City of Detroit

Surveillance Technology Specification Report (STSR)
Detroit Department of Transportation – Bus Camera System

This Surveillance Technology Specification Report (STSR) is submitted in accordance with Article V, Division 12 of the Detroit Municipal Code §§ 17-5-451 through 17-5-459, also known as the Community Input Over Government Surveillance (CIOGS) Ordinance.

The following report outlines the proposed surveillance technology, its use, purpose, and necessary safeguards, and is submitted for City Council review and approval.

1. Description of the Surveillance Technology

- Digital camera system set up to DDOT buses. It includes:
    - Interior and Exterior cameras per bus.
    - Audio recording capabilities
    - GPS integration
    - Event tagging for incidents
    - Secure video storage with access for key employees only.

2. Purpose of This Surveillance Technology

- To improve safety, security, and operational efficiency. Use cases include:
- Investigating accidents and incidents
- Monitoring operator and rider behavior
- Enhancing evidence quality for legal claims
- Supporting compliance with ADA and transit regulations

3. Criteria for Deployment

The system will deploy to additional DDOT fleet as a replacement to the current deployment of camera technology and additional units for new fleet. Activation is passive and occurs during operations. Review of footage is event-driven (incident, legal inquiry, etc.).

4. Fiscal Impact

The system is funded primarily by FTA grants under a firm fixed-price procurement. The cost includes equipment, installation, and warranty.

5. Civil Rights and Liberties Impact

The system

- Does not use facial recognition
- Does not target individuals or groups
- Does not use license plate recognition
- Is used only in support of public safety and incident investigation.
- Access is strictly role-based and logged.

6. Authorized Uses

Permitted:

- Safety and incident investigation
- Legal and insurance documentation
- Security compliance audits

Prohibited:

- Random or retaliatory monitoring
- Targeting individuals for personal reasons
- Surveillance for non-transit-related issues

7. Data Collection

Captures video, audio, GPS, and event metadata. Operators cannot manually initiate targeted surveillance. Inadvertent capture is minimized through standardized SOPs.

8. Data Protection

Two-factor authentication and VPN required for remote access. Access levels restricted by role. Comprehensive audit logs maintained.

9. Data Retention

Video retention will match state requirements. Incident-tagged video retained per Michigan Schedule #18 or longer when legally required. Secure chain-of-custody protocols used for evidence.

10. Data Sharing

Data may be shared internally with City legal, operations, and safety departments. External sharing only via FOIA request reviewed by the Law Department or through judicial subpoena.

11. Demands for Access

Only approved via formal legal process. All external requests require court order or subpoena. Internal requests logged and reviewed by DDOT Compliance and Safety Units.

12. Auditing and Oversight

Quarterly audits conducted by DDOT internal compliance team. Video access and export logs reviewed for irregularities. Reports escalated to Inspector General if needed.

13. Training

Training includes hardware operation, legal use compliance, and data handling. Provided by vendors through train-the-trainers and certification programs. Recertification is required annually.

14. Complaints and Public Feedback

Complaints can be submitted via DDOT Customer Service, Civil Rights Office, or Ombudsman. Formal response is required within 10 business days. Complaint outcomes are documented and shared publicly in quarterly reports.