FUSUS Informational Report Update: RS2024-792

Prepared by the Metro Nashville Community Review Board

An updated informational report on FUSUS, a surveillance technology contracted with the Metro Nashville Police Department.

Introduction

On November 19, 2024, the Nashville Metropolitan Council will vote on Resolution RS2024-792[1] which would extend the Metro Nashville Police Department's (MNPD) contract with FUSUS Inc., a surveillance technology company. While the department's original contract with FUSUS was not costly enough to require Metro Council approval[2], further extensions of this contract (and, consequently, increases in its value) will continue to require Metro Council approval.

Approval of RS2024-792 by Metro Council would increase the contract value to $744,900 and extend the contract in two key ways. Firstly, approval of the resolution would extend the contract term from 26 to 60 months, with a start date of September 27, 2022, and ending on September 26, 2027. Secondly, approval would give MNPD permission to "utilize the full scope of work including surveillance technology".

Moreover, RS2024-792 would be the first FUSUS amendment authorized by Metro Council, representing the most significant change to Metro's contract with FUSUS thus far. Previous attempts to extend the contract through Metro Council have been unsuccessful. On August 15, 2023, RS2023-2380, which sought to increase the contract value to $350,000 and extend the term to 24 months, was deferred indefinitely by Metro Council and was ultimately withdrawn. Despite the withdrawal in Council, MNPD successfully extended the contract term to 24 months with an administrative amendment (without a value increase). In February of 2024, a second attempt (RS2024-158) to increase the contract value to $350,000 was also withdrawn per a recommendation by Metro Council and the Administration. MNPD then administratively amended their contract again, increasing the contract value to $249,900. Interestingly, this second administrative amendment also limited the scope of FUSUS for Year 2 of the contract, and deactivated private real-time video sharing services and video live streaming from Metro-owned cameras.

Currently, MNPD continues to utilize FUSUS technology under a limited scope. While community members and business owners may register their cameras, there are no active FUSUS-integrated cameras in Nashville. Currently, there are approximately 1,300 FUSUS-registered cameras in Nashville[3]. Until a new resolution is passed by Metro Council amending the scope of surveillance allowed with FUSUS, real-time sharing of public and private video cameras is unauthorized[4].

FUSUS Overview

FUSUS is a surveillance technology platform which allows MNPD to create a "Real-Time Intelligence Ecosystem," a centralized database which grants access to both public and private cameras across

[1] https://nashville.legistar.com/LegislationDetail.aspx?ID=6889301&GUID=8C8A5313-D834-467D-8A1E-046F0CF2BB98

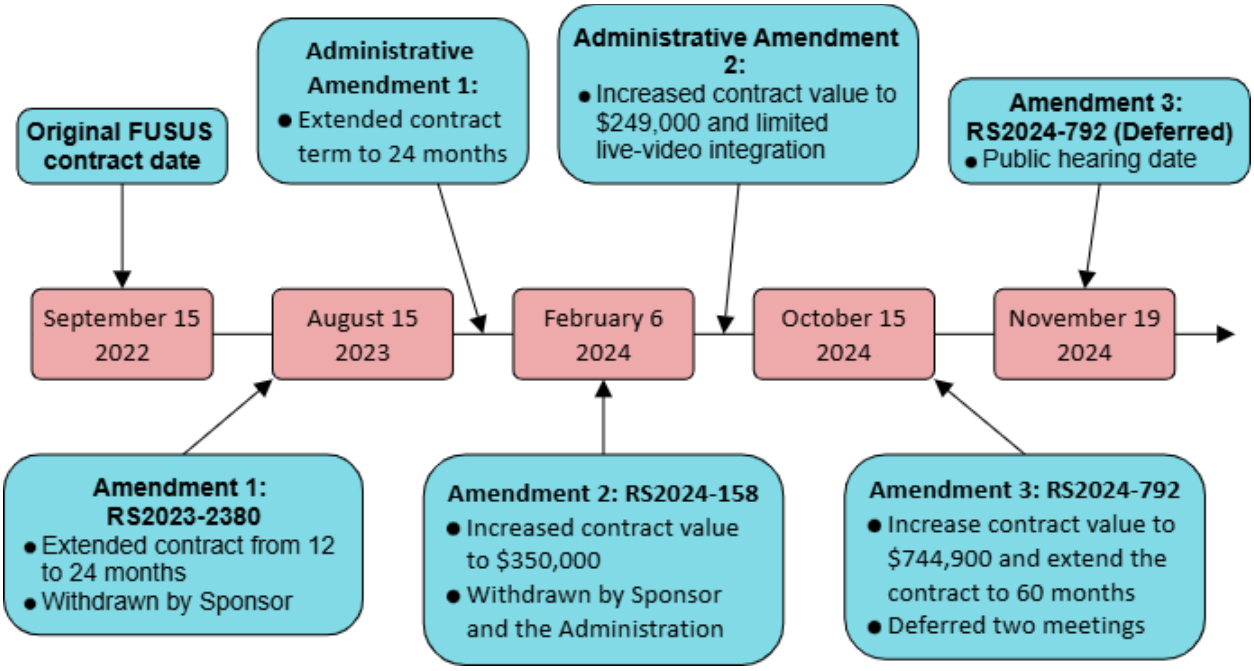
[2] Metro Council requires approval for all contracts exceeding $250,000 in value; Since the initial FUSUS contract was valued at $175,000, this contract did not require approval by the Council.

[3] https://connectmetronashville.org/

[4] https://www.nashville.gov/sites/default/files/2024-01/MNCO-FUSUS_2024_Executive_Summary-ADA.pdf?ct=1705616581

Nashville under a "single pane of glass"[5, 6]. Essentially, community members who wish to participate in the program decide whether to register or fully "integrate" their cameras. Once compiled, MNPD can view the locations of registered cameras and the real-time footage of integrated cameras, all in one place. Most cameras that are part of a wired network can be linked to FUSUS. This includes public cameras (e.g. Metro Government-owned cameras, public school cameras, license plate readers) as well as private cameras (e.g. security cameras or CCTVs)[7]. Department of Transportation cameras (i.e. NDOT and TDOT-owned cameras) will not be integrated into the FUSUS system. All FUSUS data is housed at MNPD's Community Safety Center (CSC), a facility funded by a $3,000,000 grant aimed at reducing crime rates across Nashville[8, 9].

Figure 1: Nashville FUSUS Timeline



Registration and Integration

Participants in the FUSUS program decide between two options: 1) registering their cameras or 2) fully integrating cameras to allow real-time camera access. FUSUS is a voluntary program, with private individuals choosing to opt into the program and determining their level of integration. Private individuals who register or integrate their cameras with FUSUS may voluntarily leave the program at any point. The following sections provide an overview of FUSUS registration and integration.

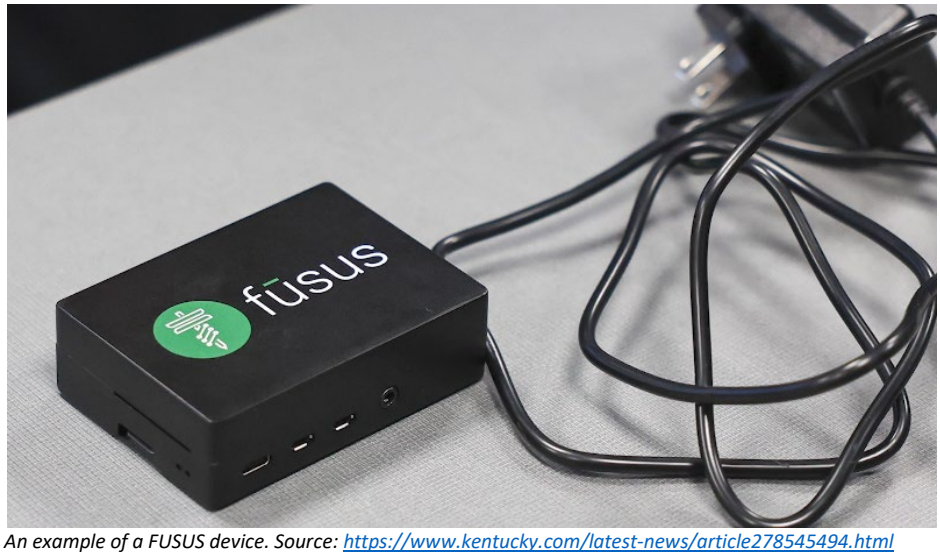
[5] https://www.fusus.com/
[6] https://www.axon.com/products/axon-fusus/single-pane-of-glass-technology-integration
[7] For more information on the linkage of Ring and FUSUS, see Bridges, Lauren. "Infrastructural obfuscation: Unpacking the Carceral Logics of the Ring Surveillant Assemblage." Information, Communication & Society 24.6 (2021): 830-849.
[8] https://www.wkrn.com/news/local-news/nashville/mnpd-applies-for-3-million-grant-to-combat-violent-crime-in-nashville/
[9] For more info about MNPD's FUSUS program visit https://www.nashville.gov/departments/police/crime-control-strategies/camera-network

Registration

Camera registration provides MNPD with the precise location of a private camera, which enables MNPD to compile a database of every FUSUS-linked camera in Nashville within a Geographic Information System (GIS). Used in conjunction with the map of active calls for service, registration of cameras streamlines the process for MNPD to request footage from community members[10, 11].

Integration

Community members also may opt into full integration of their cameras into FUSUS. With the purchase of a fususCORE device and software subscription, participants grant MNPD live camera feed access in the event of an emergency call for service. Once installed on a wired computer network, the fususCORE device encrypts and relays video and audio data from the camera to a secure, cloud-based dashboard. Data is protected using AES 256-bit encryption, a methodology established by the US National Institute of Standards and Technology (NIST)[12, 13]. Owners of fususCORE devices determine the retention rate of their device. In other words, users determine if footage will be overwritten after a period of 24 hours or up to 10 days. Anytime an authorized MNPD user accesses a private camera, an audit log records the access time and identified user.



An example of a FUSUS device. Source: https://www.kentucky.com/latest-news/article278545494.html

MNPD FUSUS Policy

At the time that RS2024-158-- the first resolution aiming to amend MNPD's contract with FUSUS-- was brought to Metro Council, MNPD did not provide a FUSUS-specific policy or Standardized Operating Procedure (SOP)[14], prompting concerns from community members about how the technology would be utilized. Since then, however, MNPD has released a draft FUSUS policy on their Community Safety

[10] NCRB (formerly MNCO) reached out MNPD Deputy Chief Gregory Blair via email correspondence on 8/15/23.
[11] MNPD FUSUS Demonstration 11/12/24
[12] "Announcing the ADVANCED ENCRYPTION STANDARD (AES)" (PDF). Federal Information Processing Standards Publication 197. United States National Institute of Standards and Technology (NIST). November 26, 2001.
[13] Westlund, Harold B. 2002. "NIST reports measurable success of Advanced Encryption Standard". Journal of Research of the National Institute of Standards and Technology.
[14] Private communication from Deputy Chief Greg Blair indicates that there is no SOP for FUSUS as of September of 2023.

Camera Network[15]. The policy begins by situating FUSUS use in accordance with all Federal, State, and City ordinances, laws, and regulations, and states their commitment to following the Commission on Accreditation for Law Enforcement Agencies (CALEA) standards regarding privacy. FUSUS technology shall not be used to target, harass, and/or intimidate individuals or groups based on actual or perceived characteristics including, but not limited to race, color, religion, sex, age, national origin or ancestry, disability, gender identity or sexual orientation. Furthermore, FUSUS technology will not be used with facial recognition technology. The policy also mentions that MNPD will maintain audit trail of access records consistent with Metro records retention scheduling. Data from Metro-owned, integrated cameras will have a retention period of 30 days.

To encourage respect of the privacy of non-participating community members, the policy outlines privacy guidelines that donors with integrated cameras must follow. For instance, only external cameras are eligible for integration, and FUSUS cameras may not be directed at private property not owned by the camera donor, nor installed anywhere where there is a reasonable expectation of privacy.

Regarding the rights and privacy of integrating users, the policy explicitly states that the donor will own all the data and footage from a camera integrated with FUSUS. If being used in an active criminal investigation, data from private cameras may be kept if it is consistent with the current rules of evidence laws, as listed in MNPD Department Manual Section 6.10: Evidence Storage Division.

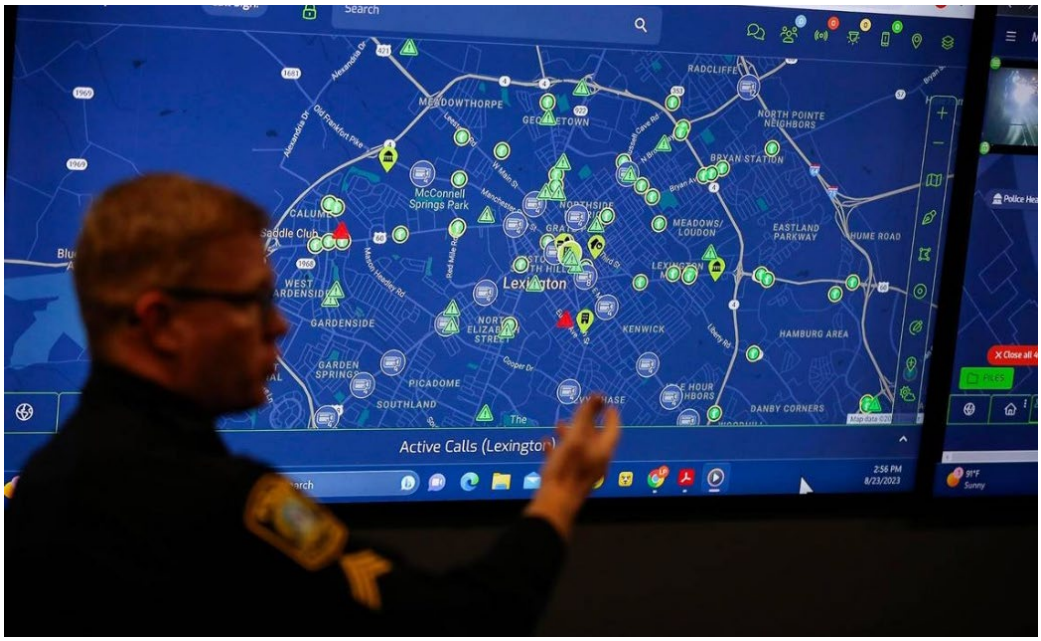
FUSUS usage in "real time." Source: https://www.fusus.com/blog/real-time-crime-center-in-the-cloud-the-next-generation-of-police-technology

Importantly, the policy states that MNPD shall not access live video feed of private cameras unless that footage is directly related to a public safety incident, call for service, or audit of the Community Safety Camera Network. Unclear, however, are the parameters set for accessing a particular camera during a call for service. For instance, the policy does not designate a certain radius from an event location where camera access is permitted, nor does it state a period after a call is initiated/completed when camera access is no longer appropriate. Lastly, the policy states that MNPD officers have a duty—

[15] https://www.nashville.gov/sites/default/files/2024-09/Community_Safety_Camera_Network_Policy.pdf?ct=1726512843

morally and legally-- to intervene if they witness any act that violates law or policy while utilizing FUSUS technology.

This policy also builds upon how FUSUS fits into MNPD Department Manual[16] Section 12.10: Security and Disposition of Law Enforcement Records and Files; and Section 12.30: Management and Utilization of Automated System. Section 12.10 covers any document stored in or displayed on any electronic file or storage medium. It prohibits MNPD personnel from sharing, or profiting from, any electronic data, which includes FUSUS data. Section 12.30 covers the management and use of automated systems, though it mostly pertains to individual personnel technology use.



Lexington police are among the most recent departments to utilize FUSUS. Source: https://www.kentucky.com/news/local/counties/fayette-county/article278520934.html

There is also a "terms and conditions" page of MNPD's FUSUS website[17], which identify two main actors: the "Partner," (private FUSUS users) and the "Agency" (MNPD). The FUSUS terms and conditions for private partners only state "it is not the intention or expectation that the public's cameras will be routinely monitored in real-time by MNPD." Videos transferred onto the FUSUS cloud will be handled with adherence to FBI Criminal Justice Information Services (CJIS) standards and compliance with applicable laws governing the storage, access, and dissemination of evidentiary data. Finally, the terms and conditions prevent MNPD from sharing the camera locations or videos with any member of the public, or anyone outside of MNPD, without prior consent from the private Partner.

FUSUS in Other Cities

While Nashville is not the first city to utilize FUSUS technology, not every city that utilizes FUSUS publishes a FUSUS policy. The below table summarizes some of the notable FUSUS polices for police departments around the country. Green cells in Table 1 indicate that the city's policy includes a listed

[16] https://www.nashville.gov/sites/default/files/2023-07/MNPD-Manual.pdf?ct=1689616240
[17] https://connectmetronashville.org/terms-conditions/

provision; red cells indicate that the city's policy does not contain the provision. For a detailed breakdown of each of the included cities' FUSUS policies, please refer to the NCRB's previous FUSUS informational report[18].

Table 1: FUSUS Policies Across US Police Departments

Police Agency	FUSUS Policy?	CALEA-Based Policy?	Authorized Users?	Limited to Public Space?	Non-Discriminatory Usage?	Prohibits Facial Recognition?	Legal Framing?	Retention Schedules?	Routine Audits?	Consulted Advocacy Groups?
Nashville, TN	✓	✓	✓	X	✓	✓	✓	✓	X	X
Lexington, KY	✓	X	✓	X	✓	X	✓	✓	✓	✓
Minneapolis, MN	✓	X	✓	✓	✓	✓	✓	✓	✓	X
South Bend, IN	✓	X	✓	✓	✓	X	✓	X	✓	X
Columbia, MO	✓	X	✓	✓	X	X	✓	X	✓	X
Providence, RI	X	✓	X	X	✓	X	✓	X	✓	X
Greenville, NC	X	✓	X	X	✓	X	✓	✓	✓	X
Miami, OH	X	✓	X	X	✓	X	✓	✓	✓	X

Nashville & Surveillance Technology

FUSUS provides MNPD with more than just a platform to view video data. Rather, it creates a foundation for compiling and integrating a variety of surveillance technology into one system. For instance, the MNPD's FUSUS system is currently integrated with TrackStar, with MNPD's CAD system, and with License Plate Readers (LPRs). Additionally, FUSUS enables the department to integrate new surveillance tools like SoundThinking (formerly ShotSpotter), a gunshot detection system that MNPD has previously expressed an interest in acquiring[19].

License Plate Readers

This third FUSUS amendment comes on the heels of the much-debated license plate reader (LPR) program, which was approved for full implementation in Nashville in August of 2023. LPRs are automatic cameras that take a picture of every license plate that passes through them, cross checks them with the National Crime and Information Center (NCIC) law enforcement database and identifies any license plates that are in the database as a "hit." MNPD is notified of all hits and verifies each one before sending it over to dispatch for law enforcement action. The LPR program gives MNPD the authority to place LPR cameras in public rights-of-way across Nashville. According to MNPD's report[20] to Metro Council on the LPR pilot program, full deployment will include an estimated 160 LPRs across Metro Nashville. MNPD can retain the data from LPRs up to 10 days, after which it will be deleted, unless that

[18] https://www.nashville.gov/sites/default/files/2024-01/MNCO-FUSUS_2024_Informational_Report-ADA.pdf?ct=1705616491
[19] https://www.nashville.gov/sites/default/files/2022-10/ShotSpotter-Informational-Report.pdf?ct=1666884022
[20] https://www.nashville.gov/sites/default/files/2023-07/LPR-Council-Report-3.pdf?ct=1689087910

data is part of an active investigation or has a written exemption. Thus, integration of LPRs[21] within FUSUS has the potential to contribute significant surveillance data to the FUSUS system.

In MNCO's Full LPR Pilot Program report, LPRs were found to be overwhelmingly placed in non-white and low-income areas[22]. Additionally, the FUSUS platform allows police departments to create and edit their own license place hotlists. This could provide MNPD with the opportunity to use more than just the NCIC law enforcement database. The creation of custom hotlists could allow police departments to create targeted lists based on LPR data without the limitations of the heavily controlled NCIC database.

A visual representation of a FUSUS-integrated system. Source: https://vimeo.com/529039664

MNPD must follow LPR guidelines clearly outlined in Metro Code 13.08.080[23] , which governs surveillance or electronic data gathering devices onto public rights-of-way. Metro Code 13.08.080 limits the retention period of data gathered by surveillance devices in public rights-of-way to 10 days, prohibits unlawful usages, and mandates equitable distribution of the devices. While FUSUS devices conduct surveillance in both public and private spaces, they are not specifically included in Metro Code 13.08.080, nor any other Metro Code. Similar areas of ambiguity between legal guidelines for the two technologies has prompted other cities to include specific policies regarding FUSUS LPR-integration[24]. For instance, without such policies in place it is unclear whether MNPD would adhere to a 10-day or 30-day retention period for LPR data recorded using a FUSUS device.

Metro Nashville Public Schools

In response to school shootings across the United States, FUSUS has advertised[25] their services for integrating FUSUS technology with school security systems to provide additional surveillance, real-time

[21] https://www.documentcloud.org/documents/23795975-fusus-hotlist-editing-redacted
[22] https://www.nashville.gov/sites/default/files/2023-08/MNCO-Full-LPR-Pilot-Program-Report.pdf?ct=1691418108
[23] https://www.nashville.gov/sites/default/files/2023-01/License-Plate-Reader-Pilot-Program-Ordinance.pdf?ct=1673289099#:~:text=1%20of%209-,13.08.,way%20requires%20metropolitan%20council%20approval.
[24] https://www.documentcloud.org/documents/23314068-cpd-draft-policy-for-fusus
[25] https://www.fusus.com/security-operations/fusus-educational-institutions

camera feed viewing, and enable faster response times in the case of an emergency event. As it stands, MNPD has a memorandum of understanding (MOU) with MNPS[26] granting MNPD "24 by 7 by 365" access to MNPS security camera systems, video management systems, and security software. Per the MOU, MNPD can only access these cameras in the event of a "health or safety emergency," including but not limited to active shootings, bomb threats, and medical emergencies. The agreement also includes specific guidelines limiting the number of officers who have access to MNPS cameras and requiring written documentation any time MNPD accesses MNPS cameras. Such written documentation must include an incident report, the timeframe of camera access, the identity of the officer who accessed the camera feed, the reason for camera access, what actions were taken by MNPD, and the specific location of camera access. The MOU also establishes that the use of FUSUS does not waive the constitutional rights of its employees or students. Finally, the document establishes that any data gathered from MNPS cameras may not be used for law enforcement purposes[27], may not violate the Family Educational Rights and Privacy Act (FERPA), or be disseminated to third parties.

Currently, no private or charter K-12 schools have FUSUS integration in Nashville, nor are there are currently any universities with FUSUS integration in Nashville. Integration with these institutions would require separate MOUs between the school, MNPD, and any independent law-enforcement agencies affiliated with the institution.

Risks Associated with Adopting FUSUS

While FUSUS has the potential to greatly enhance public safety, there are also risks associated with expanding surveillance technology; particularly as it pertains to privacy, consent, and civil liberties. Constant surveillance and filming of individuals in both public and private spaces can constitute a legal grey area with respect to 1st and 4th Amendment Constitutional rights. According to the US Department of Justice, surveillance that restricts freedoms of expression, speech, or movement, or that is used for an unreasonable or unwarranted search can be considered violations of 1st and 4th Amendment rights, respectively.

As stated in MNPD's policy, FUSUS technology shall not be used to target, harass, and/or intimidate individuals or groups based on actual or perceived characteristics (including, race, national origin or ancestry, gender identity, etc.). However, communities of color and low-income communities, historically, have experienced higher rates of surveillance technology in their communities[28], and it is important to consider how new surveillance technology may disparately affect different communities in Nashville. For instance, community members have also voiced their concerns over how FUSUS technology may play a role in Immigrations and Customs Enforcement (ICE) in Nashville. As a local law enforcement agency, MNPD does not have jurisdiction over federal law enforcement agency efforts, including immigration and customs enforcement. If ICE requests data from MNPD, they are required to do so through proper legal channels (e.g. through a court appointed subpoena). Importantly, private

[26] NCRB (formerly MNCO) received a copy of the MOU via email correspondence with MNPS on

[27] This most likely means that MNPD cannot use FUSUS footage as the basis of questioning, investigating, or apprehending a student or MNPS employee in matter unrelated to a "Health or Safety Emergency." However, until a situation like that plays out, it is only speculation as the MOU does not go into greater detail.

[28] https://www.aclu.org/report/community-control-over-police-surveillance-technology-101#:~:text=The%20proliferation%20in%20local%20police,color%20and%20low%2Dincome%20communities.

parties who integrate their cameras within FUSUS maintain legal ownership of all data from the device. Thus, extensions of FUSUS by MNPD will not necessarily alter the way that either agency operates within Nashville.

Lastly, there are significant cost associated with participating in private camera integration. Bundles combining the cost of a fususCORE device and annual subscription fee range in price from approximately $350 to $7,300. Furthermore, payment of $150 subscription fee annually is a requirement for active participation in FUSUS integration.[29] Although the expense associated with buying into the program may limit excessive proliferation of camera surveillance in Nashville, many community members interested in increasing public safety for their business or neighborhood may be priced out of participation.

Conclusion

The NCRB presents this report to increase transparency, communication, and trust with the community regarding FUSUS. MNPD entered the current contract with FUSUS more than two years ago, yet the citizens of Nashville know very little about FUSUS. Should Metro Council assent to the expansion of FUSUS, members of the public (including citizens who are interested in participating and community members who may be affected by FUSUS) have a right to understand the full scope of this new surveillance program. Public forums informing community members about FUSUS and demonstrating FUSUS integration within the Community Safety Center could significantly increase transparency and trust with MNPD with respect to this program. Additionally, collaboration with an independent agency like the NCRB on FUSUS audits could substantially improve public perceptions of MNPD's commitment to trust, accountability, and transparency.

[29] https://connectatlanta.org/shop/