

Agenda

Surveillance Technology Taskforce Overview

What we've been doing

Where we are going

Surveillance Technology Taskforce

Members

Representatives from the following organizations:

Denver City Council, Denver Mayor's Office, Colorado Immigrant Rights Coalition, State and Municipal Public Defender Offices, Office of the Independent Monitor, Denver Citizen Oversight Board, Denver District Attorney's Office, Denver City Attorney's Office, Taskforce for Re-imagining Police, ACLU of Colorado, Denver Police Department, Denver Office of Social Equity and Inclusion, Denver Technology Services, technical and legal subject matter experts

Surveillance Technology Mission

To enhance public safety and ensure public trust concerning surveillance technologies in Denver, we seek a **shared framework** and understanding between city leaders and the community to guide responsible use through **clear standards** that protect civil liberties and data privacy when leveraging these public safety tools.

What we've been working on

- ❖ Understanding of current policies and procedures
- ❖ Surveillance technology risk assessment exercise
- ❖ Technology Services Vendor Risk Assessment review

Technology Services Update

Vendor Risk Assessment Updates

Enhancements have been made to the Vendor Risk Assessment process, including links and resources to help vendors understand applicable local and federal regulations, as well as best practices.

Contract Governance Improvements

New Breach and Remedy language has been drafted for Technology Services Contracts to strengthen governance and improve enforcement of vendor non-compliance.

Data Equity and Civil Liberties

Technology Services is collaborating with the Mayor's Office of Social Equity and Innovation to develop methods for evaluating vendor data equity and ensuring vendors protect civil liberties through operational and technological safeguards.

Where we're going next

- ❖ Survey of ordinances and best practices in other cities and states
- ❖ Collaboration of potential municipal legislation



Questions



APPENDIX

DPD Technology Acquisition

- ❖ Cyber Bureau evaluates technology – Works with other agencies, DPD teams, to establish efficacy and impact to operations. Aligned with strategic goals.
- ❖ TS Intake Process – Vendor Risk Assessment (VRA), TAR (Technical Architecture Review), etc...
- ❖ Competitive Process / Purchasing Rules
- ❖ Contracting
- ❖ Policy
- ❖ Implementation and Sustainment

Vendor Risk Assessments



Identification of risk and potential mitigation



Need for additional requirements such as a data sharing agreement or contract vs. purchase order



Vendor Approval or Denial

Vendor Risk Assessments: AI & Privacy

CCD Data Lifecycle Overview

Data Collection

Data Use

Data Sharing

Data Retention

Data Storage & Security

Data Archival

Data Disposal



1. SCOPE & USE



2. RISK & IMPACT



**3. GOVERNANCE
& OVERSIGHT**

DPD Policy Controls

- ❖ DPD OMS 119.00 – Operations Technology
- ❖ Publicly accessible
- ❖ Defines technology objective, appropriate use, data governance, auditing
- ❖ Policy created based upon legal review by CAO and review of policies from other law enforcement organizations, agencies, including IACP for best practices.