aware of the adult's age and makes the report to APS.

The report shall include: the name, age, and address of the at-risk elder; the name and address of the at-risk elder's caretaker, if any; the suspected nature and extent of the at-risk elder's injury, if any; the nature and extent of the condition that will reasonably result in abuse, caretaker neglect, and/or exploitation; and other pertinent information.

X. AGENCY ROLES: Adult Protective Services is responsible for investigating reports of suspected mistreatment and/or self-neglect of at-risk adults.

The County Attorney's Office is responsible for reviewing reports of mistreatment of at-risk adults when a review is requested, when APS is considering filing for guardianship and/or conservatorship of an at-risk adult, and when an investigation involves complaints of alleged criminal activity.

Law enforcement agencies are primarily responsible for the coordination and investigation of criminal allegations involving at-risk adults and at-risk elders.

The District Attorney's Office is responsible for reviewing reports of criminal actions or threats of mistreatment of at-risk adults and at-risk elders to determine possibility of prosecution.

XI. JOINT INVESTIGATION PROCEDURE AND GUIDELINES: Some reports may need to be jointly investigated when time and resources allow. Any agency entering into this agreement may request assistance from another agency entering into this agreement in the investigation and assessment of the at-risk adult's safety and well-being. Additionally, any agency may request stand-by assistance from another agency. (For example, in situations where an APS worker's safety may be in question or where law enforcement needs assistance with a client with dementia.)

When a joint investigation is required, the APS caseworker, law enforcement officer(s), and/or the District Attorney's Office may conduct joint interviews, compare notes, and clarify information following interviews. Law enforcement shall be considered the lead agency in criminal joint investigations. APS shall be considered the lead agency in non-criminal joint investigations. Developmental disability, ombudsman or mental health staff may be present as part of the joint investigative team.

When joint investigation is required, contact law enforcement by calling dispatch, or County Hotline Staff (303) 636-1750) and contact the District Attorney's Office by calling 720-874-8500.

Joint investigation or stand by assistance may be utilized when any of the following pertain to an at-risk adult:

1. There is pain and/or physical injury, as demonstrated by, but not limited to, substantial or multiple skin bruising, bleeding, malnutrition, dehydration, burns, bone fractures, poisoning, subdural hematoma, soft tissue swelling or suffocation.
2. Unreasonable confinement or restraint has been imposed.
3. There is nonconsensual sexual conduct or contact classified as a crime under Colorado law.
4. Caretaker neglect threatens the at-risk adult's safety or well-being.
5. Financial exploitation has occurred and/or is occurring and the exploitation is a crime under Colorado law.
6. Threats of violence, presence of firearms, intoxication, or any illegal activity is present and threatens the at-risk adult or APS caseworker's safety.
7. Specialized interviewing skills might be required.

XII. CONFIDENTIALITY: Reports and investigative information shall be confidential. Disclosure of information, including the name and address of the at-risk adult, members of the adult's family, reporting party's name and address, or any other identifying information contained in reports shall be permitted only when authorized by law or ordered by the court, as outlined in Section 26-3.1-102(7), C.R.S.

Notwithstanding any provision of Section 24-72-204, C.R.S., or Section 11-105-110, C.R.S., or any other applicable law concerning the confidentiality of financial records to the contrary, designated agencies investigating the exploitation of an at-risk adult shall be permitted to inspect all records of the at-risk adult on whose behalf the investigation is being conducted, including the at-risk adult's financial records, upon execution of a prior written consent form by the at-risk adult, pursuant to Section 26-3.1-103, C.R.S.

(Remainder of this page left blank intentionally)

In addition, each agency shall maintain the confidentiality of the information exchanged pursuant to joint investigations as required by Section 26-3.1-103(2), C.R.S.

SIGNED BY:

Director, Arapahoe County Department of Human Services	Date
District Attorney, 18th Judicial District	Date
Arapahoe County Attorney	Date
Arapahoe County Sheriff	Date
Chief, Aurora Police Department	Date
Chief, Bow Mar Police Department	Date
Chief, Cherry Hills Police Department	Date
Chief, Colorado State Highway Patrol's Office	Date
Chief, Columbine Valley Police Department	Date

Chief, Denver Police Department Date

Chief, Englewood Police Department Date

Chief, Glendale Police Department Date

Chief, Greenwood Village Police Department Date

Chief, Littleton Police Department Date

Chief, Sheridan Police Department Date

Chief, Arapahoe County Community College Police Department Date

RESOLUTION NO. R2025- ____

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF AURORA, COLORADO, APPROVING THE INTERGOVERNMENTAL AGREEMENT BETWEEN THE AURORA POLICE DEPARTMENT AND ARAPAHOE COUNTY DEPARTMENT OF HUMAN SERVICES

WHEREAS, the City and the Arapahoe County Department of Human Services are constitutionally and statutorily empowered pursuant to Colo. Const., Article XIV, §18 and Sections 29-1-201, *et seq*., C.R.S. to cooperate or contract via intergovernmental agreement with one another to provide functions, services or facilities authorized to each cooperating government; and

WHEREAS, Section 10-12 of the City Charter authorizes the City Council, by resolution, to enter into contracts or agreements with other governmental units or special districts for the joint use of buildings, equipment, or facilities, and for the furnishing or receiving of services; and

WHEREAS, this Agreement is to clarify the coordinated duties and responsibilities of agencies involved in investigating reports involving possible mistreatment or neglect of at-risk adults; and

WHEREAS, this Agreement sets forth the respective roles and responsibilities in joint investigations and allows for special requests by one agency for assistance from the other agency when needed.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF AURORA, COLORADO, THAT:

Section 1. The Intergovernmental Agreement between Aurora Police Department and the Arapahoe County Department of Human Services regarding investigating possible mistreatment or neglect of at-risk adults is hereby approved.

Section 2. The Mayor and City Clerk are hereby authorized to execute the attached agreement in substantially the form presented at this meeting with such technical additions, deletions, and variations as may be deemed necessary or appropriate by the City Attorney.

Section 3. All resolutions or parts of resolutions of the City in conflict herewith are hereby rescinded.

RESOLVED AND PASSED this _____ day of _____ 2025.

_____
MIKE COFFMAN, Mayor

ATTEST:

_____
KADEE RODRIGUEZ, City Clerk

APPROVED AS TO FORM:

PETER A. SCHULTE, CITY ATTORNEY

By: Amanda MacDonald RLA
AMANDA MACDONALD, Assistant City Attorney

CITY OF AURORA
Council Agenda Commentary

Item Title: APD and ATF NIBIN Enforcement Support System MOU Addendum
Item Initiator: Danelle Carrel, Manager of Executive Support
Staff Source/Legal Source: DJ Tisdale, Lieutenant / Mandy MacDonald, Assistant City Attorney
Outside Speaker: N/A
Strategic Outcome: Safe: Promoting safety in our built environment through effective administration of city codes and ordinances and responding to emergencies appropriately to preserve and enhance the community's sense of security and well-being.

COUNCIL MEETING DATES:

Study Session: 10/6/2025

Regular Meeting: 10/20/2025

2nd Regular Meeting (if applicable): N/A

Item requires a Public Hearing: ☐ Yes ☐ No

ITEM DETAILS *(Click in highlighted area below bullet point list to enter applicable information.)*

- Waiver of reconsideration requested, and if so, why
- Sponsor name
- Staff source name and title / Legal source name and title
- Outside speaker name and organization
- Estimated time: (For Study Session items only indicate combined time needed for presentation and discussion)

Staff Source: DJ Tisdale, Lieutenant
Legal Source: Mandy MacDonald, Assistant City Attorney
Estimated Time: 5 Minutes

ACTIONS(S) PROPOSED *(Check all appropriate actions)*

☒ Approve Item and Move Forward to Study Session

☐ Approve Item and Move Forward to Regular Meeting

☐ Information Only

☐ Approve Item with Waiver of Reconsideration
Reason for waiver is described in the Item Details field above.

☐ Approve Item as Proposed at Policy Committee

☐ Approve Item as Proposed at Study Session

☐ Approve Item as Proposed at Regular Meeting

PREVIOUS ACTIONS OR REVIEWS:

Policy Committee Name: N/A

Policy Committee Date: N/A

Action Taken/Follow-up: ***(Check all that apply)***

☐ Recommends Approval ☐ Does Not Recommend Approval

☐ Forwarded Without Recommendation ☐ Minutes Not Available

☐ Minutes Attached

HISTORY *(Dates reviewed by City council, Policy Committees, Boards and Commissions, or Staff. Summarize pertinent comments. ATTACH MINUTES OF COUNCIL MEETINGS, POLICY COMMITTEES AND BOARDS AND COMMISSIONS.)*

N/A

ITEM SUMMARY *(Brief description of item, discussion, key points, recommendations, etc.)*

The underlying Memorandum of Understanding (MOU) covered the ATF NESS installation, operation, and administration for the dissemination of crime gun data to enhance the efforts of law enforcement to integrate resources to reduce firearms violence, identify shooters and sources of crime guns, and refer them for prosecution. This addendum governs the sharing of NESS data with specific third-party law enforcement partners.

FISCAL IMPACT

Select all that apply. (If no fiscal impact, click that box and skip to "Questions for Council")

☐ Revenue Impact ☐ Budgeted Expenditure Impact ☐ Non-Budgeted Expenditure Impact
☐ Workload Impact ☒ No Fiscal Impact

REVENUE IMPACT
Provide the revenue impact or N/A if no impact. (What is the estimated impact on revenue? What funds would be impacted? Provide additional detail as necessary.)

BUDGETED EXPENDITURE IMPACT
Provide the budgeted expenditure impact or N/A if no impact. (List Org/Account # and fund. What is the amount of budget to be used? Does this shift existing budget away from existing programs/services? Provide additional detail as necessary.)

NON-BUDGETED EXPENDITURE IMPACT
Provide the non-budgeted expenditure impact or N/A if no impact. (Provide information on non-budgeted costs. Include Personal Services, Supplies and Services, Interfund Charges, and Capital needs. Provide additional detail as necessary.)

WORKLOAD IMPACT
Provide the workload impact or N/A if no impact. (Will more staff be needed or is the change absorbable? If new FTE(s) are needed, provide numbers and types of positions, and a duty summary. Provide additional detail as necessary.)

QUESTIONS FOR COUNCIL

Does the Committee approve this item to move forward to full Council?

LEGAL COMMENTS

Governments may cooperate or contract with one another to provide any function, service, or facility lawfully authorized to each of the cooperating or contracting units only if such cooperation or contracts are authorized by each party thereto with the approval of its legislative body or other authority having the power to so approve. (Colo. Rev. Stat. §29-1-203(1)). City Council may, by resolution, enter into Intergovernmental Agreements with other governmental units or special districts for the joint use of buildings, equipment or facilities, and for furnishing or receiving commodities or services. (City Charter §10-12) (MacDonald)

MEMORANDUM OF UNDERSTANDING REGARDING THE NIBIN ENFORCEMENT SUPPORT SYSTEM (NESS)

Memorandum of Understanding
between
The Aurora Police Department
and the
Bureau of Alcohol, Tobacco, Firearms and Explosives

Article I. Purpose and Authority

The Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) is extending their on-going commitment to the law enforcement community by providing participating agencies with access to National Integrated Ballistic Information Network (NIBIN) data. The agency will be able to access NIBIN data through the NIBIN Enforcement Support System (NESS) via an Internet connection. The NESS application allows ATF to collect, analyze, refer, and track NIBIN and other crime gun data. Access will facilitate information sharing and provide near real-time intelligence to participating agencies. The mission of the program is to reduce firearms violence through aggressive identification, investigation, and prosecution of shooters and their sources of crime guns.

ATF has made a concerted effort to leverage existing information technology to better assist law enforcement agencies in the investigation of shooters and other armed violent offenders, prohibited persons possessing firearms, and sources of crime guns. This Memorandum of Understanding (MOU) establishes and defines a partnership between the Parties that will result in ATF NESS installation, operation, and administration for the dissemination of crime gun data to enhance the efforts of law enforcement to integrate resources to reduce firearms violence, identify shooters and sources of crime guns, and refer them for prosecution.

This MOU is entered into by the U.S. Department of Justice (DOJ), ATF, and The Aurora Police Department, hereinafter collectively referred to as "the Parties," and with The Aurora Police Department referred to as the "NESS Partner Agency." This MOU will refer to individuals employed and authorized for NESS access by the NESS Partner Agency as "Users".

The Parties agree that it is the public interest to enhance cooperation among Federal, State, Tribal, and local law enforcement and public safety agencies with regard to reducing firearms violence, identify shooters, and their sources of crime guns. The NESS Partner Agency acknowledges that ATF and the NESS program will assist Federal, State, Tribal, and local law enforcement and public safety agencies in combatting firearms violence.

This MOU is established pursuant to the authority of the participants to engage in activities related to the investigation and suppression of violent crimes involving firearms. ATF's authority is derived from, among other things, 28 U.S.C. § 599A, 18 U.S.C. § 3051, 27 CFR § 0.130, and, specifically, the Gun Control Act of 1968, 18 U.S.C. Chapter 44 and the National Firearms Act, 26 U.S.C. Chapter 53. The parties enter into this MOU pursuant to 31 U.S.C. § 6305.

Article II. Background

ATF is a law enforcement organization within DOJ with unique responsibilities dedicated to reducing violent crime and protecting the public. ATF recognizes the role that firearms play in violent crimes and pursues an integrated enforcement and regulatory strategy. Investigative priorities focus on armed violent offenders and career criminals, armed narcotics traffickers, violent gangs, and domestic and international arms traffickers.

Article III. Scope

The purpose of this MOU is to establish an interagency agreement governing the access and utilization of NESS. In addition, the MOU will designate a primary and alternate application administrator (App Admin) for the NESS Partner Agency. The agency App Admins will ensure adherence to the MOU between ATF and NESS Partner Agency Users. These App Admins are responsible for managing their agency's Users, which will include signing/approving User Access Forms and Rules of Behavior for each User, periodically validating the list of Users, and notifying an ATF Point of Contact (POC) immediately if it becomes necessary to revoke or suspend a User's account.

This MOU is effective upon the date of the last signature by the authorized representatives of the Parties and shall remain in effect until terminated by either Party.

Article IV. Interagency Communications

The Parties agree that a principal Point of Contact (POC)/App Admin within each organization shall coordinate all communications and tasks under this MOU. To ensure access is permitted to all NESS Partner Agency data, an Originating Agency Identifier (ORI Code) must be provided for each ORI code used by the NESS Partner Agency. The ATF POC can assist the NESS Partner Agency in determining what ORI Codes are appropriate. The designated POCs shall be as follows:

ATF Field Division		
Name	Denver Field Division	
Address	950 17th St., Suite 1800 Denver, CO 80202	
	Designated ATF Primary POC	**Designated ATF Alternate POC**
Name:		
Title:		
Email Address:		
Phone #:		

NESS Partner Agency		
Name	The Aurora Police Department	
Address	15001 E Alameda Pkwy Aurora, CO 80012	
	Designated NESS Partner Agency Primary App Admin	**Designated NESS Partner Agency Alternate App Admin**
Name:	Sgt. Ethan Snow	Sgt. Jason Deluca
Title:	Sergeant, Crime Gun Intelligence Unit	Sergeant, RAVEN Task Force
Phone #:	303-597-5073	720-391-3829
Email Address:	esnow@auroragov.org	jdeluca@auroragov.org
Date of Birth:		
Signature:		
Date:		
NESS Partner Agency ORIs		

Article V. Responsibilities and Procedures

In becoming an approved NESS Partner Agency of the NESS application, the involved Parties hereby acknowledge and accept the following responsibilities and procedures:

1. **Responsibilities of the NESS Partner Agency.** The NESS Partner Agency shall:

   a. Appoint primary and alternate App Admins within your agency (see table above). The appointed individuals will be responsible for creating, coordinating, and maintaining a list of all personnel, and determining the access levels for Users within the Partner Agency who will require access to NESS.

   b. If more than two App Admins are needed/wanted, a NESS Additional Application Administrator Form will be completed and signed by the same agency signatory on this MOU, or their successor.

   c. The designated App Admin(s) will immediately notify ATF in the event that a User's account needs to be suspended or revoked for any number of reasons, including (but not limited to) employee transfer, retirement, or release from employment.

   d. Complete a Request for Change of Agency Point of Contact (POC) Form if the App Admin changes.

   e. Agree to make every effort to provide complete and accurate information including

investigative reports and data related to NIBIN linked shootings and gun recoveries, to the fullest extent allowed by law. This includes general event data including case numbers, dates, locations, associated persons, etc. Partner Agencies that make a commitment to comprehensive data sharing with ATF will be provided an information platform for developing the best local investigative strategies for their community in the reduction of firearm related crime and violence. The NESS Partner Agency shall share the results of NIBIN leads/hits including arrest and prosecution data with ATF via the NESS application.

f. Provide a list of ORI numbers for the NESS Partner Agency (see table above), which will allow NESS to associate Users to the correct NESS Partner Agency NIBIN data. If the NESS Partner Agency needs to add or remove ORI numbers, it shall submit a completed Amendment of Originating Agency Identifier Form. The NESS Partner Agency shall use information generated and retrieved pursuant to this MOU, only for the purpose(s) identified in the Agreement.

2. Responsibilities of the Bureau of Alcohol, Tobacco, Firearms and Explosives:

a. **The ATF Field Division** shall:

1) Appoint primary and alternate ATF POCs.

2) Coordinate all communications and tasks listed under this MOU and serve as a liaison between the NESS Partner Agency App Admins and ATF's Firearms Operations Division (FOD).

3) Ensure data sharing processes between ATF and the NESS Partner Agency.

b. **FOD** shall:

1) Maintain the NESS application and share NIBIN Leads with the NESS Partner Agency.

2) Upon receipt of this signed MOU, provide detailed instructions to the ATF Field Division POCs on the process of requesting and receiving NESS User access for the NESS Partner Agency.

3) Maintain a copy of this MOU along with any associated User agreements.

4) Review all applications for NESS User access in a timely manner and facilitate the provisioning of accounts.

5) Upon receipt of a request for account revocation, FOD will immediately deactivate said User account.

Article VI. Conditions

Both ATF and the NESS Partner Agency acknowledge their understanding that the NESS application is "LAW ENFORCEMENT SENSITIVE" and intended "FOR OFFICIAL LAW ENFORCEMENT USE ONLY." Failure to protect and safeguard such data from loss, misuse, or unauthorized access could adversely affect law enforcement operations, including those areas related to officer safety, as well as, the fair and equitable administration of justice, and the privacy of individuals.

Information within NESS is to be used for investigative purposes only. NESS data reflects a compilation of information from multiple data sources and should not be relied upon as evidence. Investigators must collect original reports for any evidentiary purposes. NESS information should not be used to develop statistics or for reporting purposes. By providing your agency with NESS, ATF is not waiving any privileges that prevent further disclosure of the materials. No information contained therein may be duplicated, reproduced, or disseminated without the express authorization of ATF and/or the Originating Partner Agency, except as may be required by State or Federal law or court of competent jurisdiction. In accordance with Paragraph 10, Article XII, the NESS Partner Agency agrees to notify ATF prior to such a release.

The Federal government may monitor and audit usage of this system, and all persons are hereby notified that use of this system constitutes consent to such monitoring and auditing. Unauthorized attempts to upload information and/or change information on NESS are strictly prohibited and are subject to prosecution under the Computer Fraud and Abuse Act of 1986 and Title 18 U.S.C. §§ 1001 and 1030.

The Parties agree that premature disclosure of NESS data can reasonably be expected to interfere with pending or prospective law enforcement proceedings. It is agreed that the law enforcement sensitive firearms information generated pursuant to this Agreement shall not be disclosed to a third party without the consent of both Parties of this Agreement, subject to Federal and any applicable non-conflicting state law. The Parties agree to notify all other Parties to the MOU prior to the release of any sensitive firearms information to a third party under State or Federal law. The Parties acknowledge that NESS shall only be used for law enforcement purposes.

The Parties agree to define a "crime gun' as "any firearm illegally possessed, used in a crime, or suspected by law enforcement officials of having been used in a crime."

Article VII. NESS^{+} RMS (Records Management System) Data

NESS provides Partner Agencies with an option to share their RMS data via a daily automated ingestion process, either via an encrypted pathway or an Application Programming Interface (API). The NESS+RMS project involves establishing an automated process whereby the NESS Partner Agency's IT department runs a daily query and transmits shooting and firearm recovery information through an encrypted pathway/API. NESS receives the file and automatically populates the data eliminating the need for manual entry and allows Partner Agencies to more efficiently investigate NIBIN leads and combat firearm violence.

A Partner Agency may utilize personnel not under their direct employment for implementing actions related to this MOU. (hereinafter referred to as "Non-Partner Agency personnel") (Non-Partner Agency personnel may include RMS vendors, third-party contractors, third-party IT specialists, etc.

Documents, templates, processes, or other information provided by ATF to Non-Partner Agency personnel may not be used for any other purpose than the Partner Agency's NESS+ RMS project. Prior to being provided access to information, Non-Partner Agency personnel may be required to sign an ATF non-disclosure agreement.

Article VIII. Collective Data Sharing (CDS) Options

All data provided to ATF under this MOU, to include any/all RMS data provided via NESS+ RMS, is held in confidence and not provided to a third party without prior approval of the NESS Partner Agency. ATF provides an option for a Partner Agency to participate in a CDS agreement with other Partner Agencies. When a NESS Partner Agency choses to participate in CDS, all their NESS data is made available to other Partner Agencies of their choosing. Data sharing via NESS is reciprocal in that a Partner Agency does not have access to search the data pool unless they have opted in to share their NESS data with specified Partner Agencies.

A CDS addendum to this MOU, which details the particulars and allows the Partner Agency's Chief Law Enforcement or Public Safety Official to delegate authority to opt-in to CDS, must be signed/ratified in addition to this MOU.

Article IX. Applicable Laws

The applicable statutes, regulations, directives, and procedures of the United States, DOJ, and ATF shall govern this MOU and all documents and actions pursuant to it. Nothing in this MOU will prevail over any Federal law, regulation, or other Federal rule recognized by ATF. This MOU is not a funding document. All specific actions agreed to herein shall be subject to funding and administrative or legislative approvals.

Article X. Modifications and Terminations

This MOU shall not affect any pre-existing or independent relationships or obligations between the Parties. If any provision of this MOU is determined to be invalid or unenforceable, the remaining provisions shall remain in force and unaffected to the fullest extent permitted by law and regulation.

Amendments to this MOU are effective upon the date of the last signature on the Amendment, by the authorized representative(s) of the Parties. This MOU may be amended or modified only by written agreement and mutual consent of the Parties. Parties to this MOU may terminate their participation at any time upon a seven (7) day written notification of their intent to withdraw to the other Party. If either Party terminates this MOU, ATF will retain all of its interest in the electronically stored information contained in the NESS database.

Termination of the MOU by either Party will result in the revocation of all NESS accounts established under this Agreement. However, after termination, ATF agrees to provide to the NESS Partner Agency continued access to the NIBIN data associated with only cases originating from the NESS Partner Agency, subject to Federal law and regulations.

Article XI. Liability

Each Party shall assume the responsibility and liability for the acts and omissions of its own employees or agents in connection with the performance of their obligations under this Agreement that are executed within the scope of their employment, including claims for injury, loss or damage to personal property or death, except in the case of the federal Government, liability shall be determined pursuant to the Federal Tort Claims Act (FTCA – 28 U.S.C. § 1346).

No third party is intended to benefit or otherwise claim any rights whatsoever under this MOU. The rights and obligations set out in the MOU run between the signatories to this MOU only.

Article XII. User Access

Prior to gaining NESS access, each User shall execute a User Agreement and Rules of Behavior, acknowledging that the operations described in this Agreement are subject to audit by the ATF; the U.S. Department of Justice; Office of the Inspector General; the General Accounting Office; and other auditors designated by the U.S. Government.

Parties must abide by all state and federal law and regulations governing access to criminal justice databases and use and dissemination of criminal history record information. In the event of a conflict between state and federal law, federal law will control. Parties certify that they have read and are familiar with the CJIS Security Policy, the relevant parts of the NCIC 2000 Operating Manual and Title 28, Code of Federal Regulations, Part 20 and agree to be bound by their provisions.

Article XIII. Costs

The use of the NESS system is provided without charge to the NESS Partner Agency. ATF is not responsible for costs associated with the NESS Partner Agency's computer hardware, computer software (other than the NESS application), Internet connection(s), or other communications requirements associated with their use of the NESS application. ATF will maintain access to the NESS application furnished to the NESS Partner Agency and shall facilitate repairs to the NESS application in an expeditious manner, subject to availability and funding, but no guarantees as to when repairs will be completed. However, ATF will not assume maintenance or repairs required as the result of improper use of the NESS application or enhancements to the NESS application, as well as repairs to local computer hardware, computer software, or communications problems. ATF will not fund the costs associated with a NESS Partner Agency who chooses to manipulate their internal data structure for data communication and transfer reasons.

Article XIV. Limitations of the Agreement

1. **Relationship between the Parties:** The relationship between the Parties to this Agreement is and shall remain that of independent departments and entities. Nothing herein shall be construed to imply that either Party's employees are employees of the other.

2. **Resources:** This MOU does not require that the Parties are to contribute resources (financial or otherwise) to each other.

3. **Letters of Understanding:** The Parties are responsible for establishing relevant letters of

understanding or interagency agreements initiated or required as a consequence of this MOU.

4. **No Guarantee:** The NESS Partner Agency acknowledges that information is input into the NESS system based on data collected and available at the time, and that ATF makes no guarantee that said information will always be 100% accurate or up to date.

5. **Anti-Deficiency Act:** The obligations in this MOU are subject to the availability of the necessary resources to the Parties. No provision of this MOU shall be interpreted to require obligation or payment of funds in violation of the Anti-Deficiency Act, 31 U.S.C. Section 1341, or other applicable laws.

6. **Entire Agreement:** The mutual covenants and terms represent the entire Agreement and understanding of the Parties with respect to the subject matter hereof and supersede all prior and contemporaneous agreements and understandings relative to such subject matters. No representations or statements of any kind made by either Party, which are not expressly stated herein, shall be binding on such Party.

7. **Waiver:** Failure or delay on the part of any Party to exercise any right, remedy, power or privilege hereunder shall not operate as a waiver thereof. A waiver, to be effective, must be in writing and signed by the Party making the waiver. A written waiver of a default shall not operate as a waiver of any other default or of the same type default on a future occasion.

8. **Severability:** A determination that any term of this MOU is invalid for any reason shall not affect the validity of the remaining terms.

9. **Governing Law:** The terms and provisions in this Agreement shall be construed under the applicable federal laws, in conjunction with state and local laws that do not conflict with the federal mandates.

10. **Release of Information:** Releases to the media or third parties, judicial demands, public announcements, Freedom of Information Act/Privacy Act/Open Records requests, and communications with Congress concerning information generated and retrieved pursuant to this MOU shall be addressed by the Parties following coordination by authorized representatives of each Party.

Article XV. Conclusion

It is the intent of the signatories that this MOU ensures coordination, cooperation and the mutual conduct of enforcement and research activities relative to the NESS application. The result of this cooperation and coordination will be the successful prosecution of illegal firearm crimes in State and Federal jurisdictions as well as the development of an accurate picture of violent crime and the inception of new strategies to effectively disrupt the cycle of violence.

ATF and the NESS Partner Agency hereby agree to abide by the terms and conditions of this MOU, including any appendices, and all policies of the NESS Program. In witness whereof, the parties have hereby executed this MOU.

Signature Date	Signature Date
(Chief Law Enforcement or Public Safety Official)	(ATF - Special Agent in Charge)
Name	Name
Title	Special Agent in Charge Title
The Aurora Police Department NESS Partner Agency	ATF Field Division

Signature Date

Name

Chief, Firearms Operations Division
Title

Addendum to Memorandum of Understanding Pertaining to the NIBIN Enforcement Support System (NESS)

This addendum supplements the agreement between the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and the Aurora Police Department, dated _____, which established participation in the NIBIN Enforcement Support System (NESS). Specifically, the underlying Memorandum of Understanding (MOU) covered the ATF NESS installation, operation, and administration for the dissemination of crime gun data to enhance the efforts of law enforcement to integrate resources to reduce firearms violence, identify shooters and sources of crime guns, and refer them for prosecution. This addendum governs the sharing of NESS data with specific third-party law enforcement partners.

Currently, all data provided to ATF under the MOU is held in confidence and not provided to a third-party without prior coordination.

ATF has developed a feature within NESS to permit Collective Data Sharing (CDS). CDS will enable NESS participating agencies to view and share their NESS data with other law enforcement partners of their choosing. This feature significantly enhances the ability of law enforcement agencies to fight violent firearms crimes by broadening the knowledge base and access to potentially important leads in criminal investigations.

When a NESS partner agency chooses to participate in CDS, all of their NESS data is made available to the law enforcement partners of their choosing. Data sharing via NESS is reciprocal in that an agency does not have access to search the data pool unless they have opted in to share their NESS data with specified partner agencies.

By participating in CDS, NESS users will have a larger pool of data to examine and from which to develop investigative leads. Participating in CDS permits direct electronic access to crime gun information associated with other participating law enforcement agencies. Expanded analytical review of such data can provide leads in identifying persons engaged in the diversion of firearms into illegal commerce, link suspects to firearms in criminal investigations, identify potential firearm traffickers, and expose intrastate, interstate, and international patterns of sources and routes.

The parties hereby agree to the following:

All data submitted to ATF by Aurora Police Department through the NESS application, including but not limited to, investigative reports, NIBIN linked shootings data, gun recoveries, general event data (case numbers, dates, locations, associated persons, etc.) may be shared with partner law enforcement agencies chosen by the NESS Partner Agency's CDS Approver in NESS. These third-party NESS partner agencies must also agree to share data with your agency, or no data will be shared. Either agency can opt-out of CDS anytime by notifying the NESS Team via NESS_Support@atf.gov.

The NESS Partner Agency has designated the following individual as their CDS Approver. The CDS Approver is the only person who will be allowed to opt-in/out of CDS for their agency.

Name:	DJ Tisdale
Title:	Lieutenant, RAVEN Task Force Commander
Phone #:	303-597-5072
Email Address:	dtisdale@auroragov.org
Date of Birth:	
Signature:	Lt. DJ Tisdale Digitally signed by Lt. DJ Tisdale Date: 2025.09.03 14:00:10 -06'00'
Date:	9/3/2025

As a recipient of third-party CDS NESS data the

Aurora Police Department

agrees that all information within NESS shall be used for criminal investigative purposes only. NESS data reflects a compilation of information from multiple data sources and should not be relied upon as evidence. Investigators must collect original reports for evidentiary purposes. NESS information should not be used to develop statistics or for reporting purposes. No information contained therein may be duplicated, reproduced, or disseminated without the express authorization of ATF and/or the Originating Partner Agency, except as may be required by State or Federal law or court of competent jurisdiction. In accordance with Paragraph 10, Article XIV of the underlying MOU, the NESS Partner Agency agrees to notify ATF prior to such a release.

Signature Date	Signature Date
(Chief Law Enforcement or Public Safety Official)	(ATF - Special Agent in Charge)
Name	Name
Title	Special Agent in Charge Title
Aurora Police Department NESS Partner Agency	ATF Field Division

Signature Date

Name

Chief, Firearms Operations Division
Title

RESOLUTION NO. R2025- ____

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF AURORA, COLORADO, APPROVING THE MEMORANDUM OF UNDERSTANDING AND RELATED ADDENDUM BETWEEN THE AURORA POLICE DEPARTMENT AND THE BUREAU OF ALCOHOL, TOBACCO, FIREARMS AND EXPLOSIVES REGARDING THE NIBIN ENFORCEMENT SUPPORT SYSTEM

WHEREAS, City Council may, by resolution, enter into Intergovernmental Agreements with other governmental units or special districts for the joint use of buildings, equipment or facilities, and for furnishing or receiving commodities or services; and

WHEREAS, this Memorandum of Understanding establishes and defines a partnership between the Aurora Police Department (APD) and the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) that will result in ATF NIBIN Enforcement Support System (NESS) installation, operation, and administration for the dissemination of crime gun data to enhance the efforts of law enforcement to integrate resources to reduce firearms violence, identify shooters and sources of crime guns, and refer them for prosecution; and

WHEREAS, the Collective Data Sharing (CDS) Addendum governs the sharing of NESS data with specific third-party law enforcement partners; and

WHEREAS, by participating in CDS, APD will have a larger pool of data to examine and from which to develop investigative leads; and

WHEREAS, pursuant to the Addendum, CDS NESS data will only be used for criminal investigative purposes; and

WHEREAS, City Council finds that this Memorandum of Understanding and Addendum support an important partnership between the APD and ATF that will enhance APD's ability to investigate crimes, thereby promoting the health, safety, and welfare of the inhabitants of the City.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF AURORA, COLORADO, THAT:

Section 1. The Memorandum of Understanding and Addendum between APD and ATF regarding the NIBIN Enforcement Support System and Collective Data Sharing is hereby approved.

Section 2. The Mayor and City Clerk are hereby authorized to execute the attached agreement and addendum in substantially the form presented at this meeting with such technical additions, deletions, and variations as may be deemed necessary or appropriate by the City Attorney.

Section 3. All resolutions or parts of resolutions of the City in conflict herewith are hereby rescinded.

RESOLVED AND PASSED this _____ day of _____ 2025.

_____
MIKE COFFMAN, Mayor

ATTEST:

_____
KADEE RODRIGUEZ, City Clerk

APPROVED AS TO FORM:

PETER A. SCHULTE, CITY ATTORNEY

By: Amanda MacDonald RLA
_____
AMANDA MACDONALD, Assistant City Attorney

CITY OF AURORA
Council Agenda Commentary

Item Title: Aurora911 Retention Update – September 2025
Item Initiator: Yelena Emeson, Executive Administrative Supervisor of Aurora911
Staff Source/Legal Source: Tina Buneta, Director of Aurora911 / Angela Garcia, Senior Assistant City Attorney
Outside Speaker: NA
Strategic Outcome: Safe: Promoting safety in our built environment through effective administration of city codes and ordinances and responding to emergencies appropriately to preserve and enhance the community's sense of security and well-being.

COUNCIL MEETING DATES:

Study Session: N/A

Regular Meeting: N/A

2nd Regular Meeting (if applicable): N/A

Item requires a Public Hearing: ☐ Yes ☐ No

ITEM DETAILS *(Click in highlighted area below bullet point list to enter applicable information.)*

- Waiver of reconsideration requested, and if so, why
- Sponsor name
- Staff source name and title / Legal source name and title
- Outside speaker name and organization
- Estimated time: (For Study Session items only indicate combined time needed for presentation and discussion)

Aurora911 Retention Update – September 2025

ACTIONS(S) PROPOSED *(Check all appropriate actions)*

☐ Approve Item and Move Forward to Study Session

☐ Approve Item and Move Forward to Regular Meeting

☒ Information Only

☐ Approve Item with Waiver of Reconsideration
Reason for waiver is described in the Item Details field above.

☐ Approve Item as Proposed at Policy Committee

☐ Approve Item as Proposed at Study Session

☐ Approve Item as Proposed at Regular Meeting

PREVIOUS ACTIONS OR REVIEWS:

Policy Committee Name: N/A

Policy Committee Date: N/A

Action Taken/Follow-up: ***(Check all that apply)***

☐ Recommends Approval ☐ Does Not Recommend Approval

☐ Forwarded Without Recommendation ☐ Minutes Not Available

☐ Minutes Attached

HISTORY *(Dates reviewed by City council, Policy Committees, Boards and Commissions, or Staff. Summarize pertinent comments. ATTACH MINUTES OF COUNCIL MEETINGS, POLICY COMMITTEES AND BOARDS AND COMMISSIONS.)*

N/A

ITEM SUMMARY *(Brief description of item, discussion, key points, recommendations, etc.)*

Aurora911 Monthly Retention Update - Report

FISCAL IMPACT

Select all that apply. (If no fiscal impact, click that box and skip to "Questions for Council")

☐ Revenue Impact ☐ Budgeted Expenditure Impact ☐ Non-Budgeted Expenditure Impact
☐ Workload Impact ☒ No Fiscal Impact

REVENUE IMPACT
Provide the revenue impact or N/A if no impact. (What is the estimated impact on revenue? What funds would be impacted? Provide additional detail as necessary.)

N/A

BUDGETED EXPENDITURE IMPACT
Provide the budgeted expenditure impact or N/A if no impact. (List Org/Account # and fund. What is the amount of budget to be used? Does this shift existing budget away from existing programs/services? Provide additional detail as necessary.)

N/A

NON-BUDGETED EXPENDITURE IMPACT
Provide the non-budgeted expenditure impact or N/A if no impact. (Provide information on non-budgeted costs. Include Personal Services, Supplies and Services, Interfund Charges, and Capital needs. Provide additional detail as necessary.)

N/A

WORKLOAD IMPACT
Provide the workload impact or N/A if no impact. (Will more staff be needed or is the change absorbable? If new FTE(s) are needed, provide numbers and types of positions, and a duty summary. Provide additional detail as necessary.)

N/A

QUESTIONS FOR COUNCIL

N/A

LEGAL COMMENTS

This item is informational only. There is no formal council action necessary.

The City Manager shall be responsible to the Council for the proper administration of all affairs of the city placed in his charge and, to that end, shall have the power and duty to make written or verbal reports at any time concerning the affairs of the City. (City Charter, Art. 7-4(e)). (Garcia)

Aurora911 Retention Review

September 2025

Aurora911's Mission: The Right Resources to the Right Place at the Right Time, for Everyone, Every Time.

Aurora911's Vision: We are igniting a worldwide transformation in public safety communications, fueled by innovation and heartfelt **compassion.** We will bridge diverse communities and nurture an Aurora where **respect** is foundational, **integrity** preserves mutual trust, and **teamwork** is our North Star.

2025 Retention Review – August 2025

Authorized FTE: 91

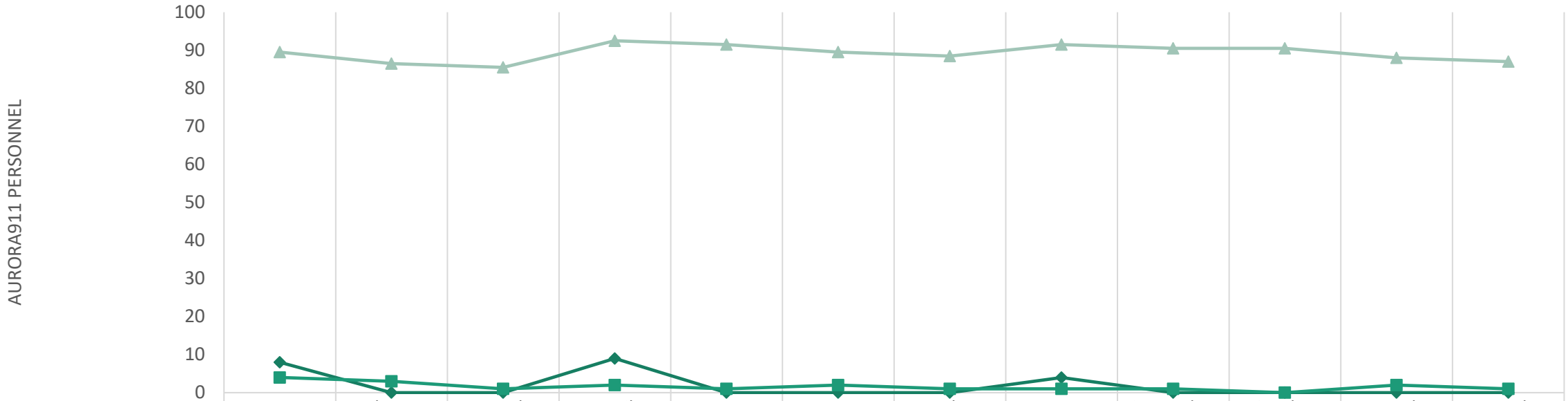
Current FTE: 88

Current Varied: 4

Current Staffing Percentage: 97%

AURORA911

2024 Monthly & Annual Turnover Rate

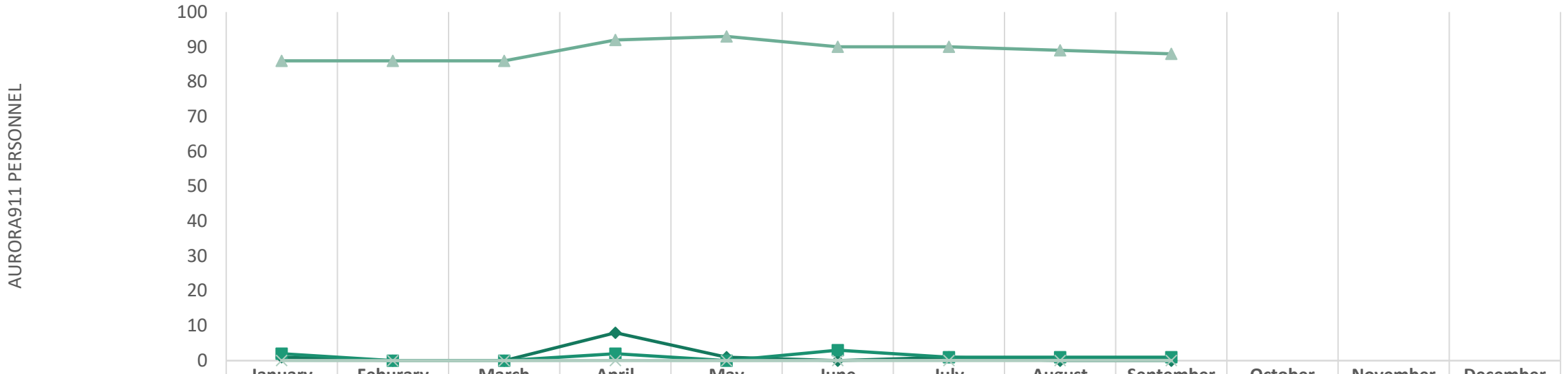


	January	Feburary	March	April	May	June	July	August	September	October	November	December
New Hires	8	0	0	9	0	0	0	4	0	0	0	0
Separations	4	3	1	2	1	2	1	1	1	0	2	1
Total Personnel	89.5	86.5	85.5	92.5	91.5	89.5	88.5	91.5	90.5	90.5	88	87

YTD Turnover Rate – 21.53%

AURORA911

2025 Monthly & Annual Turnover Rate



	January	Feburary	March	April	May	June	July	August	September	October	November	December
New Hires	1	0	0	8	1	0	1	0	0			
Separations	2	0	0	2	0	3	1	1	1			
Total Personnel	86	86	86	92	93	90	90	89	88			
Turnover Rate	2.31%	0%	0%	2.25%	0.00%	3.28%	1.10%	1.12%	1.12%			

YTD Turnover Rate – 11.5%

AURORA911

Retention Initiatives

Attention on career progression throughout the year to increase radio position skillset

Jan. 2025 – YTD

Successful Training Completions:

5 Services, 5 PD, 4 Fire

Academy Class 25-2:

Starts around October 20th, 2025

PDT – 2 FTEs – Interview Process

Operations Supervisor – 2 FTEs – Job Posted

Leadership development and employee continuing education

Aurora911 Values

Teamwork

Integrity

Compassion

Respect

Participation in community events providing public safety education.

Communications Strategist Senior Position – 1 FTE, started July 14th, 2025

Continued focus on culture and developing strong relationships with our partners and other city departments

CITY OF AURORA
Council Agenda Commentary

Item Title: Aurora Fire Rescue Retention – August 2025
Item Initiator: Inass Bounouar, Support Specialist Supervisor
Staff Source/Legal Source: Kathy Stafford, Deputy Director / Angela Garcia, Senior Assistant City Attorney
Outside Speaker: N/A
Strategic Outcome: Safe: Promoting safety in our built environment through effective administration of city codes and ordinances and responding to emergencies appropriately to preserve and enhance the community's sense of security and well-being.

COUNCIL MEETING DATES:

Study Session: N/A

Regular Meeting: N/A

2nd Regular Meeting (if applicable): N/A

Item requires a Public Hearing: ☐ Yes ☒ No

ITEM DETAILS *(Click in highlighted area below bullet point list to enter applicable information.)*

- Waiver of reconsideration requested, and if so, why
- Sponsor name
- Staff source name and title / Legal source name and title
- Outside speaker name and organization
- Estimated time: (For Study Session items only indicate combined time needed for presentation and discussion)

Aurora Fire Rescue Retention Report – August 2025

ACTIONS(S) PROPOSED *(Check all appropriate actions)*

☐ Approve Item and Move Forward to Study Session

☐ Approve Item and Move Forward to Regular Meeting

☒ Information Only

☐ Approve Item with Waiver of Reconsideration
Reason for waiver is described in the Item Details field above.

☐ Approve Item as Proposed at Policy Committee

☐ Approve Item as Proposed at Study Session

☐ Approve Item as Proposed at Regular Meeting

PREVIOUS ACTIONS OR REVIEWS:

Policy Committee Name: N/A

Policy Committee Date: N/A

Action Taken/Follow-up: ***(Check all that apply)***

☐ Recommends Approval ☐ Does Not Recommend Approval

☐ Forwarded Without Recommendation ☐ Minutes Not Available

☐ Minutes Attached

HISTORY *(Dates reviewed by City council, Policy Committees, Boards and Commissions, or Staff. Summarize pertinent comments. ATTACH MINUTES OF COUNCIL MEETINGS, POLICY COMMITTEES AND BOARDS AND COMMISSIONS.)*

N/A

ITEM SUMMARY *(Brief description of item, discussion, key points, recommendations, etc.)*

Aurora Fire Rescue Retention Report – August 2025

FISCAL IMPACT

Select all that apply. (If no fiscal impact, click that box and skip to "Questions for Council")

☐ Revenue Impact ☐ Budgeted Expenditure Impact ☐ Non-Budgeted Expenditure Impact
☐ Workload Impact ☒ No Fiscal Impact

REVENUE IMPACT
Provide the revenue impact or N/A if no impact. (What is the estimated impact on revenue? What funds would be impacted? Provide additional detail as necessary.)

BUDGETED EXPENDITURE IMPACT
Provide the budgeted expenditure impact or N/A if no impact. (List Org/Account # and fund. What is the amount of budget to be used? Does this shift existing budget away from existing programs/services? Provide additional detail as necessary.)

NON-BUDGETED EXPENDITURE IMPACT
Provide the non-budgeted expenditure impact or N/A if no impact. (Provide information on non-budgeted costs. Include Personal Services, Supplies and Services, Interfund Charges, and Capital needs. Provide additional detail as necessary.)

WORKLOAD IMPACT
Provide the workload impact or N/A if no impact. (Will more staff be needed or is the change absorbable? If new FTE(s) are needed, provide numbers and types of positions, and a duty summary. Provide additional detail as necessary.)

QUESTIONS FOR COUNCIL

N/A

LEGAL COMMENTS

This item is informational only. There is no formal council action necessary.

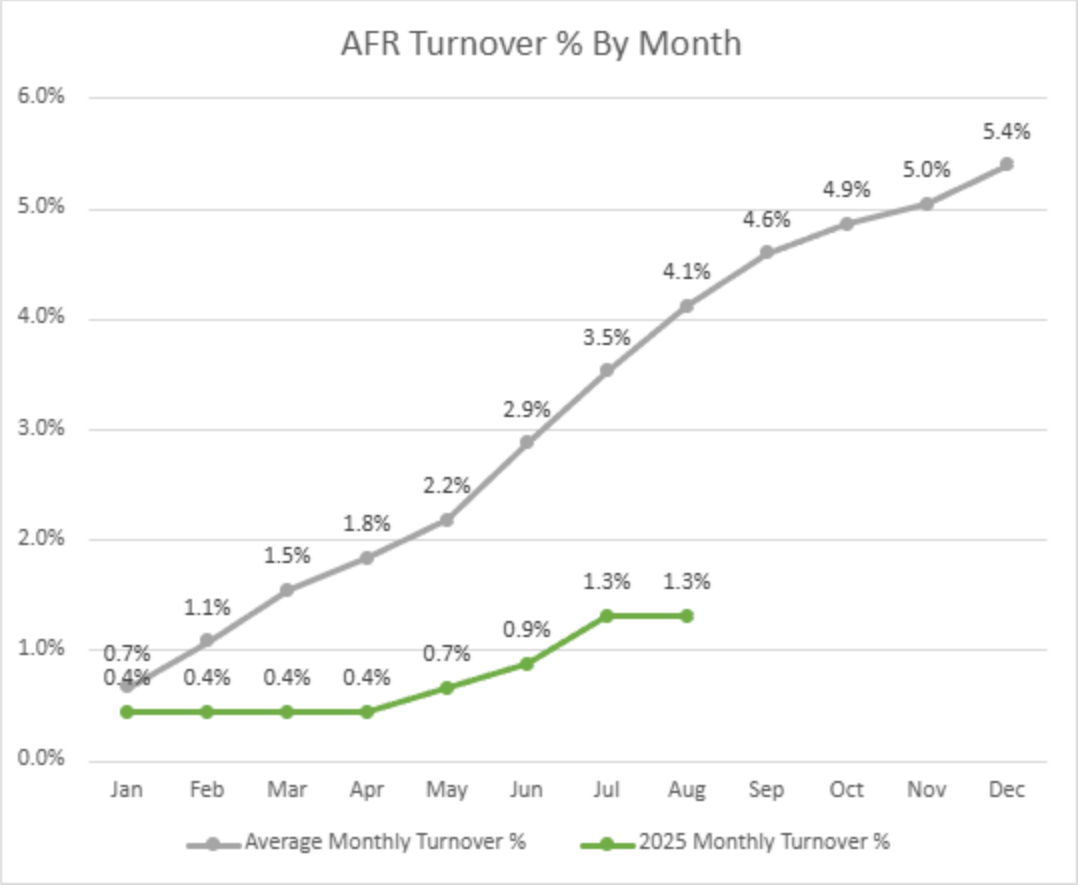
The City Manager shall be responsible to the Council for the proper administration of all affairs of the city placed in his charge and, to that end, shall have the power and duty to make written or verbal reports at any time concerning the affairs of the City. (City Charter, Art. 7-4(e)). (Garcia)

Aurora Fire Rescue
Civil FTE Attrition – August 2025

Fire Sworn Turnover
- 2024 Year End Attrition = 15 FTE
- 2025 YTD Attrition = 6 FTE
- 2025 Planned Attrition = 23 FTE

Fire Recruit Turnover
- 2024 Year End Attrition = 17 FTE
- 2025 YTD Attrition = 13 FTE
- 2025 Planned Attrition = 7 FTE

Aurora Fire Rescue
Civil FTE Attrition – August 2025



- 2025 YTD Sworn Attrition Rate = 1.3%
- 2025 Planned Attrition Rate = 5.4%

Aurora Fire Rescue
Civil FTE Retention – August 2025

2025 Aurora Fire Rescue Sworn Staffing

2025 Additions:

3 25-01 FastTrack

3 Total Adds

2025 Fire Attrition

13 Recruit Resignations
2 Resignation - Voluntary
3 Retirement
1 Disability Retirements

19 Total Losses

-16 Net Loss

CITY OF AURORA
Council Agenda Commentary

Item Title: Public Safety Action Plan Update
Item Initiator: Jason Batchelor, City Manager
Staff Source/Legal Source: Jason Batchelor , City Manager /Megan Platt, Deputy City Attorney
Outside Speaker: N/A
Council Goal: 2012: 1.1--Reduce crime rates

COUNCIL MEETING DATES:

Study Session: N/A

Regular Meeting: N/A

2nd Regular Meeting (if applicable): N/A

Item requires a Public Hearing: ☐ Yes ☒ No

ITEM DETAILS *(Click in highlighted area below bullet point list to enter applicable information.)*

- Agenda long title
- Waiver of reconsideration requested, and if so, why
- Sponsor name
- Staff source name and title / Legal source name and title
- Outside speaker name and organization
- Estimated time (For Study Session items only, indicate combined time needed for presentation and discussion)

Jason Batchelor, City Manager / Megan Platt, Deputy City Attorney
Estimated time: 15 mins

ACTIONS(S) PROPOSED *(Check all appropriate actions)*

☐ Approve Item and Move Forward to Study Session

☐ Approve Item as Proposed at Study Session

☐ Approve Item and Move Forward to Regular Meeting

☐ Approve Item as Proposed at Regular Meeting

☒ Information Only

☐ Approve Item with Waiver of Reconsideration
Reason for waiver is described in the Item Details field above.

PREVIOUS ACTIONS OR REVIEWS:

Policy Committee Name: N/A

Policy Committee Date: N/A

Action Taken/Follow-up: ***(Check all that apply)***

☐ Recommends Approval ☐ Does Not Recommend Approval

☐ Forwarded Without Recommendation ☐ Minutes Not Available

☐ Minutes Attached

HISTORY *(Dates reviewed by City council, Policy Committees, Boards and Commissions, or Staff. Summarize pertinent comments. ATTACH MINUTES OF COUNCIL MEETINGS, POLICY COMMITTEES AND BOARDS AND COMMISSIONS.)*

Council approved a Resolution authorizing the City of Aurora to tackle the increase of violent crime in the City by developing and implementing a comprehensive crime reduction plan. The plan included 5 core strategies.

1. Fully staffing the Aurora Police Department and providing ongoing and industry leading training
2. Improve data collection, utilize hot spot analysis, and improve efficiency through data analytics
3. Restore and expand the Aurora Gang Reduction Impact Program to address youth violence
4. Increase number of clinicians on Crisis Response Team to increase response to mental health calls
5. Address public health and safety challenges from encampments along highways, businesses, and in neighborhoods

The resolution required monthly updates on progress made toward each core strategy to the Public Safety Committee and quarterly updates at Study Session.

ITEM SUMMARY *(Brief description of item, discussion, key points, recommendations, etc.)*

This item is to provide a discussion and direction from the Public Safety Committee on the Format of the required updates and to identify the specific information the Committee would like to see covered in the updates.

FISCAL IMPACT

Select all that apply. (If no fiscal impact, click that box and skip to "Questions for Council")

☐ Revenue Impact ☐ Budgeted Expenditure Impact ☐ Non-Budgeted Expenditure Impact
☐ Workload Impact ☒ No Fiscal Impact

REVENUE IMPACT
Provide the revenue impact or N/A if no impact. (What is the estimated impact on revenue? What funds would be impacted? Provide additional detail as necessary.)

N/A

BUDGETED EXPENDITURE IMPACT
Provide the budgeted expenditure impact or N/A if no impact. (List Org/Account # and fund. What is the amount of budget to be used? Does this shift existing budget away from existing programs/services? Provide additional detail as necessary.)

N/A

NON-BUDGETED EXPENDITURE IMPACT
Provide the non-budgeted expenditure impact or N/A if no impact. (Provide information on non-budgeted costs. Include Personal Services, Supplies and Services, Interfund Charges, and Capital needs. Provide additional detail as necessary.)

N/A

WORKLOAD IMPACT

Provide the workload impact or N/A if no impact. (Will more staff be needed or is the change absorbable? If new FTE(s) are needed, provide numbers and types of positions, and a duty summary. Provide additional detail as necessary.)

N/A

QUESTIONS FOR COUNCIL

Information Only

LEGAL COMMENTS

This item is informational only. There is no formal council action necessary.
The City Manager shall be responsible to the Council for the proper administration of all affairs of the city placed in his charge and, to that end, shall have the power and duty to make written or verbal reports at any time concerning the affairs of the City. (City Charter, Art. 7-4(e)). (Platt))

Crime Reduction Plan Updates: September 2025 Data Report

Section 1. The City of Aurora shall provide the needed resources and other support to ensure the Aurora Police Department is fully staffed, including all specialty units critical to building and maintaining community relationships, and all officers have access to ongoing and industry-leading training.

METRICS:

Agent/Officer Staffing (**John Schneebeck**):

Assignment	Total Authorized	Hard Vacancy	Unavailable	Actual Deployment
Internal Investigations	5	0	0	5
PIO	1	0	1	0
Patrol	219	6	17	196
PAR	26	10	1	15
DART	18	0	0	18
District Criminal Investigations	26	2	0	24
Community Relations	2	0	0	2
CRT	5	0	1	4
AuroraSAVE	1	0	0	1
SRO	20	0	0	20
HART	6	0	0	6
Violent Crimes	40	3	4	33
Special Victims	39	7	1	31
RAVEN	9	1	2	6
Investigations Support	1	0	0	1
SWAT	18	3	0	15
K9	7	0	0	7
Strategic Enforcement	20	4	0	16
Traffic	16	6	0	10
MET	13	5	0	8
Traffic Investigations	6	0	0	6
Homeland Security	6	2	0	4
Academy	14	1	1	12
Range	4	0	0	4
Recruiting	3	0	0	3
Backgrounds	3	0	0	3
Cadet Program	1	0	0	1
Policy	4	2	0	2
RTIC	2	1	0	1
ESS	7	2	0	5
Property	1	0	0	1
Grand Total	**543**	**55**	**28**	**460**

Academy – Recruit Classes (Division Chief Rathbun): (Iske 08/28/25)

25-1B (Started January 13th, 2025)

- Started 50 / Graduated 36
- Graduation July 17th, 2025
- FTEP Completion October 25th, 2025

25-2B (Started May 19th, 2025)

- Started 28 / Current 20
- Graduation November 20th, 2025
- FTEP Completion February 28th, 2025

25-2L (Started July 28th, 2025)

- Started 6 / Current 6
- Graduation August 22nd, 2025
- FTEP Completion November 14th, 2025

Inservice – Training total attendance: (Schaefer 09/02/25)

Course Name	Officers Attended
2025 APD Blue Envelope Program Training	530
2025 APD Secondary Employment Update Video	386
2025 APD Q3 In-Service (POST Required) - ACT / EVOC	228
2025 APD Critical Incident Familiarization - Mandatory	103
2025 APD Domestic Violence Training - Mandatory	79
2025 APD OC Recertification Practical	67
2025 APD Taser Recertification Practical	52
2025 APD Metro Track Video - Mandatory	51
2025 APD Stop Stick & Funneling Training	39
2025 Q2 In-Service - Missing and Murdered Indigenous Relatives	38
2025 APD Rifle In-Service	36
2025 Q2 In-Service - Community Policing	31
2025 Q2 In-Service - Trespass Refresher	31
2025 Q2 In-Service - Interactions With People With Disabilities - Autism	30
2025 APD Peacekeeper RCB User Video Training	29
2025 Q2 In-Service - OC & Taser Refresher	27
2025 APD Request For Driver's Re-Examination Form DR2536 Video Training	27
2025 APD Pursuit Policy Update Video - Mandatory	17
2025 Crisis Intervention Training	8
2025 Q2 In-Service - Prone Control	6
2025 Breaching Shotgun In-Service	4
2025 APD Scott Company Drug Testing	2
2025 APD Peacekeeper RCB User Written Test	1
APD 2025-1B In-Custody Death Directive	1

Section 2. The City of Aurora police department shall improve overall data collection, utilize hot spot analysis to put more officers on patrol in key neighborhoods, and improve efficiency through data analytics.

METRICS: (Justin Bock – *updated 6/30, reflects April and May stats*)

CRIME	4-Weeks Prior	4-Weeks Current	4-Week % Change	YTD Prior Year	YTD Current Year	YTD % Change
Murder	4	3	**-25.0%**	17	16	**-5.9%**
NF Shootings	4	7	**+75.0%**	48	31	**-35.4%**
Robbery	23	24	**+4.3%**	260	158	**-39.2%**
Motor Vehicle Theft	120	137	**+14.2%**	1,865	1,144	**-38.7%**

ADDITIONAL UPDATES:

- YTD non-fatal shootings (with juvenile victims): **6**
- YTD non-fatal shootings (with known juvenile offenders): **4**

Section 3. The City of Aurora shall restore and expand the Aurora Gang Reduction Impact Program ("AGRIP") to address youth violence through immediate intervention and long-term prevention strategies. (Youth Violence Prevention Program) (Lisa Battan)

Intervention / Prevention Services	
Aurora SAVE and Youth Violence Prevention Program	**Contact and Outreach Summary:** The Aurora SAVE Team had contact with 12 SAVE candidates during custom notifications in August. The current average age of SAVE recipients is 18. The SAVE team continues to work on our call-in in September, which will be solely for juvenile SAVE candidates. Our Support & Outreach partners have been working to invite candidates to attend.

SAVE Success Stories:

1. During the month of August, Aurora SAVE community partners were able to facilitate school registration and return to school for 6 students. In one family, Aurora SAVE case manager worked with a family and Lifeline, as well as the courts to find options for a return to school. In another case, a candidate of Aurora SAVE and his brother both needed help navigating registration, and restrictions the family is facing as the two brothers cannot be classmates. One brother will be able to attend Emily Griffith, and the other brother is now enrolled at Field Academy. In the final case, Lifeline managed the school registration and navigation for Hope online for three young men living in foster care with two of them being Aurora SAVE candidates.

2. Struggle of Love donated school supplies and backpacks to the Aurora SAVE candidates and their children. Case manager was able to deliver them to each household and was also able to obtain some donations for "little extras" including special pencil cases and more feminine backpacks for a mom and her daughter that are both going to school this year. Every recipient of a backpack was delighted with their supplies and backpacks.

3. Case manager has been working with a family where the young mother is an Aurora SAVE candidate. Aurora SAVE case manager was able to help the young mom with her housing concerns without the ability to use victim's assistance. To date, case manager and the candidate have worked on several goals together, including life skills, applying for jobs, finding a daycare and getting one child on the waiting list for the daycare. The candidate has stated that she feels like the City of Aurora really does care about families.

Section 4. The City of Aurora shall increase the number of clinicians and other personnel on the "Aurora Crisis Response Team (CRT)" to increase response ability to mental health calls.

METRICS:

Crisis Response Team – CRT Calls for Service (Lisa Battan)

CRT (5 units)

Call Volume and Outcomes	
Calls for Service	320
NEW D42	33
Emergency Room Diversion	49
Jail Diversion	25
Charges Mitigated	25
Resolved on Scene	121
Courtesy Transport	3
Walk-In Crisis Center	6
Emergency Department	65
on M1 (by CRT)	26
Jail	10

CRT- Targeted Violence Prevention (1 unit)

TVP Referrals Received	3
ERPO Referrals Received	2

AMRT (3 units)

Call Volume and Outcomes	
Calls for Service	317
NEW AMRT 3	103
Emergency Room Diversion	7
Jail Diversion	4
Charges Mitigated	4
Resolved on Scene	145
Courtesy Transport	12
Walk-In Crisis Center	5
Emergency Department	47
on M1 (by AMRT)	15
Jail	6

Case Management

Follow-ups	68

SUCCESS STORIES and ACTIVITIES:

AMRT:

- AMRT was on a call with a client who has a long history of visits to Children's Hospital. With support from the client's group home, Host Home Providers, and officers on scene, AMRT successfully helped de-escalate the situation and guided the client in making the decision to return home. AMRT collaborated with both the client and Host Home to develop a safety plan. The client was transported home by AMRT, who also committed to following up with the client.
- AMRT responded to an elderly gentleman who told his nurse that he was going to shoot him. With the extensive medical history of the client it was determined that it would be best for the client to safety plan at home rather than go to the emergency room for assistance. We were able to collaborate with APD to provide the client a gun lock to keep himself safe.

CRT:

- CRT responded to a 25yo male that had reportedly taken off with his toddler, then once the toddler was returned to other family members, the male grabbed a knife during an argument with family. CRT utilized de-escalation skills and Motivational Interviewing to build rapport and develop a person-centered response. Individual was agreeable to being transported by CRT to the Walk In Center for stabilization. Had CRT not responded, this male would have been transported to the hospital.
- APD responded to a call for a 16yo that had damaged property. CRT responded to assist. This youth had become upset when Foster Parent told him that he was no longer allowed to get rides to school from his girlfriend. Youth threw rocks and smashed Foster Parent's windshield with a large rock. Foster Parent wanted charges pressed. Although the youth was charged, he was diverted from jail and transported to the ED instead.

TVP:

- TVP received a referral from APD regarding a subject who was believed to be planning an attack against the African American community as well as the LGBTQ community. Search warrant and ERPO were petitioned for through Adams County Courts due to the reports of this individual stealing his father's shotgun and sawing off the cable lock, possible elder abuse on the father, and the potential presence and creation of concerning incendiary devices. Subject was detained then arrested, father of subject was able to move to a supportive living situation and obtained a protection order and the subject was believed to have undiagnosed schizophrenia and will receive a mental health evaluation for appropriate treatment and ongoing care.

Case Management:

- CM worked on a case for about 2 weeks where the patient expressed suicidal ideations due to financial difficulties and problems with her landlord, where her landlord informed her, she would be getting evicted soon. When case management spoke to her, she began to escalate as she began to cry and state she did not want to live anymore because no one was helping her. Because of those statements CM provided crisis walk-in information and offered to send a CRT/AMRT unit to speak to her at the moment. She then became more escalated and was adamant that she did not want that as she felt that would "make things worse" she then chose to stay on the phone with CM and go over resources/options together. After some de-escalation, she was receptive towards resources. CM sent direct referral to food assistance and financial assistance as well as outpatient therapy services. CM also connected with CRT Sargeant and collaborated in order to obtain any information on a possible court date for her eviction as that was one of her major triggers. That information was able to be provided to her, which then significantly improved her SI. At the end she was extremely grateful for the resources and expressed how this was the only support she had received in months of trying to obtain resources.

Section 5. The City of Aurora shall address the public health and safety challenges created by the current encampments along our highways, in neighborhoods, and next to our businesses.

METRICS: (Emma King)

Notifications Received August 2025	
Abatements conducted August 2025	48
CDOT - related	17
Total number of people abated	32

ADDITIONAL UPDATES:

Abatements conducted – 24/25 Comparison

Month	2024	2025
January	48	58
February	19	52
March	20	66
April	32	61
May	33	64
June	30	55
July	22	65
August	31	48
YTD Total	235	469

Abatements by Ward in August 2025:

I	17
II	18
III	0
IV	7
V	6
VI	0

In mid-April, due to continuing renovations, overnight shelter transitioned from being held at the Navigation Campus to the Aurora Day Resource Center.

Average # of people per night in emergency shelter (ADRC/Nav Campus) - 101

# of people on Street Outreach caseload – 92
Best practice is 50 people or less on a street outreach caseload, per outreach worker

Percentage accepted services from outreach – 100%

STREET OUTREACH SUCCESS STORY:

CITY OF AURORA
Council Agenda Commentary

Item Title: Facial Recognition Technology for Law Enforcement
Item Initiator: Danelle Carrel, Manager of Executive Support
Staff Source/Legal Source: Chris Poppe, Commander / Mandy MacDonald, Assistant City Attorney
Outside Speaker: N/A
Strategic Outcome: Safe: Promoting safety in our built environment through effective administration of city codes and ordinances and responding to emergencies appropriately to preserve and enhance the community's sense of security and well-being.

COUNCIL MEETING DATES:

Study Session: 10/6/2025

Regular Meeting: 10/20/2025

2nd Regular Meeting (if applicable): N/A

Item requires a Public Hearing: ☐ Yes ☐ No

ITEM DETAILS *(Click in highlighted area below bullet point list to enter applicable information.)*

- Waiver of reconsideration requested, and if so, why
- Sponsor name
- Staff source name and title / Legal source name and title
- Outside speaker name and organization
- Estimated time: (For Study Session items only indicate combined time needed for presentation and discussion)

Staff Source: Chris Poppe, Commander / Mike Gaskill, Deputy Chief
Legal Source: Mandy MacDonald, Assistant City Attorney
Presentation: 10 Minutes

ACTIONS(S) PROPOSED *(Check all appropriate actions)*

☒ Approve Item and Move Forward to Study Session

☐ Approve Item and Move Forward to Regular Meeting

☐ Information Only

☐ Approve Item with Waiver of Reconsideration
Reason for waiver is described in the Item Details field above.

☐ Approve Item as Proposed at Policy Committee

☐ Approve Item as Proposed at Study Session

☐ Approve Item as Proposed at Regular Meeting

PREVIOUS ACTIONS OR REVIEWS:

Policy Committee Name: N/A

Policy Committee Date: N/A

Action Taken/Follow-up: ***(Check all that apply)***

☐ Recommends Approval ☐ Does Not Recommend Approval

☐ Forwarded Without Recommendation ☐ Minutes Not Available

☐ Minutes Attached

HISTORY *(Dates reviewed by City council, Policy Committees, Boards and Commissions, or Staff. Summarize pertinent comments. ATTACH MINUTES OF COUNCIL MEETINGS, POLICY COMMITTEES AND BOARDS AND COMMISSIONS.)*

N/A

ITEM SUMMARY *(Brief description of item, discussion, key points, recommendations, etc.)*

The Aurora Police Department is seeking approval from City Council to utilize Facial Recognition technology. This technology will provide many opportunities for the enhancement of productivity, increased crime solvability, effectiveness, and increased safety for both citizens and sworn members.

FISCAL IMPACT

Select all that apply. (If no fiscal impact, click that box and skip to "Questions for Council")

☐ Revenue Impact ☐ Budgeted Expenditure Impact ☒ Non-Budgeted Expenditure Impact
☒ Workload Impact ☐ No Fiscal Impact

REVENUE IMPACT
Provide the revenue impact or N/A if no impact. (What is the estimated impact on revenue? What funds would be impacted? Provide additional detail as necessary.)

N/A

BUDGETED EXPENDITURE IMPACT
Provide the budgeted expenditure impact or N/A if no impact. (List Org/Account # and fund. What is the amount of budget to be used? Does this shift existing budget away from existing programs/services? Provide additional detail as necessary.)

N/A

NON-BUDGETED EXPENDITURE IMPACT
Provide the non-budgeted expenditure impact or N/A if no impact. (Provide information on non-budgeted costs. Include Personal Services, Supplies and Services, Interfund Charges, and Capital needs. Provide additional detail as necessary.)

Approximately $171,000 over a 4 year period

WORKLOAD IMPACT
Provide the workload impact or N/A if no impact. (Will more staff be needed or is the change absorbable? If new FTE(s) are needed, provide numbers and types of positions, and a duty summary. Provide additional detail as necessary.)

Workload impact to existing FTEs between the Intelligence Unit and Information Management Unit

QUESTIONS FOR COUNCIL

Does the Committee approve this item to move forward to full Council?

LEGAL COMMENTS

Pursuant to City Charter, City Council has the power to enforce good government, general welfare, order and security of the City and the inhabitants thereof. (MacDonald)

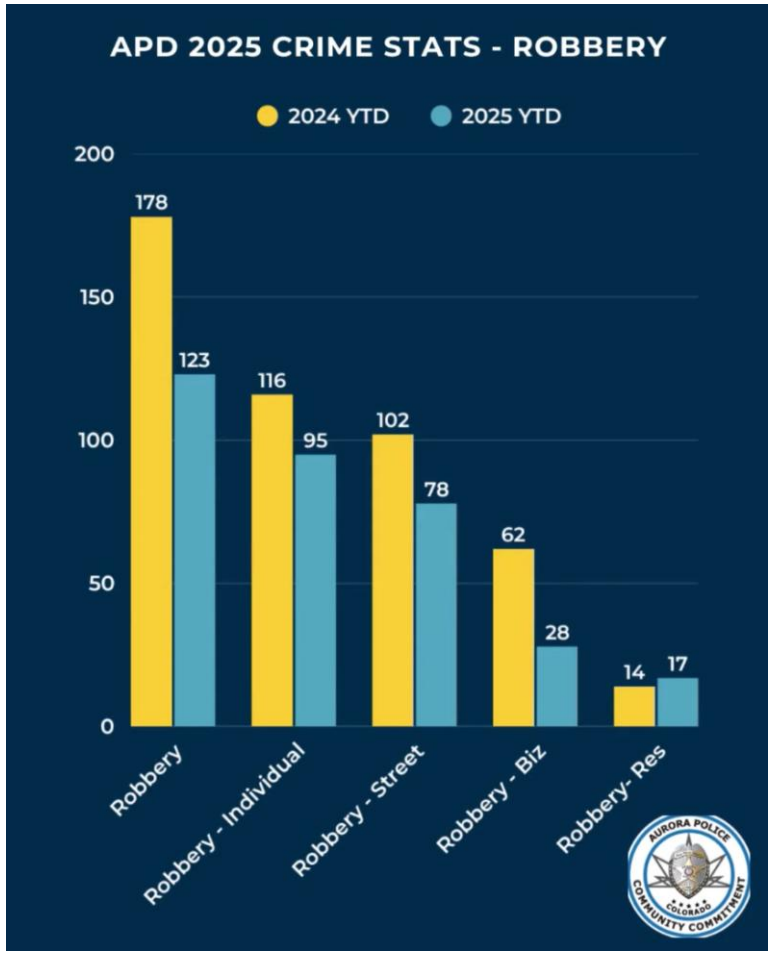
Colorado law enforcement agencies which develop, procure, or use an FRS must submit to their "reporting authority" an "accountability report" in accordance with C.R.S. § 24-18-302(4). The Aurora City Council is the Aurora Police Department's "reporting authority" as defined by C.R.S. § 24-18-301(14). The Aurora Police Department has prepared an accountability report for both FRS it plans to use, specifically Lumen and Clearview AI, which includes the information required by C.R.S. § 24-18-302(2)(a-h). (MacDonald)

Aurora Police Department
Facial Recognition project

Purpose of presentation

- The Aurora Police Department is seeking approval from City Council to utilize Facial Recognition technology

Value Proposition



- This technology will provide many opportunities for the enhancement of productivity, increased crime solvability, effectiveness, and increased safety for both citizens and sworn members.

Senate Bill 22-113

CONCERNING THE USE OF PERSONAL IDENTIFYING DATA, AND, IN CONNECTION THEREWITH, CREATING A TASK FORCE FOR THE CONSIDERATION OF FACIAL RECOGNITION SERVICES, RESTRICTING THE USE OF FACIAL RECOGNITION SERVICES BY STATE AND LOCAL GOVERNMENT AGENCIES, TEMPORARILY PROHIBITING PUBLIC SCHOOLS FROM EXECUTING NEW CONTRACTS FOR FACIAL RECOGNITION SERVICES, AND MAKING AN APPROPRIATION.

Colorado Revised Statutes 24-18 (part 3)
Use of Facial Recognition Services by State and Local Government Agencies

24-18-302. Notice of intent to use facial recognition service

(1) On and after August 10, 2022, an agency that uses or intends to develop, procure, or use a facial recognition service shall **file with its reporting authority** a notice of intent to develop, procure, use, or continue to use the facial recognition service and specify a purpose for which the technology is to be used.

(2) Except as described in subsection (8) of this section, after filing the notice of intent described in subsection (1) of this section, and prior to developing, procuring, using, or continuing to use a facial recognition service, an agency shall **produce an accountability report** for the facial recognition service.

(3) Prior to finalizing an accountability report, **an agency shall**:

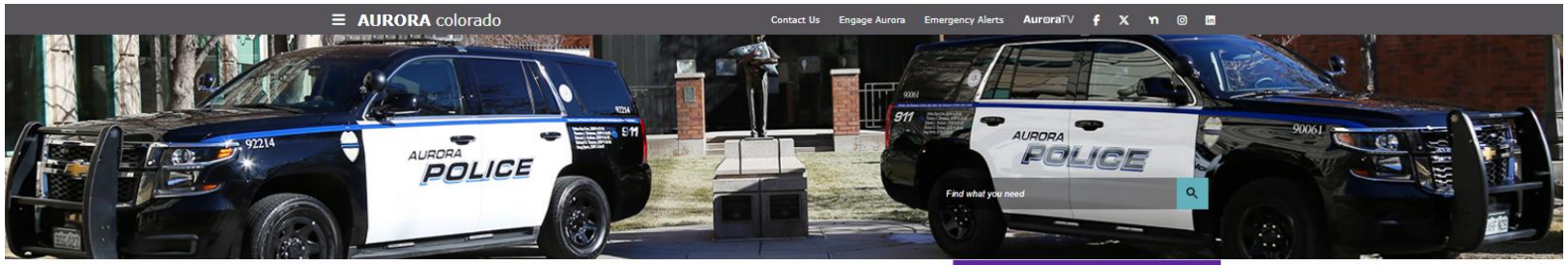
(a) Allow for a public review and comment period;

(b) Hold at least three public meetings to obtain feedback from communities; and

(c) Consider the issues raised by the public through the public meetings.

Link on APD website
(in development)

- Accountability reports publicly available for review
- Public comment form



CITY OF AURORA » RESIDENTS » PUBLIC SAFETY » POLICE

Police

APD Transparency Portal | Access Aurora
Online Crash Report | Online Crime Report

In an Emergency, Dial 911
Police Dispatch: 303.627.3100
General Information: 303.739.6000

Established in 1907, the Aurora Police Department is responsible for providing law enforcement services to a growing, urban/suburban community with unique and ever-changing needs. We strongly believe that the challenges facing the police department can only be addressed effectively by connecting with community leaders, school administrators, members of the business community, non-profit organizations, other government agencies, neighborhood groups and most importantly, individual residents. It is through this spirit of partnership that we will continue to see further reductions in crime and we will enhance the quality of life for those who live, work and play in our city.

The Aurora Police Department currently employs 748 officers and 212 professional staff employees.

- Police Districts, Assignments & Information
- Public Reports & Crime Data
- File Report, Get Records & Property Info
- Aurora Police News
- Community Engagement
- #JoinTheAPD
- Internal Affairs
- Police Area Representatives (PAR)
- Victim Services & Rights
- Youth Programs & Resources
- Get a Police Record
- Contact Us
- Commend an APD Employee
- File Complaint Against an APD Employee
- Cadet Program
- Hire an Off-Duty Officer

POLICE LINKS

Contact Us

15001 E. Alameda Pkwy
Aurora, CO 80012

303.739.6000

ContactAPD@auroragov.org

(This e-mail address is not for reporting crimes or requesting police services)

Community feedback

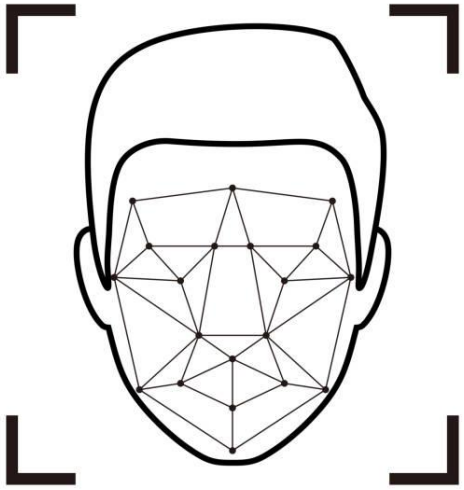
Methods of Identification

Fingerprint, DNA, and facial recognition are all distinct biometric methods of identification

Fingerprint – uses the unique patterns on a person's fingertips for identification

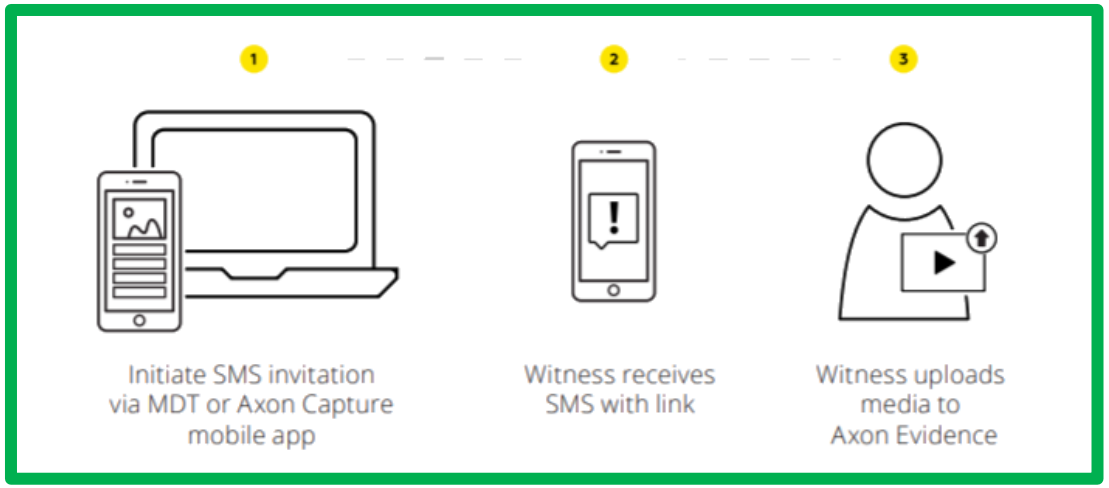
DNA – Analyzes a person's unique genetic makeup for identification

Facial Recognition – Analyzes a person's facial features and geometry to identify them



Cameras are increasingly recording criminals

Officers frequently canvas crime scenes for video evidence



Aurora Police Policy

- Increasing public safety and improving state, local, tribal, territorial, and national security.
- Minimizing the threat and risk of injury to specific individuals.
- Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.
- Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
- Protecting the integrity of criminal investigatory, criminal intelligence, and justice system processes and information.
- Minimizing the threat and risk of damage to real or personal property.
- Fostering trust in the government by strengthening transparency, oversight, and accountability.
- Making the most effective use of public resources allocated to public safety entities.

Authorized Use of Facial Recognition Information

- A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity.

- An active or ongoing criminal investigation.

- To mitigate an imminent threat to health or safety through short-term situational awareness surveillance or other means.

- To assist in the identification of a person who lacks capacity or is otherwise unable to identify themselves (such as incapacitated, deceased, or otherwise at risk).

- To investigate and/or corroborate tips and leads.

- To assist in the identification of potential witnesses and/or victims of violent crime.

- To support law enforcement in critical incident responses.

Lumen

The system compares a single “probe image” against large volumes of criminal justice record images that would otherwise require manual review.

Images include a collection of lawfully available booking photographs and other images maintained by members of the Colorado Information Sharing Consortium (CISC).

https://cisc.colorado.gov/

The Aurora Police Department is an existing member agency.

Clearview IA

Clearview App uses a machine-learning facial recognition algorithm to compare a user-uploaded “probe image” to initiate a search against Clearview’s database of 30 billion+ publicly available images from the Internet.

These results can be returned from diverse sources, such as news media sites, public arrest record websites, public social media pages, public business webpages, or public blogs.

Source of comparison images

Meaningful human review

Review or oversight by one or more individuals who are trained in accordance with Colorado Revised Statute 24-18-305 and who have the authority to alter a decision under review. This is accomplished through Facial Comparison

Per Colorado Revised Statutes §24-18-303, “An agency using a facial recognition service to make decisions that produce legal effects concerning individuals or similarly significant effects concerning individuals must ensure that those decisions are subject to meaningful human review.”

Training

Each member entrusted to access Facial Recognition software (Lumen and Clearview AI)

1. *Face Comparison and Identification Training*
    - Provides students with awareness and understanding of the face comparison discipline.
    - This training is consistent with the guidelines and recommendations outlined by the Facial Identification Scientific Working Group (FISWG).
2. *Software specific onboarding training from Vendor*

Every officer or detective with potential to receive Facial Recognition investigative lead

1. *Facial Recognition Investigative Certification Course*
    - It is imperative that law enforcement personnel understand how facial recognition leads are generated, be aware of the technological and legal limitations, and possess the necessary theoretical and operational knowledge to properly verify these leads.
    - Designed to safeguard the community from wrongful arrests, shield agencies from liability, and equip officers with the education, training, and certification needed to effectively and responsibly use this ever-evolving law enforcement tool.

Projected costs

- **Face Comparison and Identification Training** (for users).
  - Consistent with the guidelines and recommendations outlined by the Facial Identification Scientific Working Group (FISWG).
  - Available from virtually from FBI
  - NO COST
- **Lumen**
  - NO COST
- **Clearview AI**
  - 2026 - $32,490 (52% discount)
  - 2027 - $46,750 (31% discount)
  - 2028 - $67,389

- **Facial Recognition Investigative Certification Course** (for Detectives receiving FR leads)
  - Additional safeguard for agency, community and officers.
  - Facial Recognition Investigative Consultants LLC.
  - $16,000 to train 140 APD members

2025 - $16,000 (training)
2026 - $32,490 (Clearview AI)
2027 - $54,750 (Clearview AI + train 70 members)
2028 - $67,389 (Clearview AI)

- International Association of Chiefs of Police – www.theiacp.org/sites/default/files/2019-10/IJIS_IACP%20WP_LEITTF_Facial%20Recognition%20UseCasesRpt_20190322.pdf
- International Association of Chiefs of Police - www.theiacp.org/sites/default/files/2019-10/LE%20Facial%20Rec%20Guiding%20Principles%20Document%20July%202019.pdf
- Major Cities Chiefs Association - https://majorcitieschiefs.com/wp-content/uploads/2021/10/MCCA-FRT-in-Modern-Policing-Final.pdf
- US Government Accountability Office - www.gao.gov/assets/870/868079.pdf
- Security Industry Association - www.securityindustry.org/report/sia-principles-for-the-responsible-and-effective-use-of-facial-recognition-technology/

Collection of best practices

Questions

Aurora Police Department • 15151 E Alameda Parkway • Aurora, Co 80012

8.54 FACIAL RECOGNITION SYSTEMS

Approved By: ******** Chief of Police

Effective: **Enter Date Published**

Revised: **Enter Date Published**

Associated Policy: DM

References: C.R.S. § 24-18-301 -309

Review Authority: Professional Standards and Training Division Chief and APD Legal Advisor(s)

8.54.01 PURPOSE

Facial recognition technology involves the ability to examine and compare distinguishing characteristics of a human face using biometric algorithms contained within a software application. This technology can be a valuable investigative tool to detect and prevent criminal activity, reduce an imminent threat to health or safety, assist in the identification of individuals who refuse to identify themselves when required to do so by law, and help in the identification of persons unable to identify themselves or deceased persons.

This technology will provide many opportunities for the enhancement of productivity, increased crime solvability, effectiveness, and increased safety for both citizens and sworn members. This policy provides Aurora Police Department members with specific guidelines for the collection, access, use, dissemination, retention, purging of images, auditing, and related information applicable to facial recognition.

This policy ensures that all facial recognition investigations are consistent with authorized purposes while not violating anyone's privacy, civil rights, and civil liberties. Further, this policy will delineate the way requests for facial recognition information are received, processed, cataloged, and acted upon.

This directive complies with the statutory requirements described in Colorado Revised Statutes § 24-18-301 through 309.

8.54.02 SCOPE

This directive applies to all members of APD.

8.54.03 DEFINITIONS

Accountability report: A report developed pursuant to C.R.S. § 24-18-302(2).

Audit: A review conducted by the Facial Recognition Administrator to include all use of facial recognition software/technology. The audit will include all user's activity, such as user log ins and log outs, each user's activity in detail, what commands were issued to the system, and what records or files were accessed.

Candidate images: The possible results of a facial recognition search. When facial recognition software compares a probe image against the images contained in a repository, the result is a list of most likely candidate images that were determined by the software to be sufficiently similar to, or most likely resemble, the probe image to warrant further analysis. A candidate image is an investigative lead ONLY and does not establish probable cause without further investigation.

Decisions that produce legal effects concerning individuals or similarly significant effects concerning individuals: Decisions that:

- Result in the provision or denial of financial and lending services, housing, insurance, education enrollment, criminal justice, employment opportunities, health-care services, or access to basic necessities such as food and water; or

- Impact the civil rights of individuals.

Enhancement: To intensify, increase, or further improve the quality, value, or extent of an image. Image enhancement is the process of adjusting digital images so that the results are more suitable for display or further image analysis. For example, removing noise, sharpening, or brightening an image may make it easier to identify key features.

Enroll, Enrolled, or Enrolling: The process by which a facial recognition service:

- Creates a facial template from one or more images of an individual; and

- Adds the facial template to a gallery that is used by the facial recognition service for recognition or persistent tracking of individuals; or

- The act of adding an existing facial template directly into a gallery that is used by a facial recognition service.

Facial Comparison: (in facial identification) A manual process to identify similarities or dissimilarities between two (2) or more facial images or facial image(s) and a live subject for the purpose of determining if they represent the same person or a different person.

Facial recognition: The automated searching for a reference image on an image repository by comparing human facial features of a probe image with the features of images contained in an image repository. A facial recognition search will typically result in one or more likely candidate images.

Facial recognition administrator: A member designated by the Chief of Police, or designee, to be the point of contact for facial recognition software/technology access, training, and audits.

Facial recognition service: Technology that analyzes facial features to facilitate the identification, verification, or persistent tracking of individuals in still or video images. Facial recognition service does not include:

- The analysis of facial features to grant or deny access to an electronic device.

- A generally available consumer product, including a tablet or smartphone, that allows for the analysis of facial features in order to facilitate the user's ability to manage an address book or still or video images for personal or household use; or

- The use of an automated or semiautomated process by a law enforcement agency for the purpose of redacting a recording for release or disclosure to protect the privacy of a subject depicted in the recording, so long as the process does not generate or result in the retention of any biometric data or surveillance information.

Facial recognition software/technology: Third party software that uses specific proprietary algorithms to compare human facial features from one specific picture (probe image) to many others that are stored in an image repository to determine most likely candidates for further investigation.

Facial recognition user: A member who has been approved for access and granted account access by the facial recognition administrator.

Facial template: A machine-interpretable pattern of facial features that is extracted from one or more images of an individual by a facial recognition service.

Identification: The use of a facial recognition service by an agency to determine whether an unknown individual matches any individual whose identity is known to the agency and who has been enrolled by reference to that identity in a gallery used by the facial recognition service.

Image repository: A location where a group of images of known individuals and biometric templates is stored and managed. An image repository is searched during a facial recognition search process whereby a probe image is used by a facial recognition service for comparison with the images (or features within images) contained in the image repository.

Investigative lead: Any information which could potentially aid in the successful resolution of an investigation but does not imply positive identification of a subject or that the subject is guilty of a criminal act.

Meaningful human review: Review or oversight by one or more individuals who are trained in accordance with Colorado Revised Statute 24-18-305 and who have the authority to alter a decision under review. This is accomplished through Facial Comparison (defined above).

Ongoing surveillance: The continual use of a facial recognition service by an agency to track in real-time the physical movements of a specified individual through one or more public places. Ongoing surveillance does not include a single recognition or attempted recognition of an individual if no attempt is made to subsequently track that individual's movement over time with the use of a facial recognition service after the individual has been recognized.

Persistent tracking: The use of a facial recognition service by an agency to track the movements of an individual on a persistent basis without identification or verification of the individual. Tracking becomes persistent as soon as the facial template that permits the tracking is maintained for more than 48 hours after first enrolling that template or data created by the facial recognition service is linked to any other data such as the individual who has been tracked is identified or identifiable.

Nonidentifying demographic data: Data that is not linked or reasonably linkable to an identified or identifiable individual and includes information about an individual's gender, race, ethnicity, age, or location.

Probable Cause: Facts and circumstances taken as a whole that would lead a reasonable officer to believe that a particular person has committed or is committing a crime (as defined in DM 8.52.03).

Probe image: Any uploaded face image used by facial recognition software for comparison with the face images contained within a face image repository.

Reasonable Suspicion: Articulable facts and circumstances known to the member at the time of a contact when, taken as a whole, that would lead a reasonable officer to reasonably suspect that a particular person has committed, is committing, or is about to commit a specific crime(s). Reasonable suspicion is more than a hunch, however less than probable cause. The person is not free to leave during a detention based on reasonable suspicion (as defined in DM 8.52.03).

Recognition: The use of a facial recognition service by an agency to determine whether an unknown individual matches:

- Any individual who has been enrolled in a gallery used by the facial recognition service; or
- A specific individual who has been enrolled in a gallery used by the facial recognition service.

Repository: A location where a group of images of known individuals and biometric templates are stored and managed. An image repository is searched during a facial recognition search process whereby a probe image is used by facial recognition software for comparison with the images (or features within images) contained in the image repository.

RFI: Request for information.

RFI log: A credentialed log for the purposes of internal and external facial recognition data sharing and requests that documents the name of the agency/requestor, name of the person completing the request, date and time the request was completed, case number, and reason for the request. The RFI log may be a part of the software auditing process.

Social media alias: An alternative username or online identity used by a person on social media platforms, distinct from their real name.

Verification: The use of a facial recognition service by an agency to determine whether an individual is a specific individual whose identity is known to the agency and who has been enrolled by reference to that identity in a gallery used by the facial recognition service.

8.54.04 POLICY

This policy assists Aurora Police Department's use of facial recognition with:

- Increasing public safety and improving state, local, tribal, territorial, and national security.
- Minimizing the threat and risk of injury to specific individuals.
- Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.
- Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
- Protecting the integrity of criminal investigatory, criminal intelligence, and justice system processes and information.
- Minimizing the threat and risk of damage to real or personal property.
- Fostering trust in the government by strengthening transparency, oversight, and accountability.
- Making the most effective use of public resources allocated to public safety entities.

8.54.05 GENERAL INFORMATION

The use of facial recognition and access to data requires a legitimate law enforcement purpose. No member may use or authorize the use of or access to facial recognition for any other reason.

Probe images are specifically limited to those obtained lawfully and exposed to public view. Any uploaded probe image shall be that of an unknown person for the sole purpose of obtaining a possible identification and investigative lead in an official law enforcement investigation. The only exception to this requirement is if the uploading of a known probe image may result in additional investigative leads (such as the identification of potential aliases, alias social media accounts, etc.). Members shall not substantively manipulate an image for use in a facial recognition service in a manner not consistent with the facial recognition service provider's intended use and training.

Facial Recognition is an investigative tool and any law enforcement action taken based on a submission to any other facial recognition system shall be based on the agency's own identity determination and not solely the

results of a facial recognition search. The result of a facial recognition search shall only be considered as an investigative lead and **IS NOT TO BE CONSIDERED A POSITIVE IDENTIFICATION OF ANY SUBJECT OR PROBABLE CAUSE FOR ARREST**. Any possible connection or involvement of any subject to an investigation must be determined through further investigation and investigative resources.

The Department may share facial recognition data or requests with any government entity that presents an authorized law enforcement or public safety purpose. External data sharing or requests shall be at the approval of the facial recognition administrator or designee documented via the RFI process. Any data sharing or request shall abide by this facial recognition policy. The Department assumes no responsibility or liability for the acts or omissions of other agencies.

8.54.06 FACIAL RECOGNITION SERVICE SELECTION

Prior to procuring or implementing any facial recognition service, the Department shall require a provider whose facial recognition service is under consideration to disclose any complaints or reports of bias regarding the provider's facial recognition service.

The Department shall, to the extent reasonably practicable as determined by the Chief or designee, use facial recognition service providers who participate in the face recognition vendor test ongoing project of the National Institute of Standards and Technology (NIST Project). If the Department seeks to procure or implement a facial recognition service from a provider who is not participating in the NIST Project and the facial recognition service will be deployed in a context in which it will be used to make Decisions that Produce Legal Effects, the Department will test the facial recognition service in operational conditions before it is deployed.

a. The Department will follow all guidance provided by the developer of the facial recognition service to ensure the best quality results.

b. If the Department deploys a facial recognition service provider that is not participating in the NIST Project, the Department will require the provider to supply an application programming interface, or other technical capabilities, chosen by the provider, to allow for legitimate, independent and reasonable tests of the facial recognition service for accuracy and to identify unfair performance differences across distinct subpopulations, including those that are visually detectable characteristics (i.e., race, skin tone, ethnicity, gender, age, disability status). The provider will not, however, be required to provide proprietary material or provide an interface or technical capability in a way that would increase the risk of cyber-attacks.

c. If the results of independent testing identify material unfair performance differences across subpopulations, the Department will require the provider to develop and implement a plan to mitigate the identified performance differences within 90 days after receipt of the test results.

All technology associated with a facial recognition service, including all related hardware and software support, shall be bound by the Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS) security policy. Information contained within or generated through the use of a Facial Recognition Service is considered highly restricted personal information, which may only be transmitted, accessed, used, and disseminated in accordance with state and federal laws, rules, policies, and regulations; including, but not limited to, the most recent federal CJIS Security policy.

The facial recognition administrator will be responsible for deploying, managing, and controlling access to the facial recognition program and for ensuring that access, management, and use of the technology is consistent with Department policy and with statutory requirements in C.R.S. §§ 24-18-301 through 24-18-309.

Any authorization for the Department to develop, procure, use, or continue to use a facial recognition service shall comply with all applicable requirements of C.R.S. § 24-18-302.

8.54.07 PROGRAM MANAGEMENT

The Electronic Support Section Lieutenant will be responsible for deploying, managing, and controlling access to the facial recognition program. The ESS Lieutenant will designate a program manager tasked to ensure that access, management, and use of the technology is consistent with Aurora Police Department policy. The program manager will ensure that the Aurora Police Department is compliant with the statutory guidance defined in Colorado Revised Statutes (Use of Facial Recognition Services by State and Local Government Agencies 24-18-301 through 24-18-309).

The authorization to develop, procure, use, or continue to use the facial recognition services (enrollment databases) will be consistent with Colorado Revised Statute 24-19-302.
Aurora Police Department is authorized to access and perform facial recognition searches utilizing the following authorized enrollment databases.

- Lumen
- Clearview.ai platform
- Law enforcement shared gallery that meets the Aurora Police Department policy

In addition to above, the Aurora Police Department is authorized to submit requests for face recognition searches to be performed by external entities that own and maintain face image repositories (i.e., Colorado Department of Motor Vehicle / Revenue).

8.54.08 ACCESS, SECURITY, AUDITING AND RETENTION

Access to facial recognition search results will be provided only to individuals within the Aurora Police Department who are authorized to have access and have completed applicable training. Authorized access to the Aurora Police Department facial recognition software will be granted only to personnel whose positions and job duties (Investigations, Intelligence and Analysts) require such access.

The facial recognition administrator shall grant and audit all user access, following the required account approval.

All facial recognition users shall be required to have individual access for use of the facial recognition software/technology.

Approved facial recognition operators will analyze, review, and evaluate the quality and suitability of probe images, to include factors such as the angle of the face image, level of detail, illumination, size of the face image, and other factors affecting a probe image prior to performing a face recognition search.

Original probe images shall not be altered, changed, or modified to protect the integrity of the image. Any enhancements made to a probe image will be made a copy, saved as a separate image, and documented to indicate what enhancements were made, including the date and time of change.

Resulting images, if any, shall be manually compared with the probe image by the person conducting the comparison. In accordance with training, any candidate image that is incompatible with a probe shall be removed from the candidate image list.

Any upload of a probe image, query, or request shall include the name of the agency/requestor, name of the person completing the request, date and time the request was completed, case number and reason for the request. This information will be logged, tracked and available for auditing and review.

The Aurora Police Department and all authorized facial recognition users shall comply with all requirements stipulated in any Memorandum of Understanding (MOU) related to any authorized facial recognition enrollment databases. Any questions or clarification regarding an MOU should be directed to the Electronic Support Section Lieutenant or the Police Legal Advisor's Office

Images accessed by the Aurora Police Department for face recognition searches are not maintained or owned by the Aurora Police Department and are subject to the retention policies of the respective enrollment databases authorized to maintain those images.

Per Colorado Revised Statutes §24-18-303, members shall disclose the use of facial recognition technology to a criminal defendant in a timely manner prior to trial.

8.54.09 SECONDARY PEER REVIEW

Per Colorado Revised Statutes §24-18-303, "An agency using a facial recognition service to make decisions that produce legal effects concerning individuals or similarly significant effects concerning individuals must ensure that those decisions are subject to meaningful human review."

Prior to completing the facial recognition investigation, a peer review process must be implemented. The goal of this review process is to provide an additional level of consistency and control with respect to the application of standardized training practices.

A secondary (peer) review will consist of a separate facial recognition trained member reviewing the findings of the initiating investigator. This can be a review of the facial recognition report alone, or a complete secondary search of the probe imagery within the facial recognition service. During the secondary review, the reviewing peer investigator will report either a concurrence with the provided results or rejection of the provided results. The secondary reviewer will provide specific and articulable reasons for not agreeing with the provided results.

The outcome of the secondary review will be documented on the investigative lead report and subsequently reviewed by program managers. The cause for any lack of concurrence with results will be analyzed by program managers and the circumstances of the disagreement will be reviewed with the initial investigating member. The program manager will have ultimate decision-making authority on the progression of the lead after considering all the available identifying factors. The number and nature of facial recognition investigations with disagreements over the results will be monitored over time and will be included in the audit review.

8.54.10 AUTHORIZED USE OF FACIAL RECOGNITION INFORMATION

All use of facial recognition shall be for official law enforcement use only and considered law enforcement sensitive information. The following are authorized uses of facial recognition information:

- A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity.

- An active or ongoing criminal investigation.

- To mitigate an imminent threat to health or safety through short-term situational awareness surveillance or other means.

- To assist in the identification of a person who lacks capacity or is otherwise unable to identify themselves (such as incapacitated, deceased, or otherwise at risk).

- To investigate and/or corroborate tips and leads.

- To assist in the identification of potential witnesses and/or victims of violent crime.

- To support law enforcement in critical incident responses.

The results of a facial recognition service shall not be used as the sole basis to establish probable cause in a criminal investigation. The results of a facial recognition service may be used in conjunction with other information and evidence lawfully obtained by a member to establish probable cause in a criminal investigation.

Facial recognition information will be included in the case file and timely disclosed as part of the criminal discovery process.

8.54.11 UNAUTHORIZED USE OF FACIAL RECOGNITION SYSTEMS

The use of facial recognition for the sole purpose of intelligence gathering is prohibited. Additionally, the technology will not be used solely for identifying anyone exercising their constitutionally protected rights. The use of live facial recognition technology in conjunction with public safety cameras outside the above guidelines is prohibited.

The Aurora Police Department strictly prohibits access to and use of any facial recognition system, including dissemination of facial recognition search results, for the following purposes:

- Non-law enforcement (including but not limited to personal purposes).

- Any purpose that violates the U.S. Constitution or laws of the United States, including protections of the First, Fourth, and Fourteenth Amendments.

- Prohibiting or deterring lawful individual exercise of other rights, such as freedom of association, implied by or secured by the U.S. Constitution or any other constitutionally protected right or attribute.

- Harassing and /or intimidating and individual or group.

- Civil immigration enforcement

- Any other access, use, disclosure, or retention that would violate applicable law, regulation, or policy.

Per Colorado Revised Statutes (§ 24-18-307) members shall not use a facial recognition service to engage in ongoing surveillance, conduct real-time or near real-time identification, or start persistent tracking unless:

- A member obtains a warrant authorizing such use;

- Such use is necessary to develop leads in an investigation;

- The law enforcement agency has established probable cause for such use; or

- The member obtains a court order authorizing the use of the service for the sole purpose of locating or identifying a missing person or identifying a deceased person. A court may issue an ex parte order under this subsection (1)(d) if a law enforcement officer certifies and the court finds that the information likely to be obtained is relevant to locating or identifying a missing person or identifying a deceased person.

The Aurora Police Department shall not apply a facial recognition service to any individual based on the individual's religious, political, or social views or activities; participation in a particular noncriminal organization or lawful event; or actual or perceived race, ethnicity, citizenship, place of origin, immigration status, age, disability, gender, gender expression, gender identity, sexual orientation, or other characteristic protected by law.

8.54.12 TRAINING

Training will be provided to all authorized users of facial recognition software/technology. This training will be arranged and documented by the facial recognition program manager and account access will not be created or provided until training has been completed.

Training will cover both the use of facial recognition software/technology and a specific review and acknowledgment of all elements of this policy.

Per Colorado Revised Statutes (§ 24-18-305), the training will, at a minimum, include:

- The capabilities and limitations of the facial recognition service;

- Procedures to interpret and act on the output of the facial recognition service; and

- To the extent applicable to the deployment context, the meaningful human review requirement for decisions that produce legal effects concerning individuals or similarly significant effects concerning individuals.

The use of each authorized enrollment database will include specific training that includes the following process:

- An authorized user accesses their individual account.

- The authorized user shall enter the required information to support the authorized use of facial recognition satisfying an official law enforcement purpose.

- A lawfully obtained probe image of a subject meeting the required authorized use is uploaded to the system.

- The software automatically compares the probe image to candidate images within the repository.

- Results of the comparison are returned and provide a potential investigative lead.

Facial Comparison Training will also be provided to Aurora Police Department Detectives and Investigators assigned to lead investigations which may include facial recognition leads.

Updated training shall be identified with any policy revisions or updates in facial recognition software.

8.54.0X ACCOUNTABILITY

The Aurora Police Department will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with the face recognition system requirements and with the provisions of this policy and applicable law. This will include logging access to face recognition information and will entail periodic random auditing of these systems so as not to establish a discernable pattern that may influence users' actions. These audits will be mandated at least annually, and a record of the audits will be maintained by the ESS Lieutenant, or designee, pursuant to the Department's retention policy. Audits may be completed by an independent third party, a designated representative of the Aurora Police Department, or the Office of the City Auditor.

The Electronic Support Section Lieutenant, or designee, will review and update the provisions contained in this face recognition policy annually and will make appropriate changes in response to changes in applicable law, technology, and/or the purpose and use of the face recognition system; the audit review; and public expectations.

AURORA POLICE DEPARTMENT

Facial Recognition Accountability Report for
Rank One Computing Corporation's facial recognition service,
within LexisNexis' Lumen/AVCC software platform.

The Aurora Police Department submits this report pursuant to the requirements of Colorado Revised Statutes § 24-18-301 through 309. The Aurora Police Department ("APD") intends to activate the facial recognition functionality within the Lumen/AVCC software platform and to use it in support of law enforcement investigations.

The Aurora Police Department in Aurora, Colorado, intends to use the facial recognition functionality, facilitated by Colorado-based Rank One Computing, within LexisNexis' Lumen and Accurint Virtual Crime Center (AVCC) software platforms. Lumen/AVCC are software platforms that utilize the criminal justice information shared between the 140+ law enforcement member agencies of the Colorado Information Sharing Consortium (CISC). The facial recognition service within the Lumen/AVCC platforms are provided by Rank One Computing Corporation's (ROC) SDK version 2.2.1 algorithm. This software uses state-of-the-art facial recognition technology to find possible matches based on facial characteristics from a user-uploaded image to booking photos or other lawfully obtained images from CISC member agency records.

All use of facial recognition technology shall be for official law enforcement purposes only and considered law enforcement sensitive information. Per Colorado Revised Statute § 24-18-307, the Aurora Police Department will use this technology as an investigative lead only, with the full understanding that a potential match alone does not constitute probable cause.

I. Technical Description & Intended Use

The system compares a single user-uploaded "probe image" against a collection of lawfully available booking photographs and other images maintained by members of the CISC. Lumen/AVCC returns a ranked list of potential matches, each with a numerical confidence score. This score represents the likelihood of similarity, but it does not establish identity, positive identification, or probable cause.

Capabilities & Function
The Lumen/AVCC tool is designed to generate investigative leads by automating the process of comparing probe images against large volumes of criminal justice record images that would otherwise require manual review. Specifically:

- The algorithm creates mathematical templates from probe and candidate images to calculate similarity scores.

- The system uses machine-learning processes refined through operational testing, but results remain dependent on image quality and capture conditions (lighting, pose, occlusion, blur, glare, and resolution).
- Poor quality probe or candidate images may reduce accuracy.
- ROC SDK has been independently evaluated by the National Institute of Standards and Technology's (NIST) Facial Recognition Vendor Test (FRVT) and demonstrates low error rates (0.01%–0.00005%), though demographic variation exists.

The tool cannot and will not conduct real-time surveillance, live monitoring, or continuous tracking. It is strictly limited to after-the-fact investigative use.

Decision Making

Facial recognition results are investigative leads only and may not be relied upon as the sole basis for probable cause, arrest, or charging. APD personnel are required to:

- Review all results through meaningful human review by a trained investigator.
- Submit all identifications for peer review by another trained member prior to further use.
- Corroborate any potential match with independent evidence.

Intended Use and Benefits

The Lumen/AVCC facial recognition tool is intended to enhance the investigative abilities of the Aurora Police Department. This type of facial recognition technology automates the process necessary to locate potential matches between a probe image and thousands of criminal justice record images that would otherwise require a manual search by a human. The facial recognition algorithm will rank potential matches in a manner that allows for a simplified process of human review.

When provided a probe image to search against a collection of candidate images, Lumen/AVCC returns multiple results, sorted by the highest match score generated by the ROC SDK's facial recognition algorithms. Once Lumen/AVCC provides a list of results, a human investigator must review the results before making any determination of a possible match. A possible match determination may be used as an investigative lead that is treated in a similar manner as an anonymous tip. In particular, the investigative lead does not supply adequate probable cause to make an arrest without additional evidence. The intended benefit of using the Lumen/AVCC facial recognition service is to provide investigative leads that enhance follow-up inquiries and increase the likelihood of solving crimes that might otherwise remain unsolved.

In comparable use by the New York City Police Department (NYPD) since 2011, the NYPD has successfully used facial recognition to identify suspects whose images have been captured by cameras at robberies, burglaries, assaults, shootings, and other crimes. In 2019 alone, the Facial Identification Section received 9,850 requests for comparison and identified 2,510 possible matches, including possible matches in 68 murders, 66 rapes, 277 felony assaults, 386 robberies, and 525 grand larcenies, with no known instance in which a person was falsely arrested based on a facial recognition match.[1]

The use of facial recognition software will assist the Aurora Police Department with:

- Increasing public safety and improving state, local, and national security.
- Minimizing the threat and risk of injury to specific individuals.

[1] https://www.nyc.gov/site/nypd/about/about-nypd/equipment-tech/facial-recognition.page

- Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, and health.
- Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
- Reducing the opportunities for bias and prejudice to impact the criminal justice process.
- Protecting the integrity of criminal investigations, criminal intelligence, and justice system processes and information.
- Minimizing the threat and risk of damage to real or personal property.
- Fostering trust in the government by strengthening transparency, oversight, and accountability.
- Making the most effective use of public resources allocated to the police department.

Data Inputs and Generation

The Lumen/AVCC facial recognition tool uses the following types of data inputs:

- User submitted probe images collected during criminal investigations and associated information identifying the purpose of the search (such as case number, crime time, and justification for use).
- The candidate facial image data is primarily jail booking photos or other lawfully obtained images that are collected by the CISC from its member agencies who elect to share images.

The Lumen/AVCC facial recognition tool generates a template of each facial image, which is a mathematical model of the unique subject which may be compared to templates generated from other images to produce a match score. For each facial image, the tool also generates metadata including pitch, yaw, image quality estimations and facial analytics like age, gender, geographic origin, emotion, facial hair, glasses and mask estimations.

II. Data Management, Training and Use Policy

The Aurora Police Department will follow statutory requirements described in Colorado Revised Statutes § 24-18-301 through 309, in conjunction with an approved department policy. As such, the department will follow the below guidelines regarding data management, training and the authorized use of the facial recognition service.

Data Minimization

The features and functions of the Lumen/AVCC facial recognition tool effectively reduce the risk of inadvertent access to data by APD personnel. The Lumen/AVCC facial recognition tool searches only criminal justice records available to CJIS-certified law enforcement personnel of CISC member agencies. The criminal justice records available in the facial recognition tool are subject to the retention policies of the owner agencies.

Data Integrity and Retention

The designated Facial Recognition Administrator will be responsible for overseeing all Lumen/AVCC facial recognition tool permissions for the Aurora Police Department. Access to this tool will be restricted to a limited number of trained investigative and analytical personnel with individual accounts. The Facial Recognition Administrator will have the capability to audit and review any, and all usage of this facial recognition tool by any member of the department. The audit will include all user activity, such as user log ins and log outs, what commands were issued to the system, and what records or files were accessed.

All information obtained from the Lumen/AVCC facial recognition tool by any member of the police department will be collected in a formal report and retained in accordance with guidelines set forth in the record management system.

Without the express permission of APD, or as required by law, such as a judicial order, LexisNexis employees will not review APD search history within the Lumen/AVCC facial recognition tool, ensuring that sensitive investigative data will remain confidential.

All information available within the Lumen/AVCC investigative platform, including the facial recognition tool, is purged according to the retention schedule and policies set by the owner agency. For example, any information made available to other CISC member agencies by APD is purged from the Lumen/AVCC investigative platform when its retention expires inside APD's record management system.

Usage Rules and Requirements

Access to the Lumen/AVCC facial recognition tool within the Aurora Police Department will be strictly limited to set number of personnel who are trained in its use. Each authorized user will have individual credentials, and the Facial Recognition Administrator will oversee access approvals, maintain user records, and conduct audits to ensure policy compliance. Operators are responsible for reviewing the quality and suitability of probe images prior to initiating a search, with careful consideration of factors such as pose, clarity, illumination, and image resolution. Original probe images must remain unaltered; any enhancements must be applied only to copies, with documentation identifying the type of change, date, time, and operator. All comparisons are subject to human review, and results must undergo peer verification by another trained member prior to investigative use.

Every search conducted in the facial recognition system will be fully documented, including the operator's name, date and time of the request, case number, and the stated purpose of the search. This information will be logged automatically and maintained for review and auditing. Regular audits will be conducted to monitor usage, identify error rates, and ensure that no misuse or irregularities occur.

The Aurora Police Department will comply with all Colorado statutes, department directives, and any Memoranda of Understanding governing participation in shared databases. The Department does not own or permanently retain images accessed for searches; instead, candidate images remain subject to the retention policies of the source databases. Case-related results will be retained in accordance with Department policy. Pursuant to Colorado Revised Statute § 24-18-303, the Department will disclose the use of facial recognition technology to a criminal defendant in a timely manner prior to trial.

To ensure accountability and safeguard individual rights, the Department prohibits the use of facial recognition for real-time surveillance, continuous monitoring, or the creation of independent facial recognition databases. The Facial Recognition Administrator will ensure compliance with state-mandated reporting requirements, including annual monitoring of accuracy, error rates, and potential demographic bias. If error rates exceed one percent, or if evidence of disparate impact arises, the Department will suspend use until corrective measures are implemented. These rules are designed to balance the investigative value of facial recognition technology with the protection of privacy, civil rights, and public trust.

Data Security

Facial recognition data is stored securely on CJIS-compliant Lumen/AVCC servers, and access is limited to individual authorized users within Lumen/AVCC.

Lumen/AVCC is web-based software and not an application which needs to be downloaded to any City of Aurora computers. Any records exported by Aurora Police Department members shall be immediately uploaded to the department's record management system (Versadex). Versadex is CJIS compliant and maintained by the City of Aurora's Information Technology department.

Training Procedure

Training will be provided by the Aurora Police Department to all authorized users of facial recognition services. This training will be arranged and documented by the Facial Recognition Administrator and account access will not be created or provided until training has been completed.

Training will cover both the use of facial recognition software/technology as well as a specific review and acknowledgment of all elements of related department policy.

Per Colorado Revised Statute § 24-18-305, the training will at a minimum include:

- The capabilities and limitations of the facial recognition service.
- Procedures to interpret and act on the output of the facial recognition service; and
- The meaningful human review requirement for decisions that produce legal effects concerning individuals or similarly significant effects concerning individuals.

The use of the Lumen/AVCC facial recognition tool will include specific training that includes the following:

- the authorized user shall enter the required information to support the authorized use of facial recognition satisfying an official law enforcement purpose,
- a lawfully obtained probe image of a subject meeting the required authorized use is uploaded to the system,
- the software automatically compares the probe image to candidate images within the repository,
- results of the comparison are returned and provide a potential investigative lead.

Updated training shall be identified with any policy revisions or updates in facial recognition software.

III. Accuracy and Impact

Testing Procedure

In accordance with Colorado Revised Statute § 24-18-304(4), Rank One Computing submitted the ROC SDK for testing in the following series of the National Institute of Standards and Technology (NIST) Face Recognition Vendor Test (FRVT) Ongoing:

1:1 Verification:	*https://pages.nist.gov/frvt/html/frvt11.html*
1: N Identification:	*https://pages.nist.gov/frvt/html/frvt1N.html*
Quality Assessment:	*https://pages.nist.gov/frvt/html/frvt_quality.html*
Demographic Effects:	*https://pages.nist.gov/frvt/html/frvt_demographics.html*
Paperless:	*https://pages.nist.gov/frvt/html/frvt_paperless_travel.html*

Test Results

Rank One Computing's SDK facial recognition algorithm was submitted to the National Institute of Standardization and Technology (NIST) Face Recognition Technology Evaluation (FRTE) for 1:1 Verification. In that test, ROC's SDK facial recognition algorithm ranked No. 6 in the world out of 404 total entries.[2]

	FALSE NON-MATCH RATE (FNMR)							
	Constrained, Cooperative							Unconstrained, Non-Coop
Algorithm	Gallery	VISA	MUGSHOT	MUGSHOT	VISA	VISA Yaw≥45	BORDER	BORDER
	Probe	VISA	MUGSHOT	MUGSHOT ΔT≥12 YRS	BORDER	BORDER°	BORDER	KIOSK
	Date	FMR = 0.000001	= 0.00001	= 0.00001	= 0.000001	= 0.000001	= 0.000001	= 0.00001
qazsmartvisionai-004	2025-07-18	-	0.002(1)	0.002(3)	0.0014(1)	0.003(2)	0.0028(1)	0.0337(1)
viante-002	2025-06-17	-	0.0025(52)	0.0024(29)	0.0015(2)	0.0028(1)	0.0029(2)	0.0349(2)
recognito-001	2023-09-27	0.0007(2)	0.0021(4)	0.0022(14)	0.0016(3)	0.007(15)	0.0662(202)	0.1047(123)
cloudwalk-mt-007	2023-02-21	0.0007(1)	0.0023(23)	0.0019(1)	0.0016(4)	0.0036(3)	0.0032(4)	0.0394(9)
paravision-018	2025-06-12	-	0.002(2)	0.002(4)	0.0016(5)	0.0038(4)	0.0034(7)	0.0375(5)
roc-019	2025-07-21	-	0.0021(10)	0.0021(8)	0.0016(6)	0.006(11)	0.0031(3)	0.038(6)

Bias and Inaccuracy

In the NIST Demographic Effects series the ROC SDK algorithm ranked 11th worldwide (out of 597 entries) across all 70 sub-populations of the NIST test data, with the lowest scoring demographic being West African females aged 65-99 years old (0.01061% false match rate).[3] The potential for technological bias and inaccuracy is further mitigated through required meaningful human review of each potential match and secondary peer review by another trained member. Final supervisory approval is also required before any investigative lead is forwarded for follow-up

Civil Rights Impact

The Aurora Police Department recognizes the importance of safeguarding civil rights, civil liberties, and privacy in the use of facial recognition technology. To address these concerns, multiple layers of oversight and human judgment are built into every stage of the process. The Lumen/AVCC system does not make identifications or determinations of guilt; rather, it generates a ranked list of possible matches based on a submitted probe image. These results are reviewed by trained investigators, who are required to apply their professional expertise to determine whether any candidate represents a possible match. No investigative action may proceed without additional independent evidence, and a possible match may only serve as an investigative lead, comparable to an anonymous tip.

Probe images are drawn exclusively from lawfully obtained criminal justice records, such as arrest booking photographs, and are never collected from unauthorized sources. To further protect against potential bias or disparate impact, every authorized user must input a valid case number and specify the type of crime under investigation prior to initiating a search. This requirement affirms that the technology is being used exclusively to investigate crimes that have already occurred and not to monitor lawful activities, conduct "fishing expeditions," or track individuals engaged in constitutionally protected activities. Compliance with this rule will be verified through routine audits of user inputs and system usage.

[2] https://pages.nist.gov/frvt/html/frvt11.html

[3] https://pages.nist.gov/frvt/html/frvt_demographics.html

The Aurora Police Department also maintains strict adherence to APD Directive 08.32: Bias-Based Policing, which prohibits investigative activity based in whole or in part on an individual's actual or perceived race, ethnicity, gender, national origin, language preference, religion, sexual orientation, gender identity, age, or disability. Investigations may only rely on demographic descriptors when they are part of a reliable, suspect-specific description that also includes non-demographic identifying characteristics.

In addition, APD's Facial Recognition Policy requires investigators to document every search, including the requestor's name, date, time, case number, and purpose. This ensures transparency, accountability, and a record of lawful use. Audit logs will be reviewed to detect any misuse, and violations of policy will be subject to disciplinary action.

Independent testing conducted by NIST has demonstrated that the ROC SDK algorithm used within Lumen/AVCC performs with high levels of accuracy across demographic groups, with measured performance exceeding 99% accuracy in the FRVT Demographic Effects program. While no technology is free from error, these results indicate that the risk of disparate impact on marginalized communities is extremely low. Importantly, any potential error is further mitigated by the requirement for human review, corroborating evidence, and supervisory oversight before any investigative or enforcement action is taken.

Through these safeguards, the Aurora Police Department is committed to ensuring that the use of facial recognition technology supports public safety while protecting civil rights, civil liberties, and the trust of the community.

Public Feedback

The Aurora Police Department will seek approval from the Aurora City Council prior to the implementation and utilization of the Lumen/AVCC facial recognition tool. As is required by Colorado Revised Statute § 24-18-302, consideration and the opportunity for public comment will be heard at a Public Safety Committee Meeting, Council Study Session, and Council Regular meeting should the item be moved forward at each meeting respectively.

Public comments and feedback on the use of facial recognition technology can be submitted through an online form available in the Facial Recognition section of the Aurora Police website. All feedback will be reviewed and addressed in accordance with agency procedures.

AURORA POLICE DEPARTMENT

Facial Recognition Accountability Report for Clearview AI, Inc Technologies

The Aurora Police Department submits this report pursuant to the requirements of Colorado Revised Statutes § 24-18-301 through 309. The Aurora Police Department ("APD") intends to procure licenses for access to and use of Clearview AI Inc. ("Clearview") facial recognition search engine (the "Clearview App") in order to use it in support of law enforcement investigations.

The Aurora Police Department in Aurora, Colorado, proposes to procure licenses for Version 2.0 of the Clearview App, provided by Clearview AI, Inc. Clearview is an investigative application that uses state-of-the-art facial-recognition technology to match the face in a user-uploaded image to faces in publicly available images. It is designed to be used in ways that ultimately reduce violent crime, fraud, and risk in order to make communities safer. All use of facial recognition shall be for official law enforcement use only and considered law enforcement sensitive information. Per Colorado Revised Statute § 24-18-307, the Aurora Police Department will use this technology as an investigative lead only and will use any results in conjunction with other leads and evidence.

I. Technical Description & Intended Use

The Clearview App is a facial recognition search engine. It functions in a manner similar to the "reverse image search" functionality on many commonly used search engines, with enhanced utility and accuracy thanks to its machine-learning, neural-network facial recognition technology. The Clearview App is made available to government agencies and contractors.

Capabilities & Function

The Clearview App helps solve crimes after-the-fact by matching photos obtained by a government customer of suspects, persons of interest in a law enforcement investigation, and victims or possible victims of crimes against Clearview's database of more than 20 billion publicly available facial images. Specifically, the Clearview App uses a machine-learning facial recognition algorithm to compare a face in a user-uploaded image (the "Probe Image"), to initiate a search against Clearview's database of 30 billion+ publicly available images from the Internet. These results can be returned from diverse sources, such as news media sites, public arrest record websites, public social media pages, public business webpages, or public blogs. Clearview generates "vectors" from the faces in the images in order to match the faces. Faces which are extremely similar to the face in the Probe Image are returned as search results, along

with links to the online location where those images were originally posted. Law enforcement users can proceed to the third-party sites and view the images in their original context. At that point, law enforcement makes independent assessments as to if there is a match between the Probe Image and images retrieved by Clearview. These results are reviewed by trained investigators, who are required to apply their professional expertise to determine whether any candidate represents a possible match. This search process provides Aurora Police Department personnel with investigative leads after-the-fact to help them identify unknown suspects, victims or other persons of interest. This function is only available to law enforcement and other government users or their contractors.

Decision Making

Clearview App is not a final decision-making tool. It is intended to support investigations. Each decision about an identification is made by trained investigators using their professional expertise to determine whether any candidate represents a possible match. Law enforcement personnel must review the results for every search to enable human review and independent verification. Probable Cause determinations may not be based solely on these identifications. In addition, all results will be peer reviewed by other sworn members prior to utilizing any information obtained.

Intended Use and Benefits

Use of the Clearview App is intended to support and hasten investigations. The Clearview App is an effective investigative tool. According to the Government Accountability Office's August 2021 report "FACIAL RECOGNITION TECHNOLOGY: Current and Planned Uses by Federal Agencies," Clearview's technology was used successfully by multiple federal law enforcement agencies:

- The Department of Homeland Security used the Clearview App to help identify victims and perpetrators in domestic and international child exploitation cases.[1]
- The Secret Service used the Clearview App to help identify the subjects of federal criminal investigations.[2]
- The Air Force Office of Special Investigations used the Clearview App to support counterterrorism, counterintelligence, and criminal investigations.[3]
- Media coverage by *The New York Times* indicated that the Clearview App was used by various law enforcement agencies to successfully support investigations related to the January 6th, 2021, riot at the US Capitol.[4]
- Homeland Security Investigations Child Exploitation Investigations Unit used Clearview to provide a lead which resulted in the successful conviction of an individual who was sexually abusing a minor and sharing the images online.[5]

---

[1] GAO-21-526, *Facial Recognition Technology: Current and Planned Uses by Federal Agencies* https://www.gao.gov/assets/gao-21-526.pdf. Pg 20

[2] *Id.*

[3] *Id.* pg. 33.

[4] "The facial-recognition app Clearview sees a spike in use after Capitol attack." Kashmir Hill. *The New York Times.* January 09, 2021.

[5] Fed. Agency Identifies Suspect of Las Vegas Child Exploitation in Background of Social Media Profile. www.clearview.ai/post/fed-agency-identifies-suspect-of-las-vegas-child-exploitation-in-background-of-social-media-profile

- According to testimony by Clearview's CEO, the Company is aware that one unit within Federal Bureau of Investigation experienced a threefold increase in the number of child sexual exploitation victims identified while using the Clearview App in 2019.[6]

By using facial recognition software will assist the Aurora Police Department with:

- Increasing public safety and improving state, local, tribal, territorial, and national security.
- Minimizing the threat and risk of injury to specific individuals.
- Minimizing the threat and risk of physical injury or financial liability to law enforcement and others responsible for public protection, safety, or health.
- Minimizing the potential risks to individual privacy, civil rights, civil liberties, and other legally protected interests.
- Reducing the opportunities for bias and prejudice to impact the criminal justice process.
- Protecting the integrity of criminal investigations, criminal intelligence, and justice system processes and information.
- Minimizing the threat and risk of damage to real or personal property.
- Fostering trust in the government by strengthening transparency, oversight, and accountability.
- Making the most effective use of public resources allocated to public safety entities.

Data Inputs and Generation

The Clearview App uses the following types of data inputs:

- User submitted Probe Images and associated information identifying the purpose of the search (such as case number and crime time),
- Publicly available images from the Internet and the URLs where they appear which are collected by Clearview and returned as search results if they are sufficiently similar to the Probe Image.

The Clearview App generates "vector maps" from faces in images. Vector maps are machine readable coordinates in a 512-axis coordinate plane upon which more similar images of faces will be placed closer together. Upon user request, it also generates PDF reports showing the publicly available online images and links returned in response. When a user initiates a search on the Clearview App, the displayed search results contain publicly available images from the Internet, along with links to their original locations, the titles of those webpages and in some cases a small text snippet from those webpages.

II. Data Management, Training and Use Policy

The Aurora Police Department will follow statutory requirements described in Colorado Revised Statutes § 24-18-301 through 309, in conjunction with an approved department directive. As such, the department will follow the below guidelines regarding data management, training and the authorized use of the facial recognition service.

[6] *Statement of CEO Hoan Ton-That Before the Massachusetts Special Commission on Facial Recognition.* July 30, 2021.

Data Minimization

The features and function of the Clearview App effectively reduce the risk of inadvertent access to data by Aurora Police Department personnel. As noted above, the Clearview App searches only publicly available online image data and does not search information that has been restricted by a website to prevent its access by the general public. Therefore, access by Aurora Police Department personnel to private images is prevented. Additionally, the Clearview App only displays images to users when they are responsive to a search; Aurora Police Department personnel do not have access to images collected by Clearview unless they are directly responsive to a search initiated by a Probe Image. Search results returned by the Clearview App are limited to images which can be retrieved using the same algorithm and match threshold settings which achieved 99% or better accuracy for every demographic group on the NIST Facial Recognition Vendor 1:1 Verification Test - Demographic Effects Test. Therefore, the inclusion of images which are not relevant to the investigative purpose of a particular search is substantially reduced and largely eliminated. Aurora Police Department personnel do not have access to face vectors maintained by Clearview.

Data Integrity and Retention

The designated Facial Recognition Administrator will be responsible for overseeing all Clearview AI accounts for the Aurora Police Department. This person will have the capability to audit and review any, and all usage of this facial recognition software by any member of the department. The audit will include all user's activity, such as user log ins and log outs, each user's activity in detail, what commands were issued to the system, and what records or files were accessed.

All information obtained from Clearview AI by any member of the police department will be utilized in a formal report and retained in accordance with guidelines set forth in the record management system.

The collection of personal information by Clearview is limited to that which is necessary to meet Clearview's business objectives. Clearview does not share face vectors with Clearview's users.

Except with the express permission of the Aurora Police Department or as required by law, such as a judicial order, Clearview employees will not review Aurora Police Department search history within the Clearview App, ensuring that sensitive investigative data will remain confidential.

Probe images uploaded in the Clearview App will not be retained as a reference image within the platform.

Usage Rules and Requirements

The Clearview App can only be accessed by authorized users within the Aurora Police Department who are trained on its use. All agencies using the Clearview App are required to appoint at least one employee who is serving in a supervisory role as administrative user who will be able to review the search histories of agency personnel who access the Clearview App in order to ensure that their use of the Clearview App is appropriate. Within the Aurora Police Department, authorized users are approved by the Facial Recognition Administrative, who will also maintain user records and conduct audits to ensure policy compliance. All authorized and administrative users must complete training on how to use Clearview

technology before access is granted. All users must abide by the Terms of Service and Code of Conduct– Clearview reserves the right to terminate any account which violates these rules. The Clearview App may only be used for legitimate governmental purposes and requires law enforcement users to input identifying information for each search–generally including a case number and Criminal Justice Information System code for the relevant crime type pertaining to that investigation.

An agency may not share access to Clearview or the data from Clearview with any third party that is not a law enforcement agency, except as required by law.

All use of facial recognition shall be for official law enforcement use only and considered law enforcement sensitive information. The following are authorized uses of facial recognition information.

- A reasonable suspicion that an identifiable individual has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal conduct or activity.
- An active or ongoing criminal investigation.
- To mitigate an imminent threat to health or safety through short-term situational awareness surveillance or other means.
- To assist in the identification of a person who lacks capacity or is otherwise unable to identify themselves (such as incapacitated, deceased, or otherwise at risk).
- To investigate and/or corroborate tips and leads.
- To assist in the identification of potential witnesses and/or victims of violent crime.
- To support law enforcement in critical incident responses

Data Security

Clearview uses a variety of technical, physical, and administrative measures to protect all of the information that is processed, whether from users or from the Internet, against unauthorized access, use or disclosure.

Clearview's online platform and the information it processes is secured through a variety of technical measures. These include but are not limited to virtual private cloud technology, intrusion detection tools, firewalls, two-factor authentication for users and employees, vulnerability scanning, scan detection, encryption of data in transit and at rest, remote device management and endpoint protection tools. Clearview has obtained a SOC II security certification, which is the result of an independent, external audit to ensure that the company's cybersecurity and internal controls against unauthorized access to information are consistent with industry standards. Consistent with its SOC II status, Clearview also ensures security through organizational measures. These include, but are not limited to, a variety of internal security policies, such as a "principle of least privilege" policy with regard to access to data as well as security training and background checks for all employees, a bug-bounty program, regular reviews of internal user access privileges, regular penetration testing, and internal code reviews.

Clearview is web-based software and not an application which needs to be downloaded to any City of Aurora computers. As such, the security of the information collected by Clearview is overseen by their security measures noted above. Any records exported by Aurora Police Department members shall be immediately uploaded to the department's record management system (Versadex). Versadex is in compliance and maintained by the City of Aurora's Information Technology section.

Training Procedure

As part of the user onboarding process, Clearview requires users to participate in training programs before they are authorized and granted access to use the technology. Clearview trains administrative users who are appointed by command staff. Once those administrative users are fully trained, they may train additional users within their organization on how to use Clearview. Clearview provides additional training sessions to user agencies upon request.

Clearview training includes coverage of the limitations of Clearview, interpreting results, and the necessity of meaningful human review in interpreting results.

Training will be provided by the Aurora Police Department to all authorized users of facial recognition software/technology. This training will be arranged and documented by the Facial Recognition program administrator and account access will not be created or provided until training has been completed.

Training will cover both the use of facial recognition software/technology and a specific review and acknowledgment of all elements of this policy.

Per Colorado Revised Statute § 24-18-305, the training will at a minimum include:

A. The capabilities and limitations of the facial recognition service;
B. Procedures to interpret and act on the output of the facial recognition service; and
C. To the extent applicable to the deployment context, the meaningful human review requirement for decisions that produce legal effects concerning individuals or similarly significant effects concerning individuals.

The use of each authorized enrollment database will include specific training that includes the following: an authorized user accesses their individual account,

- the authorized user shall enter the required information to support the authorized use of facial recognition satisfying an official law enforcement purpose,
- a lawfully obtained probe image of a subject meeting the required authorized use is uploaded to the system,
- the software automatically compares the probe image to candidate images within the repository,
- results of the comparison are returned and provide a potential investigative lead.

Updated training shall be identified with any policy revisions or updates in facial recognition software.

III. Accuracy and Impact

Testing Procedure

In accordance with Colorado Revised Statute § 24-18-304(4), Clearview AI submitted for testing in the following series of the National Institute of Standards and Technology (NIST) Face Recognition Vendor Test (FRVT) Ongoing:

1:1 Verification:	*https://pages.nist.gov/frvt/html/frvt11.html*
1: N Identification:	*https://pages.nist.gov/frvt/html/frvt1N.html*
Demographic Effects:	*https://pages.nist.gov/frvt/html/frvt_demographics.html*
Paperless:	*https://pages.nist.gov/frvt/html/frvt_paperless_travel.html*

Test Results

Clearview's facial recognition algorithm was submitted to the National Institute of Standardization and Technology (NIST) Face Recognition Vendor Test (FRVT) for 1:1 Verification. In that test, Clearview's facial recognition algorithm ranked No. 1 in the U.S. for its performance in matching VISA Photos (99.81 percent), MUGSHOT Photos (99.76 percent), VISABORDER photos (99.7 percent) and BORDER Photos (99.42 percent), and ranked in top five worldwide in all of these categories out of 650 algorithms.

Detailed statistics on the test results can be found here.

Clearview's technology also performed highly in NIST's one-to-many search test, which is directly pertinent to the manner in which the Clearview App will be used. Clearview's first submission to NIST's FRVT for 1:N Identification ranked #2 worldwide in averaged performance across all categories, making it the highest performing facial recognition vendor in the United States at that time. Detailed statistics on the test results can be found here.

Bias and Inaccuracy

In the NIST Demographic Effects Test, Clearview's facial recognition algorithm achieved greater than 99 percent accuracy across all demographics, with false positive and false negative rates of less than 1% for all groups (see here).

Civil Rights Impact

The Clearview App only searches publicly available online images. It does not search for information that has been restricted by a website from access to the general public. As a result, use of the Clearview App, and its production of images obtained from publicly available information, does not implicate the Fourth Amendment.

Aurora Police Department personnel with access to the Clearview App are required to input a case number and crime type prior to initiating a search, affirmatively representing that the search is conducted for the purpose of investigating a crime that has been committed. As a result, the use of the Clearview App for "fishing expeditions" or monitoring persons engaged in lawful activities is curtailed. Compliance with this requirement will be verified through routine audits of user inputs and system usage.

Usage of the Clearview App by the Aurora Police Department is unlikely to have a negative impact on the civil rights, liberties, privacy, or on marginalized communities of the people of the State of Colorado. Clearview does not authorize agencies to use the appearance of a photo in its search results as admissible evidence. Results are reviewed by trained investigators, who are required to apply their professional expertise to determine whether any candidate represents a possible match. No investigative action may proceed without additional independent evidence, and a possible match may only serve as an investigative lead, comparable to an anonymous tip.

Colorado residents who wish to opt-out of Clearview search results will be able to submit a request via a dedicated webform Clearview maintains for that purpose starting in 2023, further mitigating any potential privacy impact. As noted above, Clearview's algorithm achieved greater than 99% accuracy across all demographic groups on NIST's FRVT Demographic Effects in Face Recognition test program; thus, disparate impact on marginalized communities is likely to be negligible. Lastly, suspects may be exonerated through the use of Clearview's technology, further mitigating any negative civil rights impact, and in such cases, providing a positive impact in protecting and promoting civil rights.[7]

The Aurora Police Department has clear guidelines set forth in Directive 08.32 Biased Based Policing regarding actions against traits involving a particular group.

Public Feedback

The Aurora Police Department will seek approval from the Aurora City Council prior to the implementation and utilization of the Clearview App facial recognition tool. As is required by Colorado Revised Statute § 24-18-302, consideration and the opportunity for public comment will be heard at a Public Safety Committee Meeting, Council Study Session, and Council Regular meeting should the item be moved forward at each meeting respectively.

Public comments and feedback on the use of facial recognition technology can be submitted through an online form available in the Facial Recognition section of the Aurora Police website. All feedback will be reviewed and addressed in accordance with agency procedures.

[7]Clearview facial recognition used to exonerate suspect on trial over traffic fatality. Joel McConvey. *Biometric Update.* Sept. 19, 2022. https://www.biometricupdate.com/202209/clearview-facial-recognition-used-to-exonerate-suspect-on-trial-over-traffic-fatality

GUIDING PRINCIPLES FOR LAW ENFORCEMENT'S USE OF FACIAL RECOGNITION TECHNOLOGY

What is Facial Recognition:

Facial recognition technology automates the process of comparing one photograph to other photographs to find potential matches. Facial recognition is a software application capable of potentially identifying or verifying the identity of a person by analyzing patterns based on a person's facial feature locations and contours and comparing them to those features in other photographs. The primary government applications for facial recognition in the United States are identity verification, security, and law enforcement investigations.

What Facial Recognition is NOT:

The result of facial recognition analysis is NOT a positive identification of an individual. In the law enforcement investigations context, facial recognition is a tool that potentially develops an investigative lead. Once the potential lead has been generated, human intervention is required to determine if the person in a photograph is actually the person whose identity is in question.

Principle One:

It is the responsibility of the user agency to develop appropriate facial recognition technology usage policies in accordance with the applicable laws and policies of the governmental jurisdiction to which the user agency is subject. In response to the expanding use of new and emerging technologies, the International Association of Chief's of Police (IACP) released a Technology Policy Framework to guide the development and support policies that ensure responsible and effective deployment and use of technologies.

Principle Two:

All appropriate use policies must protect the constitutional rights of all persons and should expressly prohibit any use of the technology that would violate an individual's rights under the First and Fourth Amendments.

Principle Three:

The results returned in a facial recognition candidate list are ranked based on computational analysis of the similarity of features. The candidate list may include photos of individuals who may be of a different race, gender, and/or age than the individual in the submitted probe photo.

Principle Four:

The images and information contained in the candidate list are for investigative lead generation purposes only, and are not to be considered as positive identification, or used alone as the basis for any law enforcement action.

Principle Five:

Before access to any facial recognition system is authorized, a law enforcement agency should require individual users to participate in training on how the facial recognition system functions, its limitations, the importance of using high resolution equipment and images, and the interpretation of results, as well as the implementation of and adherence to the agency's facial recognition policy.

To access the IACP Technology Policy Framework, please click on the IACP web link::
https://www.theiacp.org/iacp-technology-center

To access the IACP/IJIS Facial Recognition Use Case Catalog, please click on the IJIS Institute web link:
https://www.ijis.org/news/news.asp?id=439103&terms=%22facial+and+recognition%22

Law Enforcement Imaging Technology Task Force (LEITTF)

A joint effort of the IJIS Institute and the International Association of Chiefs of Police

July 2019

MAJOR CITIES CHIEFS ASSOCIATION

presents

Facial Recognition Technology in Modern Policing

Recommendations and Considerations

2021 Facial Recognition Working Group

Table of Contents

Introduction

The 21st century offers law enforcement an unprecedented opportunity to embrace advanced technologies to keep our communities safe. One of the most valuable of these technologies is facial recognition technology (FRT). FRT has an unprecedented ability to combat criminal activity, identify persons of interest, develop actionable leads, and close cases faster than ever before. Perhaps most importantly, the law enforcement agencies which have embraced this technology have proven its capability of assisting with the ultimate goal of keeping our communities safe.

It is this vision of protecting our communities and preventing future crime that fuels the desire of law enforcement to develop a responsible, appropriate, and effective FRT program. Technology has an ever-increasing impact on our lives. As such, it is critical that law enforcement also have access to and develop programs that leverage these advanced technologies to combat the criminal element. Even more importantly, it is important to recognize the use of such technologies comes with great responsibility.

This product's intent is to assist law enforcement agencies in developing an FRT program that is both effective in its use and responsible in its design. The core principles of such a program are transparency, accountability, and responsibility. Transparency is achieved when the public knows FRT is in use by its police agencies and how it is (and isn't) utilized. Accountability is achieved when the public is aware of its results and impact. The framework outlined in this document will help law enforcement meet the highest standards and achieve its mission of protecting the community while remaining respectful of the individual rights and privacy of the citizens within their respective communities.

There exists great promise for facial recognition technology. This is the primary reason law enforcement is rapidly developing programs that embrace it. Because of the movement towards incorporating the technology into public safety, law enforcement has recognized the need for accountability to the general public, standardized application, and the responsible continued development of policy and practice.

It is important to use this product as a guideline for current best practices in the field. Not every element is necessary for developing a robust program but should be considered to make a program as complete and fitting to the needs of a community as possible. What may work in one community, may not be necessary for another, but this working group recommends considering all options before finalizing an agency's FRT protocols and policies.

To achieve this goal, the Major Cities Chiefs Association (MCCA) assembled representatives of facial recognition programs and agencies nationwide to produce this document. With support from FRT vendors and law enforcement alike, this product is a true partnership. This product represents the working group's recommendations for the procurement, development, operation, and reporting of a well-balanced FRT program.

Much like other powerful technologies, FRT will continue to evolve. This product is intended to provide law enforcement agencies a framework to adapt policies and practices with the evolving technology and will be revisited and updated as needed to appropriately reflect changes in the policing environment.

Executive Summary

In Spring of 2021, the Major Cities Chiefs Association (MCCA) launched an effort to develop a facial recognition technology (FRT) program development guide. This product is intended to be shared with the MCCA's membership to leverage the advanced technology in their crime-fighting efforts. This technology has proven itself to be a powerful tool to combat criminal activity, identify persons of interest, develop actionable leads, and close cases faster.

As more agencies launch FRT programs or acquire software which has FRT capabilities, standard best practices must be discussed regularly in order to ensure this technology is being used with the best intentions which includes the protection of the privacy and civil liberties of citizens. This product discusses many areas of FRT including FRT basics, methodology, program design, program management, qualitative review, and technical evaluation. This document was formulated to discuss all aspects of FRT, yet leaves room for an agency to develop a program which meets its specific needs. Should an agency choose not to utilize all suggestions discussed, it was the intent to also discuss the potential ramifications of omitting certain aspects of FRT best practices.

Stakeholders concerned about FRT generally focus on the following: algorithmic accuracy and bias concerns, threats to privacy (surveillance), chilling effects on first amendment rights, and defendants' rights, or in other words the general lack of disclosure of the use of the technology in their case. It would be irresponsible on the part of law enforcement to ignore these concerns. However, it is our position that all of these can be sufficiently mitigated or eliminated through thoughtful policy, intentional protocols, and responsible program management. While there are documented misuses of FRT results, these would have been avoided had best practices been employed. These cases should serve as a cautionary reference for those wishing to run a successful program. It is important to recognize the overwrought rhetoric and misinformation which is often promoted.

To this end, this report focuses on the building of an FRT program keen on transparency, responsibility, and accountability. Following the recommendations outlined in this product will enhance an agency's ability to straightforwardly address the concerns listed above. Not only does this product serve as a template to design and operate a working FRT program but also serves as a guide to an operational FRT program that is defensible by nature while responsible in its use.

Finally, it should be noted that just like technology itself, the standards surrounding the use of FRT are ever-changing. For this reason, this should be considered more of a living document rather than a finalized product. As the conversation surrounding FRT progresses, so will the guidelines detailed in this product.

Key Recommendations

The widely varying size and scope of MCCA member agencies necessarily requires the key recommendations in this document to be broad in their scope and applicability. Much effort was given to making both the content as a whole and the recommendations below as relevant as possible to all agencies. In general terms, it is the view of the FRT working group that each of the following key recommendations be implemented with the launch of a new FRT program. However, these recommendations are not provided as bright-line requirements for the implementation of FRT at the reader's agency, rather they are meant to serve as important guide posts in any agency's development of a responsible FRT program.

Transparency

- Law enforcement agencies seeking to procure FRT platforms should engage both public and government stakeholders for the purposes of feedback and transparency.
- The documented results of an FRT investigation should be made subject to discovery in the criminal process.
- The eventual outcome of any criminal investigation that utilizes FRT should be captured as part of the agency's data collection process.

Accountability

- Access to an agency's FRT platform should be limited to those members having specialized training in facial identification methods and the application of the technology should be performed by individuals who are not directly involved with a particular investigation.
- Restricting access to an agency's FRT platform to only those members with specialized training in facial identification methods will reduce contextual bias in particular investigations.
- If possible, the application of FRT should be performed by trained individuals who are not directly involved with a particular investigation.
- The identification of a potential lead during an FRT investigation should be documented on a standardized form which requires sufficient detail about the morphological basis of the facial identification process.
- For those agencies wishing to implement the use of FRT, but who are unsure on how to move forward, collaboration with other entities who have already developed robust, responsible programs is recommended.

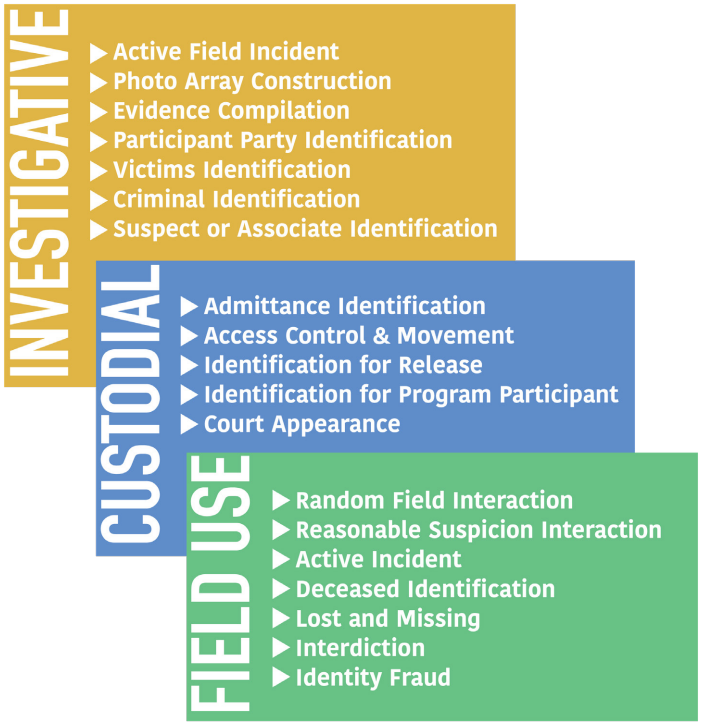
Responsibility

- Careful consideration should be given to the specific and most privacy-conscious approach to what gallery image library is used.
- Agencies should identify an FRT program manager who will be tasked with both the initial deployment and continued oversight and development of the FRT program.
- The results of FRT investigations should be handled as tips/leads only due to the limitations of FRT and the potential consequences of its misuse as outlined in this document.
- FRT examiner training should specifically include familiarization with standardized methods for performing facial identification.
- The initial findings of an FRT investigation should be confirmed by a secondary examiner.

What is Facial Recognition?

What type of program does this product address?

Before we address the recommendations and considerations outlined in this product, we must define the specific type of facial recognition system that is being referenced throughout the majority of this report. There exist three primary applications of FRT platforms: facial verification, field identification, and facial identification. All three applications of FRT serve a purpose and may play a role in law enforcement operations. However, it is the facial identification type of FRT that presently garners widespread public and government concerns. In an effort to lay the foundation of the rest of this document, we must explicitly state the similarities and differences between these three primary applications of FRT.



Facial Verification

This application of FRT employs the use of a computer FRT platform to explicitly confirm a subject's identity. This is the same mode of FRT deployed in many modern-day cellular devices. In law enforcement, this type of FRT can be useful in correctional facilities to grant access to secured areas, confirm inmate identity in a booking or release environment, or confirm identity at border crossings as a few examples.

Field Verification

Field verification is the use of FRT in the field for the purpose of identifying an individual during a live interaction. This mode of FRT is primarily used to attempt to "fill the gaps" in available information such as when a subject lacks formal issued identification or is uncooperative and refuses to give proper identification. This type of FRT can aid in confirming who a subject is claiming to be.

Facial Identification

Facial identification is the most common application of FRT used by law enforcement. It is a direct use of FRT during a law enforcement investigation in which digital imagery of an unknown subject is available. This imagery is uploaded to an FRT platform which has a gallery of previously enrolled images for the specific purpose of identifying unknown subjects. Generally speaking, this is also a two-step process involving a combination of both FRT platform and human involvement with defined roles for both steps of the process.

The first step is the processing of the image through the FRT platform which creates a biometric facial template from the enrolled image and compares it to its gallery of facial templates. The system then returns a list of the enrolled images whose biometric facial template is sufficiently similar to the

submitted probe image's template. The second part of the process, and arguably the most important, involves a trained facial recognition examiner conducting a detailed review of the imagery returned by the system through a manual process of examining the morphological similarities or differences with the unknown subject. The examiner ultimately produces a finding based on the existence of or lack of articulable similarities between a probe and gallery image.

In contrast to the above, there exist FRT platforms that do not require a facial recognition examiner to be involved in the process which simply produces automated findings. These types of systems fail to allow any input or evaluation from an examiner. Although there exist use cases for this type of FRT, this product's recommendations and considerations are not designed for that type of system. Rather, the content found in this product is specific to a two-step FRT program that employs human oversight in the process of facial identification.

Other Uses

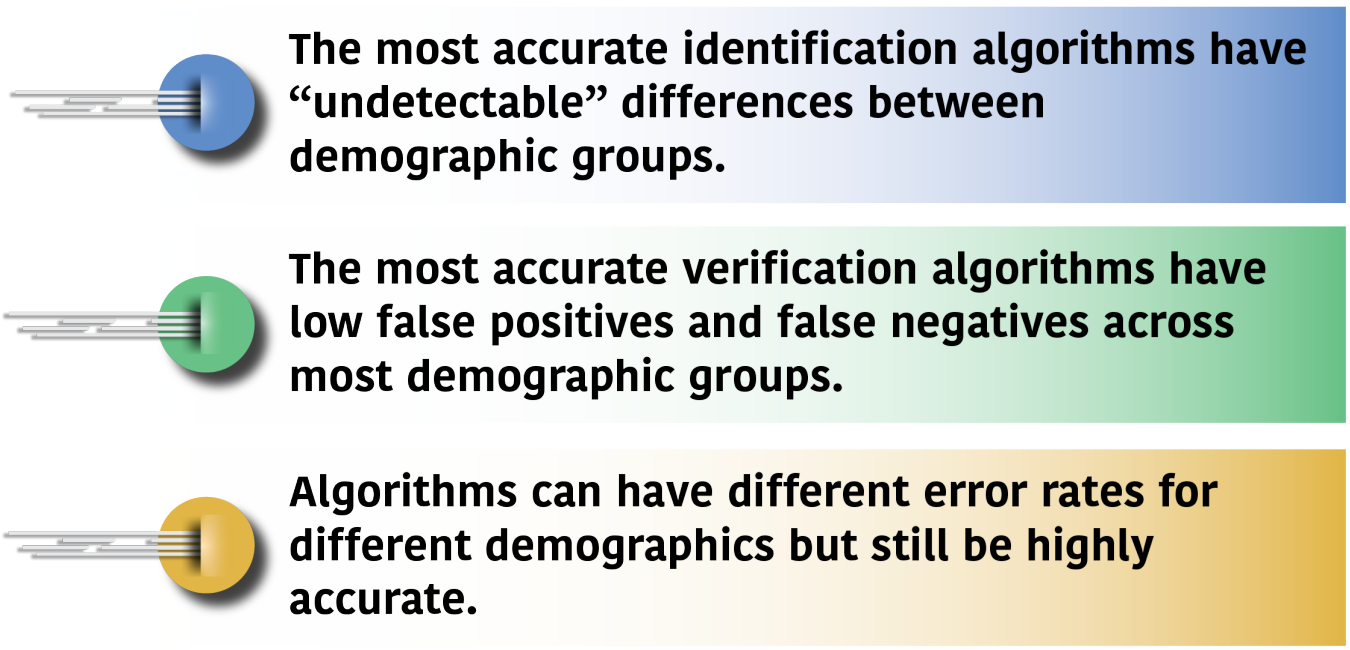
Finally, FRT platforms have the capability of being used as a surveillance tool by identifying persons in real-time using video feeds layered with FRT technology. Known instances of this type of use of FRT can be found in foreign nations and among certain private sector businesses. **MCCA best practices for law enforcement agencies utilizing FRT is to not utilize FRT in this manner except under the most exigent of circumstances or when explicitly permitted under legal authority (e.g., court order).**

Myths and Misconceptions

The above provides a quick snapshot of the real-world uses of facial recognition technology. In contrast, there is a general lack of publicly available information regarding the use of FRT by law enforcement. This has caused popular media to be a primary source for the general public's understanding of FRT. This situation is part of the impetus of this document. Reviewing the widespread myths and misconceptions about FRT in law enforcement is an integral part of any agency understanding the social context the technology currently sits within. At the end of this report in Appendix B, you will find a detailed exploration of many of the common misconceptions about FRT and supporting information to help in the process of educating stakeholders.

In an effort to provide some context on this, we offer the following example. There exists the perception that facial recognition algorithms are inherently biased and perform significantly less reliably among some demographic groups. However, a recent report that analyzed the findings on the National Institute of Standards and Technology (NIST) testing of FRT platforms revealed that: [1]

NIST FRT Algorithm Testing - Findings



1: McLaughlin, Michae; Castro , Michael (2021, September). *The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist.* ITIF. https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms

Methodology

The MCCA Facial Recognition in Modern Policing report serves as a comprehensive document containing recommendations and considerations for the use of FRT. This includes the processes, protocols, procedures, and responsibilities a law enforcement agency should embrace within its use of the valuable technology. This report provides recommended guidelines which are divided into three primary categories including technical considerations, program design, and program management.

Program Design

The Program Design section of this document is intended to provide decision-makers with important guidelines and a road map for designing a responsible FRT program that is both effective in its use, but also mindful of personal privacy and rights of individuals that the program may impact.

Chronological Process

This piece of the report is intended to provide the user an instructional guide on the steps to be taken as well as the correct order in the development of a facial recognition program. The suggestions made can empower a program manager to make responsible decisions in the most appropriate order as an FRT program is being built.

Responsible Procurement

This report will also help guide decision-makers in identifying the most well-respected FRT platforms available to law enforcement. A well-respected FRT platform will be both effective in the algorithmic testing, but also comprehensive in its overall design and supported by responsible ownership. This insight can both help save law enforcement agencies time in determining which FRT programs are available to law enforcement, and which are appropriate to use in terms of their algorithmic capabilities.

SME Training/Development

The third area focuses on a key component of an appropriate facial recognition program: training. Traditionally, law enforcement places great emphasis on the value of best practices training related to all aspects of public safety. Due to the increased concern regarding FRT, a well-designed examiner training and development program is a key piece of the responsible deployment of FRT. There is significant value in developing qualified and expert examiners. This expertise contributes to the quality of FRT investigative findings which ultimately result in increased public safety and confidence in our law enforcement agencies.

Program Management

The Program Management section of this document focuses on the operation and management of an agency's FRT program following the design and launch of the program. Even if an agency carefully considers and implements many of the recommendations in the Program Design portion of this document, each agency's community expectations, environmental challenges, and program management experience will almost certainly require specific adaptations of the recommendations outlined below.

Operational Workflow

The main area of focus in this section is the development of a workflow process related to facial recognition investigations. This piece highlights processes that can be adopted to ensure an organized investigative process which include the investigative request, first and secondary examiner steps, program oversight, and the distribution of findings. Most importantly, the suggested protocols provide a foundation for which an agency can collect comprehensive data points related to their facial recognition program for both operational oversight and reporting purposes.

Program Oversight

One of the essential elements of FRT program management is a carefully crafted oversight strategy. This area addresses program pieces that can be adopted that help both program managers and ultimately, high-level decision-makers evaluate overall FRT program status, value, and impact. It also helps provide the law enforcement agency with statistical reporting figures that allow its use and purpose to be shared with interested parties which may include but are not limited to legislative oversight groups, public oversight committees, and the media in general.

Operational Concerns

Policing agencies that implement an FRT program to improve operational efficiency and outcomes also need to be aware of the legitimate concerns that accompany such an implementation. The use of FRT, the utility of the technology, and the resulting outcomes are of great concern to the general public. A thorough understanding of the concerns of FRT is critical to a responsible program design. More importantly, a program must implement thorough policy and protocol processes that mitigate or eliminate the very real liabilities associated with FRT. This section will address the concerns of FRT and make clear recommendations on how those concerns can be alleviated and or even eliminated through responsible program design.

Technical Evaluation

An important topic covered in this report is a technical evaluation of facial recognition technology. As indicated in the opening of this report, it has become increasingly important to ensure technology adopted by law enforcement meets expectations. More simply stated, the adoption of any new technology requires knowing whether it works and whether it is worth adopting. Another critical question that needs to be answered regarding technical capabilities is if the technology works efficiently enough to ensure the data it provides law enforcement is relevant and accurate. This evaluation is essential in assuring law enforcement and the community alike that the quality of data being produced will contribute to law enforcement's primary goal of keeping our community safe. The technical evaluation in this document is divided into two subtopics.

Program Design

Facial recognition's inherent ability to help identify persons of interest assists law enforcement in solving cases and protecting our communities. However, there are also some real and perceived concerns regarding the use of this emerging technology, and ensuring proper oversight and privacy protection is among the most important. Police agencies have a duty to protect the privacy and civil rights of the community, just as much as it has the responsibility to enforce the law, apprehend criminals, and assist victims. To ensure both objectives are met, it is essential law enforcement agencies take careful steps to develop a facial recognition program that is effective, but appropriate. Taking a thoughtful approach to the application of this technology and design of the program allows for its use in a responsible manner is crucial.

To accomplish this goal, it is recommended that any facial recognition program be mindful of a few key points of interest for both law enforcement and the public alike. Those include proper policies, gallery image sources, controlled access, specialized training, and oversight, each of which are detailed below.

Proper Policies

Ensuring proper policies and procedures are in place for an agency's facial recognition program is critical. FRT policy should direct the purpose, general use, and processes involving facial recognition investigations. These policies will provide the framework by which an agency can simultaneously reap the benefits of the technology and be respectful of the individual privacy and civil rights of the public. Similarly, consistent policies will assist in protecting the integrity of criminal investigations, criminal intelligence, and justice system processes. They should also ensure all deployments of facial recognition will only be for official investigations. Policy and procedure elements should cover the following components:

- Community directed statement on why the agency is establishing an FRT capability
- The purpose of the policy
- General use of the technology
- Clearly defined program oversight roles and responsibilities
- The FRT vendor and system name/type
- Gallery sources
- Who is authorized to access the system
- Any required training for both examiners and officers
- The request and operational and investigative procedures
- The value an investigator should put on a positive FRT finding
- Clear guidance to investigators on being transparent in use and reporting in arrests reports
- Auditing responsibilities

Establishing clearly defined rules and processes on how FRT can be used, how investigations can be conducted, and the value of the findings of an investigation is the best way to minimize the risk of improper use of FRT. These policies should also be made available to the public when required by law or when appropriate.

Self-Restricted Data

Despite the laws in many states permitting the use of public driver's license photos, social media photos, or other publicly available photos for facial recognition gallery use, consideration should be given to the specific and most privacy-conscious approach to what library is used. This could include limiting the facial recognition gallery to photos of persons who have been previously arrested (i.e., mugshots). Although restrictive in nature, this ensures the probe images of suspected criminals are only being compared against images of persons who have previously been involved in criminal investigations in a specific geographic area and whose image has been obtained by law enforcement directly.

Some jurisdictions utilize DMV image databases. In those instances, it is supported by laws that govern the use of such images for FRT. It is also recommended community involvement be a part of that consideration. However, some concerns should be understood before embracing such a strategy. Images collected as a matter of practice in the arrest/booking process may be viewed differently than images in which the subject voluntarily submits to being photographed as a condition of operating a motor vehicle. Second, the inclusion of said galleries can impact the investigative process and place a greater burden on the human review step of the total process due to a larger gallery database.

Specialized Training

One of the primary reasons a two-part FRT examination process is so effective is because of the introduction and role of the trained human examiner. This human element is arguably the most important part of the total process[2]. The value of a technically trained examiner in the practice of facial identification and comparison cannot be overstated. Still, it is similarly important the investigator who is ultimately acting on any intelligence derived from a facial recognition investigation also be appropriately trained. The focus of the recommended training can be broken down into two parts.

"The value of a technically trained examiner in the practice of facial identification and comparison cannot be overstated."

First, it is critical that the examination part of the process is conducted by those who have been specially trained. To be considered an examiner or a subject matter expert in facial recognition technology it is recommended that the examiner complete the following types of training; Many agencies require their examiners to participate in the Federal Bureau of Investigation (FBI) Facial Identification training course.[3] This training focuses on understanding the foundations of facial components, stability of features over time, and other factors such as perspective distortion. It is widely accepted that a morphological analysis approach be used for facial comparison. A morphological analysis is a method of facial comparison in which the features and components of the face are compared. It is based on the evaluation of the correspondence among facial features such as the nose, mouth, ears, eyes, and facial lines and their respective component characteristics. Research has shown that examiners who are trained in the science of face comparison are better at recognizing individuals.

Similarly, it is equally critical that an examiner be trained on, and familiar with, the version of FRT

2: A Government Accountability Office report notes that the process and considerations for face identification are consistent with other forensic identification techniques, specifically latent prints and DNA. (See: Technology Assessment - Forensic Technology – Algorithms Strengthen Forensic Analysis, but Several Factors Can Affect Outcomes, GAO-21-435SP, US Government Accountability Office, July 2021).

3: FISWG, Facial comparison Overview and Methodology Guidelines version 1.0 2019.10.25

software that the agency uses. This training should be supported by vendors and include the operational processes, technical requirements, and a general understanding of how the system functions.

In addition to the initial onboarding training of skills and system familiarity, an examiner should become familiar with all processes and procedures in place for the FRT program. During the onboarding process, it is recommended that examiners in training shadow more experienced FRT examiners to ensure the application and understanding of the skills learned are being executed correctly. Additionally, their work product should be reviewed for accuracy and correct application of the received training. Finally, it is recommended that regular in-house training is completed for skills refreshment, general awareness of FRT case law, and awareness of trends and patterns.

Because examiners using an FRT system can, and often will be, requested to testify in both criminal and civil court cases, expert witness testimony training is also highly recommended. An expert witness is one with expertise in FRT and morphological comparison that far exceeds knowledge levels of a trier of fact. As an expert in FRT, it is important that an examiner be able to effectively communicate findings in a way that courts can best understand and learn strategies for effective direct and cross examination. Expert witness testimony training should also encompass topics that include a general understanding of the court process, roles of prosecutor, defense, jury, and judge and expert witness, as well as the qualification process for expert witnesses.

Additionally, comprehensive training should be provided to any investigator/officer who will be taking any action on the results of facial recognition investigations. Investigators should have a basic understanding of how the system operates, the role of the examiner, and applicable laws and policies that govern the use of FRT in a particular jurisdiction. These key agency members should be aware of the major capabilities and limitations of facial recognition technology broadly as well as the specific implementation of their agency's FRT program. **The limitations of FRT and the potential consequences of its misuse, as outlined in this document, are the main reasons that results of facial recognition examinations should only be used as a tip or lead by investigators.**

Investigators should also understand the importance of documenting the use of FRT technology in case reports as well as the need to disclose its use in applicable arrest documents and the discovery processes.

Limited Access

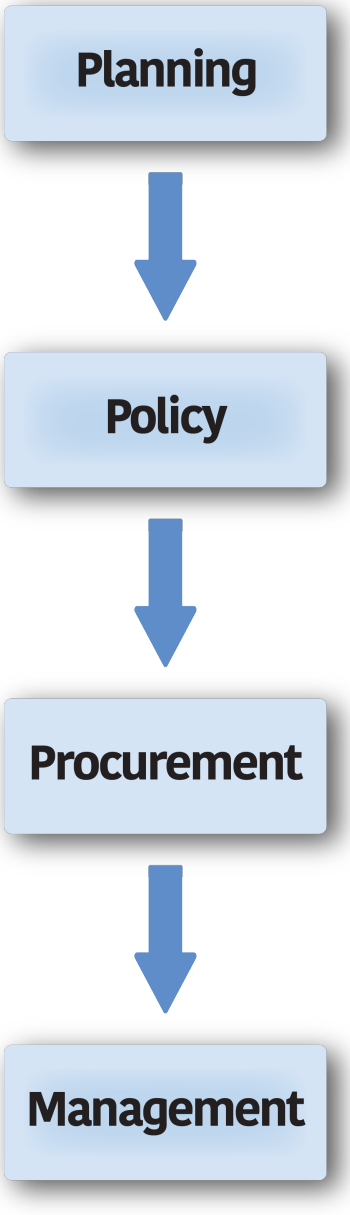
Numerous benefits are gained from the strategic design of centralizing the use and access of FRT to specific entities and restricting access to the technology to only those who have been specially trained in facial recognition. This strategy enhances trust in law enforcement and investigative processes as well as makes the implementation of the other components of a well-balanced program like management, reporting, and responsible use more easily achievable. **Having FRT examiners that are uninvolved with an investigation outside of the FRT component can help ensure FRT findings are consistent with program design and use.** Additionally, it can reduce the concern of investigators becoming overly reliant on the technology.

"Numerous benefits are gained from restricitng access to the technology to only those who have been specially trained in facial recognition."

Another benefit of a centralized program with limited size and access is that the implementation of best practices regarding FRT is more easily achieved. For example, should the vendor release a new version of FRT, only a small group of examiners would require the updated instruction versus training a large group of investigators. An additional benefit is that it streamlines the ability of an agency to collect valuable statistical use. With broad agency access and use, collecting important statistics becomes difficult if not impossible. Furthermore, the management of the program is simplified with a restricted deployment. Ultimately, ensuring processes, protocols, and policies are being strictly followed in a more tightly controlled environment is a goal to strive for.

Program Roadmap

Many aspects of program design have been covered in this section. The following bullet points are presented in a proposed phased order as a basic roadmap for the creation of a new FRT program.



- Establish FRT Goals/Expectations
- Identify Internal Stakeholders
- Engage Private Stakeholders for Feedback
- Identify Acceptable Gallery Sources
- Identify Acceptable Use Cases
- Develop Budget

- Develop Interagency Plan (MOU's) if Applicable
- Integrate Stakeholder Feedback
- Establish Internal Management Personnel
- Define Specific Usage Parameters and Restrictions
- Establish Oversight Measures and Requirements

- Engage with Multiple Vendors in Initial Procurement
- Engage with Client Agencies for Feedback
- Seek input from Citizen/Privacy Advocates
- After Selection of Vendor:
  - Develop Vendor-Specific Training
  - Engage All Stakeholders in "Soft Launch"
  - Monitor Initial Challenges if Any

- Refine/Develop Training, Scale-Up Program
- Finalize Reporting/Auditing Mechanisms
- Implement Continuous Assessment/Management
- Report Successes and Challenges to Stakeholders
- Engage with Partner Agencies Using FRT

Responsible Procurement

When procuring facial recognition technology (FRT) platforms or any other product with privacy and civil liberty implications, law enforcement agencies should seek stakeholder feedback and buy-in during the early stages of the procurement process. Because advanced technology such as FRT may delve into uncharted territory, it is not unreasonable for the public to question law enforcement's intentions and motivations. In January 2020, The New York Times published a piece under the headline, "The Secretive Company That Might End Privacy as We Know It."[4] The article (along with several others published contemporaneously) raised several valid concerns, including but not limited to the following: could rogue officers use the technology to identify and stalk an attractive stranger? Without policies prohibiting such conduct, could law enforcement use the technology to identify organizers of peaceful protests? Could programs that scrape the open web for images contribute to misidentifications? In the absence of model policies for novel or emerging technologies, news and opinion pieces can serve as a starting point in developing policies that address privacy and other concerns surrounding civil liberties. Soliciting stakeholder feedback and early involvement by citizens and privacy advocates at the beginning stages of an FRT program is also crucial.

"Law enforcement agencies should seek FRT software that delivers the most accruate results possible while also being developed by companies whose missions, visions, and values align with their own."

Law enforcement agencies should seek FRT software that delivers the most accurate results possible while also ensuring that the software is developed by companies whose missions, visions, and values align with their own.

Law enforcement agencies should conduct an appropriate degree of market research, which should include a trial of the product and conversations with existing customers to evaluate the product's performance in a real-world setting. While there is a certain degree of calculated risk involved in beginning a trial period before engaging stakeholders for their feedback in policy development and implementation, law enforcement agencies that adopt such an approach will have the ability to highlight initial successes with the technology thereby creating the opportunity to provide tangible examples to their stakeholders of how FRT serves to enhance public safety. Should an agency engage in a pilot program, it is vital to adopt a strict policy on how any information should be used in the course of investigations until a final protocol and all other areas of the program are formalized.

The importance of obtaining stakeholder feedback early in the procurement process cannot be understated. Program managers should make every effort to embrace a spirit of transparency, to accept critical feedback from stakeholders, and to attempt to address concerns concretely. It is sometimes possible to address specific concerns of the public by adopting specific measures in an agency's FRT program policy.

4: Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," New York Times, January 18, 2020, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html

As an example of this type of suggested engagement with interested stakeholders, we offer an example; one major metropolitan police department met with representatives of a civil liberties advocacy organization in which some advocates voiced concerns. With the expressed concerns in mind, the agency incorporated the following into its FRT policy:

- A prohibition on the use of FRT to monitor any person(s) in "real-time"
- A requirement that all FRT leads for a particular case (not just the cases resulting in arrests) be included in official case files and be considered discoverable under applicable rules of evidence
- The inclusion of unambiguous language prohibiting arrests based solely on FRT leads
- An admonishment that end users be aware of the possible existence of algorithmic biases inherent in FRT platforms

Feedback from other stakeholders, such as an agency's procurement department, prosecutor's office, and civilian oversight board (if applicable) are also invaluable. It is also advised to engage with an agency's in-house legal department or corporation counsel on any parameters which need to be considered.

While local procurement ordinances vary across jurisdictions, it is imperative that those ordinances, along with broader guiding principles, are followed when procuring an FRT platform. The National Institute of Governmental Purchasing's (NIGP) Values and Guiding Principles of Public Procurement are one such set of broad principles which should be followed in any procurement process. The Guiding Principles are as follows:

- **Accountability:** Taking ownership and being responsible to all stakeholders for our actions. This value is essential to preserve public trust and protect the public interest.
- **Ethics:** Doing the right thing. This value is essential to deserve the public's trust.
- **Impartiality:** Unbiased decision-making and actions. This value is essential to ensure fairness for the public good.
- **Professionalism:** Upholding high standards of job performance and ethical behavior. This value is essential to balance diverse public interests.
- **Service:** Obligation to assist stakeholders. This value is essential to support the public good.
- **Transparency:** Easily accessible and understandable policies and processes. This value is essential to demonstrate responsible use of public funds.[5]

Obtaining stakeholder feedback and buy-in, conducting diligent market research, adhering to procurement ordinances, along with broader guiding principles and values, and balancing privacy interests with public safety interests will aid law enforcement agencies in the successful procurement of an FRT platform(s).

5: National Institute of Governmental Purchasing: The Institute for Public Procurement. Enduring Beliefs or Ideals Shared by Public Procurement and Stakeholders, Values and Guiding Principles of Public Procurement - https://www.nigp.org/our-profession/values-and-guiding-principles-of-public-procurement

Program Management

We have so far visited several considerations any agency wishing to implement an FRT program should address. The design phase of an FRT program is the essential groundwork necessary to set an agency up for success. However, successful implementation of FRT does not stop at the moment of program launch. Ensuring operational transparency, accountability, and responsibility in the use of the technology requires continuing management and oversight. In this section, we will explore the general workflow of an operational FRT program and several considerations that should be made every step of the way.

Operational Workflow

The operational workflow phases detailed below include a series of elements and considerations which are important to address in the scope of this document. Although the specific structure and size of any agency's FRT program may differ, this section outlines a complete process in a stepwise format that should apply at least in part to any agency's program.

Submission

Submission is the phase of the program where an authorized user has obtained an image of an unknown individual and intends to submit that image for the application of FRT. To support both the overall process of performing an FRT examination and the subsequent auditing and control of the program the following key elements should be implemented in the submission process.

Vendor/Process Isolation

With few exceptions, an agency's access to an FRT is predicated on access to a third-party platform. Most FRT vendors are continuously developing and changing their platforms to meet various customer demands. This can result in widely varying capabilities concerning the capture of the important case and process information. The fast pace of this development thus presents the risk of disrupting an agency's ability to properly manage and audit their FRT programs in the case of over-reliance on a vendor's case management and/or auditing capabilities. Therefore, it is recommended that the FRT program implement solutions for managing the submission of probe imagery and the management of FRT requests/cases outside of the FRT Platform software.

Initial Capture of Case Information

The submission of probe imagery to an FRT program should require sufficient information from the requestor such that the nature and appropriateness of the request can be determined without immediate follow-up. The information required should mirror both the legal and policy stance of the agency concerning FRT.

In addition to allowing the FRT program to determine appropriate use, the initial case information captured will often assist FRT examiners. For example, specific intelligence about the unknown subject may allow an FRT examiner to eliminate or confirm a possible candidate as a potential lead in the case.

Agency members submitting requests should provide adequate contact information such that any follow-up can be completed during the review of the request.

Evaluation

The evaluation phase of the FRT program combines the initial receipt of an FRT request with an overall triaging of the request and probe imagery. The elements of the phase ensure the request adheres to defined protocols and the imagery is appropriate for use on the agency's FRT platform.

Case Review

Any agency members that have been trained and authorized to perform an FRT Examination should be considered subject matter experts in the application of the technology. As such, Case Review is the final phase where the legality and procedural appropriateness of the use of FRT can be ensured.

Imagery Management

Due to the innumerable potential sources of probe imagery, requestors sometimes submit probe imagery in obscure formats or embedded in digital documents and/or video. This is sometimes due to the ability of investigators to access digital devices or having to rely on a multi-step process to obtain and/or isolate imagery or video themselves.

As such, it is incumbent upon FRT examiners to be proficient in the interpretation of various file formats and their use as well as the methods needed to isolate facial probe imagery from whatever file or format submitted.

Imagery Review

Following the isolation and management of FRT probe imagery, the FRT examiner must perform a review of the imagery. This review relies upon the examiner's training in FRT techniques and their familiarity with the FRT vendor's product capabilities to determine an image's viability for use in FRT.

The goal of the image review should be to determine whether the submitted imagery is viable for the application of FRT. This process need not produce an objective measure or value to determine the viability of probe imagery. Some parts of this review are necessarily subjective.

It is recommended that this review process be completed before searching for or obtaining any results from the specific FRT platform. Completing this holistic review of the submitted probe imagery before upload to the FRT platform provides an additional layer of objectivity to the process. Many FRT platforms will return possible results on extremely poor imagery. This can lead to situations where an FRT examiner is presented with possible candidates who can strongly resemble the person pictured in an extremely poor-quality probe image. This resemblance has the potential to create an element of confirmation bias in FRT examiners where the quality of the discrete morphological comparisons in reporting potential leads can suffer.

Once the FRT examiner has determined the imagery is appropriate for FRT, it can then be uploaded into the FRT platform.

Examination

The examination phase of the FRT program is the phase during which the results returned from the specific FRT platform are assessed by the FRT examiner. The steps before this process and those that follow are designed to reduce the overall reliance upon the FRT algorithm in the law enforcement/public safety decision-making process. The goal of the examination phase is to locate a candidate image within the returns from the FRT algorithm which can be adequately confirmed as a potential lead. The consistent application of established facial morphological analysis between the probe image and the returned results is the cornerstone of producing these facial recognition leads.

Performing Initial Search

The search process in most FRT platforms have configuration options that relate to the operation of the platform and the number/type of search results that are returned. These options can limit and/or refine the gallery images that the probe imagery is compared to. The higher number or increasingly specific search parameters that are defined will necessarily limit the size of the search gallery.

The application of specific filters on physical descriptors should be limited to the amount of specificity that is known about the unknown person. For example, age ranges should only be limited by the extremes in age that are apparent in the probe imagery. This will allow the reasonable elimination of persons that the probe imagery is compared to. However, care must be taken when considering the use of metadata (such as age) when the reliability of that data – for both the unknown person and those included in the database – may be questionable. The goal is to reduce the statistical possibility of misidentification while not negatively impacting the possibility for a potential lead.

FRT platforms may provide configuration options related to the number of possible candidates that are returned. This configuration option should be weighted to the highest number to make the comparison of probe imagery to each candidate practicable in terms of time.

Initial Assessment of Candidates

In a review of a pool of possible candidates returned by an FRT platform, a trained FRT examiner will often be able to eliminate some candidates as potential leads immediately. The initial assessment of the pool of candidates should be focused on this "first pass" elimination.

Detailed Comparison

Once the pool of possible candidates has been reduced to those candidates that cannot be quickly eliminated, a detailed comparison should be performed on each remaining candidate. This detailed comparison should involve a systematic one-to-one comparison of the probe imagery to the remaining possible candidates. Most FRT platforms provide digital tools and techniques to assist in this process.

The goal of the detailed comparison is to locate a series of discrete morphological similarities between the probe image and a single candidate image. This set of similarities should be composed of commonly defined elements that are ideally from two or three different portions of the face. As an example, identifying morphological similarities between the nose, ear, and mouth is more desirable than identifying multiple similarities between only the ears of the imagery.

When sufficient detail is present in both the probe image and candidate image such that a morphological similarity can be articulated with specific language, that similarity might be referred to as a "lock." Such "locks" are what is necessary in the human assessment and confirmation of a candidate as a potential lead.

Three possible scenarios exist as an outcome of the detailed comparison step:

- One potential lead
- No potential lead
- Multiple potential leads
    - Although likely extremely rare, the technical possibility of two different individuals presenting sufficient locks with the probe imagery may occur. For the purposes of this document and the considerations presented, this scenario should be treated as a "no potential lead".

Facial Recognition Lead Production

When in the event one potential lead is located in the candidate pool during the detailed comparison, the findings of the detailed comparison should be documented in a standardized form. This form can be produced by the agency or can be a technical tool provided by the FRT platform. The standardization of the lead documentation provides a level of objectivity to the process by defining the level of detail and the specific information that will be provided as a return to the requestor.

Review

Prior to completing the FRT investigation and before returning the findings of the primary FRT examiner, a review process should be implemented by the FRT program. The goal of this review process is to provide an additional level of consistency and control with respect to the application of standardized training practices.

Secondary Review

A secondary review should consist of a separate FRT examiner reviewing the findings of the primary examiner. This can be a review of the facial recognition lead report alone, or a complete secondary search of the probe imagery within the FRT platform. During the secondary review, the reviewing FRT examiner should report either a concurrence with the provided results or rejection of the provided results. The secondary reviewer should be able to provide specific and articulable reasons for not agreeing with the provided results.

The outcome of the secondary review should be documented in the FRT request and subsequently reviewed by program managers. The cause for any lack of concurrence with results should be analyzed by program managers and the circumstances of the disagreement should be reviewed with the primary FRT examiner. The number and nature of FRT investigations with disagreements over the results should be monitored over time.

Management Review

A management review should be implemented on as many FRT investigations as practicable. This review is intended to ensure the proper application of the technology generally as well as adherence to all applicable policies and procedures. The management review should periodically include the auditing of the FRT platform for each reviewed FRT investigation. **This management review should be completed prior to returning results on the FRT investigation.**

Distribution

The results of any application of FRT should be documented and retained for historical reference. This should include those FRT examinations that return no results. The return of facial recognition lead reports to requestors should be standardized and it is suggested to also include the following key pieces of information:

- The agency's stance concerning the use of FRT information.
- Agency policy on disclosure of the use of FRT on arrest documents.
- Any significant applicable laws on FRT.
- Any agency's policy requirements on how investigators are to proceed with the investigation (i.e., not rely strictly on a photo line-up to establish probable cause.)

The distribution phase is also an ideal opportunity to remind investigators that the collection of data related to the results of the investigation after the use of FRT is valuable. As previously mentioned, a comprehensive auditing and reporting process provides a greater foundation for an accurate evaluation of the technology.

Auditing and Reporting

The documentation of an agency's FRT program processes is a critical part of a transparent and accountable FRT program. The existence of an FRT request in a criminal case, the outcome of the subsequent FRT investigation, as well as the eventual use of the findings in the criminal case are the main data points that should be captured.

This documented data ultimately provides a statistical snapshot of the impact the technology has within the greater mission of responding to and preventing crime. **A comprehensive auditing and reporting process provides a foundation for a true evaluation of the technology and how it improves policing outcomes for both the agency and the community.**

FRT data collection serves three primary purposes. First, data collection on every FRT investigation conducted should be made to understand the purpose of the investigation. Second, data collection on the part of an examiner including all important details of the examination phase helps to ensure quality control measures are being met. Finally, a detailed analysis of the data and any metrics designed to measure the data help identify program deficiencies that may include training, timeliness, process hurdles, etc.

This data can and should be converted into measurements that provide clear information on FRT use, investigative results, and compliance with the policy. Similarly, it provides an FRT program an opportunity to share success cases that denote the value of the technology, the contribution of the examiners, and the impact of the technology in the broad crime-fighting mission.

An added benefit of maintaining statistical usage data is that it potentially can identify deficiencies that

need to be addressed. Deficiencies can normally be alleviated through training. However, that need for mitigation may not ever become known without data and metrics that paint a full picture.

Program Oversight

Strong program oversight enhances the ability to develop proper policies, perform relevant training, and ensure responsible use. Established oversight allows an agency to properly manage any existing or emerging operational concerns. Therefore, it is recommended that agencies have a clearly defined program management component of their FRT program.

To ensure the program is operating responsibly, it is the recommendation of this report that a program manager is identified and assigned to operate an FRT program. This individual should be well versed in the use of the technology, have a sound understanding of the analysis of facial identification as a human examiner, and should be empowered to ensure the program is following protocols, policy, applicable law, and the expectations of the agency.

A well-defined program management structure promotes community trust that the regulations, protocols, and policies governing the use of FRT are in place and being followed. Similarly, it provides the community a point of contact to provide feedback, education, and transparency. It also enhances the ability of an agency to work closely with their FRT platform vendor. Even well-defined operational processes and procedures can mean little if there isn't a responsible party who ensures those procedures are being executed in their intended manner.

It is recommended that the program manager collect and report regularly on the use of the technology. A snapshot of a program can provide not just heads of agencies but also concerned members of the public insight into how FRT is being used to affect crime.

A program manager should be expected to stay current on changes and emerging trends of FRT and be expected to ensure that protocols and department policies are current and properly address any changes or advancements in the technology broadly.

A program manager should be expected to ensure the FRT examiners are properly trained. That responsibility may include the initial training of the technology and also in the discipline of facial identification and comparison. A manager should also ensure that regular on-gong training is being fulfilled.

Finally, having a program manager affords both an agency and the FRT vendor a clear point of contact. This can enhance the communication between agency and vendor which is desirable for both parties. On the part of law enforcement, it affords the agency a better opportunity to share with the vendor any challenges that they may experience. For example, an agency may identify an area in the system processes that needs enhancement or possibly identify a deficit in the reporting and auditing capabilities of the system. In both examples, good communication between the agency and vendor would enhance the ability of both parties to resolve any issues that arise and to improve upon the FRT platform.

In conclusion, it is our recommendation that a program manager be an integral part of the program design from the program's inception. Additionally, the program manager should be tasked with ensuring the program strictly follows all policy, protocols, and design pieces that enhance responsibility and accountability.

Operational Concerns

When developing a FRT program, it is imperative that law enforcement agencies consider the legitimate operational concerns that exist with the use of FRT. Some of the concerns when utilizing FRT include threats to privacy, violations of civil rights and personal freedoms, and potential data theft by both authorized and unauthorized users of the platform.

In order to address these concerns, agencies should have policies and safeguards in place to prevent such misuse of the system. Additionally, agencies using FRT should have adequate data storage capabilities and should have clearly established record retention and purging policies with regard to the images stored within the FRT platform.

"The documentation of an agency's FRT program processes is a critical part of a transparent and accountable FRT program."

Another consideration is the challenge of the collection of data that demonstrates the efficacy and or the ultimate results produced from FRT examinations. This is specifically due to the fact the technology is used as an investigative tool and a potential lead may not result in a successful arrest and prosecution of the identified subject. Since it is common for FRT examiners to be removed from the investigation, FRT programs often encounter difficulty in collecting valuable data regarding the final outcomes of the investigations. Highly respected existing FRT programs have countered this concern through data collection starting at the investigative inception. It is suggested that follow-up be made after the results are returned to the investigators to determine case status. **It is advised that an agency put in place a system or process to the extent possible to capture the end results of an investigation that utilized FRT.**

Qualitative Review

In order to support a complete picture of any one product, it can be important to research both past successes of an agency using a prospective FRT product and to analyze the measured impacts and successes of FRT technology broadly. In this section, we explore a specific FRT program and its statistics, as well as highlight some success stories directly attributable to the technology.

Working FRT Program Statistics

The Integrated Justice Information Systems (IJIS) Institute and the International Association of Chiefs of Police (IACP) collaborated to produce a Law Enforcement Facial Recognition Use Case Catalog that lays out 19 common and beneficial use cases of Facial Recognition Technology in Law Enforcement . They also support the use cases with some real-world examples of each. In this section, we supplement this excellent reference with an example of an established (multi-year) program in a major US city that operates in accordance with the processes and policies outlined in this document.

The program is operated by the police department of a large US city and has been operational for several years. The enrollment database used by the department to conduct investigations consists solely of their own booking images so they are high-quality images. The following statistics and examples are from Full-Year 2020:

- Over 1000 facial recognition investigation requests were received by the program and serviced by a dedicated facial recognition team of approximately 20 trained examiners.
- Of the requests received, 49.8% were determined to be suitable for examination: The facial recognition examiners and tools determined that about half of the images submitted were not of sufficient quality to conduct further analysis for a potential lead.
- Of the requests that were processed, 71.7% resulted in a potential lead (or 35.7% of the total submissions): Many of the investigations yielded leads that were pursued in combination with other information and investigative efforts.
- Many Positive Outcomes: Multiple crimes (many serial) were solved across areas including Robbery/ Theft, Larceny, Homicide, Financial/Fraud, Sexual Assault / Trafficking, Drugs and Explosives.
- Zero Wrongfully Arrested: There are no known instances (in 2020 or the history of the department) of individuals being wrongfully accused due to FRT.

Real-World Success Stories

To supplement the technical evaluation, this report also includes use case examples based on success stories. These excerpts are from real law enforcement events involving facial recognition. Collectively, they provide a snapshot of the value of FRT and its positive influence on public safety concerns. Also included is a review of an active agency's FRT program along with a hypothetical comparison of NIST's findings of an FRT program.

Sex Crime - Facial Recognition Request Assists with a Priority Sexual Assault Case: a request was submitted by sex crimes detectives who were on the scene of a sexual assault involving a juvenile victim. Within an hour of receiving the request, facial recognition technology was able to identify a likely candidate of the suspect involved. The information was shared with the lead detectives who were then able to positively identify the subject through additional investigative methods.

Financial Crime - Facial Recognition Helps with a Financial Crimes Investigation: Detectives submitted a

facial recognition investigation request seeking to identify a female responsible for withdrawing money from a victim's bank account at different ATM locations. The investigation led to a potential lead and her identifiers were shared with the investigating detectives. They later confirmed that this female had been involved in several other cases for obtaining money under false pretenses and other financial crimes.

Grand Larceny - Facial Recognition Assists with a Grand Larceny Auto Investigation: Detectives submitted a facial recognition investigation request seeking assistance with the identification of a subject suspected of stealing multiple vehicles from a rental car company. This had been part of an ongoing series with multiple related events. The facial recognition investigation yielded a likely candidate, and this information was given back to the detectives who were able to confirm that the subject identified was the suspect involved.

Counter-Terrorism - Facial Recognition Helps Identify a Person of Interest in Explosive Device Investigation: A request for facial recognition to assist in identifying a person of interest in a case involving a believed explosive device was submitted. Surveillance footage captured an image of a driver of a vehicle who was believed to be responsible. A facial recognition investigation identified a potential lead. Detectives contacted the subject and confirmed the lead was accurate. Detectives obtained additional evidence and probable cause to continue their investigation, leading to an arrest warrant being obtained.

Narcotics - Investigation Helps Identify Drug Suspects Involved in Shooting: Patrol detectives were seeking assistance identifying two suspects who were involved in a drug transaction. Those same suspects were also responsible for firing several shots at a victim. Social media account information was provided to assist with the investigation. Once two potential leads were identified, the subjects' information was relayed back to detectives who confirmed the identity of both subjects.

Robbery - Ending a Violent Robbery Series Using Facial Recognition: Robbery detectives submitted a request to assist with a facial recognition investigation for a suspect responsible for multiple business robberies. On several related events, the suspect would enter the business, batter the clerk, and then take cash out of the register. A potential lead was identified through the investigation and detectives were able to positively identify the suspect via additional investigative means including several victims who all identified the same suspect through a photo lineup.

Homicide - Facial Recognition Technology Helped with a Homicide Investigation: Detectives requested a facial recognition investigation for a violent assault/battery incident. The victim was knocked unconscious during the incident and hospitalized for several weeks with a brain injury. Later, he died as a result of those injuries. The facial recognition investigation assisted detectives with the suspect's identity. The suspect was arrested on the appropriate charges.

Technical Evaluation

As noted above, facial recognition may be used in different scenarios. It may be used to search a database to generate a lead, or it may be used to verify the identity of a user before granting a privilege, such as unlocking a mobile phone or allowing a border crossing. How well a given facial recognition algorithm works in verification is easier to understand than in the search scenario even though law enforcement overwhelmingly uses search more than verification. To further enhance the evaluation of FRT technology in real-world scenarios, a qualitative review is also presented which focuses on use cases and statistical impacts.

Algorithm Evaluation

At the heart of any FRT platform is the underlying algorithm used to perform both analysis and comparison of digital face imagery. Generally speaking, any computer program which is designed to solve a problem based on its inputs is an algorithm. The code written in Microsoft Excel which sorts an arbitrary list of numbers is an algorithm. The computer routine in our smartphones that decides the best route to a destination is an algorithm.

Most algorithms can be assessed against a provable successful output; such is the case with sorting where the "quality" of the algorithm comes down to the speed at which it can perform the sort. This is because the output of a sorting algorithm can be easily checked for accuracy. Other algorithms, such as an algorithm routing a road trip to a list of destinations cannot be easily checked for optimal solutions, therefore the "quality" of these algorithms must be assessed over both the speed and the quality of the outputs of the algorithm.

In the case of facial recognition algorithms, the size of the image galleries and the utilization of one probe image in most cases rarely causes the duration of the algorithm to be a factor. Hence, assessing the quality of an FRT algorithm necessarily involves analyzing the accuracy of the output of the algorithm. In this section, the various use cases of FRT algorithms and how the accuracy can be assessed are explored.

Accuracy of Verification Algorithms

In a phone unlock verification case, there are only two possible inputs – either the owner of the device is trying to get in, or an imposter is trying to get in. The system works "perfectly" if the owner always gets in and all imposters are kept out. The attached diagram depicts the range of outcomes.

	System 'says'	
Ground Truth	**Owner**	**Imposter**
Owner ("Match")	**UNLOCKS (True Positive)**	**DOES NOT UNLOCK (False Negative)**
Imposter ("No Match")	**UNLOCKS (False Positive)**	**DOES NOT UNLOCK (True Negative)**

In a facial recognition verification use case like this, the system acquires a "live" facial image, extracts a template from that image, and compares it against a facial template stored on the device. If the match score exceeds an established threshold value, the system will unlock the phone because a "match" has occurred. If the match score does not exceed the threshold score, the request to unlock is rejected. The system is making a "decision" based on a comparison of the threshold score with the score generated by the live image versus the template.

Although the template stored on the phone is fixed, the "live" face image will change from an attempt to attempt, due to changes in pose, illumination, and expression. The threshold score is a critical aspect of this process – if the threshold is set too low, then there is a better chance that an imposter can unlock a phone, but if the threshold is too high, an owner might not be able to get into their phone, because the system cannot accommodate normal changes in the face. Therefore, mobile phone security settings are likely to incorporate lower thresholds than other security systems, such as in a border crossing, because phone sellers don't want customers to get frustrated with overzealous security settings.

How does a threshold get determined and what does that mean for accuracy? Facial recognition algorithm developers rely upon "match score distributions" to help identify threshold scores. A match score distribution allows one to plot the match scores generated for a large number of true matches and non-matches. In a "perfect" system, all true matches would generate scores above all non-match scores. Refer to Figure #1 below. In this case, a threshold score could be set at a value in between the non-match (red) and true match (green) scores and accuracy would be perfect. Every true match would be declared a "match" and every non-match would be declared a "non-match." Numerically, we would describe the "true match" accuracy rate as 100%, with a false match rate of 0%. "False Match" and "False Positive" represent the same thing.

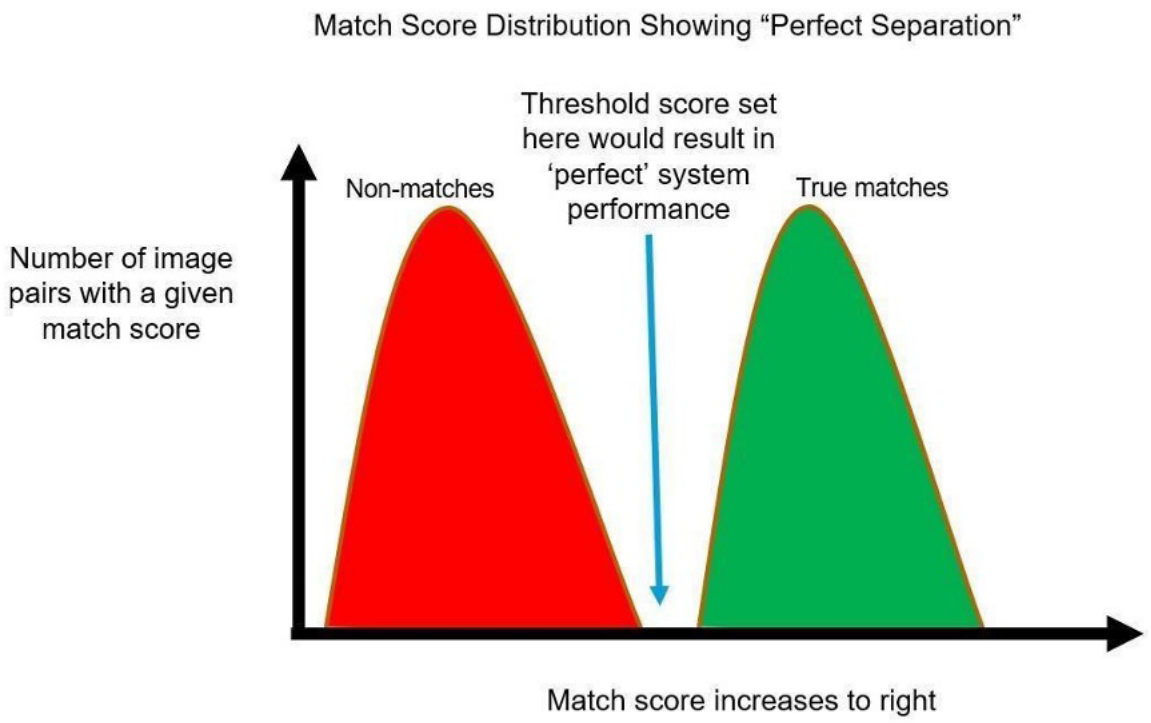


Figure #1

In reality, no biometric system is this perfect. Changes in pose, illumination, and expression, among other factors, can reduce the match score generated for a true match pair, while twins and other "look-alikes" can lead to non-match pairs with high scores, as depicted in Figure #2 below.

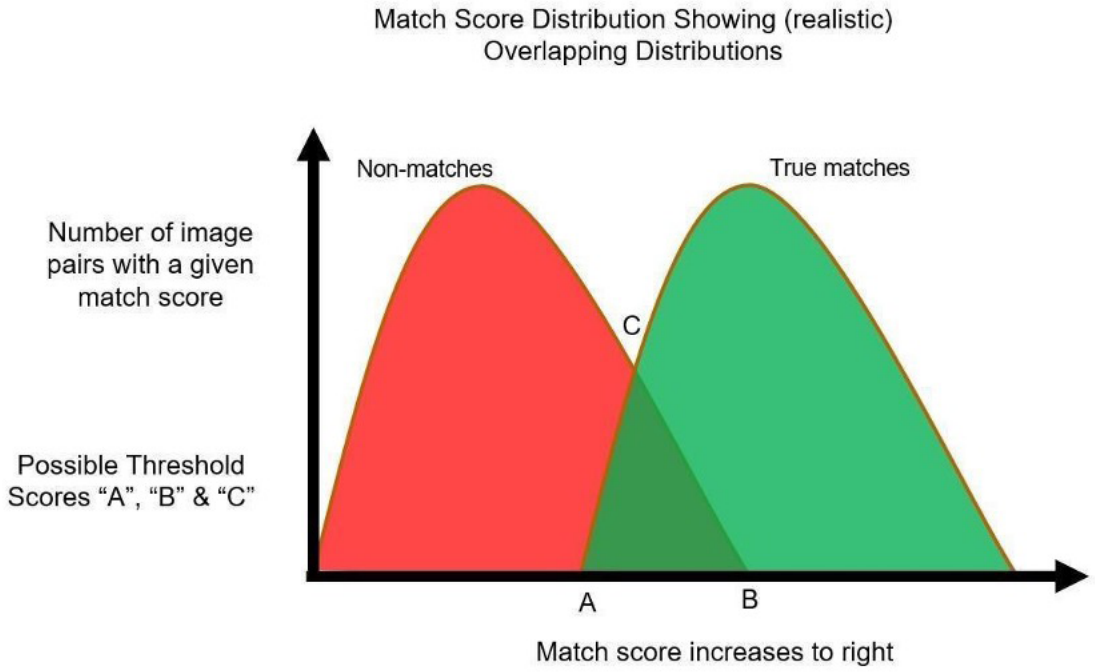


Figure #2

With a match score distribution as depicted in Figure #2, different thresholds will lead to different outcomes. If the threshold score is set at "A," then all true matches will be declared as such. In the mobile phone example, the user would always get in, but at the risk that others could also get in – and that would be declared a "false match." If we were to determine that the total number of non-matches (red) represented above score "A" is about 20% of the total number of true matches (green), then for any given comparison that resulted in a score above "A", the distribution implies that an imposter might get in once every five comparisons.

If the threshold score were set at "B," then the user could have some assurance that no one else could get into their phone, but the owner might be rejected more often than is desired – approximately 40% of the time if you throw out all true match pairs represented to the left of "B."

The threshold score "C" represents a score that occurs just as often for matches as it does for non-matches. According to this distribution, either decision – "match" or "non-match" is just as likely to be correct for that specific score.

The match score distribution in Figure #2 is closer to reflecting the real-world scenario for most biometric algorithms today than the "perfect" distribution in Figure #1. As the score increases from position "C", the probability increases that a given pair of images is an actual match, while below that score it is more likely to be a non-match.

In order to provide an "apples-to-apples" comparison of the accuracy of different algorithms, it is common practice to report the percentage of true matches that are missed (the "False Non-Match Rate" or FNMR) for all scores at or above the score above which a false match has a fixed rate. At the time of this writing, according to the NIST FRVT website, the very best algorithm for 1:1 verification had an FNMR of 0.0022 (22-in-10,000) using a threshold set for a False Match Rate (FMR) of 1-in-100,000. In terms of "hits", this would mean the algorithm had a true match rate of 99.78%.

Prior to 2018, NIST frequently used a fixed false match rate of 1-in-1,000 to define the threshold score for a given algorithm. The reduction of fixed false match rate to 1-in-100,000 (or sometimes 1-in-a-million) is an indication of how good the algorithms have become.

Accuracy of 1:N Search Algorithms

The primary law enforcement use of facial recognition is not for verification, but lead development through 1-to-many (1:N) searches. When a probe is searched against a gallery using a facial recognition system, the system returns a list of the highest-scoring candidates, which are then reviewed by trained personnel to see if a viable lead is present. The "decision" of whether a viable lead has been identified is not made by the algorithm, but by the reviewer. In other words, the system is not declaring a "match" so there can be no "false match" that would otherwise be wholly attributed to the system.

Technical Considerations

Assessing the Efficacy of Facial Recognition Platforms

The Face Recognition Vendor Test (FRTV) program run by the National Institute of Standards and Technology (NIST) is currently the only publicly available option where products may be voluntarily submitted for accuracy characterization. This is an excellent reference and resource; however, some interpolation is required to map their published results to law enforcement use cases and conditions.

Generally, there are two major aspects associated with assessing the efficacy of a particular product: Accuracy and Demographic Bias.

Accuracy

NIST's Facial Recognition Vendor Test program assesses voluntarily submitted algorithms for Identification (1:N) accuracy in various combinations of image types; however, they do not have a test series that assesses algorithms with the lowest quality probe input images (e.g.,'wild'images in their terminology are the lowest quality images) which are typically more challenging. The typical usage for law enforcement involves probe images that are not posed (e.g., sourced from video surveillance cameras, smartphones, etc.) being searched against an enrollment database that is composed of high quality, posed images (e.g., booking photos). The closest approximation to this in the 1:N NIST test results is believed to be input images sourced from the 'webcam' case which is the lowest quality image used. The verification tests (1:1) results produced by NIST do include a test case against 'wild' images so these results also provide an indication of a product's performance; however, the wild images may not be curated in a way that allows for accurate testing of demographic variation.

The typical concern with face identification accuracy is a false positive identification (incorrectly matching a probe image with an entry in the enrollment database). As explained above, there is a tradeoff between the minimization of false positives and false negatives (failing to match a probe image with an entry in the enrollment database). Increased accuracy of one results in diminished accuracy of the other. In their testing, NIST holds the maximum false positive rate constant (typically fractions of a percent but this threshold varies across different test cases) and reports the false negative rate that results from those conditions. The better performing algorithms generate low false negatives while still operating at or below the prescribed false positive rate. In general, the highest quality products (upper 25%) are exceptionally accurate in that they produce fractions to up to only 2-3 percentage points of false negatives depending upon the test configuration while maintaining a false positive rate in the fractions of a percent.

According to a report[6] that assessed the accuracy of humans of different training and innate talents, the accuracy of quality FRT products exceeds that of humans; however, process and human analysis is very important to the overall outcome. The report further found that the most accurate result (100% in their test case) was achieved through the combination of a trained human examiner supported by FRT technology which is better than the technology or humans individually could achieve.

Demographic Bias

This relates to inconsistency of product's accuracy across images of individuals of different race, gender and/or ethnicity. This was a pronounced problem years ago, but once it was identified, there has been considerable technical progress in improving this condition. NIST published a specific analysis of product sensitivity to demographic effects that found very small to undetectable differences in result accuracy due to demographic effects for high performing products. The Information Technology & Innovation Foundation, among others, analyzed the results and concluded the following :

- The most accurate identification algorithms have "undetectable" differences between demographic groups
- The most accurate verification algorithms have low false positives and false negatives across most demographic groups

6: Proceedings of the National Academy of Sciences. (2021, September). Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms. https://www.pnas.org/content/115/24/6171

- Algorithms can have different error rates for different demographics and still be highly accurate

An important consideration in facial identification is the enrollment database itself. In principle, the database can be composed of anything that the agency is authorized to collect that provides a useful backdrop for its identification use cases. Variables associated with the enrollment database that may influence the program include:

- **Size:** The number of enrolled images may have implications on the sheer accuracy of the search results and/or performance (processing time). These effects are not significant with reasonably sized databases and are largely insignificant for most applications, but this may provide an important assessment criterion of technology partners.
- **Quality:** Image quality plays an important role in the effectiveness of the tool (as well as the effectiveness of any human analysis). Quality images with structured pose, lighting, and resolution provide the best results and typically this type of image (captured in controlled environments) is what is used by law enforcement.
- **Accuracy:** The correctness and completeness of the metadata attached to images in the enrollment database are essential to ensure proper identification as well as to facilitate match verification via contextual information.
- **Source:** This plays a key role in the aforementioned attributes of size, quality, and accuracy but also is an important component of how the program is perceived relative to privacy and surveillance of society.

The source and composition of the enrollment database is a function of other policy decisions for the program; however, the process described above is independent of that since it is largely founded on human analysis and adjudication.

A technology product plays two important functions in the FRT identification process:

1. It performs the actual FRT search and match assessment through comparison of templates generated from the probe image and all images in the enrollment database.
2. It enforces access control, records all the examination steps for audit, and documents the process to produce the comprehensive facial recognition lead report (output).

As with any outcome that leverages technology, especially for critical applications such as FRT, there must be a trusted partnership between the user and technology provider (a technology provider may be a vendor, another agency, or indigenous).

FRT technology providers should be expected to:

- Ensure that their products are regularly characterized for accuracy under realistic conditions.
  - Submit their products to objective benchmarking and disclose their results. The Face Recognition Vendor Test (FRTV) program run by the National Institute of Standards and Technology (NIST) is currently the only available public option but it requires some interpolation to map their results to law enforcement use cases and conditions. It is important to ensure that the submitted algorithm(s) translate to the product (vs. a specialized implementation that is tuned to a particular case or that may not scale).
  - Agencies may be able to assess the overall accuracy as well as susceptibility to demographic bias themselves through other testing regimens and indeed they should have representative cases (typical probe images and enrollment database) that they can use to assess and continually revalidate providers.
- Be transparent about their product's operation, efficacy under relevant conditions, as well as how they test and continuously improve their products.

- If artificial intelligence and machine learning is the basis of their algorithm, the partner should disclose the source of their training data, their legal entitlement to that data as well as how they continue to curate the training data set.
- Have thoughtful controls built into their products such that users can be authenticated/authorized, users can be properly constrained (aka 'guard rails') in their application of the technology (e.g., not employ it outside of other workflows), and that usage can be audited for compliance with policies.
- Offer comprehensive training on their product that clearly articulates its intended usage as well as any limitations or constraints.
- Demonstrate efficacy and internal processes that ensure responsibility, accountability, and ethics in the contemplation, design, development, cybersecurity, deployment, and support of products that contain sensitive technologies such as FRT and that manage sensitive data.
- Demonstrate a track record of ethical and responsible technology.
- Have methods to systematically obtain feedback and data from the system in operation to assess performance and troubleshoot problems. The partner should have well-defined, privacy-respecting mechanisms and procedures in place leaving all control of any data that is disclosed with the program administrator.

If the product is consumed as-a-service and hosted by a technology provider (vs. an on-prem dedicated deployment), additional considerations apply since in this case the provider stores and processes the enrollment database, as well as any searches, conducted. These considerations include:

- Providers should have the necessary facilities and certifications to process this type of data (e.g., CJIS and FedRAMP compliant data centers and processes).
- Providers should be able to offer a DPIA (Data Privacy Impact Assessment) for their program.
- Providers should have a clear data policy.
- Contractually they should not impose terms that give them entitlement to any agency data (i.e., the agency is the controller of all data that they submit or that is generated on their behalf during processing).

Conclusion

As stated in the introduction, this product has been designed to be continually updated with the best practices, design mechanics, and up-to-date information when needed. From the information provided in this first version of this document, it is clear that facial recognition technology is a complex and ever-evolving tool for law enforcement which must be revisited often to ensure it is being used in a way to assist law enforcement in solving crime, but also protecting the public from misuse and privacy violations.

We are still in the beginning stages of knowing the vast uses and ways to use facial recognition technology to aid in investigations. It is necessary to keep a dialogue going with all various stakeholder groups - law enforcement at the federal, state, and local level, privacy and civil liberty advocates, private sector specialists, and local communities.

While this product exclusively explores the use of two-part verification facial recognition technology for facial identification, some agencies may choose to employ a different model. It is within the right of an agency to employ a FRT program which is most fitting for their needs and the desire of a community, but with any choice there are advantages and disadvantages, and it is suggested that all agencies wishing to deploy any type of facial recognition technology use the tenets discussed in this document to make the best choice for their agency.

For those agencies wishing to implement the use of FRT, but who are unsure on how to move forward, collaboration with other entities who have already developed robust, responsible programs is recommended. The sharing of best practices in crime-fighting technology among law enforcement has a history of beneficial impacts. Law enforcement has an obligation to be good stewards of information and policies and they must be willing to share this with fellow law enforcement agencies wishing to begin using FRT.

Facial recognition technology is being used daily to aid law enforcement in capturing the most violent criminals in our country and bringing closure for victims. It has been proven to be highly successful in solving various types of crimes afflicting our communities when used with the highest degree of responsibility, transparency, and accountable management.

The Major Cities Chiefs Association will continue to monitor this growing and developing technology as well as how it is being used across its member's jurisdictions and release updated versions of this product when appropriate. The MCCA will continue to engage all stakeholders with an interest in this evolving sector and communicate the latest information with its membership for member agencies to adjust their best practices as needed.

Acknowledgements

This product was put together in partnership and through the efforts, knowledge, and expertise of the following individuals. The Major Cities Chiefs Association is grateful for the work done by this working group for all their time and effort toward bettering the operations of law enforcement. This list is not exhaustive, not all persons with significant contributions to this product can be listed. A special thanks goes out to the technical advisors from vendors and law enforcement.

Armando R. Aguilar
Assistant Chief of Police
Miami Police Department, Florida

●

Bill Steinmetz
Lieutenant
Las Vegas Metropolitan Police Department, Nevada

●

Christian P. Quinn
Senior Director of Government Affairs
Brooks Bawden Moore LLC

●

Ivonne D. Valdes
Sergeant
Miami Police Department, Florida

●

Jim Lowery
Deputy Chief
Arlington Police Department, Texas

●

Kelcy McArthur
Statewide Network of Agency Photos Unit Manager
Michigan State Police

●

Kelly Bluth
Detective
Las Vegas Metropolitan Police Department, Nevada

Krystal Howard
Departmental Manager
Michigan State Police

●

Laura Cooper
Executive Director
Major Cities Chiefs Association

●

Megan Noland
Director of Special Projects
Major Cities Chiefs Association

●

Paden Weber
Officer
Las Vegas Metropolitan Police Department, Nevada

●

Patricia Williams
Associate Director
Major Cities Chiefs Association

●

Patrick T. Quinn
Lieutenant
Chicago Police Department, Illinois

●

Resource Guide and Further Reading

There exists an extensive amount of resources applicable to the content in this product. Some of the most relavant resources for continued reading, research, and application are listed below for convenience.

- Major Cities Chiefs Association - http://www.majorcitieschiefs.com
- National Institute of Standards and Technology (NIST) - Biometrics -https://www.nist.gov/biometrics
- Congressional Research Service - Federal Law Enforcement Use of Facial Recognition Technology (Oct. 27, 2020)- https://crsreports.congress.gov/product/pdf/R/R46586
- Congressional Research Service - Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations (Sept. 24, 2020) - https://crsreports.congress.gov/product/pdf/R/R46541
- ITIF Report - The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist - https://itif.org/publications/2020/01/27/critics-were-wrong-nist-data-shows-best-facial-recognition-algorithms
- House Judiciary Committee Testimony - Mr. Barry Friedman - Jacob D. Fuchsberg Professor of Law and Faculty Director, Policing Project, New York University School of Law (Jul. 13, 2021) - https://docs.house.gov/meetings/JU/JU08/20210713/113906/HMTG-117-JU08-Wstate-FriedmanB-20210713.pdf

Appendix A

Terminology and Definitions

Algorithm – an algorithm is a set of rules that instruct a computer on how to accomplish a task or solve a problem. A facial recognition algorithm is the software implementation of techniques used to verify or determine an individual's identity by processing a video frame or a digital image in which the individual's face is visible. Typically, the algorithm compares facial features in an image to faces contained within a database or gallery.

Candidate List - in facial identification, a rank-ordered list generated from a facial recognition search. (Source: Standard Terminology Relating to Forensic Science, ASTM 1732-19, by ASTM International, 2020)

Examiner - in facial identification, a forensic face examiner is a trained specialist at analyzing images of faces and comparing them for identification purposes to determine if the images are of the same individual.

Facial Identification - (1) the process of determining the identity of an unknown person from a photo database, known as the enrollment database or gallery to answer the question, "Can this unknown person be matched to any image enrolled in the database?" It is often referred to as one-to-many matching (1:N) because it compares a probe image to all images in the enrollment database. (Source: Accuracy and Bias of Face Recognition Technology and Law Enforcement Use: Factual Background, NYU Policing Project, 2021.) (2) the process of searching a probe into a gallery (Source: Face Recognition Vendor Test (FRVT) Part 3 Demographic Effects, NISTIR-8280, by NIST, 2019.)

Facial Recognition - in facial identification: (1) by automated systems, the automated searching of a facial image as a probe in a facial recognition system (one-to-many), typically resulting in a group (candidate list) of facial images being returned to a human operator in ranked order based on system-evaluated similarity; (2) by humans, the mental process by which an observer identifies a person as being one they have seen before. (Source: Standard Terminology Relating to Forensic Science, ASTM 1732-19, by ASTM International, 2020)

Facial Verification - (1) the process of authenticating a person's asserted identity by comparing two image templates to answer the question, "Are these two images the same person?" It is also referred to as one-to-one (1:1) matching because a probe image—the image inputted into a face recognition system—is only compared to one other stored image (Source: Accuracy and Bias of Face Recognition Technology and Law Enforcement Use: Factual Background, NYU Policing Project, 2021.) (2) the process of comparing two samples to determine if they belong to the same person or not. (Source: Face Recognition Vendor Test (FRVT) Part 3 Demographic Effects, NISTIR-8280, by NIST, 2019.)

Facial Comparison (in facial identification) - a manual process to identify similarities or dissimilarities between two (or more) facial images or facial image(s) and a live subject for the purpose of determining if they represent the same person or different person. (Source: Standard Terminology Relating to Forensic Science, ASTM 1732-19, by ASTM International, 2020)

Facial Identification (FI) - the discipline of image-based comparisons of human facial features. (Source: Standard Terminology Relating to Forensic Science, ASTM 1732-19, by ASTM International, 2020)

Facial Recognition (FR) - see face recognition. (Source: Standard Terminology Relating to Forensic Science, ASTM 1732-19, by ASTM International, 2020)

Facial Review - in facial identification, an adjudication of a candidate list. (Source: Standard Terminology Relating to Forensic Science, ASTM 1732-19, by ASTM International, 2020)

False Negative - in facial identification, is when the face recognition system fails to match a person's face to an image that is, in fact, contained in a database. In other words, the system will erroneously return zero results in response to a query. Also referred to as 'false non-match'. (Source: Electronic Frontiers Foundation – Face Recognition)

False Positive - in facial identification, is when the face recognition system does match a person's face to an image in a database, but that match is actually incorrect. Also referred to as 'false match'. (Source: Electronic Frontiers Foundation – Face Recognition)

Gallery - in facial identification, an FR system's database, which typically contains all known-person biometric references (samples or templates, or both). Also referred to as 'enrollment database' (Source: Standard Terminology Relating to Forensic Science, ASTM 1732-19, by ASTM International, 2020)

Morphological Analysis - in facial identification, direct comparison of class and individual facial characteristics without explicit measurement. (Source: Standard Terminology Relating to Forensic Science, ASTM 1732-19, by ASTM International, 2020)

Probe - in facial identification, a facial image or template searched against the gallery in a facial recognition (FR) system. (Source: Standard Terminology Relating to Forensic Science, ASTM 1732-19, by ASTM International, 2020)

Third-party Imagery - in facial identification, images used in facial recognition (FR), or facial identification (FI) that were not captured by the agency performing the comparison (for example, family snapshots of a missing person). (Source: Standard Terminology Relating to Forensic Science, ASTM 1732-19, by ASTM International, 2020)

Uncontrolled Image or Ad-hoc Image - in facial identification, an image not captured in accordance with facial identification/facial recognition (FI/FR) standards or guidelines (for example, a surveillance image). (Source: Standard Terminology Relating to Forensic Science, ASTM 1732-19, by ASTM International, 2020)

Appendix B

Misconceptions and Reality

Myth:

Most community members oppose law enforcement using facial recognition.

Reality:

Despite how vigorously privacy advocates and other special interest groups have recently opposed FRT, there is little public support for banning or substantially limiting the responsible use of FRT by law enforcement. Polling conducted by NetChoice in 2020 revealed most Americans would prefer state and local governments work with law enforcement to improve the use of facial recognition (83%) rather than banning the technology (17%).

Similar findings were found in 2020, by the polling firm, Schoen Cooperman Research, when they conducted a comprehensive nationwide poll regarding Americans' opinions on FRT. Their survey found that 68% of Americans believe facial recognition can make society safer, 70% feel it is sufficiently accurate in identifying people of all races and ethnicities, and 66% believe law enforcement's use of facial recognition is appropriate.

The PEW Research center also conducted extensive research on the topic in 2019. They found that when the public was asked about their confidence that different entities will use facial recognition tools responsibly, they express much greater trust in law enforcement agencies than in advertisers or technology companies. A majority of U.S. adults (56%) trust law enforcement agencies at least somewhat to use facial recognition technologies responsibly, with 17% indicating that they trust these agencies a great deal to use facial recognition.

By contrast, only around one-third of U.S. adults trust technology companies to use FRT responsibly, and just 18% trust advertisers with these technologies. Trust in law enforcement does vary based on demographic factors such as race, age, and political affiliation. White adults express higher levels of trust in the use of FRT by law enforcement than black adults (43%). Generally, older adults have greater trust in law enforcement's use of FRT than persons who are 18-29 years old.

These findings do not indicate that most community members don't want police leveraging FRT technology to keep their communities safe. It does affirm that there is a need to engage every community in a transparent and intentional way, particularly those that have historically been marginalized or over-policed.

Reference(s):

More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly | Pew Research Center
https://www.securityindustry.org/report/u-s-public-opinion-research-on-the-support-of-facial-recognition/
https://netchoice.org/media-press/americans-want-facial-recognition-use-by-law-enforcement-improved-but-not-banned/

Myth:

Many states and local communities are already banning facial recognition from use because of the dangers it poses.

Reality:

Despite the headlines, legislation introduced to ban or significantly limit the use of FRT actually have had very little support. Proposed bills failed to advance, or were completely rejected by legislatures in at least 17 states during the 2020 and 2021 sessions including California, Colorado, Hawaii, Kentucky, Maine, Maryland, Massachusetts, Michigan, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, New York, Oregon, South Carolina, and Washington.

Vermont and Virginia are the only states that have banned law enforcement's use of FRT, and in both states, the laws have already resulted in unintended consequences. Haphazard outright bans fail to consider exemptions that allow for the use of other tools that rely on digital face comparison technology not necessarily used to investigate specific suspects. Such tools are critical in child sexual exploitation and human trafficking investigations. Similar tools are used in digital forensics to categorize media and parse digital evidence files. Vermont passed a bill in May, just months after enacting the law, to exempt such software from the ban.

The new Virginia law, which went into effect July 1, 2021, eliminated a regional program in operation since 2017 which was utilized in over 14,000 instances, with no reported misidentifications. Among its many successes, the program is credited with helping to exonerate an innocent man accused of a violent crime in Virginia, identify a veteran posting suicidal messages online, arrest multiple bank robbery suspects, close down an organized identity theft ring, and further numerous investigations into gun trafficking and other violent crimes.

Massachusetts established defined use conditions applicable only to law enforcement, through its police reform measure. While a broad public sector ban was initially considered in Maine, the legislature passed an amended measure in June that allows for law enforcement use under narrow conditions. Washington State's 2020 law establishing conditions for public sector applications of facial recognition went into effect on July 1, 2021.

In March, Utah enacted comprehensive policy safeguards for government applications. The measure, supported both by the Utah Department of Public Safety as well as the American Civil Liberties Union, establishes requirements for public-sector and law enforcement use, including conditions for access to identity records held by the state, and transparency requirements for new public sector applications of facial recognition technology.

At the municipal level, only three localities in the United States enacted broad bans of FRT in 2021: Minneapolis and King County, Washington, passed bans on government use, while the Baltimore City Council recently approved an expansive ban that restricts government, personal, and commercial use.

Reference(s):

Most State Legislatures Have Rejected Bans and Severe Restrictions on Facial Recognition | Security Industry Association
http://www.mainelegislature.org/legis/bills/getPDF.asp?paper=HP1174&item=3&snum=130
https://le.utah.gov/~2021/bills/static/SB0034.html

Myth:

Authorizing the use of FRT is too great a risk as it will likely lead to over-utilization.

Reality:

FRT is often discussed as an all-or-nothing option, with critics calling for increased bans and moratoriums. This narrative fails to consider the opportunities that communities have to leverage this powerful tool to keep people safe and give victims justice, while still adhering to democratic policing principles. Effective policy creation, where both community members and law enforcement collaborate to define program guardrails and best practices can preserve equity for all community members. Mutually beneficial outcomes can still be realized without regarding privacy and public safety as mutually exclusive concepts. Communities have the ability to define program elements such as appropriate use cases, nature of image repository, data governance, information sharing, and minimum standards regarding both the technology adopted and the personnel authorized to use it.

Myth:

Facial recognition violates basic privacy protections and its utilization will lead to mass surveillance initiatives as seen in other countries, infringing upon people's basic right to assemble and exercise their First Amendment rights.

Reality:

FRT in the United States is used primarily as a back-end investigative tool after a crime has already occurred. FRT platforms as used by law enforcement in the United States, are generally not configured to interface with any other systems to perform real-time analysis using live video surveillance, such as security cameras, drone footage, body-worn cameras, in-car-video, or other sources that would potentially enable the real-time tracking of a specific individual via their facial features.

FRT is utilized by law enforcement in a very limited scope, and usually for specific use cases. Most uses of FRT with a nexus to protests or demonstrations involve efforts to identify a specific actor who committed a crime in the presence of others who were demonstrating. Communities can adopt policies, to include restrictions barring FRT from being used to gather intelligence related to First Amendment-protected speech, associations, or activity. Exceptions can be memorialized in policy authorizing the use of FRT if a crime is committed during such activity. Furthermore, the use of FRT can be specifically limited in scope to investigate only a specific criminal actor.

Myth:

The use of FRT has already been the reason numerous people have been unjustly arrested.

Reality:

While the thought of any innocent person being arrested by police is extremely troubling, FRT has actually been linked to very few cases involving the arrest of the wrong subject. Relative to the scope of utilization, these instances can be characterized statistically as extremely rare. Police leaders and subject matter experts with specific knowledge of the events attribute the outcomes in these cases more to flawed human processes, such as insufficient investigative follow-up, as opposed to flawed technology.

The risk of misidentification due to FRT can be effectively mitigated with certain use policies, including a mandated requirement for trained human review, and adopting the stance that FRT findings constitute

solely an investigative lead. Facial recognition findings should always be based on a two-part process involving both the technology and a person. Appropriately implemented, FRT enhances and accelerates human decision-making, but should never replace it.

If an investigator cuts corners, the remedy to such issues is holding them accountable for their actions and omissions if they fail to appropriately corroborate an investigative lead before taking enforcement action. These circumstances can be mitigated by crafting sound policies and effectively training personnel on concepts such as cognitive bias and potential demographic performance variations of FRT platforms. Many agencies declare in both policy, and on their report of investigative findings that the results do not substantiate a positive identification, independently establish probable cause, or otherwise merit the conclusion that a person is guilty of any criminal act.

Unfortunately, there is no identification technology that is absolutely perfect. However, with a tested accurate platform and trained examiner operating within appropriate policies, FRT can serve as a tool of precision that is far better than many alternatives. Due to a host of factors, FRT is expected to be perfect or better than perfect despite it already having an arguably more reliable record than other forms of identifying unknown subjects, especially eyewitness input, such as photo line-ups, suspect "show-ups", and similar unscientific processes.

Founded in 1992, the Innocence Project seeks to exonerate persons wrongly convicted and to reform the criminal justice system to prevent future injustices. Their research substantiates that relying solely on eyewitness identification is the leading cause of wrongful convictions:

Eyewitness misidentification is a consistent and outsized contributor to wrongful convictions. Nationally, 69% of DNA exonerations — 252 out of 367 cases — have involved eyewitness misidentification, making it the leading contributing cause of these wrongful convictions. Further, the National Registry of Exonerations has identified at least 450 non-DNA-based exonerations involving eyewitness misidentification.

It is not that people have ill intentions or are inherently inattentive. Human memory is complex and memories themselves are "fragile." People perceive events from a single perspective and their own recollection of events can be incomplete or mistaken. Furthermore, over time memories usually deteriorate and can even be altered as we attempt to recall things, especially when influenced by new information. Generally, people tend to be even less accurate when attempting to identify members of a race that is different than their own. Excluding FRT as a tool available to law enforcement leaves investigators with limited, unscientific subjective options to make critical decisions such as who should be arrested.

Reference(s):
https://innocenceproject.org/how-eyewitness-misidentification-can-send-innocent-people-to-prison/

Myth:

Facial recognition algorithms have been found to be consistently unreliable and are still too inaccurate to be used by law enforcement. Facial recognition technology consistently misidentifies women and people of color and only exacerbates the constant surveillance and criminalization that marginalized community members already face.

Reality:

There is understandably no greater concern related to law enforcement's utilization of facial recognition than the fear that it may exacerbate historic challenges to social justice or further strain the relationship between marginalized communities and the police officers who serve them. Even if FRT is sufficiently technically proficient, the perception that it is not, especially in the case of communities of color, can erode public trust and undermine police legitimacy.

Therefore, it is imperative that law enforcement strives to be transparent in the adoption of FRT, how it works, and how it will be specifically utilized. The promise of FRT is that it may serve as a tool of precision to home in on a specific suspect, based on a comparative scientific process, rather than conducting blanket sweeps of a geographic area, imposing on persons who are only guilty of wearing the same clothes or fitting the physical description of a suspect, as reported by a victim or witness.

In 2019, a Montgomery County, Maryland bank was robbed. Detectives arrived on scene and collected images of the suspect from the bank's security system. A potential suspect was quickly developed using FRT. Based on the lead, police responded to a location associated with the subject where they observed him outside still wearing the same clothes that he had on during the robbery. Ideally, this is an example of how FRT can serve not only to locate a dangerous subject at large but also to minimize the impact of enforcement efforts on the broader community.

The perception of facial recognition being biased began with early versions of the technology showing inconsistent accuracy rates across different demographics such as age, gender, and skin color. In the past, these inconsistencies stemmed from multiple causes, including a lack of demographically representative data used to train algorithms, cosmetic appearance modifications, and the physics of light reflection which can specifically contribute to technical challenges in detecting skin tone variations in digital images. Today, the general accuracy of facial recognition technology has improved substantially and like most technology, rapidly continues to more so every year.

A 2018 report is often cited as showing a 35% error rate for FRT in the identification of black women. In fact, those researchers tested older "face gender classification technologies" which are not used for identification by law enforcement. FRT compares two or more images for similarities to help identify a specific person based on their unique facial morphological features. By discussing these technologies interchangeably and citing outdated research that doesn't pertain to current FRT, many publications and even media reports have attributed exaggerated rates of racial disparity to FRT that are misleading. A review of impartial sources examining the current state of the science is imperative. The National Institute of Standards and Technology (NIST) is part of the U.S. Department of Commerce and is highly regarded as an authority to provide impartial scientific assessments. NIST has assessed the accuracy of facial recognition algorithms across different demographic groups and continually updates their findings. The most recent update was issued January 19, 2021, and can be accessed via: https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf

NIST assessed the false-positive and false-negative rates of facial recognition algorithms using various types of digital images. Several key findings include:

- The most accurate of the algorithms tested have such minute differences between racial/demographic groups that they are considered "undetectable."
- Many substantially outperform non-scientific methods of identification traditionally used by law enforcement.
- The most accurate algorithms have low false positives and false negatives across most demographic groups.
- Algorithms can have different error rates for different demographics but still be highly accurate. An algorithm's rate of demographic variance can be dependent upon system thresholds applied by an end-user.
- Lower performing algorithms do show measurable differences in performance, a critical issue that must be addressed through continual accuracy improvements and exclusion from the use by law enforcement.

The Critics Were Wrong: NIST Data Shows the Best Facial Recognition Algorithms Are Neither Racist Nor Sexist | ITIF

The soundest alternative to banning FRT is adopting appropriate regulations mandating that only thoroughly-trained image analysis algorithms, meeting certain accuracy thresholds be utilized by law enforcement and that assessment by independent testers be funded to ensure continuous improvement of the technology so that only the most effective tools are deployed in the field.

Reference(s):

- https://www2.montgomerycountymd.gov/mcgportalapps/Press_Detail_Pol.aspx?Item_ID=31818
- Motorola Solutions, Facial Recognition Technology, Advancing Public Safety Capabilities, 2021
- https://www.securityindustry.org/2021/07/23/what-science-really-says-about-facial-recognition-accuracy-and-bias-concerns/
- https://www.ibia.org/download/datasets/5124/NIST%20Report%20on%20Facial%20Recognition-%20A%20Game%20Changer.pdf
- https://pages.nist.gov/frvt/reports/11/frvt_11_report.pdf
- https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8280.pdf#page=6

Myth:

FRT lends itself to use for certain types of offenses more than others, such as crimes where there is a digital image of a suspect e.g., bank robberies, assaults, and theft on public transportation, burglary, identity theft, etc. The utilization of FRT will lead to over-enforcement of these types of crimes because of the increased opportunities available to leverage facial recognition technology's capabilities.

Reality:

While perhaps well-intentioned, assertions of this nature confuse general criminal justice reform initiatives that desire to see fewer people facing penalties for criminal activity, with the functional equivalent of hindering the police so they don't have the capability to investigate and solve more crime. In essence, this concern acknowledges that FRT works, but seeks to limit the frequency that people are arrested and prosecuted for crimes, and therefore introduced into the criminal justice system. Similar flawed logic is offered by suggesting FRT should only be used to investigate the most egregious crimes or in exigent situations.**Myth:**
Mandating that a search warrant be required for law enforcement to utilize FRT is an effective way to allow the technology to be used while maintaining some degree of oversight.

Reality:

Most successful law enforcement facial recognition programs rely, at least in part, on the utilization of arrest photos as an element of the image repository to check probe photos against. Law enforcement agencies or their partners are often not only the originator of the images but the custodian of them. Requiring law enforcement to obtain a search warrant before conducting an FRT query of these images is procedurally ambiguous. In essence, it necessitates that police departments serve search warrants on themselves or partner law enforcement agencies.

This practice is legally unnecessary and likely to hamper collaboration and/or delay critically important investigations, potentially jeopardizing public safety. Additionally, to obtain a search warrant, one must articulate specific things such as:

- A reasonable description of the person or place be searched and the items to be searched for;
- Facts constituting probable cause supporting the issuance of a warrant;
- And and explanation as to how the thing to be searched for constitutes evidence of the commission of the said offense.

The search warrant requirement would impose barriers to law enforcement agencies from accessing records owned by them, that would otherwise be made readily available to most members of the community upon request.

Myth:

Law enforcement's use of FRT will lead to the creation of digital databases that store unique biometric identifying information, which will be vulnerable to data breaches or misuse.

Reality:

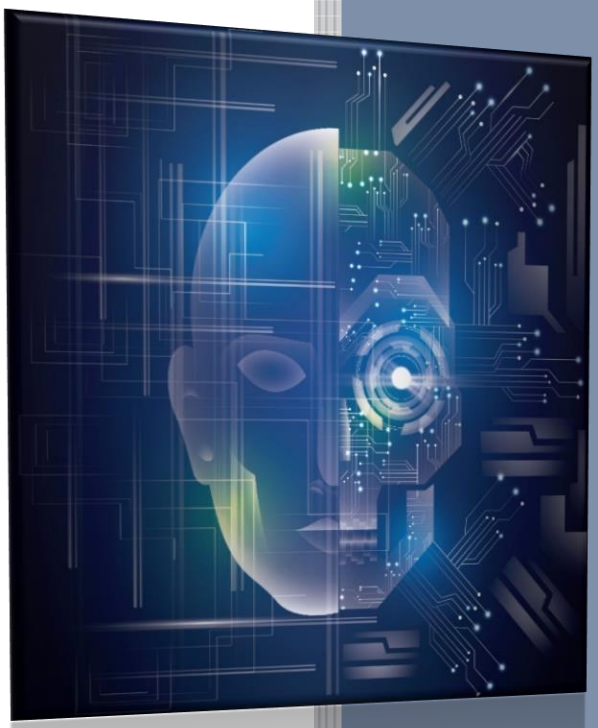
FRT, like any other government database, must rely upon best practices for cyber-security and all users must employ good cyber hygiene to safeguard systems. Most FRT programs do not involve the creation of new stand-alone platforms with unique cyber vulnerabilities. FRT programs are built on existing platforms akin to automated fingerprint systems or other electronic record management systems used by law enforcement.

Specific practices related to data governance, access, retention, and purging procedures are recommended for FRT programs including but not limited to:

- Dedicated role-based oversight of FRT programs to ensure compliance with applicable laws, regulations, standards, and policies related to data governance.
- Identification of an authorizing official to control access to the system and ensure that end-users meet all requirements required by law or articulated in policy prior to being given access.
- Utilizing credentialed, role-based access criteria with least privilege enforcement as appropriate, within all FRT platform access points.
- Ensuring that user accounts and associated authorizations are validated regularly and maintained in a secure "need-to-know" status - deleting any accounts found to be inactive.
- Enforcing the use of multi-factor authentication access controls.
- Ensuring protocols are followed to purge facial recognition data (including probe images) in accordance with an adopted retention policy.
- Conducting and documenting random audits to ensure user compliance and system functionality.
- Maintaining current, supported operating systems and frequently patching systems based on the manufacturer's recommendations to safeguard against new malware, viruses, and other vulnerabilities.
- Suspending or rescinding access if a user is found to be in non-compliance with cyber policies.

IJIS Institute

LAW ENFORCEMENT FACIAL RECOGNITION USE CASE CATALOG



Law Enforcement Imaging Technology Task Force

A joint effort of the IJIS Institute and the International Association of Chiefs of Police

March 2019

ACKNOWLEDGEMENTS

The IJIS Institute and the International Association of Chiefs of Police (IACP) would like to thank the following contributors for supporting the creation of this document:

Contributors

- Patrick Doyle – LEITTF Co-Chair and New Jersey State Police, Lieutenant (Ret.)
- Bonnie Locke – LEITTF Co-Chair and Nlets Business Development Director
- Jamie Algatt – Senior Product Manager, RapidDeploy USA
- Steve Ambrosini – Program Director, IJIS Institute
- Ben Bawden – Partner, Brooks Bawden Moore LLC Consultants
- Maria Cardiellos – Director of Operations, IJIS Institute
- Robert E. Greeves – Senior Policy Advisor, National Criminal Justice Association
- Pete Fagan – Virginia State Police, Lieutenant (Ret.)
- Jenner Holden – Chief Information Security Officer, Axon
- Robert May – Program Director, IJIS Institute
- James Medford – USAF Lt. Col. (Ret.)
- Catherine Miller – National Capital Region NCR-LInX Program Manager
- Dave Russell – Director, Northern Virginia Regional Identification System
- Pam Scanlon – IACP CJIS Committee Chair and Director, ARJIS/San Diego
- David M. Shipley – Executive Director, Colorado Information Sharing Consortium
- Robert Turner – President, CommSys Incorporated
- Gerald L. Ward, Ph.D. – MTG Management Consultants, LLC
- Heather Whitton – Cincinnati Police License Plate Reader Program Manager

EXECUTIVE SUMMARY

This Law Enforcement Facial Recognition Use Case Catalog is a joint effort by a Task Force comprised of IJIS Institute and International Association of Chiefs of Police. The document includes a brief description of how facial recognition works, followed by a short explanation of typical system use parameters. The main body of the catalog contains descriptions and examples of known law enforcement facial recognition use cases. A conclusion section completes this catalog, including four recommended actions for law enforcement leaders.

TABLE OF CONTENTS

FOREWARD

Police work is constantly adapting to an ever-changing environment, yet it has always been grounded in one simple, founding principle – to make the world a safer place.

To that end, law enforcement agencies, and other public safety entities must not only stay abreast of the latest tactics and technologies used by criminals, but also deploy every available method to maintain order, thwart wrongdoing, and ensure that those who threaten the peace are held accountable for their actions – all while respecting the rights of those involved.

However, new police technologies and procedures do not automatically coincide with new laws, rules, or policies governing their use. Their initial deployment can sometimes be misunderstood, and, in some cases, technological capabilities in the hands of law enforcement can exceed the public's comfort level. It can take some time before both citizens and the courts widely accept high-tech police tools. Such a learning curve and adjustment period has occurred with everything from issuance of police firearms to traffic radar speed monitoring devices.

What is unknown is often feared – or at least misunderstood – sometimes leading to overreactions and overreaching by policy makers. This response can limit the extraordinary new ways these advances can help ensure public safety.

Today, law enforcement is wrestling with similar issues in the case of facial recognition, which is sometimes referred to as facial analysis or face matching. Facial recognition is a remarkable development that helps law enforcement exonerate the innocent, narrow searches for the guilty, and otherwise maximize limited resources. Simply put, it greatly expedites certain police functions through the rapid comparison of one facial image to many others.

While the term *facial recognition* has become somewhat synonymous in the media and among other stakeholder groups to describe all uses of this technology, such systems used by law enforcement provide recognition of *potential* candidates, not recognition of *exact* matches as the name might insinuate. Law enforcement best practices for all known use cases still requires a human examiner to confirm that one of the computer-provided candidates matches the submitted image. The computer or software system does not make the final decision regarding an exact match when proper police procedures are being followed – a trained person does.

Public safety professionals use facial recognition in various ways to help them discover or find individuals, and to assist with the identification of people. But, because facial recognition uses the very personal and particular attributes within an image of the human face, it has a very private and individual connotation to it. The fact that it can help sort through great volumes of images, and that citizens aren't necessarily aware their own faces are in such comparative databases, only heighten the potential anxiety over the use of facial recognition technologies. These issues, , have created an environment where something as promising as facial recognition has the potential to be viewed as a problem itself, rather than an answer to one.

What appears to be immediately needed is a balanced and well-informed approach to facial recognition by law enforcement, which will help ensure public understanding of the way in which the technology is used by law enforcement, and to what end.

PURPOSE OF THIS CATALOG

The IJIS Institute and the International Association of Chiefs of Police (IACP) are both research entities and policy development bodies, but each has different core memberships. The combination of these two groups into a task force provides a multi-faceted perspective to technology issues. IJIS is a nonprofit alliance of industry representatives, technology developers, practitioners, national associations, and academic organizations, while IACP is comprised largely of justice leaders and law enforcement practitioners, the blend of experience and competencies between these organizations is a desired benefit in this catalog.

With a combined global membership of more than 31,000 , IJIS and IACP together have deep knowledge, academic prowess, and practical experience to investigate emerging issues and technologies. The organizations have created a joint research effort known as the Law Enforcement Imaging Technology Task Force (LEITTF) to review emerging trends and technologies such as facial recognition.

The LEITTF has created this document as a catalog of facial recognition use cases for criminal justice agencies, which includes uses by police officers, sheriff's deputies, investigators, and supporting personnel wherever they exist. This examination of uses covers typical settings wherever law enforcement interacts with persons such as large venues, transportation hubs, correctional facilities, motor vehicle stops, crime scenes, and other everyday situations.

The intention of this effort is to briefly describe facial recognition systems and their parameters, determine the ways in which facial recognition is being used, and, most importantly, to document cases which demonstrate the technology's ability to protect the public. The objective is to empower public safety practitioners and industry innovators to communicate the ability of facial recognition to policy makers and the public, while reducing misunderstanding and minimizing the potential for misuse.

The LEITTF has chosen to catalog and explain facial recognition use cases (as opposed to creating model policy, conducting a scientific analysis, or examining other elements of facial recognition) in order to fulfill an immediate need to improve visibility into how these systems are used. Providing real examples from the field further strengthens the context of facial recognition usage so that those outside of law enforcement can appreciate its necessity. It is hoped such details will help encourage outreach from police to concerned citizen groups and, in general, establish a better understanding of facial recognition. Describing the way in which facial recognition is successfully deployed should increase awareness and alleviate at least some of the public's concerns, and perhaps spur healthy discussion into the benefits of using this technology. As has been proven with every successful deployment of technology and law enforcement effort to combat crime, "you cannot police a community without effectively working with that community."[1]

HOW DOES FACIAL RECOGNITION WORK?

Facial recognition has been in limited use for many years. Recent improvements in system accuracy combined with higher demands for biometric identification capabilities have led to more widespread use in private industry such as corporate settings, with public and law enforcement use lagging slightly behind but certainly on the rise.

A typical facial recognition system uses the layout of a subject's facial features, and their relative distance from one another, for identification comparison against a separate image, or perhaps even against thousands or even millions of separate images in a database or gallery of faces. The subject's facial image attributes are derived from either a still or video image – physical presence is not always required.

Computer algorithms then measure the differences between the face being searched and the enrolled faces in a chosen gallery, such as a government database of images. The smaller the differences between the faces considered, the more likely those faces will be recognized and presented as potential matches. Through statistical analysis of the differences, a facial recognition system can provide a list of candidates from the gallery and rate the most likely matches to the image of the subject's face. Using suggested law enforcement best practices (see Summary Recommendation # 4), a trained face examiner would then make the final selection, potentially determining one of the candidates is very likely a match to the original submission. Of course, some facial recognition searches result in no high-probability match candidates. Even if the computer algorithm does return potential match candidates, it is possible, and, in fact, common, that the trained human examiner does not agree, nor does he or she select any candidate as a likely match.

Perhaps the most important element regarding the use of facial recognition by law enforcement is not within the technology itself, but what follows once the computer has suggested candidates and the human examiner determines a likely match exists in a particular case. It is at this point that the police have a strong clue, and nothing more, which must then be corroborated against other facts and investigative findings before a person can be determined to be the subject whose identity is being sought. Therefore, a candidate match, even after confirmation by a trained user, is, in most jurisdictions, not enough evidence for police to detain or arrest a person. All facts, and the totality of circumstances regarding the investigation or search, should be considered before any action is taken.

[1] William Bratton, former NYPD and Boston Police Commissioner, and LAPD Chief.

Facial Recognition Use Types

Facial recognition technology is broadly used in two different sorts of law enforcement situations:

Identify	It can help **identify** a subject face against a known image. For example, this would help confirm that a person's face matches to the digital image of a face embedded in a document presented to law enforcement, such as a passport. This is sometimes known as **one-to-one analysis**, since facial recognition is being asked to provide guidance on whether one submitted sample image is likely the same person as in another image. 
Discovery	Facial recognition technology can also help compare the image of a face to numerous known faces within an array or database. For example, this helps police use technology to suggest if a criminal or terrorist in a surveillance video or still image may match any mug shot photos of people previously arrested or convicted. This function is typically called **discovery** and is sometimes referred to as a **one-to-many analysis** since it seeks to compare one image to multiple other images to find candidates for potential matching. 

Facial Recognition System Parameters

There are several elements of a facial recognition system which are somewhat similar to other database-reliant technologies. For instance, digital fingerprint systems retain a repository of collected prints, and in many cases, newly submitted prints are often compared to those in the database to see if there are potential prints which may match the sample. It is also possible to compare one set of collected prints to another collected set or print, such as from a crime scene. Facial recognition is often used in similar ways – comparing one-to-one, or comparing-one-to-many. However, there are several distinct differences. For instance, facial recognition is currently somewhat unregulated by laws, policies, and practices regarding image capture, usage, retention, accuracy, and human oversight.

Also, face images can be collected much more easily than fingerprints, sometimes without the person knowing an image of their face has been captured. Most people that are fingerprinted have either consented to prints being taken or have been arrested and have no choice. Face images are sometimes collected with consent, such as with a driver's license photo, but an extended or implied consent over its future use in a repository is not usually given. In some cases, governments prohibit implied consent or do not allow the agency capturing the original photo to even ask for it.

However, in some regions, consent to capture the photo for one purpose does not always expressly prohibit its use by law enforcement. Therefore, some police agencies may use captured images without a person's implied consent.

These types of image captures, uses, and retentions, and the lack of consistent laws or rules throughout many states, provinces, territories, and countries, have helped cause misunderstandings and some resistance to facial recognition systems.

Facial recognition accuracy is also an unsettled discussion in many regions. This technology is without question much more efficient at scanning through large numbers of photos to find potential candidates than could be scanned by manual human comparison, but there are questions about whether the faster, technological approach can ever be 100% accurate.

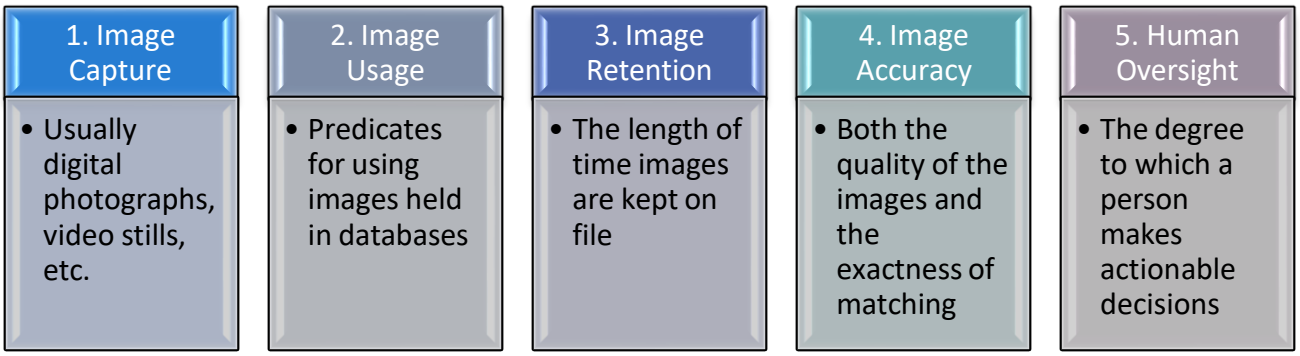
Some facial recognition research, such as the Georgetown Center for Privacy and Technology Report,[2] have widened the gap between supporters and detractors through suggestions that the systems are at least partially biased toward minorities, and because of such inherent risks, should only be used by police to find very serious criminals. Other recent studies, such as the latest reports by Massachusetts Institute of Technology's (MIT) Computer Science and Artificial Intelligence Lab[3] and IBM,[4] each suggest facial recognition bias can be mitigated through improvements in algorithmic structure, more racially inclusive data sets, and broader facial data point collection. Greater overall independent study is needed, and transparency regarding the results will be essential to maintain public confidence in the technology as the science is refined and fear is mitigated.

There are also media and watchdog group assertions that the technology is in some cases being used to single out a person based *only* upon a computer-driven algorithm's decision, without any significant amount of human oversight to the process. Many of these anecdotal complaints involve alleged use cases where denial of entry or services is the result, such as admission to a sports stadium, *not* detention, arrest or formal criminal prosecution. However, any alleged decision by law enforcement personnel reportedly made solely by facial recognition software, no matter how inconsequential the decision may seem, is alarming to some stakeholder groups. Media reports of this alleged facial recognition usage certainly have stirred criticism, which is also to some degree fueled by reported accuracy improvements made by technology providers. Some media reports allege law enforcement agencies are relying on greater system accuracy to select matching candidates, and less on trained facial recognition human examiners. However, police agencies can avoid such criticism by ensuring facial recognition systems are supported by strong policy, training standards, and human oversight, regardless of increasing accuracy, especially when criminal investigations are being conducted or other impactful actions may be taken which affect the public.

[2] Georgetown Law School Center for Privacy and Technology Report, *The Perpetual Line-Up*, October 2016 https://www.perpetuallineup.org/.
[3] Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory Study, *Uncovering and Mitigating Algorithmic Bias Through Learned Latent Structure*, January 2019, http://www.aies-conference.com/wp-content/papers/main/AIES-19_paper_220.pdf.
[4] IBM Corporation, *Diversity in Faces Study*, January 2019, https://www.ibm.com/blogs/research/2019/01/diversity-in-faces/.

Typical Elements of Facial Recognition System Deployments

Facial recognition systems generally involve five significant elements or activities:



These five aspects each have important variables, leading to potentially different best practices, policies, laws, limitations, and concerns depending on the exact use cases.

Here are the five system aspects listed again, with potential questions about usage parameters following each that law enforcement users may be asked and be prepared to answer:

Image Capture	Who captured the image? When was it captured? How was it captured? Why was it captured? Was consent given to capture it?
Image Usage	Who will use the image? When will it be used? How will it be used? Why will it be used? Will consent be given each time it is used?
Image Retention	Who has the right to retain the image? When do they have the right to retain it? How will it be retained? How long will it be retained?
Image Accuracy	Are image quality, capture, and comparison methods standardized? Are both sample and gallery images similarly standardized? Are accuracy errors random or patterned by sex, race, skin color, affliction, style choices, image accuracy, etc.?
Human Oversight	Are trained examiners the ultimate decision makers? Are examiners trained to certain standards? How often?

Some of these questions may each be answered differently, depending on how facial recognition is being used at the moment, and under what pretenses, and by which type of agency. That is why this catalog presents the following actual known law enforcement use cases of facial recognition systems. These use cases should provide context as to why the public's opinion of this technology may be quite different depending on the actual circumstances of its use and may further depend on the timing of such police use within the justice continuum. What is publicly acceptable for law enforcement to use when detaining known criminals or investigating crimes may not be tolerable for those situations where police are conducting broad surveillance, or routinely patrolling neighborhoods. Examination of law enforcement facial recognition uses cases may help both the police and the public come to terms with how this technology is, and should be, deployed.

USE CASES

Police officers are generally very adaptive and ingenious. The nature of protecting the public usually requires quick-thinking, and the use of things which may go beyond their original intended design is sometimes a necessity.

Such is the case with facial recognition, which was originally intended as a specific investigative tool to help narrow the field of suspects down to a manageable amount. However, law enforcement professionals quickly learned to deploy it as a means of exonerating the falsely accused, identifying the mentally ill, helping return children to their parents, and determining the identity of deceased persons, in addition to other innovative uses.

This Task Force found 19 known uses of facial recognition for law enforcement.
These uses involve both overt, and covert, facial image capture and observation techniques.

Law Enforcement Facial Recognition Use Case Categories

The different ways in which this technology is being used generally fit into three different groupings, based upon the activity or required tasks of the law enforcement professional using facial recognition:

1. Field Use
2. Investigative Use
3. Custodial and Supervisory Use

Many of the 19 uses can also be performed with two distinctly different intentions:

- **Discovery** – helping to find one person among many persons
  (One-to-Many Comparison)
- **Identification** – helping to verify one person is in fact the person being helped or sought
  (One-to-One Comparison)

The database of comparative photos use in each use case can also differ. For example, some law enforcement agencies may use images from public sources (such as department of corrections records) to compare with a recently captured image of a suspect. Other police departments may also use, with appropriate legal authority, a privately-owned gallery, such as one maintained by a sports venue security firm, which, for example, may have been created from video surveillance or ticket-use photo identification databases.

Therefore, each use case may have several variables, such as the intended outcome to either *discover* a person, or *identify* a person, plus be conducted using comparison to either public and private sources of photos, or both, and at different points in an investigation or inquiry into a matter brought to the attention of police, Figure 1.

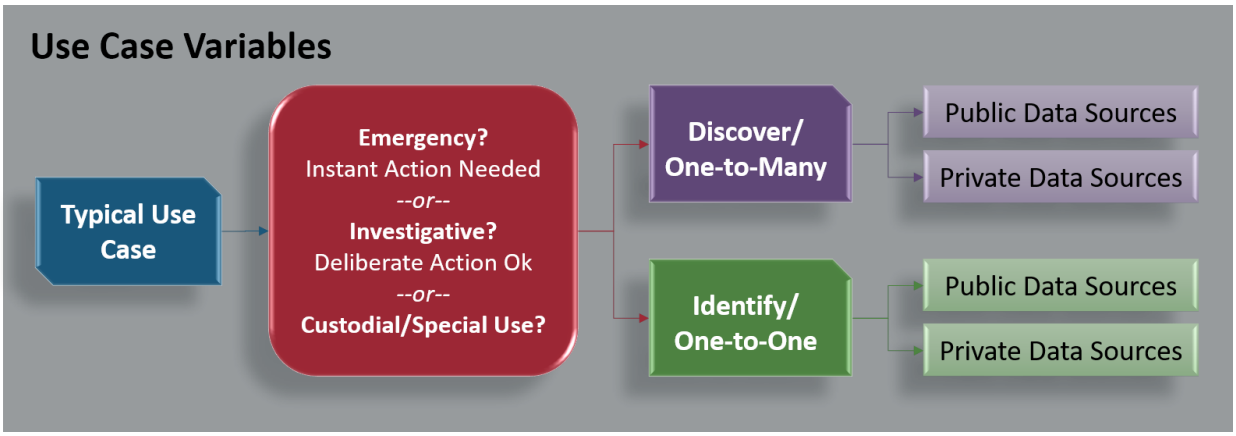


Figure 1

In the following use case descriptions, actual instances or example scenarios follow each use case to further clarify the ways in which facial recognition may be used by law enforcement.

Field Use

The following situations generally occur where an officer uses facial recognition to help positively identify an individual during a face-to-face interaction, or during some other active, uniformed-police response to an incident.

Random Field Interaction

An officer on patrol in the field may be alerted that an individual's image actively captured on an operating in-car or body worn camera may be a possible candidate for a match to a subject in a wanted persons image database.

Example Scenario

Police officers assigned to foot patrol in a business district may be required to operate their body worn cameras during all substantive interactions with the public. During such patrol duties they are often interact with citizens at which time face images captured via activated body worn camera footage may be compared in near real time to a criminal warrants database of fugitive images.

Reasonable Suspicion Interaction

An officer may be alerted to unusual or furtive activity by a person, which presents reasonable suspicion to capture an image of the individual to protect the officer's safety, or to potentially explain the suspicious activity.

Actual Instance - Fugitive Apprehended

In January 2017, an officer assigned to a fugitive task force observed a transient male that matched the description of a known wanted subject. The male was uncooperative and refused to identify himself. The officer captured a photograph of the subject and used facial recognition as one tool to help identify him. The officer then queried NCIC and was informed that the subject had an active felony warrant. He was booked and the case was closed.[5]

Active Incident

During an active criminal situation, video or pictures obtained by officers could be used to potentially help identify individuals and guide active response efforts.

Example Scenario

A situation might occur where a field officer records video of a person's face, such as with an in-car or body worn camera system, and the person then flees the scene of the encounter. Facial recognition could be used to compare the recorded image of the person's face against a database to help determine who the person might be, or why they fled.

Deceased Identification

Deceased individuals can be more quickly identified in the field with facial recognition systems providing possible matched images to a captured imaged of the victim.

Actual Instance - Facial Recognition Used to ID murder victim

Police received a 9-1-1 call of a male subject lying in the street. Officers arrived and located an obviously deceased adult male victim in the roadway. There was evidence of trauma to the victim's body and it would eventually be learned that a homicide had occurred. The victim did not appear to possess any identification and responding detectives were initially unable to identify the subject. A photograph was taken at the crime scene and submitted through a facial recognition program. Within minutes, a candidate photograph was returned, helping to identify the victim as 21-year-old male. This identification was corroborated by other facts obtained in the early stages of the investigation. The speedy identification of the unknown victim in this case was a huge benefit, making it possible for timely notification to the family, and moving the investigation forward towards its eventual resolution through the arrest of two suspects.[6]

[5]Automated Regional Justice Information System, San Diego, California.
[6]Automated Regional Justice Information System, San Diego, California.

Lost & Missing

Lost children or missing adults could be located and identified when encountered by officers during interactions, whereby facial recognition is used to help provide clues to determine identity.

Example Scenario

A situation might occur where a field officer encounters a lost child or disoriented adult and captures an image of the person's face for comparison with a database of lost or missing persons to help identify them.

Interdiction

An individual of interest who is actively avoiding identification can potentially be located at a checkpoint, with facial recognition providing clues for officers to investigate.

Actual Instance - Illegal Alien Attempts Entry

In August 2018, a 26-year-old man traveling from Brazil entered Washington Dulles International Airport and presented agents with a French passport. Agents used facial recognition to compare his passport photo to a database of known images with identities and were alerted that the man's photo might not be a match to his stated identity. The man became nervous when agents referred him for a secondary search. The agents discovered the man's real identification card in his shoe, and it was revealed he hailed from the Republic of Congo. Charges are pending.[7]

Identify Fraud

Incidents often occur where a person presents identification documents to fraudulently obtain access or services, benefits, or credit privileges, and facial recognition can be used to alert officers to possible mismatches.

Actual Instance - Credit Card Fraud

An unknown female pictured in surveillance photos entered a costume store attempting to purchase multiple wigs with a credit card that was stolen from a vehicle earlier in the day. The transactions could not be completed as the cardholder had already canceled the stolen cards. At this time, it is unknown whether the pictured female was also involved in the vehicle trespass. The female was described as having a heavier-set build and dark, shoulder length hair. Checking the surveillance photos against a correctional mug shot database with the agency's facial recognition application revealed the identity of a high-probability candidate, who is now under investigation for use of the stolen credit card.[8]

Actual Instance – Retail Fraud

On March 5, 2018, investigators opened a case involving fraud and the use of counterfeit traveler's checks ranging from $5,000 to $20,000 in multiple jurisdictions. A male and female

[7]United States Customs and Border Protection.
[8]Arapahoe County, Colorado Sheriff's Department.

suspect had opened a membership at a Costco and began using the checks as payment. The investigating agency submitted the new member photos to a facial recognition application and investigators were able to locate candidates in the system and eventually confirm the identities of both suspects. Charges are pending.[9]

Actual Instance - Retail Fraud and Theft

Around April 13, 2018, investigators received an Asset Protection Alert from a local Home Depot not in their jurisdiction. The suspects in these cases have stolen over $5,000.00 in tools from Home Depot stores in nine separate cases and five different stores. The investigator used the agency facial recognition application to compare surveillance photos of the suspect with photos from a correctional mug shot database. The application returned a high-probability candidate now under investigation by Home Depot retail crime investigators and local authorities. Charges are pending.[10]

Actual Instance - Retail Fraud

On June 20, 2018, investigators received a bulletin advising that a suspect has committed two high-dollar thefts at The Home Depot. The suspect was targeting Milwaukee power tools. Total loss for the two cases $1,097.00. Surveillance photographs were entered into the agency's facial recognition application used to search the correctional mug shot database. The application identified two high-probability candidates that additional investigation confirmed were the involved suspects and resulted in recovery of the stolen tools and pending charges.[11]

Investigative

The following use cases generally involve law enforcement using facial recognition technologies to assist in solving crimes, such as use to gather evidence or aid in investigations.

Active Incident

During an active criminal situation, surveillance video can be used to provide images of suspicious persons which may help to identify suspects or witnesses, thereby guiding active response efforts.

Example Scenario

A situation might occur where a terrorist attack is made, and surveillance video of the area prior to the event is obtained. Images of suspicious persons in the video can be entered into other monitoring systems, which can then search for potential matches among other video feeds.

[9]Arapahoe County, Colorado Sheriff's Department.
[10]Arapahoe County, Colorado Sheriff's Department.
[11]Arapahoe County, Colorado Sheriff's Department.

Photo Array Construction

The creation of photo arrays can be automated using an existing suspect photo along with other biometrics information to find similar photos, thereby creating a photo array to be shown to a witness or victim for suspect identification.

Actual Instance - Armed Robbery Suspect Apprehended

An Indiana detective used facial recognition software to help identify a convicted serial robber as the alleged stickup man of a payday loan business. The business' cashiers told police the suspect ran around the counter and flashed a firearm before ordering them to empty two cash registers. Records show that the suspect ordered a cashier to open the store's safe but fled after he noticed a customer walking out of the business on her cellphone. The suspect's face was visible on the store's surveillance footage. Police released footage of the suspect the week after the robbery, but no leads were developed.

A detective then turned to the department's facial recognition software and put a photo of the suspect from the surveillance footage into the system which came up as a possible match. The detective showed the cashiers a photo array, which included the suspect's photo, and they identified him as the robber. The suspect had absconded from parole earlier in Illinois after serving part of a 12-year prison sentence for a string of armed robberies in the northwest Chicago suburbs, according to Illinois Department of Corrections records. He had committed nine robberies over the course of the prior 7 years.[12]

Actual Instance - Sexual Assault Suspect Apprehended

A 15-year old girl was sexually assaulted by an adult male she met online. The girl was only able to provide suspect personal information from his online profile but had also obviously met him in person, so she was familiar with what he looked like in real life and had access to online images of him. Police were able to use facial recognition on one of the digital images, which when compared to DMV photos, provided some candidates from which the girl was able to select a match. Authorities obtained a search warrant for the home of the identified suspect, who later admitted to the crime.[13]

Evidence Compilation

Photos of a known suspect can be used to search across existing traditional photo databases, or even situation-specific databases created from voluntary submissions, surveillance videos, or social media, yielding possible candidates which may match the suspect.

Actual Instance – Jewelry Thief Apprehended Via CrimeStoppers Comparison

On November 3, 2017, an unknown subject was caught on surveillance video at a Jeweler store, taking control over eight gold rings worth $2,000. The Hamilton County Sheriff's Office was asked to assist with the investigation and was in the process of testing its new facial recognition system. Deputies decided to use the jewelry investigation request as a training exercise. They used to publicly-submit CrimeStoppers photos to learn how to analyze the jewelry suspect image

[12]Munster, Indiana Police Department.
[13]Scranton, Pennsylvania Police Department.

to a candidate pool of images and were surprised that after just a dozen or so photos were compared, a strong candidate for a match was found. Detectives took this legitimate lead and started working with investigators from the jurisdiction where the CrimeStoppers submission was made, piecing together the true identity of the suspect. The thief's identity was determined, and he was located and arrested for the jewelry theft, the CrimeStoppers Case and four other outstanding felony warrants.[14]

Actual Instance - Social Media Photo Helps Identify Suspect

A woman was victimized by a stranger whom she met on a dating website. The perpetrator's name and other personal information on his social network page were intentionally deceptive, but the photograph was genuine because his intent was to eventually meet the victim in person. Biometric search of the dating website profile photograph produced a possible match, which after further investigation, led to an arrest.[15]

Actual Instance - Suspect Misidentifies Sex to Avoid Arrest

A police officer used a facial recognition application to help identify a girl who was pretending to be a guy (Justin) instead of a female (Jamie), all to avoid being arrested on a warrant. No record came up on names and DOBs. Field officers used the available facial recognition application by snapping a photo of her in disguise and comparing it to the 4+ million booking photographs in the system. The suspect's FEMALE photograph returned as the #3 candidate. Immediate action on the returned information exposed the disguise and resulted in an arrest.[16]

Actual Instance - Shooting Suspect Identified

On October 17, 2018, a suspect identified by a witness as a tattoo artist and recently-released inmate, known only by the monikers Dough Boy *or* Dough Blow*, shot and seriously injured another person. Using information developed through a bulletin and photos from social media posts made by the suspect, the agency facial recognition application returned a high-probability candidate from a mug shot database. Further investigation revealed a high-probability candidate that the continuing investigation confirmed as the suspect in the shooting. The investigation continues.*[17]

Participant Party Identification

Facial recognition can be used to help confirm a witness, victim, or perpetrator was at a specific crime scene, or associates with a specific suspect or group.

Actual Instance – CCTV Helps Confirm Suspect was at Crime Scene

A crime occurred in view of a local CCTV camera system, and recorded video captured an image of a potential perpetrator's face. Facial recognition was used to compare the image to a photo database, which produced two potential suspects. Further investigation by detectives

[14] Springfield Twp. Police and Hamilton County Sheriff's Office, Ohio.
[15] Safran MorphoTrust Corporation.
[16] Lakewood, Colorado Police Department/Colorado Information Sharing Consortium.
[17] Denver, Colorado Police Department.

in the field helped confirm one of the suspects was at the scene, ultimately leading to his arrest for the crime.[18]

Victims Identification

Facial recognition can assist in potentially identifying victims of crimes, in situations where traditional methods of identification are not available.

Example Scenario

A situation might occur where a victim of a crime appears in a videotape or photograph, such as with a teenager being used in sexually explicit materials, but no report of crime is made to police by the victim or his/her guardians. The image of the victim can be used to search available databases for potentials candidates to be identified.

Criminal Identification

During the monitoring of high risk transit locations, areas of persistent criminal activity or other high-risk locations, images of known wanted persons can be compared against images captured on surveillance video to help locate potential matches.

Example Scenario

A situation might occur where a defiant trespasser or registered sex offender is not allowed on certain public properties, such as playgrounds or schools, because of prior criminal convictions. Facial recognition could be used to monitor surveillance video for potential candidates who might match the identity of the prohibited person.

Suspect or Associate Identification

Facial recognition can be used to acquire images and potentially help identify existing or new subjects of investigations or assist in exoneration of suspects.

Actual Instance - Smart Phone Digital Photo Comparison Exonerates Suspect

A witness in a gang-related assault case provided smartphone photos of the suspects to the detective working the case. One of the photos of a suspect was able to be run using facial recognition software and an investigative lead was developed. Upon further investigation confirmation of the suspect's name was made and during the investigation it was found that the suspect was in jail in another location at the time of the crime. Verification of the suspect was made based on the photo of him and the tattoos on his arm. Apparently, the witness provided an incorrect photo of one of the suspects and the facial recognition system, along with further investigation, saved investigators time, and more importantly, saved the individual from being arrested for a case in which he was not involved.[19]

[18] Safran MorphoTrust Corporation.
[19] United States National Capital Region Facial Analysis Pilot Test Project.

Actual Instance - Homicide Suspect Identified

In April of 2018, Edgewater, Colorado, Police had a shooting death resulting from an attempted random street robbery and at the onset of the investigation had no suspect information or leads. From leads that were eventually put together, police were able to identify a suspect vehicle which was impounded. A receipt to a 7-Eleven was found in the vehicle and grainy footage from the store video system was obtained showing the suspects inside the store approximately one hour after the homicide. Three of the four parties seen in the video were identified by traditional means and subsequently arrested.

A fourth suspect/witness was seen but detectives were unable to identify her. With Wheat Ridge Police help, detectives used a facial recognition program to help identify and locate this female. This person ended up being in the car at the time of the homicide and was able to tell us exactly what happened the night of the homicide, who pulled the trigger and what other roles other people inside the vehicle played.

During subsequent follow up, the suspects made incriminating statements to multiple people on Facebook about the homicide. Detectives used the facial recognition program to help identify pictures of people found on their Facebook profiles since nobody uses their real name.[20]

Actual Instance - Theft Case Solved

An investigator had a theft case where the victim met the suspect for a date. When she went to the restroom, he stole her wallet. The only thing she knew about him was his first name. She had downloaded a picture of him on her phone. The agency's facial recognition application and the statewide mug shot database, identified a high-probability candidate, returning both identity information and extensive arrest information. The detective used the application's photo lineup feature, showed it to the victim and she recognized the identified candidate immediately. Charges are pending.[21]

Actual Instance - Carjacking Suspects Found

Two men attempted a robbery of a woman in the parking lot of a liquor store. The woman bravely fought off attempts to have her wallet and car taken, and the men fled. The store owner provided surveillance video of one of the men, who had entered the store to make a small purchase while stalking the victim. The video provided an image of the suspect, which was compared to a correctional photo database, revealing potential suspect candidates. Further investigation led to the apprehension of both the man in the video and his accomplice brother.[22]

Custodial & Supervisory

The following use cases use facial recognition technologies to potentially identify and track candidates as part of efficiently operating criminal justice system programs.

[20] Edgewater, Colorado Police Department.
[21] Arapahoe County, Colorado Sheriff's Department.
[22] Greenville County, South Carolina Sheriff's Department.

Admittance Identification

Facial recognition can be used to help authenticate the identity of arrested persons being booked into detention.

Example Scenario

A person arrested by a police officer for a crime might refuse to identify themselves. The suspect is often brought to a correctional facility. Booking officers usually obtain a photo upon processing, thereby comparing it to existing photos on file to potentially positively identify the suspect.

Access Control & Movement

Identity verification of inmates or other persons can be aided via facial recognition, helping to control access to certain areas of a detention facility, or assist in confirming identity before receiving medication, privileges, or access to items restricted to other inmates.

Example Scenario

A correctional facility controls access to certain privileged areas and needs to ensure inmates required to present themselves for certain actions are properly identified. Officers can use facial recognition to corroborate with other means of identification, such as ID bracelets, RFID devices, and other biometric indicators.

Identification for Release

Confirming an inmate's identity prior to approved temporary or permanent release can be aided by facial recognition.

Example Scenario

A correctional institution obviously needs to control egress from its facility. Facial recognition can be used to help ensure an inmate presenting him or herself for work furlough, or release at the end of their sentence, is in fact the prisoner which should be allowed to leave the facility.

Identification for Program Participation

Facial recognition can be used to help confirm identity for special program participation, such as parole, probation, or sex offender registry.

Example Scenario

A parole or probation officer may be required to positively identify a person presenting himself for a urine test or mandated parole check-in visit. Facial recognition may be used to help establish a positive identity in concert with other biometric systems or identification processes.

Court Appearances

Identification of a court defendant or witness can be further corroborated using facial recognition.

Example Scenario

A judge may order a defendant appearing before her positively identified, especially in cases of identity fraud, exact twins or undocumented aliens with no official government identification. Court officers could use facial recognition to assist in the positive identity of the person by comparing the person's face with available databases.

CONCLUSION

Technologies like facial recognition systems are essential to help police maintain order in the modern world. However, their success as an effective tool for law enforcement are dependent upon ensuring that they are properly deployed and used. Additionally, law enforcement agencies must work closely with the communities to explain their use, educate the public on the capabilities, and demonstrate how the use of facial recognition technology will benefit public safety.

Recommendation #1: Fully Inform the Public

Law enforcement should endeavor to completely engage in public dialogue regarding purpose-driven facial recognition use, including how it operates, when and how images are taken and retained, and the situations in which it is used.

With facial recognition systems, the most powerful aspect is its use to compare as many images as possible in a short amount of time. It helps automate a laborious manual process to aid in many public safety efforts. Therefore, maximizing lawful and accepted use of images should be paramount, and providing the public with confidence that such capture and comparison are done fairly will ultimately ensure the most successful use of facial recognition.

[23] This idiom is widely attributed to an unknown contributing author of the National Convention Decrees during the French Revolution, May 8, 1793

[24] Sir Robert Peel, British Statesman and founder of the London Metropolitan Police in 1829.

Recommendation #2: Establish Use Parameters

Appropriate system use conditions, even preliminary ones, must be established as soon as possible to engender public confidence it its use and avoid any further proliferation of mistrust.

The use cases within this document demonstrate the varied ways in which this one technology can be deployed into many aspects of public safety. No doubt more uses will arise over time, bringing facial recognition systems to bear against all manner of crime, and on behalf of many victims, just as fingerprinting and DNA matching have done in the past.

The real cases presented are but a small sampling of the numerous success stories, many exonerating the wrongly accused as well as bringing the correct criminal to justice. It is hoped that more cases will be brought to light through enlightening discussions such as those this document attempts to create.

Recommendation #3: Publicize its Effectiveness

All public safety agencies should widely publish facial recognition success stories to heighten overall awareness of its usefulness, especially those cases in which suspects are exonerated, or where facial recognition is used to protect vulnerable persons.

This description of facial recognition systems and the ways in which it is being used by police is a starting point. While it is most often used to apprehend criminals, it is also used to find missing children, identify deceased persons and help prevent the innocent from being accused. Through consideration of the identified issues and these use cases, human reference points will be created so that the technology's interactions with citizens will be less mysterious and more appreciated for the service if provides. It is also hoped that by outlining how it is used throughout law enforcement, it will help stimulate needed conversation, policy creation and baseline training standards that can be tailored to each use within accepted community tolerances.

Recommendation #4: Create Best Practice Principles and Policies

Model law enforcement facial recognition guidance and regulation documents should be immediately established and broadly adopted, to include training benchmarks, privacy standards, human examiner requirements, and anti-bias safeguards.

Initial training and periodic re-training certifications are required as a part of most law enforcement technologies, and facial recognition seems to need such best practice standards to ensure both the courts and the public have a confidence in its consistent, fair use. Only after a broader public and judicial acceptance of facial recognition is created and stabilized can it then realize its full potential in becoming one of the most efficient and amazing law enforcement tools every deployed.

None of this catalog's representations, nor its recommendations will be constants – things change at a record pace these days, and so too must the ways in which we view and regulate ourselves as well as our machines. However, the use cases presented, and the suggestions within this report to improve the standing of facial recognition, should be immediately useful to help get this technology back on a positive trajectory.

The LEITTF believes strongly in facial recognition abilities and reasonable use conditions, and highly recommends enlisting the public more directly to generate wide support for our collective mission – to make the world a safer place.

RESOURCES

For more information about facial recognition technologies and opposition to it:

❖ IACP Technology Policy Framework	https://www.theiacp.org/sites/default/files/all/i-j/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf
❖ City of Palo Alto Surveillance Technology Ordinance	https://www.cityofpaloalto.org/civicax/filebank/documents/66597
❖ U.S. Bureau of Justice Assistance Policy Development Template	https://www.bja.gov/Publications/Face-Recognition-Policy-Development-Template-508-compliant.pdf
❖ Georgetown Center for Privacy & Technology Face Recognition Use Policy	https://www.perpetuallineup.org/appendix/model-police-use-policy
❖ Electronic Frontier Foundation Police Uses of Facial Recognition	https://www.eff.org/wp/law-enforcement-use-face-recognition

❖ Cardiff University Evaluation of Police Facial Recognition Use Cases	https://crimeandsecurity.org/feed/afr
❖ ACLU Report on Test Use of Facial Recognition at U.S. Capitol	https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28
❖ Michigan State University Case Study of Facial Recognition Use in Boston Bombing Investigation	http://biometrics.cse.msu.edu/Publications/Face/KlontzJain_CaseStudyUnconstrainedFacialRecognition_BostonMarathonBombimgSuspects.pdf
❖ Draft Facial Recognition Policy (James Medford, USAF Lt. Col. (Ret.)	https://drive.google.com/open?id=1BzKrSo-kLUV8uI88gwUm_1Du3ewePwVZ

REFERENCES

Georgetown University Law School Center for Privacy and Technology Report, *The Perpetual Line-Up*, October 2016, https://www.perpetuallineup.org/.

Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory Study, *Uncovering and Mitigating Algorithmic Bias Through Learned Latent Structure*, January 2019, http://www.aies-conference.com/wp-content/papers/main/AIES-19_paper_220.pdf.

IBM Corporation, *Diversity in Faces Study*, January 2019, https://www.ibm.com/blogs/research/2019/01/diversity-in-faces/.

ABOUT THE IJIS INSTITUTE

The IJIS Institute is a nonprofit alliance working to promote and enable technology in the public sector and expand the use of information to maximize safety, efficiency, and productivity.

The IJIS Institute has members and associates working within and across several major public-sector domains as our areas of focus:

- Criminal Justice (Law Enforcement, Corrections, Courts)
- Public Safety (Fire, EMS, Emergency Management)
- Homeland Security
- Health and Human Services
- Transportation

IJIS Institute is the only national membership organization that brings together the innovative thinking of the private sector and the practitioners, national practice associations, and academic organizations that are working to solve public sector information and technology challenges. IJIS Institute advocates for policies, processes, and information sharing standards that impact our safety and security, builds knowledge on behalf of our stakeholder groups, and connects the organizations and leaders within the communities of interest.

The IJIS Institute provides a trusted forum within and across our areas of focus where resources are developed, collaboration is encouraged, and public-sector stakeholders can realize the benefits of technology and the power of information to keep our communities safe, healthy, and thriving.

Founded in 2001 as a 501(c) (3) nonprofit corporation with a national headquarters in Ashburn, Virginia, the IJIS Institute has grown to nearly 400 member companies and individual associates from government, nonprofit, and educational institutions from across the United States.

The IJIS Institute thanks the Law Enforcement Imaging Technology Task Force for their work on this document. The IJIS Institute also thanks the many companies who have joined as Members that contribute to the work of the Institute and share in our mission to drive public-sector technology innovation and empower information sharing to promote safer and healthier communities. For more information on the IJIS Institute, visit our website at http://www.ijis.org/.

ABOUT THE INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE

The International Association of Chiefs of Police (IACP) is the world's largest and most influential professional association for police leaders. With more than 30,000 members in over 150 countries, the IACP is a recognized leader in global policing. Since 1893, the association has been speaking out on behalf of law enforcement and advancing leadership and professionalism in policing worldwide.

The IACP is known for its commitment to shaping the future of the police profession. Through timely research, programming, and unparalleled training opportunities, the IACP is preparing current and emerging police leaders—and the agencies and communities they serve—to succeed in addressing the most pressing issues, threats, and challenges of the day.

The IACP is a not-for-profit 501c(3) organization headquartered in Alexandria, Virginia. The IACP is the publisher of The Police Chief magazine, the leading periodical for law enforcement executives, and the host of the IACP Annual Conference, the largest police educational and technology exposition in the world. IACP membership is open to law enforcement professionals of all ranks, as well as non-sworn leaders across the criminal justice system. Learn more about the IACP at www.theIACP.org.

About the Law Enforcement Imaging Technology Task Force

The Law Enforcement Imaging Technology Task Force was formed in 2015 as a joint project of the IJIS Institute and the International Association of Chiefs of Police (IACP). This Task Force was created to study new imaging software, devices, and methods as a means of ensuring successful, principled, and sustainable use which is both supported by citizen and aligned with the ultimate mission – to improve public safety.

Federal Law Enforcement Use of Facial Recognition Technology

October 27, 2020

Congressional Research Service
https://crsreports.congress.gov
R46586

CRS REPORT
Prepared for Members and
Committees of Congress

Congressional Research Service
Informing the legislative debate since 1914

Federal Law Enforcement Use of Facial Recognition Technology

SUMMARY

Law enforcement agencies' use of facial recognition technology (FRT), while not a new practice, has received increased attention from policymakers and the public. Some of the concerns raised revolve around the accuracy of the technology, including potential race-, gender-, and age-related biases; the process of collecting, retaining, and securing images contained in various facial recognition databases; public notification of the use of facial recognition and other image-capturing technology; and policies or standards governing law enforcement agencies' use of the technology. Some of these concerns have manifested in actions such as federal, state, and city efforts to prohibit or bound law enforcement agencies' use of FRT. In addition, some companies producing facial recognition software have placed new barriers to law enforcement using their technologies.

FRT is one of several biometric technologies employed by law enforcement agencies, which also include fingerprint, palm print, DNA, and iris scans. FRT can be used by law enforcement for a variety of purposes such as generating investigative leads, identifying victims of crimes, helping sort faces in photos that are part of forensic evidence, and helping verify the identity of inmates before they are released from prison. However, the frequency and extent to which FRT is used at various phases of the criminal justice system is unknown. It is most often discussed by law enforcement officials as being used to help identify suspects.

R46586

October 27, 2020

Kristin Finklea, Coordinator
Specialist in Domestic Security

Laurie A. Harris
Analyst in Science and Technology Policy

Abigail F. Kolker
Analyst in Immigration Policy

John F. Sargent Jr.
Specialist in Science and Technology Policy

The Federal Bureau of Investigation (FBI) is a leading federal law enforcement agency in the use of FRT. The bureau operates two programs that support the use of the technology: (1) the Next Generation Identification–Interstate Photo System (NGI-IPS), largely supporting state and local law enforcement; and (2) the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit, supporting FBI investigations. NGI-IPS contains criminal mugshots, and the system allows authorized law enforcement users (primarily state and local) to search the database for potential investigative leads. The FACE Services Unit supports FBI investigations by searching *probe* photos of unknown persons against faces in NGI-IPS and other federal and state facial recognition systems authorized for FBI use. A facial recognition search alone does not provide law enforcement with a positive identification; the results need to be manually reviewed and compared by an officer trained in facial comparison. Further, law enforcement agencies are prohibited from relying solely on the results of a search in NGI-IPS to take a law enforcement action (e.g., making an arrest). The FBI maintains an NGI Policy and Implementation Guide that outlines policies surrounding use of NGI-IPS. Authorized law enforcement users of NGI-IPS are required to follow these policies as well as established standards for performing facial comparison.

While FRT is generally used by law enforcement agencies to help generate potential investigative leads, it is also employed by U.S. border enforcement officials to assist with verifying travelers' identities. The Department of Homeland Security (DHS) and Customs and Border Protection (CBP) use the Traveler Verification Service (TVS). TVS compares the travelers' *live photographs* (taken, for example, by a gate agent) to a gallery of photographs and provides a *match* or *no match* result; a no match results in a manual check by an official to verify a traveler's identity.

Guidelines and recommendations regarding law enforcement use of FRT have been produced by the Facial Identification Scientific Working Group (FISWG). FISWG is one of the various scientific working groups that support the Organization of Scientific Area Committees for Forensic Science (administered by the National Institute of Standards and Technology, which facilitates standards development, including for FRT). FISWG has published a number of FRT-related documents for forensic science practitioners. For instance, they have guidelines and recommendations for establishing and conducting training on facial comparison, guides for capturing facial images that can be used in facial recognition systems, and recommended methods and techniques for using facial recognition systems.

As policymakers consider legislation and oversight on law enforcement agencies' use of FRT, they may evaluate how the accuracy of these systems is defined and assessed by law enforcement; how to support or restrict the technology's use by federal, state, and local law enforcement—and potential implications; and how to balance privacy and security concerns with supporting lawful criminal justice activities.

Contents

Appendixes

Contacts

Law enforcement agencies' use of facial recognition technology (FRT), while not a new practice, has received increased attention from policymakers and the public. In the course of carrying out their duties, federal law enforcement agencies may use FRT for a variety of purposes. For instance, the Federal Bureau of Investigation (FBI) uses the technology to aid its investigations, and the bureau provides facial recognition assistance to federal, state, local, and tribal law enforcement partners. State, local, and tribal law enforcement have also adopted facial recognition software systems to assist in various phases of investigations. In addition, border officials use facial recognition for identity verification purposes.

The use of FRT by law enforcement agencies has spurred questions on a range of topics. Some primary concerns revolve around the accuracy of the technology, including potential race-, gender-, and age-related biases; the collection, retention, and security of images contained in various facial recognition databases; public notification regarding the use of facial recognition and other image capturing technology; and policies or standards governing law enforcement agencies' use of the technology. Some of these concerns have manifested in actions such as federal, state, and city efforts to prohibit or bound law enforcement agencies' use of FRT.[1] In addition, some companies producing facial recognition software, such as Microsoft, IBM, and Amazon, have enacted new barriers to law enforcement using their technologies.[2]

This report provides an overview of federal law enforcement agencies' use of FRT, including the current status of scientific standards for its use. The report includes a discussion of how FRT may be used by law enforcement agencies with traditional policing missions as well as by those charged with securing the U.S. borders. It also discusses considerations for policymakers debating whether or how to influence federal, state, and local law enforcement agencies' use of FRT.

Conceptualizing Facial Recognition Technology

The term *facial recognition technology* can have different meanings for law enforcement agencies, policymakers, and the public, and the process of using facial recognition in a law enforcement context can involve various technologies and actors. Broadly, as technology experts have noted, "[t]here is no one standard system design for facial recognition systems. Not only do organizations build their systems differently, and for different environments, but they also use different terms to describe how their systems work."[3] The following key terms are provided to help in understanding facial recognition technologies and processes in this report.[4]

Face detection technology determines whether a digital image contains a face.

Facial classification algorithms analyze a face image to produce an estimate of age, sex, or some other property, but do not identify the individual. An example application of this would be

[1] See, for example, Dave Lee, "San Francisco is First US City to Ban Facial Recognition," *BBC*, May 15, 2019; and Dustin Gardiner, "California Blocks Police From Using Facial Recognition in Body Cameras," *San Francisco Chronicle*, October 8, 2019.

[2] See, for example, Jay Greene, "Microsoft Won't Sell Police Its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM," *The Washington Post*, June 11, 2020.

[3] Partnership on AI, *Understanding Facial Recognition Systems*, February 19, 2020, p. 3, https://www.partnershiponai.org/wp-content/uploads/2020/02/Understanding-Facial-Recognition-Paper_final.pdf.

[4] These terms are taken or adapted from the Facial Identification Scientific Working Group (FISWG), *FISWG Glossary Version 2.0*, October 25, 2019; FISWG, *Facial Comparison Overview and Methodology Guidelines*, October 25, 2019; and National Institute of Standards and Technology (NIST), *Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects (NIST IR8280)*, December 19, 2019, https://doi.org/10.6028/NIST.IR.8280. Some editorial changes have been made.

retail stores using facial classification to gather data on the gender and age ranges of people visiting a store, without identifying each shopper individually.

Facial comparison and **facial identification** are often used in the same context. They involve a human manually examining the differences and similarities between facial images, or between a live subject and facial images, for the purpose of determining if they represent the same person. Facial comparison has three broad categories: assessment, review, and examination. Facial assessment is a quick image-to-image or image-to-person comparison, typically carried out in screening or access control situations, and is the least rigorous form of facial comparison. Facial review (often used in investigative, operational, or intelligence gathering applications) and facial examination (often used in a forensic applications) are increasingly rigorous levels of image comparison and should involve verification by an additional reviewer or examiner. They may involve a formal, systematic examination of facial images.

Facial recognition broadly involves the automated searching of a facial image (a probe) against a known collection or database of photos.

Facial recognition algorithms compare identity information from facial features in two face image samples and produce a measure of similarity (sometimes called a match score) between them; this information can be used to determine whether the same person is in both images. Images that have a similarity score above a defined threshold are presented to the user. There are two ways in which facial recognition algorithms work to compare images:

- One-to-one verification algorithms compare a photo of someone claiming a specific identity with a stored image(s) of that known identity to determine if it is the same person. Uses of these algorithms can include unlocking a smartphone and verifying identities at a security checkpoint.
- One-to-many identification search algorithms compare features of a probe photo with all those in a gallery of images. The algorithms can provide either a fixed number of the most similar candidates, or all candidates with a similarity score above a preset threshold, for human review.[5] These algorithms may be used for purposes such as identifying potential suspect leads from a mugshot database.

Probe refers to the facial image or template searched against a gallery or database of photos in a facial recognition system.

Real-time facial recognition involves facial recognition algorithms that can be used while a video recording is taking place in order to determine in real time whether an individual in a video matches with a list of candidates in a database of photos.

Threshold refers to any real number against which similarity scores are compared to produce a verification decision or gallery of images.

Scientific Standards and Facial Recognition Technology

NIST's Role in Facial Recognition Technology

The National Institute of Standards and Technology (NIST) is a non-regulatory federal agency within the Department of Commerce charged with promoting U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology. Among its key

[5] This process is described in more detail in the "Accuracy and Interpretation of Results" section of this report.

roles, NIST is the lead federal agency for metrology (the science of measurement) and facilitates standards development, two key elements in the development and deployment of FRT.[6]

NIST's work in FRT includes the following:

- **Research** to improve the accuracy, quality, usability, interoperability, and consistency of FRT identity management systems;
- **Testing and Evaluation** to provide tools and support for evaluating the effectiveness of FRT prototypes and products;
- **Technical Guidance and Support** to assist federal law enforcement and other federal government agencies in the use of FRT; and
- **Standards** to facilitate the development of scientifically valid, fit-for-purpose FRT standards and to ensure that U.S. interests are represented in international arenas.

NIST collaborates with other federal agencies, law enforcement agencies, industry, and academic partners in these and related activities. Detailed information on NIST efforts in research, testing and evaluation, technical guidance and support, and standards development related to FRT are included in the **Appendix**.

Facial Identification Scientific Working Group

NIST administers the Organization of Scientific Area Committees (OSAC) for Forensic Science, which is a collaboration of more than 550 forensic scientific practitioners and experts across government, academia, and industry.[7] The OSAC for Forensic Science works to facilitate "the development of technically sound, science-based standards through a formal standard developing organization (SDO) process."[8] It also evaluates existing standards developed by SDOs and may place them on the OSAC Registry,[9] which contains approved scientifically sound forensic science standards for specific disciplines, such as facial identification, digital evidence, or bloodstain pattern analysis. The OSAC also promotes the use of these OSAC Registry-approved standards by the forensic science community.

The OSAC for Forensic Science is supported by a number of scientific working groups, which are collaborations between forensic science laboratories and practitioners "to improve discipline practices and build consensus standards."[10] There are over 20 scientific working groups across a range of disciplines including facial identification, DNA analysis, and latent fingerprint examination. The mission of the Facial Identification Scientific Working Group (FISWG) "is to develop consensus standards, guidelines and best practices for the discipline of image-based comparisons of human features, primarily face, as well as to provide recommendations for research and development activities necessary to advance the state of the science in this field."[11]

FISWG has published a number of guidelines and recommendations for forensic science practitioners. For instance, they have guidelines and recommendations for conducting and

[6] Facial recognition technology is a subfield of biometrics. Biometrics is the measurement and analysis of unique physical or behavioral characteristics.

[7] For more information, see https://www.nist.gov/topics/organization-scientific-area-committees-forensic-science.

[8] Ibid.

[9] See https://www.nist.gov/topics/organization-scientific-area-committees-forensic-science/osac-registry.

[10] See https://fiswg.org/about_swgs.html.

[11] See https://fiswg.org/objectives.html.

establishing training on facial comparison, guides for capturing facial images that can be used in facial recognition systems, and recommended methods and techniques for using facial recognition systems.[12]

How FRT May be Used by Federal Law Enforcement Agencies

Law enforcement agencies' use of FRT has received attention from policymakers and the public over the past several years. There have been heightened concerns following several revelations, including that Clearview AI, a company that developed image-search technology used by law enforcement agencies around the country, had amassed a database of over 3 billion images against which probe photos could be compared.[13]

FRT is one of several biometric technologies employed by law enforcement agencies, which also include fingerprint, palm print, DNA and iris scans. FRT can be used by law enforcement for a variety of purposes such as generating investigative leads, identifying victims of crimes, facilitating the examination of forensic evidence, and helping verify the identity of individuals being released from prison.[14] Press releases and statements from the Department of Justice (DOJ) highlight how the technology has been used in the criminal justice system.

- FRT has been used to help generate suspect leads. In one case, FBI agents used the technology, via the Mississippi Fusion Center, to identify a potential suspect in an interstate stalking case who had allegedly been harassing high school girls through their Twitter accounts.[15] The suspect was later sentenced to 46 months imprisonment and three years of supervised release for this stalking.[16]
- FRT may also be used to help identify victims. For example, officials have noted FRT was used to help identify "an accident victim lying unconscious on the side of the road."[17]
- FRT, along with other pieces of evidence, has been used to support probable cause in affidavits in support of criminal complaints. In one case, an FBI agent cited the use of FRT in a criminal complaint against a bank robbery suspect. The agent noted that images from the bank's surveillance footage were run against facial recognition software, and a photo of the suspect was returned as a possible match. Investigators then interviewed associates of the suspect, who identified him as the man in the bank surveillance footage.[18]

[12] See https://fiswg.org/documents.html.

[13] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It," *The New York Times*, February 10, 2020.

[14] Remarks by an FBI representative at the President's Commission on Law Enforcement and the Administration of Justice, April 21, 2020.

[15] U.S. Attorney's Office, Southern District of Indiana, "Mississippi man faces interstate stalking charges for five-year-long crime against Evansville area high schoolers," press release, June 28, 2018.

[16] U.S. Attorney's Office, Southern District of Indiana, "Mississippi man sentenced for internet stalking young Evansville women," press release, August 5, 2019.

[17] Remarks by an FBI representative at the President's Commission on Law Enforcement and the Administration of Justice, April 21, 2020.

[18] United States of America v. Terrance Maurice Goss, U.S. District Court for the Middle District of Florida, Criminal

Notably, the frequency and extent to which FRT is used at various phases of the criminal justice system (from generating leads and helping establish probable cause for an arrest or indictment, to serving as evidence in courtrooms) is unknown.[19] It is most often discussed as being employed during investigations by law enforcement officials. Of note, FRT is generally used by law enforcement in one-to-many searches to produce a gallery of potential suspects ranked by similarity and not to provide a single affirmative match. As such, the technology currently might not be relied upon in the same way that other biometric evidence might. Rather, it is the results of an investigator's facial review between a probe face and the gallery of images produced from running a probe face through facial recognition software that might be used as evidence contributing to an arrest and prosecution.

While FRT is used by a number of federal law enforcement agencies, the next section of this report highlights the FBI's use of it, as the bureau has a leading role in federal law enforcement's employment of the technology.

FBI Use of FRT

The FBI's Criminal Justice Information Services (CJIS) Division operates two programs that support the FBI's use of FRT: (1) the Next Generation Identification–Interstate Photo System (NGI-IPS), largely supporting state and local law enforcement; and (2) the Facial Analysis, Comparison, and Evaluation (FACE) Services Unit, supporting FBI investigations.

Next Generation Identification–Interstate Photo System (NGI-IPS)

NGI-IPS contains criminal mugshots that have associated 10-print fingerprints and criminal history records. This system allows authorized federal, state, local, and tribal law enforcement users to search the database for potential investigative leads. To use NGI-IPS,

> [a] law enforcement agency submits a "probe" photo that is obtained pursuant to an authorized law enforcement investigation, to be searched against the mugshot repository. The NGI-IPS returns a gallery of "candidate" photos of 2-50 individuals (the default is 20). During the second step of the process, the law enforcement agencies then manually review the candidate photos and perform further investigation to determine if any of the candidate photos are the same person as the probe photo.[20]

The FBI notes that a facial recognition search in NGI-IPS cannot alone provide a positive identification; the results need to be manually reviewed by a trained officer.[21] Further, law enforcement agencies that submit a probe photo for a search in NGI-IPS are prohibited from relying solely on the results of this search to take a formal law enforcement action (e.g., making an arrest).[22]

Complaint, January 18, 2019.

[19] In at least one case, in California, a judge allowed a suspect's criminal defense team to introduce evidence from biometric facial recognition technology. For more information, see "A First: Biometrics Used to Sentence Criminal," *Homeland Security Newswire*, February 1, 2011.

[20] FBI testimony before U.S. Congress, House Committee on Oversight and Reform, *Facial Recognition Technology (Part II): Ensuring Transparency in Government Use*, 116th Cong., 1st sess., June 4, 2020.

[21] As noted elsewhere, authorized users of NGI-IPS must receive training in the use of facial recognition technology.

[22] See https://www.fbibiospecs.cjis.gov/Face.

Photos in NGI-IPS

NGI-IPS "contains over 93 million civil photos, criminal photos, and scars, marks and tattoo images. Of this number, over 38 million criminal photos are available for facial recognition searching by law enforcement agencies."[23] The photos in NGI-IPS are separated into various groups: a criminal identity group (mugshots pursuant to arrest),[24] a civil identity group (those submitted for criminal background checks for non-criminal justice purposes such as employment and security clearances), and an unsolved photo file (UPF, which contains photos of unknown subjects reasonably suspected of a felony crime against a person). The criminal identity group is automatically available for facial recognition searching. If an individual has photos associated with both the criminal and civil identity groups, all photos become associated with the criminal identity group and are available for searching. A law enforcement agency submitting a probe photo to NGI-IPS for searching can affirmatively request to search against the UPF in addition to the criminal identity group.

Facial Analysis, Comparison, and Evaluation (FACE) Services Unit

While NGI-IPS primarily supports state, local, and tribal law enforcement partners, the FACE Services Unit supports FBI investigations. Specifically, FACE Services supports FBI field offices, operational divisions, and legal attachés (and sometimes federal partners) on open investigations and, in limited circumstances, on closed cases. The FACE Services Unit searches "probe photos that have been collected pursuant to the Attorney General guidelines as part of an authorized FBI investigation, and they are not retained."[25] These probe photos are searched against faces in NGI-IPS as well as other federal and state facial recognition systems authorized for FBI use. The FACE Services Unit then, through facial review, compares the probe photo against the candidate gallery of faces produced from the search to help identify potential investigative leads.

FRT Used by Law Enforcement Agencies at the Border

While FRT is generally used by law enforcement agencies to help generate potential investigative leads, it is also employed by U.S. border enforcement officials to assist with verifying travelers' identities. The Department of Homeland Security (DHS) is developing an automated biometric entry-exit system for foreign nationals traveling into and out of the country.[26] The entry system has been implemented,[27] but the exit system has yet to be fully operationalized.[28] In developing the exit system, DHS and Customs and Border Protection (CBP) have piloted various programs using an array of biometric technologies (e.g., fingerprints, iris scans, and facial recognition) and determined that facial recognition was the optimal approach because of the speed with which it could be used and its relative accuracy. The FRT program they have implemented is the Traveler Verification Service (TVS).[29]

TVS is a public-private partnership between the federal government and private airlines, airports, and cruise lines. It is deployed by CBP and the Transportation Security Administration (TSA). TVS currently operates in 27

[23] FBI, *Privacy Impact Assessment for the Next Generation Identification – Interstate Photo System*, October 29, 2019.

[24] The mugshots taken pursuant to arrest are not indicative of actual criminality or guilt.

[25] FBI testimony before U.S. Congress, House Committee on Oversight and Reform, *Facial Recognition Technology (Part II): Ensuring Transparency in Government Use*, 116th Cong., 1st sess., June 4, 2020. Department of Justice policies and procedures—including guidelines for investigations—are outlined in the *Justice Manual*, available at https://www.justice.gov/jm/justice-manual.

[26] For more information, see CRS In Focus IF11634, *Biometric Entry-Exit System: Legislative History and Status*.

[27] The entry system, fully implemented in December 2006, utilizes biometrics such as fingerprints and digital photographs.

[28] There have been "various longstanding planning, infrastructure, and staffing challenges" to developing and implementing the biometric exit system, including airports' lack of secure inspection areas for outbound travelers. See U.S. Government Accountability Office, *DHS Has Made Progress in Planning for a Biometric Air Exit System and Reporting Overstays, but Challenges Remain*, GAO-17-170, February 17, 2017.

[29] Additional information, including privacy documents, is available at https://www.dhs.gov/publication/dhscbppia-056-traveler-verification-service.

airports, 7 seaports, and 5 border locations across the United States, as well as 4 international preclearance locations. TVS currently captures roughly 60% of *in-scope* travelers (i.e., foreign nationals aged 14-79) departing the United States via commercial air carriers and 20% of in-scope arriving travelers.[30] CBP's goal is to capture 97% of all in-scope departing commercial air travelers by 2022.[31] TVS compares the travelers' *live photographs* (taken, for example, by a gate agent) to a gallery of photographs. The composition of the galleries depends on the travel context. For air and sea travelers, CBP uses biographic data obtained from flight and ship manifests via the Advance Passenger Information System[32] to gather all associated facial images from DHS holdings (e.g., photographs from U.S. passports, U.S. visas, CBP entry inspections, and any other DHS encounters). For pedestrians and vehicle travelers, the gallery consists of photographs of frequent crossers at that port of entry. TVS provides a *match* or *no match* result within two seconds.[33] In case of the latter result, the traveler's identity is checked manually by a CBP agent.

Federal Law Enforcement FRT Policy Guidance

The FBI maintains an NGI Policy and Implementation Guide that outlines policies surrounding use of NGI-IPS. Authorized law enforcement users of NGI-IPS are required to follow these policies as well as FISWG standards for performing facial comparison.[34] Policies outlined in the guide include information on how to

- submit photos for enrollment in NGI-IPS,
- conduct an investigative photo search,
- retrieve additional biometrics associated with a probable candidate generated from a search of NGI-IPS,
- notify the FBI of a potential match resulting from an investigative photo search,
- request an audit trail for a biometric set that an authorized user enrolled in NGI-IPS, and
- delete a biometric set that an authorized user enrolled in NGI-IPS.[35]

The FBI outlines technical requirements for using NGI-IPS in an Electronic Biometric Transmission Specification document that it provides to system users. In addition, it asks that users of NGI-IPS use its Mugshot Implementation Guide as a reference for submitting proper facial images to the FBI. The guide notes that image quality is affected by the camera, background, lighting, and subject posing.[36]

The FBI requires that users of NGI-IPS complete facial recognition training that meets FISWG guidelines. To facilitate this requirement, the FBI provides facial comparison and identification

[30] Based on CRS discussions with CBP officials on January 30, 2020, and CRS email communication with CBP officials on August 12, 2020.

[31] Department of Homeland Security (DHS), *Transportation Security Administration and U.S. Customs and Border Protection: Deployment of Biometric Technologies*, Report to Congress, August 30, 2019, p. 5.

[32] APIS collects biographic data such as gender, date of birth, travel document type and number, and nationality, Ibid. p. 30.

[33] U.S. Customs and Border Control, *Traveler Verification Service for Simplified Travel*, August 2018.

[34] FISWG has Guidelines and Recommendations for Facial Comparison Training to Competency, available at https://fiswg.org/FISWG_Training_Guidelines_Recommendations_v1.1_2010_11_18.pdf.

[35] FBI, *Next Generation Identification (NGI) Interstate Photo System (IPS) Policy and Implementation Guide: Version 1.3*, April 23, 2015.

[36] FBI, *Mugshot Implementation Guide: Photographic Considerations Related to Facial Recognition Software and Booking Station Mug Shots*, April 25, 2013.

training, which "is designed to provide the skills and knowledge to professionals from the law enforcement and intelligence communities working in the fields of face recognition and face comparison. It also provides students with awareness and understanding of the face comparison discipline. This training is consistent with the guidelines and recommendations outlined by [FISWG]."[37] FISWG notes that "[t]he level of training necessary to conduct facial comparison is dependent upon the source, quality, quantity, and complexity of the images that are being analyzed and the purpose of the analysis."[38] As outlined by FISWG, basic level training for facial comparison includes, among other things, an understanding of the principles of facial comparison, including

- assessing the quality of a facial image to determine the value for examination;
- using a process of "Analysis, Comparison, Evaluation, and Verification (ACE-V)";
- understanding the methods of comparison, such as one-to-one facial examination;
- understanding the levels of conclusion;
- having the ability to render proper conclusions;
- understanding the concept and effects of cognitive bias, including confirmation bias; and
- understanding the benefits of verification by another qualified reviewer or examiner.[39]

The FBI has also conducted audits to evaluate whether users of its facial recognition systems are in compliance with the policies surrounding their use. In congressional testimony, the FBI indicated that as of May 2019, nine FBI audits of NGI-IPS revealed no findings of non-compliance and no observations of unauthorized requests or misuse of NGI-IPS; in addition, a 2018 FBI audit of the FACE Services Unit indicated that the unit is operating in accordance with FBI policies and relevant privacy laws.[40]

Policy Considerations Surrounding Federal Law Enforcement Use of FRT

Accuracy and Interpretation of Results

The accuracy of FRT has come under scrutiny, independent of law enforcement's use of the technology including an officer's review of potential matches. When considering accuracy, there are a number of possible outcomes in both one-to-many identification searches (such as those used by the FBI's NGI-IPS) and one-to-one verifications (such as those used by the CBP's TVS).

[37] FBI, *Biometric and Criminal History Record Training*, https://www.fbi.gov/services/cjis/fingerprints-and-other-biometrics/biometric-and-criminal-history-record-training.

[38] FISWG, *Guide for Role-Based Training in Facial Comparison*, July 17, 2020, pp. 1-2.

[39] FISWG, *Guidelines and Recommendations for Facial Comparison Training to Competency*, November 18, 2010, pp. 1-2.

[40] Statement for the Record of Kimberly Del Greco, Federal Bureau of Investigation, before U.S. Congress, House Committee on Oversight and Reform, *Facial Recognition Technology: Ensuring Transparency in Government Use*, 116th Cong., 1st sess., June 4, 2019.

Facial recognition systems may return an accurate match (i.e., a true positive result, or hit),[41] an accurate non-match (i.e., a true negative, or correct rejection),[42] an inaccurate match (i.e., a false positive, or false alarm),[43] or an inaccurate non-match (i.e., a false negative, or miss).[44] It is the two types of errors—inaccurate matches and inaccurate non-matches—that have been of particular interest to policymakers.

- An inaccurate match, or *false positive,* result occurs when there is an erroneous association between images from two different people, which can occur when the digitized faces of two different people are highly similar.
- An inaccurate non-match, or *false negative,* result occurs when there is a failure to match images of the same person in two different photos. This could occur due to factors such as a change in the person's appearance or discrepancies in the quality of the images. Variations in pose, illumination, and expression may contribute to false negatives.[45]

Notably, there are both technical and human factors that contribute to the overall accuracy of facial recognition searches as performed by law enforcement officers.

Matching a probe to a gallery of images or a reference image depends on the threshold set for the similarity scores generated by the facial recognition algorithm. Similarity scores indicate the similarity between the probe and reference or gallery images.[46] For example, if using a zero-to-one scale, a similarity score of one would indicate that the two images are most similar (not necessarily that the two face images belong to the same person) in that system. Further, similarity scores are system specific (i.e., a similarity score from a system developed by company A is not necessarily comparable to a similarity score from a system from company B).[47]

When trying to decide whether a probe image matches any images in a given database, setting a higher threshold will return fewer potential results and setting a lower threshold will return a greater number of potential results. Generally, the threshold is initially set by the algorithm developer. Depending on the system, the user can choose to keep or change this threshold. As with similarity scores, thresholds do not indicate accuracy of a system (i.e., adjusting a threshold to a higher value does not mean the results returned are more accurate); rather, the decision of where to set a threshold is based on how the system is being used and what the developer or user

[41] In a one-to-many identification search, this occurs when the probe face matches a face in the database and is one of the faces returned in the gallery of potential matches. In a one-to-one identity verification, this occurs when the probe face submitted matches a photo of the same individual in a database, and a match is confirmed.

[42] In a one-to-many identification search, this occurs when the probe face does not match a face in the database and a gallery of potential matches is not returned. In a one-to-one identity verification, this occurs when the probe face does not match any faces in a database, and a match is not confirmed.

[43] In a one-to-many identification search, this occurs when the probe face does not match a face in the database, but a gallery of potential matches is returned. In a one-to-one identity verification, this occurs when the probe face does not match a face in the database, but a match is confirmed.

[44] In a one-to-many identification search, this occurs when the probe face submitted matches a face in the database, but a gallery of potential matches is not returned. In a one-to-one identity verification, this occurs when the probe face matches a face in the database, but a match is not confirmed.

[45] See NIST, *Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects (NIST IR8280)*, December 19, 2019, https://doi.org/10.6028/NIST.IR.8280.

[46] Similarity scores are sometimes referred to as *confidence scores*, but they do not represent a degree of certainty or confidence in the matches returned to the user or the accuracy of the system.

[47] For additional explanations of match scores and thresholds, see Partnership on AI, *Understanding Facial Recognition Systems*, February 19, 2020, pp. 6-7.

wants to optimize (e.g., reducing the chance of false positives or false negatives).[48] Notably, when considering where to set the threshold, there is also consideration of the inherent tradeoff in error rates—one can minimize the false positive rate or the false negative rate by resetting the threshold, but not both at the same time.[49]

There is also a range of possible accurate and inaccurate outcomes when the probe face and any gallery of potential matches are subject to facial review by a human. For instance, in one-to-many searches a reviewer can correctly match the probe face to the same individual's photo returned in the gallery of potential matches, or a reviewer can correctly reject the probe face as a match to faces in the gallery if the FRT software has returned a gallery that does not contain a match. In addition, a reviewer can incorrectly identify the probe face as a match to a face in a returned gallery (in either a gallery that correctly contains or incorrectly does not contain a match); alternatively, a reviewer could fail to identify the probe face as a match when a gallery contains the correct match. In one-to-one identity verifications, such as those used to confirm a traveler's identity, there may be follow-up facial comparison by an official in the instance of a no-match returned by the technology. In this case, the comparison can result in one of the same outcomes as one-to-many searches subject to follow-up review by a human.

Effects of Errors

False positives and negatives returned by FRT have come under scrutiny because of their potential implications. In one-to-many identification searches used by law enforcement, false positives could potentially contribute to errant investigative leads and false accusations. False negatives could potentially result in loss of evidence that could support a case. In one-to-one verifications used by border officials, false positives pose potential security risks because they may not flag a traveler using an assumed identity. False negatives could result in enhanced questioning, surveillance, or disrupted travel of individuals for whom it was not necessary.[50] According to CBP internal analysis, the estimated false positive rate of TVS is .0103%.[51] (It did not report the false negative rate.) Further, in September 2020, the Government Accountability Office (GAO) reported that CBP "met or exceeded" its facial recognition accuracy requirements for its air exit system.[52]

A December 2019 NIST study of both one-to-many identification search algorithms and one-to-one verification algorithms found that FRT algorithms' accuracy rates can vary by demographic

[48] Ibid.

[49] This tradeoff is demonstrated by plots that incorporate false negative and false positive identification rates with a threshold value; these plots are called detection error tradeoff (DET) characteristic or receiver operating characteristic (ROC) curves. For additional information see the 2019 NIST FRVT Part 3: Demographic Effects report, p. 23; and for further discussion, see Lucas D. Introna and Helen Nissenbaum, *Facial Recognition Technology: A Survey of Policy and Implementation Issues*, The Center for Catastrophe Preparedness and Response, New York University , 2009, pp. 14-15.

[50] As a 2019 NIST study notes, "in a one-to-one access control, false negatives inconvenience legitimate users; false positives undermine a system owner's security goals. On the other hand, in a one-to-many deportee detection application, a false negative would present a security problem, and a false positive would flag legitimate visitors." Patrick Grother, Mei Ngan, and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, National Institute of Science and Technology, December 2019.

[51] Department of Homeland Security (DHS), *Transportation Security Administration and U.S. Customs and Border Protection: Deployment of Biometric Technologies*, Report to Congress, August 30, 2019, p. 30. CBP does not provide the methodology for calculating the false positive rate.

[52] U.S. Government Accountability Office (GAO), *Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, GAO-20-568, September 2020, p. 50.

factors such as age, sex, and race.[53] For example, false positive rates tended to be higher for Asian and African American faces compared to those of Caucasians, which may be due to the data used to train the algorithm; an explanation that the NIST study did not explore. However, NIST noted that there is wide variation among algorithms, with some producing significantly fewer errors, and errors of different types, than others.[54] Policymakers may wish to exercise oversight over the *specific* FRT algorithms employed by federal law enforcement agencies, and the data on which those systems are trained, as they evaluate the accuracy and use of facial recognition. They may also debate whether or how to provide legislative direction aimed at maximizing the accuracy of FRT algorithms used by federal law enforcement entities. In attempting to maximize accuracy, developers and users of FRT must weigh the consequences of errors (false positives and false negatives) for different communities and decide which error measure is of higher priority to minimize, depending on how the threshold is set.

NIST researchers and collaborators have also studied the facial recognition accuracy of forensic examiners, *superrecognizers*, and face recognition algorithms.[55] They found that while the "best machine performed in the range of the best-performing humans, who were professional facial examiners … optimal face identification was achieved only when humans and machines collaborated."[56] Policymakers may consider this as they evaluate the accuracy of law enforcement use of FRT—such as the FBI's NGI-IPS, which requires manual review of the gallery of faces produced by submitting a probe face to the FRT algorithm.

Potential Restrictions on Law Enforcement Use of FRT

Recent policy debates surrounding law enforcement agencies' use of FRT have included discussions about potential prohibitions, restrictions, or moratoriums on the technology's use. In these discussions, policymakers may consider issues such as the following:

How is law enforcement conceptualized in this context? As noted, law enforcement agencies with various missions—from those like the FBI's to investigate violations of federal criminal law to those like CBP's to support border enforcement—have employed FRT. Policymakers may consider whether proposals to specify whether or how law enforcement agencies may use FRT have also factored in which type of law enforcement activities might be affected.[57]

How might restrictions on the use of FRT affect emergencies or cases involving threats to national security? Policymakers debating bounds on law enforcement agencies' use of FRT may consider whether restrictions should apply equally in all circumstances. For example, while many tools and technologies used by law enforcement agencies to aid investigations have not been specifically permitted or prohibited by law, Congress has legislated on and conducted oversight of

[53] Patrick Grother, Mei Ngan, and Kayee Hanaoka, *Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects*, National Institute of Science and Technology, December 2019.

[54] Ibid. Also, testimony by Charles H. Romine, NIST Director, before U.S. Congress, House Committee on Homeland Security, *About Face: Examining the Department of Homeland Security's Use of Facial Recognition and Other Biometric Technologies: Part II*, 116th Cong., 2nd sess., February 6, 2020.

[55] P. Jonathon Phillips, Amy N. Yates, and Ying Hu et al., Proceedings of the National Academy of Sciences, *Face Recognition Accuracy of Facial Examiners, Superrecognizers, and Face Recognition Algorithms*, April 2018. Researchers note that superrecognizers are "untrained people with strong skills in face recognition."

[56] Testimony by Charles H. Romine, NIST, before U.S. Congress, House Committee on Oversight and Reform, *Facial Recognition Technology: Ensuring Transparency in Government Use*, 116th Cong., 1st sess., June 4, 2019.

[57] The Bureau of Justice Statistics' Census of Federal Law Enforcement Officers may help inform this discussion. The most recent survey provides data from 2016. Bureau of Justice Statistics, *Federal Law Enforcement Officers, 2016-Statistical Tables*, October 2019.

certain technologies that could affect individual privacy. With electronic surveillance, for instance, investigators must generally obtain a warrant to conduct wiretaps;[58] however, exceptions exist for emergency situations that may involve death or serious injury, threaten national security, or involve conspiracies of organized crime.[59]

How might policymakers influence law enforcement use of FRT at the federal level as well as state and local levels?

Policymakers can legislate directly on federal law enforcement agencies' ability to utilize facial recognition and other biometric technologies, as well as specify under which circumstances federal law enforcement may use these tools. They can also direct federal departments and agencies to develop or rely on established guidelines surrounding the technologies, require them to use technology and FRT algorithms that meet specified standards, and conduct broad oversight of agencies' use of FRT.

Congress could also influence state, local, and tribal use of these technologies through the provision or withholding of grant funding. Programs such as the Edward Byrne Memorial Justice Assistance Grant (JAG) program[60] and the Community Oriented Policing Services (COPS) program[61] have been used to incentivize activities of state and local law enforcement and may be leveraged to support or restrict agencies' use of FRT. For instance, Pinellas County, FL, law enforcement has used COPS funding to develop a facial recognition system.[62]

Another way the federal government can affect state, local, and tribal policies, without the provision or withholding of grant funding, is through the transfer of knowledge and expertise—via training, research and guiding documents, and model legislation. For instance, the Bureau of Justice Assistance published a guidance document for state, local, and tribal criminal intelligence and investigative entities to aid in developing policies around the use of FRT.[63]

Privacy and Security

In a September 2019 survey by the Pew Research Center, 56% of surveyed Americans indicated that they trust law enforcement agencies to use FRT responsibly, and 59% indicated it is acceptable for law enforcement agencies to use these technologies to assess security threats in public.[64] Further, the American public generally has more trust in law enforcement agencies using FRT responsibly than it does in technology companies or advertisers. This trust, however, has some notable demographic variances. Older Americans indicated they had more trust in law enforcement using FRT responsibly than did younger Americans. Further, White respondents (61%) reported more trust in law enforcement using the technology responsibly than did Hispanic respondents (56%), who in turn reported more trust than Black respondents (43%). Nonetheless,

[58] 18 U.S.C. §2510, et seq. See also Department of Justice, *Justice Manual, Title 9, 9.7000: Electronic Surveillance.*

[59] 18 U.S.C. §2518.

[60] For more information, see CRS In Focus IF10691, *The Edward Byrne Memorial Justice Assistance Grant (JAG) Program*.

[61] For more information, see CRS In Focus IF10922, *Community Oriented Policing Services (COPS) Program*.

[62] National Law Enforcement and Corrections Technology Center, *Florida Facial Recognition System Unmasks Identity, Boosts Arrests*, August 2010. Pinellas County, FL, law enforcement agencies had previously received, through the FY2001 appropriations, $3.5 million in funding for a demonstration grant "to demonstrate with the Florida Department of Motor Vehicles how facial recognition technology may be used by police." See H.Rept. 106-1005.

[63] Bureau of Justice Assistance, *Face Recognition Policy Development Template*, December 2017.

[64] Aaron Smith, Pew Research Center, *More Than Half of U.S. Adults Trust Law Enforcement to Use Facial Recognition Responsibly*, September 5, 2019.

policymakers, advocates, and the public have raised questions about how these technologies might affect privacy as well as the security of facial recognition systems' data.[65] Questions for policymakers to consider include the following:

Is there public awareness and notification surrounding federal law enforcement use of FRT? Some have questioned whether or how individuals might know that their faces are included in databases searched by FRT for law enforcement purposes. For example, federal law enforcement agencies may rely on FRT to search against a number of databases to help identify suspects.[66] The FBI's FACE Services Unit can search probe photos against faces in NGI-IPS as well as other federal and state facial recognition systems authorized for FBI use. Some states allow FBI access to driver's license/identification photos, mugshot photos, and state department of corrections photos; some allow access to some portion or subset of those photos; and some prohibit access.[67] The FBI is required to provide information to the public on its facial recognition systems through Privacy Impact Assessments (PIAs) and System of Records Notices (SORNs).[68] Policymakers may question whether these are sufficient measures to notify the public about federal law enforcement agencies use of FRT to search against databases in which individuals' photos are held. In addition, they may conduct oversight over the timeliness with which federal law enforcement agencies publish and update relevant PIAs and SORNs.

There are also concerns about CBP's use of FRT. U.S. citizens are allowed to opt out of TVS biometric exit participation and can instead undergo manual review of travel documents. CBP notifies travelers of this alternative through its website, physical signs and verbal announcements at the ports of entry, and an FAQ sheet upon request.[69] However, a September 2020 GAO report found that "notices to inform the public of facial recognition contained limited privacy information and were not consistently available."[70] Policymakers may examine whether CBP provides U.S. citizens with adequate notice about TVS and explains its opt-out procedures clearly.[71]

---

[65] The issues discussed in this section are focused on FRT as used by law enforcement to generate potential investigative leads and by border enforcement for identity verification. There are other potential uses of FRT in the criminal justice system, not discussed here, such as compelling an individual to use the facial recognition feature to unlock a mobile device such as an iPhone. Of note, "at least one court has upheld compelled use of a facial recognition unlock feature." See Joey L. Blanch and Stephanie S. Christensen, "Biometric Basics: Options to Gather Data from Digital Devices Locked by a Biometric "Key"," *Emerging Issues in Federal Prosecutions*, vol. 66, no. 1 (January 2018), p. 6.

[66] The same may be true for state and local law enforcement, but this varies by jurisdiction.

[67] GAO, *Face Recognition Technology: DOJ and FBI Have Taken Some Actions in Response to GAO Recommendations to Ensure Privacy and Accuracy, But Additional Work Remains*, GAO-2019-579T, June 4, 2019.

[68] Ibid. This requirement is not specific to the FBI. Federal agencies are subject to requirements under Section 208 of the E-Government Act of 2002 (P.L. 107-347) regarding the protection of personal information collected, maintained or disseminated using information technology. For more information, see Office of Management and Budget, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, M-03-22, September 26, 2003. In this guidance, a PIA is defined as "an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks." In addition, SORN is required to be published for any newly created or revised system of records.

[69] DHS, *Privacy Impact Assessment for the Traveler Verification Service*, DHS/CBP/PIA-056, November 14, 2018, p. 19.

[70] GAO, *Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, GAO-20-568, September 2020, p. 39.

[71] Letter from 23 Members of Congress to Kevin McAleenan, former Acting Secretary of Homeland Security, June 13,

How might the use of FRT affect police-community relations? In the national debate about police-community relations,[72] there have been concerns about whether race, gender, and age biases in some FRT algorithms could contribute to tensions between the police and the communities they serve. Further, in the midst of these discussions, some companies producing facial recognition software have decided to cease production or have enacted new barriers to law enforcement use of their technologies.[73] Some have been less concerned with potential errors produced by the technology and more apprehensive with how the technology may be *used* by law enforcement; specifically, the concern is whether law enforcement agencies' use of the technology can "strip individuals of their privacy and enable mass surveillance."[74]

Policymakers may continue to question whether federal law enforcement agencies have assessed—or have policies for ongoing assessments of—potential biases in the specific facial recognition technologies (and associated algorithms) that they use. This could include policies for ongoing assessments by NIST. Policymakers may also look into whether federal grants for state, local, and tribal law enforcement use of FRT include requirements that grantees are using facial recognition technologies that have been assessed for biases. In addition, they could continue to examine how federal law enforcement agencies, as well as state, local, and tribal recipients of federal grants, utilize the technology in their policing.

How do federal law enforcement agencies employing FRT retain and secure the data? The security of data held by federal agencies and their contractors is of ongoing interest to Congress. For instance, in June 2019, CBP revealed that images of faces and license plates were compromised in a cyberattack on one of its subcontractors that provides automated license plate recognition technology to the agency.[75] This breach reportedly exposed confidential agreements, hardware schematics, and other records related to border security.[76] Breaches like this highlight the vulnerability of data, including face image data captured and held by governmental agencies. In evaluating the security of federal law enforcement data systems, policymakers may pay particular attention to the security of facial recognition and other biometric data.

For example, the FBI's NGI-IPS contains mugshot photos against which probe photos are compared. The FBI notes that "after the facial recognition search is performed, the probe photo is not retained in the NGI-IPS. This ensures that the Criminal Identity Group of the NGI-IPS remains a repository of mugshots collected pursuant to arrest."[77] While NGI-IPS is often used by state, local, and tribal law enforcement agencies, the FACE Services Unit supports FBI investigations. The FACE Services Unit submits probe photos to NGI-IPS (which does not retain probe photos) as well as other federal, state, and local systems (which may have different policies on photo retention); when the FBI submits probe photos to entities outside the bureau, it is the

2019, https://wild.house.gov/sites/wild.house.gov/files/CBP%20Facial%20Recognition%20Ltr.%20final.%20.pdf.

[72] For more information, see CRS Report R43904, *Public Trust and Law Enforcement—A Discussion for Policymakers*.

[73] See, for example, Jay Greene, "Microsoft Won't Sell Police Its Facial-Recognition Technology, Following Similar Moves by Amazon and IBM," *The Washington Post*, June 11, 2020. See also Dustin Gardiner, "California Blocks Police From Using Facial Recognition in Body Cameras," *San Francisco Chronicle*, October 8, 2019.

[74] Osonde A. Osoba and Douglas Yeung, *Bans on Facial Recognition Are Naive. Hold Law Enforcement Accountable for Its Abuse*, RAND, June 17, 2020.

[75] For more information, see CRS Insight IN11143, *Exposed Data Highlights Law Enforcement Use of Selected Technologies*.

[76] Drew Harwell, "Surveillance Contractor That Violated Rules by Copying Traveler Images, License Plates Can Continue to Work with CBP," *The Washington Post*, October 10, 2019.

[77] FBI, *Privacy Impact Assessment for the Next Generation Identification – Interstate Photo System*, October 29, 2019, p. 2.

other agency that is responsible for conducting the search. The FBI notes that "to accommodate certain states that have auditing and/or logging requirements that necessitate retention of probe photos and candidate galleries, the FBI constructs [memoranda of understanding] in compliance with these requirements while also requiring state maintenance of only the minimum information necessary, for the shortest time period necessary, and notification to the FBI of any potential or actual breach of that information."[78]

CBP stores photographs of foreign nationals and U.S. citizens differently. All photographs are purged from the TVS cloud after 12 hours, regardless of citizenship status.[79] However, CBP stores photographs of foreign nationals for 14 days in the Automated Targeting System (ATS) Unified Passenger Module (UPAX).[80] These photographs are then transmitted to the Automated Biometric Identification System (IDENT), where they are retained for up to 75 years.[81] In contrast, photographs of U.S. citizens are immediately deleted after the matching process.[82] While CBP requires its commercial partners to follow these data retention requirements, a September 2020 GAO report found that CBP does not adequately audit its airline partners.[83]

Going Forward

There are currently no federal laws specifically governing law enforcement agencies' use of FRT,[84] and law enforcement agencies around the country may rely on a patchwork of technology platforms and algorithms for their facial recognition systems. As such, policymakers may question how federal law enforcement agencies assess and ensure the accuracy and security of their FRT systems as well as the policies governing their use. They may also examine the oversight of federal grants used to support or restrict the use of FRT by state, local, and tribal law enforcement. Policymakers may further consider how FRT is used more broadly in various phases of the criminal justice system, from generating leads and helping establish probable cause for an arrest or indictment, to serving as evidence in courtrooms and confirming prisoners' identities before release; this may help inform oversight and legislative efforts to enhance or bound aspects of how law enforcement uses the technology. In addition, policymakers may question whether or how recommendations from FISWG are adopted by federal law enforcement agencies; their state, local, and tribal partners; and law enforcement grant recipients.

[78] FBI, *Privacy Impact Assessment for the Facial Analysis, Comparison, and Evaluation (FACE) Phase II System*, July 9, 2018, p. 8.

[79] Ibid., p. 9.

[80] DHS, *Privacy Impact Assessment for the Traveler Verification Service*, DHS/CBP/PIA-056, November 14, 2018, pp. 9, 21.

[81] Ibid., pp. 8, 21.

[82] Ibid., p. 10.

[83] GAO, *Facial Recognition: CBP and TSA are Taking Steps to Implement Programs, but CBP Should Address Privacy and System Performance Issues*, GAO-20-568, September 2020, p. 46.

[84] For a discussion of relevant constitutional considerations surrounding law enforcement use of FRT, see CRS Report R46541, *Facial Recognition Technology and Law Enforcement: Select Constitutional Considerations*.

Appendix. NIST Efforts on Facial Recognition Technology

NIST work on FRT includes research, testing and evaluation, technical guidance and support, and standards.[85]

Research

NIST work in biometrics dates back to the 1960s. The agency's efforts span a wide range of activities to help improve the ability to establish or verify the identity of humans based upon one or more physical (e.g., face, fingerprint, iris images) or behavioral (e.g., signature analysis) characteristics.

The Information Technology Laboratory (ITL), one of six NIST research laboratories, is a measurement and testing facility that develops and deploys standards, tests, and metrics to make information systems more secure, usable, interoperable, and reliable. Among its functions, ITL conducts research on issues related to biometric measurement and testing and facilitates standards development, including those related to FRT. According to NIST, ITL has measured the core algorithmic capability of biometric recognition technologies and reported on the accuracy, throughput, reliability, and sensitivity of biometric algorithms with respect to data characteristics and subject characteristics.

NIST states that its biometric evaluations advance measurement science by providing a scientific basis for what to measure and how to measure it. These evaluations also help facilitate development of consensus-based standards by providing quantitative data for development of scientifically sound, fit-for-purpose standards. In addition, these evaluations help federal agencies determine how best to deploy FRT.

NIST's FRT research includes a wide span of activities as illustrated by the following examples:

In 2018, the National Academies published research conducted by NIST and three universities testing facial forensic examiners ability to match identities across different photographs.[86] The intent of the study was to find better ways to increase the accuracy of forensic facial comparisons. The study concluded that:

> Examiners and other human face "specialists," including forensically trained facial reviewers and untrained super-recognizers, were more accurate than the control groups on a challenging test of face identification. It also presented data comparing state-of-the-art facial recognition algorithms with the best human face identifiers. The best machine performed in the range of the best-performing humans, who were professional facial examiners. However, optimal face identification was achieved only when humans and machines collaborated.[87]

[85] Much of the information in this appendix is drawn from testimony given on February 6, 2020, by Charles H. Romine, Director of the National Institute of Standards and Technology's Information Technology Laboratory before the House Committee on Homeland Security.

[86] Jonathon Phillips, Amy N. Yates, and Ying Hu, "Face recognition accuracy of forensic examiners, superrecognizers, and face recognition algorithms," *Proceedings of the National Academy of Sciences*, vol. 115, no. 24 (June 12, 2018), pp. 6171-6176, https://doi.org/10.1073/pnas.1721355115.

[87] Testimony of Charles H. Romine, Director, NIST Information Technology Laboratory, before U.S. Congress, House Committee on Homeland Security, *Facial Recognition Technology (FRT)*, 116th Cong., 2nd sess., February 6, 2020,

In addition, NIST conducted the Face in Video Evaluation (FIVE) program to assess the capability of facial recognition algorithms to identify individuals appearing in video sequences. NIST documented the outcomes of FIVE in its report, *Face In Video Evaluation (FIVE) Face Recognition of Non-Cooperative Subjects (NIST IR8173)*, which discusses the accuracy and speed of FRT algorithms applied to the identification of individuals appearing in video sequences drawn from six video datasets.[88] NIST completed this program in 2017. The report found that:

> High accuracy recognition of passively-imaged subjects is only achievable with: a) a small minority of the algorithms tested [under this program]; b) a dedicated and deliberate design effort that must embed optical, architectural, human factors, operations-research, and face recognition expertise; c) galleries limited to small numbers of actively curated images; and d) field tests with empirical quantitative calibration and optimization.[89]

Further, the report states that with "better cameras, better design, and the latest algorithm developments, recognition accuracy can advance even further," but notes that "even with perfect design, some proportion of a non-cooperative population will not be recognized" due to failure to acquire cases where subjects never look toward the camera or because their faces were occluded.[90]

The report concluded, in part, that:

> Deployment should proceed only after quantitative assessment of objectives, alternatives, ease of evasion or circumvention, enrolled population sizes, search volumes, the proportion of searches expected to have an enrolled mate, accuracy requirements, consequences and procedures for resolution of errors, and speed and hardware cost constraints. In particular, deployers must weight their tolerance for misses and their risk appetite. In addition, when non-cooperative face recognition is used to identify individuals nominated to a watchlist, human reviewers must be employed to adjudicate whether candidate matches are true or false positives … [and that] overall error rates of the hybrid machine-human system must be understood and planned for.[91]

NIST has also conducted a number of FRT-related "Grand Challenge" competitions—including the Face Recognition Grand Challenge (2004-2006) and the Multiple Biometric Grand Challenge (2008-2010) programs—to encourage the FRT community to break new ground in solving biometric research problems.

Testing and Evaluation

Since 2000, NIST has operated a Face Recognition Vendor Testing (FRVT) program to assess the capabilities of facial recognition algorithms for one-to-many identification and one-to-one verification. The voluntary program is open to any organization worldwide, and participants may submit their algorithms on a continuous basis for evaluation. Users include corporate research and development laboratories and universities. Submitted algorithms include commercially available products and prototypes that are not necessarily available as final products ready for integration in

https://www.nist.gov/speech-testimony/facial-recognition-technology-frt-0 (hereinafter, Romine FRT testimony).

[88] NIST, Face In Video Evaluation (FIVE) Face Recognition of Non-Cooperative Subjects (NIST IR8173), March 2017, https://doi.org/10.6028/NIST.IR.8173.

[89] Ibid.

[90] Ibid.

[91] Ibid.

FRT systems. NIST posts performance results for evaluated algorithms on its FRVT website along with the name of the organization that developed the algorithm.[92]

According to NIST, the FRVT program does not train face recognition algorithms.[93] NIST does not provide training data to the software under test, and the software is prohibited from adapting to any data that is passed to the algorithms during a test.[94]

With respect to its 2019 FRVT activities, NIST reported that:

> The 2019 FRVT quantified the accuracy of face recognition algorithms for demographic groups defined by sex, age, and race or country of birth, for both one-to-one verification algorithms and one-to-many identification search algorithms. NIST conducted tests to quantify demographic differences for 189 face recognition algorithms from 99 developers, using four collections of photographs with 18.27 million images of 8.49 million people. These images came from operational databases provided by the State Department, the Department of Homeland Security and the FBI. Previous FRVT reports documented the accuracy of these algorithms and showed a wide range in accuracy across algorithms. The more accurate algorithms produce fewer errors and can therefore be anticipated to have smaller demographic differentials.
>
> NIST Interagency Report 8280,[95] released on December 19, 2019, quantifies the effect of age, race, and sex on face recognition performance. It found empirical evidence for the existence of demographic differentials in face recognition algorithms that NIST evaluated. The report distinguishes between false positive and false negative errors, and notes that the impacts of errors are application dependent.[96]

In interpreting the results of the 2019 FRVT report on demographic effects, one should note that the study used high-quality, standards-compliant images, not image data from the Internet nor from video surveillance. Thus, demographic differentials from images in such everyday scenarios were not evaluated. Some stakeholders have criticized such limitations in analyzing FR algorithms and called for more testing "in the field under real-life conditions."[97]

With respect to its 2018 FRVT, NIST reported that:

> The 2018 FRVT tested 127 facial recognition algorithms from the research laboratories of 39 commercial developers and one university, using 26 million mugshot images of 12 million individuals provided by the FBI. The 2018 FRVT measured the accuracy and speed of one-to-many facial recognition identification algorithms. The evaluation also contrasted

[92] NIST, "FRVT 1:1 Leaderboard," https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt. The FRVT 1:1 Leaderboard shows the top performing 1:1 algorithms measured on false non-match rate across several different datasets.

[93] According to NIST, "The process of training a face recognition algorithm (or any machine learning algorithm) involves providing a machine learning algorithm with training data to learn from. The training data shall contain the correct answer, which is known as ground-truth label, or a target. The learning algorithm finds patterns in the training data that map the input data attributes to the target and builds a machine-learning model that captures these patterns. This model can then be used to get predictions on new data for which the target is unknown." See Romine FRT testimony.

[94] Romine FRT testimony.

[95] NIST, *Face Recognition Vendor Test (FRVT), Part 3: Demographic Effects (NIST IR8280)*, December 19, 2019, https://doi.org/10.6028/NIST.IR.8280. This is the third in a series of reports on the 2019 FRVT activities that extends the evaluations from parts 1 and 2—which covered the performance of one-to-one and one-to-many face recognition algorithms, respectively—to document accuracy variations across demographic groups.

[96] Romine FRT testimony.

[97] Darrell M. West, *10 Actions That Will Protect People From Facial Recognition Software*, Brookings report, October 31, 2019, https://www.brookings.edu/research/10-actions-that-will-protect-people-from-facial-recognition-software/.

> mugshot accuracy with that from lower quality images. The findings, reported in *NIST Interagency Report 8238*,[98] showed that massive gains in accuracy have been achieved since the FRVT in 2013, which far exceed improvements made in the prior period (2010-2013).
>
> The accuracy gains observed in the 2018 FVRT study stem from the integration, or complete replacement, of older facial recognition techniques with those based on deep convolutional neural networks. While the industry gains are broad, there remains a wide range of capabilities, with some developers providing much more accurate algorithms than others do. Using FBI mugshots, the most accurate algorithms fail only in about one quarter of one percent of searches, and these failures are associated with images of injured persons and those with long time lapse since the first photograph. The success of mugshot searches stems from the new generation of facial recognition algorithms, and from the adoption of portrait photography standards first developed at NIST in the late 1990s.[99]

Technical Guidance and Scientific Support

NIST provides technical guidance and scientific support to various U.S. government and law enforcement agencies for the use of FRT. For example, NIST's research supported DHS's transition from a 2-fingerprint to a 10-fingerprint collection standard for visa application and entry into the United States to prevent terrorism and identity fraud as well as to prevent criminals and immigration violators from crossing U.S. borders. In addition, NIST is working with CBP to analyze performance effects of image quality and traveler demographics, and to provide recommendations regarding match algorithms, optimal thresholds, and match gallery creation for TVS. NIST's work also supports the FBI and the Office of the Director of National Intelligence's Intelligence Advanced Research Projects Activity (IARPA).[100]

[98] NIST, *Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification (NIST IR8238)*, November 2018, https://doi.org/10.6028/NIST.IR.8238. This report was subsequently updated and extended by NIST as *Face Recognition Vendor Test (FRVT) Part 2: Identification, NIST Interagency Report 8271*, September 2019, https://doi.org/10.6028/NIST.IR.8271.

[99] Romine FRT testimony.

[100] Romine FRT testimony.

Standards

The United States has a voluntary, consensus-based standards development system.[101] Under the National Technology Transfer and Advancement Act of 1995 (P.L. 104-113)[102] and OMB Circular A-119,[103] NIST is charged with promoting coordination between the public and private sectors in the development of standards and in conformity assessment activities, encouraging and coordinating federal agency use of voluntary consensus standards in lieu of government-unique standards, and coordinating federal agency participation in the development of relevant standards.

NIST leads national and international consensus standards activities in biometrics, such as FRT, to ensure that they are interoperable, reliable, secure, and usable.

The following examples of NIST consensus standards development activities illustrate NIST's role in this arena:

Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information (ANSI/NIST-ITL 1-2011 Update: 2015), published by the American National Standards Institute and NIST, is a biometric standard used in 160 countries to facilitate the exchange of biometric data across jurisdictional lines and between dissimilar systems. This standard allows accurate and interoperable exchange of biometrics information by law enforcement agencies globally, assisting in the identification of criminals and terrorists. The standard continues to evolve to support government applications, including law enforcement, homeland security, and other identity

[101] According to the American National Standards Institute (ANSI):

> The U.S. standardization system reflects a market-driven and highly diversified society. It is a decentralized system that is naturally partitioned into industrial sectors and supported by independent, private sector standards developing organizations (SDOs). It is a demand-driven system in which standards are developed in response to specific concerns and needs expressed by industry, government, and consumers. And it is a voluntary system in which both standards development and implementation are driven by stakeholder needs…. Voluntary standards serve as the cornerstone of the distinctive U.S. infrastructure. These documents arise from a formal, coordinated, consensus-based and open process. Their development depends upon data gathering, a vigorous discussion of all viewpoints, and agreement among a diverse range of stakeholders…. Voluntary refers only to the manner in which the standard was developed; it does not necessarily refer to whether compliance to a consensus standard is optional or whether a government entity or market sector has endorsed the document for mandatory use. Most other countries adhere to a "top-down" approach to standardization where the government or groups closely coupled to government either serve as the standards setter or mandate what standards will be developed.

(American National Standards Institute, "Overview of the U.S. Standardization System," https://www.standardsportal.org/usa_en/standards_system.aspx.) ANSI was founded in 1918 by five engineering societies and three federal agencies (the Departments of War, Navy, and Commerce). ANSI is the sole U.S. representative and dues-paying member of the two major non-treaty international standards organizations, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

[102] Codified at 15 U.S.C. Section 272(b), which directs the Secretary of Commerce, through the NIST director, "to facilitate standards-related information sharing and cooperation between Federal agencies and to coordinate the use by Federal agencies of private sector standards, emphasizing where possible the use of standards developed by private, consensus organizations" and "to coordinate technical standards activities and conformity assessment activities of Federal, State, and local governments with private sector technical standards activities and conformity assessment activities, with the goal of eliminating unnecessary duplication and complexity in the development and promulgation of conformity assessment requirements and measures."

[103] Executive Office of the President, Office of Management and Budget, Circulars, https://www.whitehouse.gov/omb/information-for-agencies/circulars/.

management applications. According to NIST, the standard is used for nearly all law enforcement biometric collections worldwide.[104]

NIST has also led and provided technical expertise for the development of international biometric standards in ISO/IEC Joint Technical Committee 1, Subcommittee 37 (JTC1/SC37) – Biometrics.[105] The standards developed by the subcommittee, which was established in 2002, are broadly used nationally and internationally. Since 2006, the subcommittee has published standards on biometric performance testing and reporting (including guidance on principles and framework, testing methodologies, modality-specific testing, interoperability performance testing, and access control scenarios), drawing upon NIST technical contributions.

Author Information

Kristin Finklea, Coordinator
Specialist in Domestic Security

Abigail F. Kolker
Analyst in Immigration Policy

Laurie A. Harris
Analyst in Science and Technology Policy

John F. Sargent Jr.
Specialist in Science and Technology Policy

Disclaimer

[104] Romine FRT testimony.

[105] ISO is the International Organization for Standards. IEC is the International Electrotechnical Commission.

RESOLUTION NO. R2025- ____

A RESOLUTION OF THE CITY COUNCIL OF THE CITY OF AURORA, COLORADO, ACCEPTING SUBMISSION OF THE AURORA POLICE DEPARTMENT'S FACIAL RECOGNITION ACCOUNTABILITY REPORTS IN ACCORDANCE WITH C.R.S. § 24-18-302(4)

WHEREAS, in 2022, Senate Bill 22-113 was signed into law by Governor Polis, which set forth certain requirements for use of facial recognition services (FRS) by law enforcement agencies; and

WHEREAS, among the requirements, Colorado law enforcement agencies which develop, procure, or use an FRS must submit to their "reporting authority" an "accountability report" in accordance with C.R.S. § 24-18-302(4); and

WHEREAS, the Aurora City Council is the Aurora Police Department's "reporting authority" as defined by C.R.S. § 24-18-301(14); and

WHEREAS, the Aurora Police Department has prepared an accountability report for both FRS it plans to use, specifically Lumen and Clearview AI, which includes the information required by C.R.S. § 24-18-302(2)(a-h); and

WHEREAS, FRS is a valuable investigative tool which can enhance the Aurora Police Department's ability to identify criminal suspects, develop leads in criminal investigations, and provide quicker resolution to victims of crime within the city; and

WHEREAS, FRS will also enhance the Aurora Police Department's ability to identify deceased persons and other individuals who need assistance but are unable to identify themselves due to injury or other incapacity; and

WHEREAS, the Aurora Police Department now submits its accountability reports for Lumen and Clearview AI to City Council; and

WHEREAS, the City Council find that the Aurora Police Department's use of FRS will promote the health, safety, and welfare of the city.

NOW, THEREFORE, BE IT RESOLVED BY THE CITY COUNCIL OF THE CITY OF AURORA, COLORADO, THAT:

Section 1. The City Council accepts submission of the Aurora Police Department's Facial Recognition Accountability Reports for Lumen and Clearview AI in accordance with C.R.S. § 24-18-302.

Section 2. This Resolution shall take effect immediately without reconsideration.

RESOLVED AND PASSED this _____ day of _____ 2025.

_____
MIKE COFFMAN, Mayor

ATTEST:

_____
KADEE RODRIGUEZ, City Clerk

APPROVED AS TO FORM:

PETER A. SCHULTE, CITY ATTORNEY

By: Amanda MacDonald RLA
AMANDA MACDONALD, Assistant City Attorney

Office of the Chief of Police
Memorandum

Date: September 1, 2025

To: Mayor Coffman and City Council

From: Todd Chamberlain, Chief of Police

Through: Jason Batchelor, City Manager

Re: Notice of Intent to Use Facial Recognition Services

Notice of Intent to Use Facial Recognition Services

In 2022, the Colorado legislature passed Senate Bill 22-113, which added sections 24-18-301 through 309 to the Colorado Revised Statutes. The Aurora Police Department (APD) is required under C.R.S. § 24-18-302 to notify City Council of our intent to use Facial Recognition Services (FRS). The Aurora Police Department intends to use FRS primarily as a tool to assist in investigations by enhancing our ability to identify suspects, develop leads, and provide quicker resolutions to victims of crime within the city. FRS will also assist APD in the identification of deceased persons and other individuals who need assistance but are unable to identify themselves due to injury or other incapacity.

Further, in accordance with state law:

- Accountability reports for the specific FRS services that APD intends to use, Lumen and Clearview AI, are included in the materials submitted to City Council for public review and comment;
- A proposed policy governing APD's use of FRS is included in the materials submitted to City Council for public review and comment;
- An online form will be posted on APD's website through which the public can also submit comments to APD; and
- Multiple public meetings on APD's use of FRS will be held through the City Council process, beginning with presentation at the Public Safety, Courts, and Civil Service Committee on September 11, 2025.

Pursuant to C.R.S. § 24-18-302, a Resolution has been presented to City Council seeking acceptance of APD's accountability reports for Lumen and Clearview AI.

CITY OF AURORA
Council Agenda Commentary

Item Title: Photo Speed Enforcement Update
Item Initiator: Danelle Carrel, Manage of Executive Support
Staff Source/Legal Source: Chris Amsler, Lieutenant / Mandy MacDonald, Assistant City Attorney
Outside Speaker: N/A
Strategic Outcome: Safe: Promoting safety in our built environment through effective administration of city codes and ordinances and responding to emergencies appropriately to preserve and enhance the community's sense of security and well-being.

COUNCIL MEETING DATES:

Study Session: N/A

Regular Meeting: N/A

2nd Regular Meeting (if applicable): N/A

Item requires a Public Hearing: ☐ Yes ☐ No

ITEM DETAILS *(Click in highlighted area below bullet point list to enter applicable information.)*

- Waiver of reconsideration requested, and if so, why
- Sponsor name
- Staff source name and title / Legal source name and title
- Outside speaker name and organization
- Estimated time: (For Study Session items only indicate combined time needed for presentation and discussion)

Staff Source: Chris Amsler, Lieutenant
Legal Source: Mandy MacDonald, Assistant City Attorney

ACTIONS(S) PROPOSED *(Check all appropriate actions)*

☐ Approve Item and Move Forward to Study Session
☐ Approve Item and Move Forward to Regular Meeting
☒ Information Only
☐ Approve Item with Waiver of Reconsideration
Reason for waiver is described in the Item Details field above.

☐ Approve Item as Proposed at Policy Committee
☐ Approve Item as Proposed at Study Session
☐ Approve Item as Proposed at Regular Meeting

PREVIOUS ACTIONS OR REVIEWS:

Policy Committee Name: N/A

Policy Committee Date: N/A

Action Taken/Follow-up: ***(Check all that apply)***

☐ Recommends Approval ☐ Does Not Recommend Approval

☐ Forwarded Without Recommendation ☐ Minutes Not Available

☐ Minutes Attached

HISTORY *(Dates reviewed by City council, Policy Committees, Boards and Commissions, or Staff. Summarize pertinent comments. ATTACH MINUTES OF COUNCIL MEETINGS, POLICY COMMITTEES AND BOARDS AND COMMISSIONS.)*

N/A

ITEM SUMMARY *(Brief description of item, discussion, key points, recommendations, etc.)*

Presentation to the Committee for overview of the Verra Mobility devices.

FISCAL IMPACT

Select all that apply. (If no fiscal impact, click that box and skip to "Questions for Council")

☐ Revenue Impact ☐ Budgeted Expenditure Impact ☐ Non-Budgeted Expenditure Impact
☐ Workload Impact ☒ No Fiscal Impact

REVENUE IMPACT
Provide the revenue impact or N/A if no impact. (What is the estimated impact on revenue? What funds would be impacted? Provide additional detail as necessary.)

BUDGETED EXPENDITURE IMPACT
Provide the budgeted expenditure impact or N/A if no impact. (List Org/Account # and fund. What is the amount of budget to be used? Does this shift existing budget away from existing programs/services? Provide additional detail as necessary.)

NON-BUDGETED EXPENDITURE IMPACT
Provide the non-budgeted expenditure impact or N/A if no impact. (Provide information on non-budgeted costs. Include Personal Services, Supplies and Services, Interfund Charges, and Capital needs. Provide additional detail as necessary.)

WORKLOAD IMPACT
Provide the workload impact or N/A if no impact. (Will more staff be needed or is the change absorbable? If new FTE(s) are needed, provide numbers and types of positions, and a duty summary. Provide additional detail as necessary.)

QUESTIONS FOR COUNCIL

Information Only

LEGAL COMMENTS

The City Manager shall be responsible to the council for the proper administration of all affairs of the City placed in his charge and, to that end, he shall have the power and duty to make written or verbal reports to the Council concerning the affairs of the city under his supervision. (City Charter §7-4(e)). (MacDonald)

Photo Speed Enforcement Update

Photo Speed Enforcement Update

Since January 2025

- February 18th, 2025 the Request for Proposal (RFP) was published.
- Several vendors expressed interest in bidding, however only two submitted proposals.
  - Verra Mobility
  - Emergent Enforcement Solutions
- **Verra Mobility** was selected to provide photo speed enforcement services for the City of Aurora.
  - 30 years of experience in the field of photo enforcement.
    - Largest photo enforcement company in operation in the U.S. providing services to Denver, New York, Washington D.C. and Seattle
  - 25 years of operation in Colorado
    - They currently have photo speed enforcement contracts with Boulder, Colorado Springs, Denver, Fort Collins, Golden, Greeley, Loveland, and Sheridan.
  - They have a variety of equipment options for photo enforcement, including automated systems.
  - Charge per month to the City of Aurora for 24-hour, 7 day a week coverage is $17,000 a month.
  - Per Verra Mobility the anticipated ticket volume will be 2,203 tickets a month.
  - Anticipated gross violation revenue is $61, 684 a month.
    - 2 tickets an hour from 2 units, 70% payment rate of the standard $40 violation.

Photo Speed Enforcement Update

Verra Mobility

- NK7 transportable photo speed enforcement devices.
- The devices smaller footprint allow for unrestricted deployment in compact areas.
- Each unit is equipped with GPS units, geofencing, anti-tip/shaking and movement alarms. Designed to withstand extreme weather and deter vandalism.
- The devices is equipped with state-of-the-art RADAR and video equipment.
- 2 devices will be deployed on residential streets, school zones and roadways bordering municipal parks.
- They will be deployed at a new location on a weekly or bi-weekly basis.
- Each device is battery operated to ensure 24-hour a day coverage.

Photo Speed Enforcement Update

Verra Mobility

- Verra Mobility will be responsible for the deployment, maintenance and upkeep of the devices.
- They are creating a "back-office" software system for the processing of violations and notices. This also includes data tracking.
  - All violation reviews will be conducted by a COA contract employee (who started on September 2nd) to verify that a violation has occurred before a notice is sent to the registered owner.
- They will provide customer support through a website and telephone phone center.
  - Public can view the evidence.
  - Request a hearing on-line
  - A customized FAQ section.
- They will handle payment processing to include process server and collection services.
  - Payments are accepted by mail, on-line, phone or in-person
- Other services they will provide:
  - Training
  - Expert testimony
  - Public relations support

Photo Speed Enforcement Update

Next Steps

- Finishing up the business rules and contract amendment for process server and collection services (Verra & COA).
- Building of the back-office software system (Verra).
- Equipment construction expected to be completed on October 5th (Verra).
- Training of police and other city staff on the use of the back-office software expected to take place in October.
- Public awareness campaign. Verra and APD Public Information staff have already begun discussions and planning (Verra & COA).

Photo Speed Enforcement Update

Next Steps

- Warning live date: October 28th, 2025

- Violation live date: **November 27th, 2025**

Aurora Police Department
Traffic Section

CITY OF AURORA
Council Agenda Commentary

Item Title: Socioeconomic Sales and Services Impact Permit
Item Initiator: Trevor Vaughn, Manager of Licensing, Finance Department
Staff Source/Legal Source: Trevor Vaughn, Manager of Licensing / Hanosky Hernandez, Sr. Assistant City Attorney
Outside Speaker: N/A
Strategic Outcome: Safe: Promoting safety in our built environment through effective administration of city codes and ordinances and responding to emergencies appropriately to preserve and enhance the community's sense of security and well-being.

COUNCIL MEETING DATES:

Study Session: 10/6/2025

Regular Meeting: 10/20/2025

2nd Regular Meeting (if applicable): 11/3/2025

Item requires a Public Hearing: ☐ Yes ☐ No

ITEM DETAILS *(Click in highlighted area below bullet point list to enter applicable information.)*

- Waiver of reconsideration requested, and if so, why
- Sponsor name
- Staff source name and title / Legal source name and title
- Outside speaker name and organization
- Estimated time: (For Study Session items only indicate combined time needed for presentation and discussion)

Sponsor: Danielle Jurinsky
Staff Source / Legal Source: Trevor Vaughn, Manager of Licensing / Hanosky Hernandez, Sr. Assistant City Attorney
Estimate Time : 15 minutes

ACTIONS(S) PROPOSED *(Check all appropriate actions)*

☒ Approve Item and Move Forward to Study Session
☐ Approve Item as Proposed at Policy Committee
☐ Approve Item and Move Forward to Regular Meeting
☐ Approve Item as Proposed at Study Session
☐ Information Only
☐ Approve Item as Proposed at Regular Meeting
☐ Approve Item with Waiver of Reconsideration
Reason for waiver is described in the Item Details field above.

PREVIOUS ACTIONS OR REVIEWS:

Policy Committee Name: Public Safety, Courts & Civil Service

Policy Committee Date: 9/11/2025

Action Taken/Follow-up: ***(Check all that apply)***

☐ Recommends Approval

☐ Does Not Recommend Approval

☐ Forwarded Without Recommendation

☐ Minutes Not Available

☐ Minutes Attached

HISTORY *(Dates reviewed by City council, Policy Committees, Boards and Commissions, or Staff. Summarize pertinent comments. ATTACH MINUTES OF COUNCIL MEETINGS, POLICY COMMITTEES AND BOARDS AND COMMISSIONS.)*

N/A

ITEM SUMMARY *(Brief description of item, discussion, key points, recommendations, etc.)*

This item is a proposed ordinance establishing a Socioeconomic Impact Permit, designed to prevent the overconcentration of certain retail sales and services that disproportionately target diverse, lower-income communities. Concentrations of such businesses have been found to contribute to the appearance of blight, increase both the incidence and fear of crime, and exacerbate negative health and economic outcomes within these communities.

The American Planning Association's *Equity in Zoning Guide*, Permitted Use Policy #11, recommends that communities "revise permitted use regulations to reverse the overconcentration of convenience stores, cannabis outlets, safe injection sites, and other facilities that provide easy access to health-compromising substances like alcohol and tobacco in historically disadvantaged and vulnerable communities."

The proposed permit will grandfather in existing businesses, which will automatically be issued a permit corresponding with the term of their General Business License. The proposal takes the form of a permit, rather than a zoning regulation, in order to address not only spacing requirements but also operational standards consistent with Crime Prevention Through Environmental Design (CPTED). This approach also allows for a dynamic process to prevent such operations from concentrating in dilapidated shopping centers or in areas identified as having elevated crime risk through Risk Terrain Modeling (RTM).

When concentrated, these operations also detract from a balanced retail environment and can trigger a downward spiral of blight. In coordination with the derelict property ordinance recently adopted by City Council, this ordinance will apply pressure to commercial property owners to reinvest in their properties in order to attract a healthier and more balanced retail mix.

The ordinance classifies the following operations as Socioeconomic Impact Retail Sales and Services with the number of estimated operations in the city:

- Secondhand buyers (excluding specialty retailers) - 3
- Pawnshops - 14
- Head shops - 1
- Vape and smoke shops - 62
- Rent-to-own stores - 4
- Bail bond services - 1
- Check-cashing and payday loan businesses - 10
- Extended-occupancy motels - 16
- Retail liquor stores - 85
- Marijuana retail stores - 24
- Convenience stores that sell alcohol or tobacco - 148
- Bars, hookah lounges, and event centers operating after midnight in areas of elevated risk – N/A

Additionally, there are four bus junctions and nine light rail stations identified as major transit locations for purposes of spacing the operations.

Permit Provisions

Permits will be issued automatically to existing businesses but may be revoked if the operation:

- Consistently exhibits a pattern of neglect,
- Ceases operation for six months or more, or
- Commits public nuisance violations in an area of elevated risk.

In evaluating violations, the extent to which an operation has incorporated CPTED practices will be considered an aggravating or mitigating factor. The General Business License will serve as the application for the permit, but supplemental information will be required if the proposed operation is located in an area of elevated risk.

Spacing and Location Requirements
The ordinance establishes the following restrictions:

- No new businesses of the same type within 2,000 feet (e.g., a new liquor store must be at least 2,000 feet from an existing liquor store).
- No Socioeconomic Impact operation may locate within 300 feet of another Socioeconomic Impact operation.
- No operation may locate within 1,000 feet of an extended-occupancy motel.
- No operation may locate within 500 feet of a light-rail station or major bus junction.
- No operation may locate in a retail center exhibiting blight or with more than 50% vacancy.

Bars, hookah lounges, and event centers operating after midnight are not subject to spacing restrictions.

Only convenience stores that sell alcohol, tobacco or other age restricted substances will be considered Socioeconomic Impact operations subject to distance limitations (including the 2,000-foot separation requirement). Convenience stores that do not sell age restricted substances will not be considered Socioeconomic Impact operations.

Current distance restrictions include two miles between pawnshops, 1,500 feet in state law between liquor stores, 500 feet from schools for alcohol and tobacco sales. No distance restrictions on tobacco sales regarding concentration.

The permit could also allow for a fee upon renewal to cover costs for a Risk Terrain Modeling software to establish the areas of elevated risk and to assist in policing and other community interventions in those areas. The city has not yet acquired such software and would need to continue evaluating the feasibility of its incorporation. The cost is estimated to be $24,000 annually. The number of anticipated number of permit holders is 370 which would equate to an estimated $130 biennial permit cost to cover the costs of the software.

FISCAL IMPACT

Select all that apply. (If no fiscal impact, click that box and skip to "Questions for Council")

☒ Revenue Impact ☒ Budgeted Expenditure Impact ☐ Non-Budgeted Expenditure Impact
☒ Workload Impact ☐ No Fiscal Impact

REVENUE IMPACT
Provide the revenue impact or N/A if no impact. (What is the estimated impact on revenue? What funds would be impacted? Provide additional detail as necessary.)

Estimated annual revenue of $24,000 upon renewal of permit.

BUDGETED EXPENDITURE IMPACT
Provide the budgeted expenditure impact or N/A if no impact. (List Org/Account # and fund. What is the amount of budget to be used? Does this shift existing budget away from existing programs/services? Provide additional detail as necessary.)

Estimated $24,000 for Risk Terrain Modeling software.

NON-BUDGETED EXPENDITURE IMPACT
Provide the non-budgeted expenditure impact or N/A if no impact. (Provide information on non-budgeted costs. Include Personal Services, Supplies and Services, Interfund Charges, and Capital needs. Provide additional detail as necessary.)

N/A

WORKLOAD IMPACT

Provide the workload impact or N/A if no impact. (Will more staff be needed or is the change absorbable? If new FTE(s) are needed, provide numbers and types of positions, and a duty summary. Provide additional detail as necessary.)

There will be additional workload for reviewing and processing the permits and spacing analysis. Potential long term reduction in need for city services.

QUESTIONS FOR COUNCIL

Does council approve of forwarding the ordinance for full council consideration at study session?

LEGAL COMMENTS

The City Council shall have and shall exercise the powers, privileges and duties granted and conferred by the state constitution, statute, or City Charter. The City Council shall have power to make and publish from time to time ordinances, and to pass Resolutions and Motions, not inconsistent with the laws of the state for carrying into effect or discharging the powers and duties conferred by the state constitution, statute or City Charter and such as it shall deem necessary and proper to provide for the safety; preserve the health; promote the prosperity; and improve the morals, order, comfort and convenience of the city. City Code Section 2-32. The City Council has found and determined that approving the licensing permit and the business restrictions included in this ordinance fulfill these purposes. City Council shall act only by ordinance, resolution or motion. All legislative enactments must be in the form of an ordinance and tthis action will amend the Aurora City Code and therefore shall be taken in the form of an ordinance and shall require a vote of the majority of the Council to be approved. Section 5-1 Aurora City Charter. (Hernandez)

Completed in partial fulfillment of National Institute of Justice (NIJ) award #2012-IJ-CX-0038

A Multi-jurisdictional Test of Risk Terrain Modeling and a Place-based Evaluation of Environmental Risk-Based Patrol Deployment Strategies

Study Overview: A place-based method of evaluation and spatial units of analysis were used to measure the extent to which allocating police resources to high-risk areas, derived from risk terrain modeling (RTM), affects the frequency and spatial distribution of new crime events. This quasi-experimental project had two primary goals: 1) to replicate and validate RTM in multiple jurisdictions and across many different crime types; and, 2) to evaluate intervention strategies targeted at high-risk micro-level environments across 5 cities[1]: Chicago, IL; Colorado Springs, CO; Glendale, AZ; Kansas City, MO; and Newark, NJ.

In completing the risk terrain models[2], we used the RTMDx Utility, developed by the Rutgers Center on Public Security[3]. Following the RTM analysis in each city, each Police Department developed an intervention strategy that targeted the spatial influences of select significant risk factors. The Police Department also worked with the research team in the selection of target areas for the intervention. In evaluating the intervention, statistical comparisons were made to equivalent control areas locally within each city. Control areas were matched to treatment areas through Propensity Score Matching (PSM). Interventions in each city lasted approximately 3 months, and were implemented in 2013 and/or 2014. The post-intervention period was 90 days (3 months).

General Findings:

Q: Do RTM outputs inform crime intervention planning and policing activities in ways that result in significant crime reductions in targeted areas?

A: Yes. Results across all study settings allow for a general conclusion that certain actions performed by police and intended to mitigate the spatial influence of risky features at high-risk places results in both short- and long-term crime reductions. RTM enabled police to make informed decisions and develop strategies about where to allocate resources and what to do when they got there. Spatial information produced through RTM to select target areas, develop place-based risk reduction strategies, and deploy resources was applied to a variety of crime types and customized for different settings in measured, transparent and sustainable ways. Crime reductions were best achieved by police with a concerted and consistent application of intervention activities geared toward mitigating the spatial influence of crime attractors at the high-risk places within a jurisdiction.

Specific Findings:

Colorado Springs

Risk Terrain Modeling Analysis:

The Colorado Springs Police Department (CSPD) identified Motor Vehicle Theft as their priority crime. A Risk Terrain Model was found that contains 6 risk factors (out of 19 tested): Disorder Calls for Service (RRV^4=5.61), Multifamily Housing Units (RRV=2.75), Foreclosures (RRV=2.64), Parks (RRV=1.76), Sit-down Restaurants (RRV=1.51), and Commercial Zoning (RRV=1.37). Highest risk places[5] have 48 times greater likelihood of crime than some other locations. Conjunctive Analysis of Risk Factor Configurations (CARFC) found that the highest risk behavior settings[6] for Motor Vehicle Theft cover about 4% of the study area and account for nearly 43% of all crime incidents.

Risk-Based Intervention:

To reflect the RTM findings CSPD designed their intervention strategy with an array of activities performed by various CSPD units for the purpose of mitigating disorder problems in the target area: Code Enforcement property inspections, Community Service Officer Neighborhood Cleanups, Community Meetings, Proactive Police Enforcement against disorder offenses, Proactive Traffic Enforcement, and the deployment of License Plate Recognition (LPR) devices for the purpose of identifying stolen Motor Vehicles in the target area.

- A Motor Vehicle Theft reduction of 33% was achieved in the target area compared to the control area during in the post-intervention period. There was a slight diffusion of benefits.
- At the micro level, "code enforcement" was associated with reduced levels of Motor Vehicle Theft throughout the target area (p<0.01). "Code enforcement" activities have an exceptionally strong and significant crime reduction benefit at high-risk places (p<0.01).

Colorado Springs Summary: *The cumulative findings suggest that CSPD's risk-based intervention effectively addressed Motor Vehicle Theft. CSPD's targeting of disorder incidents was an effective crime control strategy. The micro-level analysis suggests that code enforcement focused at micro-level high-risk places is a particularly promising tactic.*

Newark

Risk Terrain Modeling Analysis:

The Newark Police Department (NPD) identified Gun Violence as their priority crime. A Risk Terrain Model was found that contains 11 risk factors (out of 17 tested): Narcotics Arrests (RRV=3.53), Foreclosures (RRV=3.36), Restaurants (RRV=2.76), Gas Stations (RRV=2.54), Convenience Stores (RRV=2.32), Food Take Outs (RRV=2.19), Bars (RRV=2.01), Abandoned Properties (1.43), Schools (RRV=1.38), Liquor Stores (RRV=1.34), and Problem Housing (RRV=1.34). Highest risk places have 58 times greater likelihood of crime than some other locations. CARFC found that the highest risk behavior settings for Gun Violence cover about 5% of the study area and account for nearly 30% of all crime incidents.

Risk-Based Intervention:

To reflect the RTM findings, NPD designed their intervention strategies to generate checks and manager contacts at three business types: Restaurants, Food Take Outs, and Gas Stations. Each day during the intervention, a task force comprised of 3 officers, under the supervision of a Lieutenant, visited businesses located within the target area. Upon visiting the business, officers were required to meet with the on-duty manger and have them sign the sheet, to ensure that proper contact was established.

- A Gun Violence reduction of approximately 35% was achieved in the target area compared to the control area during the post-intervention period. There was a slight diffusion of benefits.
- At the micro level, the intervention activities were associated with a reduction of Gun Violence within the portions of the target area identified as high-risk. The reduction approached statistical significance (p=0.06).

Newark Summary: *The NPD task force's intervention activities were a promising approach to gun violence. The strategy generated a large reduction of gun violence, and had a particularly great impact at high-risk portions of the target area. Newark's outcome evaluation was inherently an assessment of the use of a "task force" as well as the "intervention actions" performed by the task force. Ultimately, significant crime reductions can be achieved when a task force consistently and thoughtfully implements intervention activities at high-risk places.*

Kansas City

Risk Terrain Modeling Analysis:

The Kansas City Police Department (KCPD) identified Aggravated Violence as their priority crime: all shooting incidents (hits and homicides), aggravated assault (with a firearm), and street robbery (with and without a weapon). A significant Risk Terrain Model was found that contains 15 risk factors (out of 21 tested): Bus Stops (RRV=3.38), Weapon Offending Parolees and Probationers (RRV=3.20), Suspicious Person with a Weapon Calls-for-service (RRV=2.43), Variety Stores (RRV=2.28), Packaged Liquor Stores (RRV=2.28), Hotels (RRV=2.27), Fast Food Restaurants (RRV=2.18), Drug Markets (RRV=2.11), Bars (RRV=2.05), Rental Halls (RRV=1.61), Restaurants (RRV=1.41), Convenience Stores (RRV=1.41), Grocery Stores (RRV=1.28), Foreclosures (RRV=1.27), Liquor Licensed Retailers (RRV=1.24). Highest risk places have 46 times greater likelihood of crime than some other locations. CARFC found that the highest risk behavior settings for Aggravated Violence cover about 4% of the study area and account for nearly 38% of all crime incidents.

Risk-Based Intervention:

To reflect the RTM findings, KCPD designed their intervention strategies to address nightclubs, suspicious person with a weapon calls-for-service, weapon offending parolees and probationers, drug sales, packaged liquor stores, and liquor licensed retailers[7]. An array of activities intended to mitigate the spatial influences of these risk factors, enhance community awareness, and deter motivated offenders was conducted by various KCPD units and city officials in the target area: Code Enforcement, Directed Patrols, Licensing and Inspection checks, meet-and-greets with known offenders juxtaposed with social service referrals/support, CPTED inspections, Pedestrian Checks, Area Presence, Residence Checks, Traffic Violations, and Building Checks. A new protocol for dispatching officers to certain calls-for-service locations was also enacted.

- Aggravated Violence decreased by 12% in the target area compared to the control area during the post-intervention period, but the findings did not achieve statistical significance.
- At the micro level, and in the during-intervention period, Pedestrian Checks, Area Presence, and Residence Checks were each associated with lower levels of Aggravated Violence throughout the entirety of the target area. In the post-intervention period, Building Checks conducted within high-risk areas were associated with reduced crime levels.

Kansas City Summary: *RTM enabled Kansas City police officials to make decisions about where to allocate resources and what to do when they got there in order to suppress crime in the short-term and reduce crime occurrence over the long-term. Intervention activities affect crime differently over varying times and places. Synthesizing results from the micro level analyses, it can be generally concluded that "pedestrian checks", "directed patrol", and "knock-and-talks" have the greatest impact on reducing crime among all places within*

the target areas when sustained, whereas longer-term crime reduction benefits at high-risk places are best achieved via "building checks".

Glendale

Risk Terrain Modeling Analysis:

The Glendale Police Department (GPD) identified Robbery as their priority crime. A Risk Terrain Model was found that contains 7 risk factors (out of 11 tested): Drug-related Calls for Service (RRV=15.56), Convenience Stores (RRV=2.88), Take Out Restaurants (RRV=2.54), Apartment Complexes (RRV=2.53), Gang Member Residences (RRV=2.41), Liquor Stores (RRV=2.30), and Bars (RRV=2.19). Highest risk places have 58 times greater likelihood of crime than some other locations. CARFC found that the highest risk behavior settings for Robbery cover about 1% of the study area and account for nearly 17% of all crime incidents.

Risk-Based Intervention:

To reflect the RTM findings, GPD designed their intervention strategy to address all 7 risk factors. The activities included Directed Patrols, Flyer Distribution, Community Meetings and Engagement Activities, Proactive Stops, and Proactive Arrests.

- Robbery decreased by 42% in the target area compared to the control area during the intervention period. There was a very strong diffusion of benefits effect.
- At the micro level, and in the during-intervention period, Directed Patrols were associated with lower levels of Robbery. Flyer Distribution activities were associated with fewer Robberies in the post-intervention period, with the reduction approaching statistical significance (p=0.09).

Glendale Summary: *The intervention produced a statistically significant reduction of Robbery throughout the target area during the intervention period. In addition, there was a diffusion of benefits beyond the targeted area. "Directed patrol" had the greatest impact on reducing crime among all micro-level places within the target areas during the intervention period, whereas longer-term crime reduction benefits were best achieved via "flyer distribution".*

Chicago

Risk Terrain Modeling Analysis:

The Chicago Police Department (CPD) identified Shootings as their priority crime. A Risk Terrain Model was found that contains 10 risk factors (out of 15 tested): Foreclosures (RRV=5.38), Problem Buildings (RRV=3.72), Gang Hotspots (RRV=2.86), Laundromats (RRV=2.27), Liquor Stores (RRV=1.92), Gas Stations (RRV=1.65), 311 Lights Out Calls (RRV=1.41), Schools (RRV=1.35), Bus Stops (RRV=1.33), Bars (RRV=1.28). Highest risk places have 76 times greater likelihood of crime than some other locations. CARFC found that the highest risk behavior settings[8] for Shootings cover about 15% of the study area and account for nearly 56% of all crime incidents.

Risk-based Intervention:

To reflect the RTM findings the CPD designed an intervention strategy that focused on Foreclosures and Problem Buildings. The strategy entailed the CPD working in partnership with other City of Chicago departments to conduct site visits of known problem properties throughout the city to improve conditions conducive to crime and, when necessary, issue citations for code violations. City agencies also sought to work with private lenders to address the broader scope of the foreclosure crisis.

- A process evaluation found that CPD could not manage to collect measurement data in a systematic or coordinated way to allow for adequate evaluations of outcomes. Cumulative totals of building inspections and citations were 280 and 24, respectively. But CPD was unable to provide incident-specific information including the precise date, time, and location of each action. Therefore, we were unable to complete an outcome evaluation of CPD's intervention[9].

Endnotes

[1] Originally, 6 cities were proposed as study settings for interventions. However, Arlington, TX withdrew from the study early on due to excessive turnover of personnel within the department.
[2] Using then-current data from calendar year 2012
[3] www.rutgerscps.org
[4] Relative Risk Value (RRV)
[5] Places with risk values greater than 2 standard deviations above the mean risk value, according to the risk terrain map.
[6] The behavior settings with a relative frequency of crime (RFC) above the mean
[7] "Packaged liquor stores" refer to businesses whose primary purpose is to sell liquor. "Liquor licensed retailers" are facilities that are in business to sell other items, but also sell liquor, such as convenience stores, grocery stores, etc.
[8] The behavior settings with a relative frequency of crime (RFC) above the mean
[9] It should be noted that during this project, there were mayoral elections (and subsequent run-off elections), internal transfers/promotions of police personnel, and multiple other research projects (unaffiliated with ours) that may have strained CPD's data management resources.

ORDINANCE NO. 2025- ____

A BILL

FOR AN ORDINANCE OF THE CITY COUNCIL OF THE CITY OF AURORA, COLORADO, AMENDING THE AURORA CITY CODE BY AMENDING DIVISION 4 OF ARTICLE VI OF CHAPTER 86 ESTABLISHING A SUPPLEMENTAL LICENSE FOR SOCIOECONOMIC IMPACT RETAIL SALES AND SERVICES

WHEREAS, the City of Aurora, Colorado, (the "City"), is a home rule municipality, organized and existing under and by virtue of Article XX, Section 6 of the Colorado Constitution, and it has the power to regulate matters of local concern; and

WHEREAS, the City recognizes certain types of retail businesses that have been associated through academic research with elevated rates of crime and public disorder in surrounding areas, especially when concentrated; and

WHEREAS, these types of businesses often cluster in low-income neighborhoods, disproportionately impacting communities that already face economic and social challenges; and

WHEREAS, the overconcentration of such establishments can undermine neighborhood vitality, deter investment, and contribute to a cycle of blight, vacancy, and diminished public safety through the increase of related crimes; and

WHEREAS, repeated patterns of co-location among high-risk business types can facilitate illicit activities, including open-air drug markets, fencing of stolen goods, and loitering, thus creating conditions that are harmful to public health, safety, and quality of life; and

WHEREAS, the City has a compelling interest in protecting public safety, promoting a healthy and sustainable business environment, and preventing the displacement or marginalization of residents due to the unchecked proliferation of such business operation, and the spacing requirements, caps on business types, and mitigation standards such as lighting, surveillance, and good-neighbor plans are effective tools to manage and reduce cumulative harm without banning lawful business operations; and

WHEREAS, this ordinance is intended to provide reasonable regulations to prevent the overconcentration of such businesses, improve neighborhood conditions, and promote equitable access to a safe and healthy commercial environment for all residents; and

WHEREAS, the City Council hereby finds that it is in the best interest of the City and its citizens to adopt reasonable regulations to promote community health, wellbeing, reduce crime, and support the economic vitality of the city.

NOW, THEREFORE, BE IT ORDAINED BY THE CITY COUNCIL OF THE CITY OF AURORA, COLORADO:

Section 1. The City Code of the City of Aurora is hereby amended by adding a new Division 4 to Article VI to section 86, that shall read as follows:

DIVISION 4. SOCIOECONOMIC IMPACT PERMIT

Sec. 86-696. Definitions.

The following words, terms and phrases, when used in this division, shall have the meanings ascribed to them in this section, except where the context clearly indicates a different meaning:

***Area of Elevated Risk* means an area identified as being elevated risk by the risk terrain model adopted by the City.**

***Bail Bond Office* means a business whose primary purpose is to act as a surety to secure the presence of an accused person at a court proceeding in a criminal manner.**

***Check Cashing or Pay-Day Loan Service Provider* means a non-depository financial institution that provides monetary loans or advances in exchange for a postdated check, electronic access to a bank account, title to a vehicle, or other collateral; or offers to cash checks, drafts, money orders, or other monetary instruments for a fee. This use includes but is not limited to payday lenders, check-cashing businesses, car title loan businesses, and deferred deposit loan providers. This use excludes state or federally chartered banks, credit unions, or savings and loan associations.**

***Convenience Store with Regulated Substances* means any business that is primarily engaged in the retail sale of convenience goods, or both convenience goods and gasoline, and has less than 10,000 square feet of retail floor space and also sells any of the following; Alcohol, Tobacco, Kratom, or Tobacco or Drug Paraphernalia. Convenience store does not include any business where there is no retail floor space accessible to the public.**

***Crime Prevention Through Environmental Design (CPTED)* means architectural design, site design, operational, and landscape design principles and standards intended to reduce the fear and incidence of crime, and to improve the quality of life.**

***Extended Occupancy Motel* means: A facility originally constructed as a motel or hotel for transient occupancy, which offers rooms or units for rent without a lease, but where most occupants stay for extended periods of time (typically**

30 days or more), often using the premises as a primary or long-term residence. These establishments may advertise daily or weekly rates but effectively function as long-term housing without the protections or infrastructure associated with permanent residential use.

Head Shop or Drug Paraphernalia Store **means a retail establishment that substantially sells, offers for sale, or displays for sale any drug paraphernalia as defined by state or local law, including but not limited to pipes, water pipes, bongs, rolling papers, roach clips, grinders, scales, vaporizers, or other items designed or marketed for use with marijuana, tobacco, or controlled substances.**

High Risk After Midnight Operations **Tavern, Bar, Hookah Lounge, or Event Center as defined in the unified development ordinance with operations after midnight located in an area of elevated risk.**

Rent-to-Own Store **means a business that offers rental agreements with optional ownership terms for furniture, electronics, or appliances, where customers make periodic payments with no obligation to purchase. This definition applies only to businesses where rent-to-own is the primary method of transaction and does not include general retail stores or electronics/furniture outlets offering traditional sales or third-party financing.**

Retail Liquor Store **means a type of retail sales that includes a business licensed by the state for the retail sale of alcoholic beverages in original packages for consumption off the premises, in which those sales are the primary goods being sold and generate the majority of the revenue generated by the business. The accessory sales of food or other items shall not result in the business being a general retail sales business if the above conditions are met.**

Risk Terrian Model **means the risk assessment technique and diagnostic method for identifying the spatial attractors of criminal behavior and environmental factors that are conducive to crime.**

Socioeconomic Impact Sales and Services Business **means:**

(1) Secondhand buyers, head shops or drug paraphernalia stores, vape and smoke shops, rent-to-own stores, bail bond office, check cashing or payday loan service provider, extended occupancy motel, pawnbroker, retail liquor stores, marijuana retail stores, convenience stores with regulated substances.

(2) High risk after midnight operations when located in an area of elevated risk.

Secondhand Buyer **means a secondhand dealer or scrap metal buyer engaged in the purchase and resale of used or secondhand tangible personal property as a principal component of its operations, where such property includes a broad range of merchandise not limited to a specific product category or engages in purchases primarily for wholesale. This includes, but is not limited to, businesses that routinely acquire items such as electronics, jewelry, tools, small appliances, personal devices, or other portable goods commonly associated with theft. A Secondhand Buyer shall not include Specialty Secondhand Retailers.**

Specialty Secondhand Retailer **means a secondhand dealer primarily engaged in the retail sale of goods within a narrow and defined category such as books, video games, musical instruments, vintage clothing, children's goods, or sporting goods and for which the purchase of secondhand goods is incidental to the primary retail purpose and limited to items within that specialized category.**

Vape Store or Smoke Shop **means a retailer business or any person that: sells, offers for sale, or offers to exchange for any form of consideration, tobacco, nicotine, hemp products, kratom products, tobacco paraphernalia, marijuana paraphernalia, vaping devices, or other drug paraphernalia; and has fifteen percent (15%) or more of the square feet in the establishment used for the sale or display of those products.**

Sec. 86-697. Permit Required

(a) It shall be unlawful for any person to operate a socioeconomic impact sales or service business without a socioeconomic impact permit.

Sec. 86-698. Term

(a) Socioeconomic Impact Permits shall correspond with the term of the General Business License.

(b) Socioeconomic Impact Sales and Services in operation upon the effective date of this ordinance shall automatically be issued a Socioeconomic Impact Permit.

(c) Permits shall renew concurrently with the General Business License, unless revoked or non-renewed, provided the business remains in operation and complies with all applicable conditions and regulations.

Sec. 86-699. Suspension or revocation.

(a) In addition to the reasons set forth in section 86-47, the director shall suspend or revoke any permit issued under this division if they find that

the permittee has committed a violation of any of the provisions of this division.

(b) If the permit holder is located in an area of elevated risk:

1. **Violations of 86-47(10) shall be considered an aggravating factor in any suspension or revocation proceeding if those violations are contributing factors to the elevated risk.**
2. **To the extent the permit holder has or has not implemented Crime Prevention Through Environmental Design strategies shall be considered as mitigating or aggravating factors.**

(c) A permit may also be suspended, revoked or not renewed if:

1. **The property where the business is located exhibits a consistent pattern of neglect or code violations.**
2. **The business discontinues operations for six or more consecutive months.**
3. **The business fails to adhere to the approved operational or mitigation plan submitted with the application.**
4. **Violations of 86-47(9).**

Sec. 86-700. Permit application.

(a) The application for a general business license application shall also function as the application for the permit.
(b) In areas of elevated risk, the application for a permit will need to be supplemented with information demonstrating a realistic business and financial plan with investment and other operational offsets and Crime Prevention Through Environmental Design measures to demonstrate that the issuance of the permit will not further elevate the risk level of the area.

Sec. 86-701. Permit denial.

(a) The director shall deny the permit if the location does not meet the distance restrictions identified in section 86-971.
(b) Subsection (a) shall not apply to businesses in operation, or any businesses already under a review or approval process, prior to the effective date of the ordinance and such businesses shall be permitted to sell their operation to a new operator as long as the business is continuously operated as the same or similar nature of business and does not otherwise violate this section leading to revocation or non-renewal of the permit.

Sec. 86-702. Location of Socioeconomic Impact Retail Sales and Services.

(a) No permit shall be issued if the socioeconomic impact sales and services business is:

1. **Within 2,000 feet of a business of the same type unless more restrictive by the city's uniform development ordinance (UDO) or otherwise restricted by state and local licensing codes.**
2. **Within 1,000 feet of an extended occupancy motel.**
3. **Within 300 feet of another socioeconomic impact sales and services business.**
4. **Within 500 feet of a light rail station or transit junction wherein more than one bus line operates through the junction every 15 minutes or more frequently.**
5. **In a retail center exhibiting blight, or with more than 50% vacancy whether or not the units are leased.**
6. **In an area of elevated risk unless the applicant supplements their application with information demonstrating a business and financial plan with investment and other operational offsets as well as CPTED measures to demonstrate that the issuance of the permit will not increase the risk level of the area.**

(b) The distance limitations in subsection (a) numbers 1. through 4. shall not apply to or from high risk after midnight operations.

(c) Distances shall be measured by the nearest portion of the building or unit to be occupied by the applicant to the nearest portion of the building or unit occupied by the existing operation. Distances from the transit junction shall be from the nearest property line of the station parcel or the nearest portion of any transit structure if there is not a separate parcel.

Sec. 86-703. Application to other licenses.

Failure to obtain or maintain the permit required by this section may be used as a basis for denial, nonrenewal, or revocation of any license required by chapter 86 or chapter 6 of the Aurora City Code.

Section 86-704. Rulemaking powers. The City Manager, the Director of Finance, or designee, is hereby authorized and shall make all necessary rules and regulations, including the imposition of fees to cover the costs for the administration of this Division.

Section 2. Severability. The provisions of this Ordinance are hereby declared to be severable. If any section, paragraph, clause, or provision of this Ordinance shall, for any reason, be held to be invalid or unenforceable by a court of competent jurisdiction, the

invalidity or unenforceability of such section, paragraph, clause, or provision shall not affect any of the remaining provisions of this Ordinance.

Section3. Pursuant to Section 5-5 of the Charter of the City of Aurora, Colorado, the second publication of this Ordinance shall be by reference, utilizing the ordinance title. Copies of this Ordinance are available at the Office of the City Clerk.

Section 4. Repealer. All orders, resolutions, or ordinances in conflict with this Ordinance or with any of the documents hereby approved, are hereby repealed only to the extent of such conflict. This repealer shall not be construed as reviving any resolution, ordinance, or part thereof, heretofore repealed.

INTRODUCED, READ AND ORDERED PUBLISHED this _____ day of _____, 2025.

PASSED AND ORDERED PUBLISHED this _____ day of _____, 2025.

_____
MIKE COFFMAN, Mayor

ATTEST:

_____
KADEE RODRIGUEZ, City Clerk

APPROVED AS TO FORM:

PETER A. SCHULTE, CITY ATTORNEY

By: Hanosky Hernandez HK
HANOSKY HERNANDEZ, Sr. Assistant City Attorney