RECOMMENDATION TO COUNCIL

Public Safety Commission

Recommendation Number XXXXXXXX-XXX: Strengthening TRUST Act Oversight, Transparency, and Data-Sharing Safeguards

WHEREAS, the Austin Public Safety Commission serves as an advisory body to the City Council on all budgetary and policy matters concerning public safety; and

WHEREAS, the City Council adopted the Transparent and Responsible Use of Surveillance Technology (TRUST) Act to promote transparency, community participation, protection of civil liberties, and responsible use of surveillance technology; and

WHEREAS, surveillance systems, data-sharing networks, and advances in artificial intelligence may allow City personnel to access or analyze information collected by vendors, private entities, or other governmental jurisdictions without the City owning or directly operating the underlying technology; and

WHEREAS, experience in Texas and nationally demonstrates both the public-safety value of appropriate information sharing and risks from overly broad access, unauthorized use, onward dissemination, and vendor-controlled sharing; and

WHEREAS, effective oversight should protect privacy and civil liberties without impeding lawful incident-specific evidence sharing or public-safety operations through transparency regarding external data sources, auditable access records, independent review, and clear limitations on exceptions to ordinary approval requirements;

NOW, THEREFORE, BE IT RESOLVED, the Public Safety Commission recommends that City Council direct the City Manager to strengthen implementation of Transparent and Responsible Use of Surveillance Technology (TRUST) Act, and return with amendments where necessary, to address the following:

1. External surveillance data. Clarify that the TRUST Act applies when a City department obtains standing, recurring, or functionally equivalent access to surveillance information controlled by another entity, including but not limited to an account, portal, searchable database, live feed, bulk transfer, reciprocal network, or regular provision of surveillance data. Receipt of discrete evidence related to a reported incident, specific investigation, missing or endangered person, or specific and documented time-limited public-safety incident should not by itself require separate Council approval, provided it does not create ongoing access or unrelated use or retention.

2. Transparency and independent review. Ensure that the planned publicly accessible online and regularly updated inventory of surveillance technologies and recurring external surveillance-data sources, responsible department, applicable Privacy Impact Assessment (PIA) and Surveillance

Use Policy (SUP), retention and sharing rules, and relevant contracts or agreements are readily available to the public through an online portal, subject to lawful protection of sensitive investigative information.

3. High-risk technologies and exigent use. Require written notice to Council within seven days of any exigent acquisition or use of technologies presenting significant privacy or civil-liberties risks, and Council authorization for continued use beyond 30 days, with appropriate provisions for delayed public disclosure when necessary to protect an active investigation. As is defined in the TRUST Act, such technologies include at minimum automated license plate readers, biometric identification, persistent location tracking, AI-enabled identification or surveillance analytics, and systems providing standing access to external surveillance networks. Such technologies should not qualify for a "minimal or no risk" exception.

4. Access, sharing, auditing, and compliance. For covered systems, external access should be affirmatively authorized rather than automatically or network-wide shared by default, with limits on onward dissemination. Material or repeated violations, or unauthorized vendor or third-party access, should trigger prompt review and, when appropriate, suspension of the affected access or technology until corrected. Emergency information sharing necessary to protect life or required by court order or other binding legal process, should not be delayed but should remain logged and reviewable.

BE IT FURTHER RESOLVED, the Public Safety Commission recommends that these safeguards apply consistently across City departments, including public safety, transportation, and parks, so that substantially similar surveillance activities receive substantially similar oversight regardless of department, funding source, vendor, or ownership of the underlying technology.

Date of Approval:

Motioned By: Seconded By:

Vote:

For:

Against:

Abstain:

Off the dais:

Absent:

Attest: _____

DRAFT