Brooklyn Defenders

Brooklyn Defender Services
177 Livingston St, 7th Fl
Brooklyn, NY 11201

Tel (718) 254-0700
Fax (347) 457-5194
info@bds.org@bds.org

April 22, 2026

Janell Cleary
Contract Manager
New York City Department of Corrections
75-20 Astoria Blvd.
East Elmhurst, NY 11370

RE: **Public Comment in Opposition to Proposed Contract Award to Securus Technologies LLC (EPIN 07224P0002002)**

Dear Janell Cleary,

Brooklyn Defender Services (BDS) submits this public comment in strong opposition to the proposed five-year, $23.2 million contract award to Securus Technologies LLC for the Person-in-Custody Communication System at New York City Department of Correction (DOC) facilities.

For 30 years, BDS has worked, in and out of court, to protect and uphold the rights of individuals and to change laws and systems that perpetuate injustice and inequality. After 29 years of serving Brooklyn, we expanded our criminal defense services to Queens. We represent over 40,000 people each year who are accused of a crime, facing the removal of their children, or at risk of deportation. Our staff consists of attorneys, social workers, investigators, paralegals and administrative staff who are experts in their individual fields. BDS provides additional services for our clients, including civil legal advocacy, assistance with the educational needs of our clients or their children, housing and benefits advocacy, as well as immigration advice and representation.

In addition to zealous legal defense, BDS seeks to address the causes and consequences of legal system involvement. We have built a practice around supporting people who are detained pretrial to mitigate the burdens and trauma created by confinement. Through our jail-based programming, we advocate for our clients to access services they are entitled to such as medical care and educational access. Additionally, our established presence in New York City jails allows us to monitor and document the conditions New Yorkers encounter when incarcerated and advocate for the basic human rights, health, and safety of incarcerated people. Furthermore, many of the people that we serve live in heavily policed and highly surveilled communities.

BDS has represented people incarcerated in City jails for decades and writes with direct knowledge of what the DOC-Securus surveillance system does and whom it harms. BDS, along with co-counsel Bronx Defenders and New York County Defender Services, filed an Article 78 action in 2024 against DOC, detailing how, over the last 10 years, DOC and Securus replaced a simple telephone service with a mass community surveillance system that extracts, indexes, and databases biometric and associational information from people in custody and the people who communicate with them. And DOC did so without adequate safeguards in place for protecting privileged communications and with a vendor notorious for data leaks and disregarding federal

and state law. *Reid v. NYC Dept of Corr*, No. 806245/2024E (Sup. Ct. Bronx Cty.) (class action petition in New York State Supreme Court seeking, among other relief, termination of the Securus contract and appointment of a monitor to ensure DOC's compliance with its constitutional and legal obligations). That litigation remains pending and DOC is now moving forward with a new five-year contract with the same vendor, using the same unconstitutional community surveillance system.

This contract is being pushed through with a bare-minimum public comment window, no visible solicitation notice, and no evidence of a competitive process. We urge DOC to terminate its relationship with Securus and we ask the NYC Comptroller not to certify this contract. Instead, the city should pursue an alternative approach to jail communications that does not expose tens of thousands of New Yorkers to mass surveillance, ongoing constitutional violations, and the risk of having their most intimate personal data flow across the country into law enforcement systems, including into federal immigration enforcement systems.

A. The DOC-Securus Partnership Violates New Yorkers' Constitutional Rights and Puts Their Personal Information at Risk

Family, loved ones, and friends are an irreplaceable source of support for people who are incarcerated and play an important role in the mental health of people in custody, including improving rates of recidivism. The original purpose for telephone installation in jails was to maintain community ties between incarcerated people and their support systems, because those ties improved public safety outcomes. DOC's contracting with Securus to collect, index and database call recordings, biometric, and financial data as well as build associational networks of community members, frustrates this purpose by chilling the much-needed positive support from loved ones and friends. The DOC-Securus relationship has turned a tool meant for community connection into a surveillance network that undermines the very purpose for phones in jails and undermines the privacy, speech, and associational freedoms of New Yorkers.

Securus provides its communication services to DOC through the NextGen Secure Call Platform, a cloud-based surveillance and data collection infrastructure that captures and houses multiple streams of Securus-collected data. For every call placed from a DOC facility, the following data is captured, indexed, and stored in the Securus system: full audio recordings and machine-generated transcriptions; voiceprints (permanent biometric identifiers) of both the incarcerated caller and every person who receives their call, including family members and children; billing names and addresses associated with landlines, and phone numbers of call recipients; and financial transaction data from commissary deposits.

- **Call Recordings and Transcriptions.** Every non-privileged call placed through the Securus system is recorded in full and stored in Securus's cloud infrastructure. These recordings are actively transcribed by machine into searchable text, enabling searches across call content the database by keyword.

- **Voiceprint Biometric Data.** The NextGen SCP has embedded various datamining tools, including the Continuous Voice Certification that digitally captures and maps a person's

unique patterns in voice and speech—a biometric identifier known as a "voiceprint." Through Continuous Voice Verification, Securus captures and permanently stores the voiceprints of incarcerated callers and people who receive their calls. This form of biometric identification is applied to call recordings to identify the people who are speaking. These voiceprints are indexed in Securus's system, making it possible to search all calls across the platform and identify a specific community member's voice.[1] Continuous voice verification allows for the identifying and monitoring not merely of activity inside of detention facilities, but more specifically thoughts, communication, and relationships outside of those facilities within the broader community.

All of this data captured from New Yorkers, both inside the city jails and in the community, is then indexed and analyzed by Securus through THREADS—Securus's flagship analytics platform. THREADS conducts pattern-recognition and creates social network maps that pull together call recordings, transcriptions, voiceprints, financial transaction records from money transfer services, and tablet data from across all facilities in the Securus network.[2] In 2017, Securus reported that its THREADS database already contained data from more than 1.55 million incarcerated and non-incarcerated individuals, drawn from approximately 2,200 facilities processing more than one million calls per day. The majority of people whose information resides in THREADS were not incarcerated, but had their information harvested because they were on a phone call with a loved one who was incarcerated.[3] That data can be aggregated across correctional facilities nationwide and made accessible to law enforcement agencies that have purchased or been offered a free subscription to THREADS. Through its THREADS analytics platform, Securus creates AI-generated social network maps showing who an incarcerated person contacts, in what sequence, and how their outside contacts relate to one another.[4] The majority of people whose data is captured have never been incarcerated: they are family members, friends, children, advocates, and community members who care for and communicate with someone in our city jails.

Moreover, the multiple streams of data—call recordings, transcriptions, voiceprints, phone numbers, mailing addresses, and communication patterns—that New York City pays Securus to collect, are being actively used to train Securus's artificial intelligence systems. Securus president Kevin Elder confirmed in 2025 that the company began building AI tools in 2023, using its massive

[1] Affirmation of Elizabeth Daniel Vasquez in Support of Verified Article 78 Petition, *Matter of Marcus Reid et al. v. NYC DOC*, Index No. 806245/2024E (Bronx County Clerk Apr. 15, 2024) ("Vasquez Aff.") ¶¶ 49-58; DOC-Securus Contract, Appendix B, at 1–2.

[2] Vasquez Aff. ¶ 73 (quoting FCC Ex Parte Submission at 21, 24, 30).

[3] Vasquez Aff. ¶ 76 (citing FCC Ex Parte Submission at 24).

[4] Vasquez Aff. ¶¶ 49, 72; Securus, THREADS website (archived), https://securustechnologies.tech/securusthreads.

archive of recorded calls to train large language models designed to detect "criminal activity."[5] One such model was trained on seven years' worth of calls from Texas prisons alone.

There are no use restrictions on Securus in terms of how they may use New York data internally. THREADS was initially offered in New York's contract at no cost because the storage and use of data to improve the AI models within THREADS serve as a benefit to the company. That data, which includes some of the most intimate details of individuals' conversations, deep analysis of family ties and social connections, and geographic mapping all live on a platform outside of New York City's oversight and control. The risk posed is severe: the use of New York data in AI training sets, as well as storage of their data on a third-party, cloud-based platform like NextGen, makes that data vulnerable to backend attacks by hackers and comingling into datasets shared with partner companies.

While DOC specifically "retains sole ownership and intellectual property rights in and to all information, data (call records and recordings), data compilations, reports, charts, graphs, diagrams, or other information provided or made accessible by the DOC to [Securus], or created by [Securus] pursuant to the Agreement" under its prior contract with Securus, that contract specifically permitted use of "general knowledge, skills, . . . techniques . . . learned . . . during the performance of . . . obligations under the Agreement." In a machine learning world, the Use of General Knowledge clause gives Securus the ability to profit from access to DOC data, while allowing DOC to appear to retain data ownership.

The families of incarcerated New Yorkers are notified that calls are recorded, but they are not informed that their voiceprint, words, and relationships are being analyzed and fed into AI training datasets. Requiring them to accept this as the price of maintaining contact with a loved one constitutes coercive consent and chills communication. The harms stemming from DOC's surveillance practices disproportionately impact Black and brown New Yorkers and the families of people who lack the resources to pay bail.

B. The DOC-Securus Partnership Puts Immigrant New Yorkers At Risk and Undermines the City's Sanctuary Laws

The privacy risks inherent in sharing highly personal data with companies that build and create AI software are a serious threat to all New Yorkers, and the risks are even higher for immigrant New Yorkers. Securus has marketed THREADS as having integration capabilities with Palantir,[6] a company that has developed applications used by ICE to track and target immigrants for enforcement, including ImmigrationOS and ELITE, and that is actively seeking to accumulate

[5]MIT Technology Review, "An AI model trained on prison phone calls now looks for planned crimes in those calls" (Dec. 1, 2025); Futurism, "Prisoners Alarmed to Discover That a Startup Is Training an AI Based on Their Phone Calls" (Dec. 6, 2025).

[6] Securus, Best and Final Offer ('BAFO'), at 2–3 ('Threads Data Analytics Program currently used by [the NYPD] including integration capabilities with Palantir'); Vasquez Aff. ¶¶ 89–93.

as much data as possible to power those tools.[7] The high risk of this chain of exposure from a phone call at Rikers to an immigration enforcement dossier is an architectural feature of the system DOC is proposing to fund for another five years.

Palantir acquires vast amounts of information from different sources such as government databases, commercial data brokers, law enforcement records, and private contractors to power its intelligence software. Integration between THREADS and Palantir means that data residing in THREADS could potentially be ingested into Palantir's systems and cross-referenced against other datasets. Once data enters Palantir's ecosystem, it becomes available for use across the government contracts Palantir holds. In this way, the voiceprints, phone numbers, addresses, and social network maps of New Yorkers are further exposed to being shared with ICE.

The chain of exposure is as follows: New Yorkers' data collected through the DOC-Securus call surveillance system enters Securus's NextGen SCP and gets analyzed in the THREADS database. That data is analyzed by and used to train THREADS, which Securus markets as having integration capabilities with Palantir. Palantir ingests that data alongside other data sources. ICE agents access Palantir's ELITE app and receive a map populated with "deportation targets." Through the sharing and comingling of datasets, a person who spoke to a family member detained at Rikers may now appear in an AI-generated ICE dossier alongside their address, phone number, and social network.[8]

---

[7] In July 2025, ICE awarded Palantir a $30 million contract to build ImmigrationOS, a platform described as providing "near real-time visibility" on people targeted for deportation, incorporating passport records, Social Security files, IRS data, and license plate reader information. *See* American Immigration Council, *ICE to Use ImmigrationOS by Palantir, a New AI System, to Track Immigrants' Movements* (Aug. 22, 2025), https://www.americanimmigrationcouncil.org/blog/ice-immigrationos-palantir-ai-track-immigrants/; Palantir also developed ELITE—Enhanced Leads Identification and Targeting for Enforcement. ELITE populates a map interface with potential deportation targets and provides detailed dossiers drawn from Medicaid records, immigration records, and commercial data sources. *See 404 Media, ELITE: The Palantir App ICE Uses to Find Neighborhoods to Raid* (Jan. 20, 2026), https://www.404media.co/elite-the-palantir-app-ice-uses-to-find-neighborhoods-to-raid/. ICE officers have confirmed under oath that ELITE was used to find immigrants for arrest and detention. *See* IBTimes UK, *ICE Officers Confirm Under Oath That Palantir's ELITE App Identified Arrest Targets* (Mar. 15, 2026), https://www.ibtimes.co.uk/ice-palantir-elite-app-controversy-oregon-court-1785617.

[8] Documented, *ICE May Still Have Massive Access to Rikers Island Data Despite City's Sanctuary Status* (July 2, 2025), https://documentedny.com/2025/07/02/ice-may-still-have-massive-access-to-rikers-island-data-despite-citys-sanctuary-status/; *see also* Vasquez Aff. ¶ 71 (noting Securus's expansion beyond corrections agencies to city, county, state, and national law enforcement).

The prior DOC-Securus contracts contain no provisions requiring Securus to comply with NYC sanctuary policies, no restrictions on how Securus may use New York data internally, no requirement that Securus notify DOC before disclosing data to federal immigration authorities, and no audit mechanism to verify compliance.[9] Unless DOC publicly demonstrates that these deficiencies have been corrected, the Comptroller should not certify an award that may itself constitute an unlawful expenditure of city resources in furtherance of immigration enforcement under Administrative Code § 10-178.

New York City has made a categorical legal commitment to protecting immigrant New Yorkers. Mayor Mamdani's Executive Order No. 13 prohibits city agencies from sharing New Yorkers' private data with federal immigration authorities without legal justification.[10] NYC Administrative Code § 10-178 bars the use of any city resources in furtherance of immigration enforcement. Administrative Code § 23-1202 prohibits city employees, contractors, and subcontractors from disclosing identifying information to outside parties, including federal agencies, absent narrow exceptions.[11] DOC's use of Securus's mass surveillance systems violates these regulations.

C. DOC Has Been on Notice For Years That Securus Has an Unremedied Record of Serious Legal Violations

DOC has been on notice for years that there are serious issues with Securus. DOC is proposing to continue contracting—now, with a new long-term contract—with a vendor with a documented, nationwide pattern of violating the constitutional rights of the people it surveils.[12]

---

[9] DOC-Securus Contract, §§ 5.08, 7.2, 7.3; Vasquez Aff. ¶ 81.

[10] N.Y.C. Exec. Order No. 13 (Feb. 6, 2026) (prohibiting non-city law enforcement from entering city property without a judicial warrant; directing city agencies to audit compliance with sanctuary laws and appoint privacy officers; establishing interagency response committee; and prohibiting sharing of New Yorkers' private data with federal immigration authorities without legal justification), available at https://www.nyc.gov/mayors-office/news/2026/02/executive-order-13.

[11] N.Y.C. Admin. Code § 10-178 (enacted as Local Law 228 of 2017, eff. Jan. 30, 2018; am. L.L. 2026/063, eff. Jan. 29, 2026) (prohibiting use of city resources for immigration enforcement and requiring recordkeeping of requests from non-local law enforcement); N.Y.C. Admin. Code § 23-1202 (enacted as Local Law 247 of 2017) (prohibiting disclosure of identifying information, including biometric data, by city employees, contractors, and subcontractors to outside parties except in narrowly defined circumstances); see also NYC Comptroller, Letter to Commissioner Castro re: Sanctuary Laws (Dec. 16, 2024), https://comptroller.nyc.gov/reports/letter-to-commissioner-castro-re-sanctuary-laws/

[12] Securus's recording of privileged attorney-client calls is a documented, nationwide pattern. The company has faced lawsuits in at least seven states for recording attorney-client communications and in some cases sharing them with prosecutors, settling repeatedly without

The Sixth Amendment guarantees people facing criminal charges the right to communicate confidentially with their attorneys. The DOC and Securus contractual relationship has already produced systematic violations of that right: more than 3,800 privileged attorney-client calls were recorded and turned over to prosecutors, NYPD, and the Department of Investigation. DOC was notified of this problem repeatedly, beginning in at least 2018, and failed to act for years.[13]

The Do Not Record list that should protect legal and clergy phone numbers has failed repeatedly, and DOC has admitted it does not have direct access to Securus's system to verify whether numbers are properly protected. The legal calls that have been and could be recorded have had a chilling effect on legal communications and, accordingly, people in custody's access to substantive conversations with their defense teams is restricted. Further, breaches of the attorney-client privilege cause a *per se* harm because they undermine the integrity of the legal system. The criminal legal system is predicated on the notion that attorneys can communicate confidentially with their clients.

Securus's record of violations is not limited to New York. The company has been sued in at least ten jurisdictions for recording privileged attorney-client communications, paying millions of dollars in settlements without implementing systemic remediation. It paid a $1.7 million civil penalty to the FCC for providing misleading information to federal regulators. In 2015, a data breach exposed 70 million call recordings in 37 states, including 14,000 attorney-client calls that were unlawfully recorded.[14] These incidents reflect a company that, as one FCC Commissioner put it, "has shown it is willing to operate on the bleeding edge of legality."[15]

Equally serious is the failure of informed consent. Community members who receive calls through the Securus system are told that calls may be recorded, but they are not told that their voiceprints are being permanently captured as biometric identifiers, that their social networks are being mapped by AI, that their data is being used to train machine learning models, or that it may be shared with law enforcement agencies nationwide through THREADS. The gap between what

---

admitting fault. *See* Joseph Cox, Prison Phone Companies Are Recording Attorney-Client Calls Across the US, Motherboard (Feb. 22, 2021),

[13] Verified Article 78 Petition, *Matter of Marcus Reid et al. v. NYC DOC*, Index No. 806245/2024E (Bronx County Clerk Apr. 15, 2024) ("*Reid* Art. 78 Petition"), ¶ 49; *see also* VICE, *Prison Phone Companies Are Recording Attorney-Client Calls Across the US* (Dec. 13, 2021), https://www.vice.com/en/article/prison-phone-companies-are-recording-attorney-client-calls-across-the-us/.

[14] Order, Consent Decree, Securus Techs., Inc., File No. EB-IDH-000225128 (F.C.C. Oct. 30, 2017); The Intercept, *Not So Securus: Massive Hack of 70 Million Prisoner Phone Calls Indicates Violations of Attorney-Client Privilege*, (Nov. 11, 2015), https://theintercept.com/2015/11/11/securus-hack-prison-phone-company-exposes-thousands-of-calls-lawyers-and-clients/.

[15] Statement of Comm'rs Mignon L. Clyburn & Jessica Rosenworcel, Dissenting, *In re* Securus Techs., Inc., File No. ITC-T/C-20170511-00094 (F.C.C. Oct. 30, 2017).

people are told and what is actually done with their data is a legal and ethical problem that a new five-year contract will entrench. The previous NYC Comptroller recognized the seriousness of these concerns: when DOC sought to award Securus a separate contract for tablet entertainment services, the Comptroller refused to certify it, citing Securus's "history of data privacy violations" and finding the contract was "inappropriately sole-sourced" and "no-bid."[16] Those concerns apply here with far greater force.

The chilling effect of DOC's surveillance practices has alienated people in custody from their loved ones, damaging their mental health and disconnecting them from their community in an already stressful jail environment. Phone calls with family and loved ones are regularly turned over to prosecutors in criminal cases without a judicial subpoena or a showing that the conversations would be relevant. Often such calls are deeply personal, ranging from intimate discussions of relationships, traumatic events either or both parties have experienced, and even reasons to live, if people in custody are struggling with suicidal ideation. All of these calls are recorded, indexed, databased and made available to prosecutors or other law enforcement for their review. They are also exploited to train Securus' AI tools.

The rationale that Securus' surveillance tools are needed for jail security are not supported by the facts. Recorded phone calls from incarcerated people are seldom used for assessing jail safety concerns but are routinely provided to prosecutors for use in criminal cases when the person they are prosecuting is detained. Furthermore, DOC officials review only a fraction of the millions of recorded phone calls—within a two-year period (2020-2022), less than 1.7 precent of phone call recordings were accessed by DOC officials.[17] In response to a BDS FOIL request, DOC was unable to provide any data or records about instances in which listening to the calls of people in custody led to the interception of contraband, the disruption of smuggling networks, or the prevention of threatened violence within DOC's facilities.[18] Instead, under the previous New York City administration, levels of administrative dysfunction and institutional violence reached an all-time high.[19]

D. <u>This Procurement Is Procedurally Deficient</u>

The DOC is not providing the public and stakeholders with a sufficient amount of time to share its significant concerns with the DOC-Securus contractual relationship. The public comment period following the announcement of this contract renewal is eight days, *the bare minimum* permitted under PPB Rules §2-11(a) and (c)(1). For a $23.2 million contract with a vendor whose

[16] N.Y. Daily News, *NYC Comptroller Nixes Contract for Rikers Jails Detainee Video Vendor*, (Feb. 22, 2024), https://www.nydailynews.com/2024/02/22/nyc-comptroller-brad-lander-nixes-contract-for-rikers-jails-detainee-video-vendor/.

[17] *Reid* Art. 78 Petition, ¶¶163-69.

[18] *Id.*

[19] *See, e.g., Nunez v. N.Y.C,* et al., 11-cv-5845 (LTS), ECF No. 961 (appointing remediation manager in order to bring DOC in substantial compliance with the contempt provisions).

prior relationship with the City has produced constitutional violations and is the subject of pending litigation brought by the City's own public defenders, eight days is not a good-faith invitation to public participation.

More importantly, no notice of solicitation for EPIN 07224P0002002 appears in the City Record Online for any period prior to the April 14 public comment notice. PPB Rules §3-03(d)(1)(ii)(A) require that a notice of solicitation be published in the City Record not less than twenty days before the proposal opening date. DOC has not disclosed the proposal due date, making it impossible to verify compliance. DOC must produce the solicitation notice, the proposal due date, and proof of distribution to vendors on the appropriate citywide bidders list before any contract is certified.

DOC justified its February 2026 six-month extension by stating it needed time to complete the new procurement "with integrity and due diligence."[20] During that extension period, no solicitation notice appeared in the City Record, and there is no public record of DOC making a good-faith effort to evaluate whether an alternative vendor or model is available. Further, the prior contracts were extended repeatedly through negotiated acquisition extensions, allowing Securus's scope of services to expand dramatically away from basic phone service without any evaluation of each new capability for efficacy, data security, or legal compliance.

PPB Rules §2-08[21] requires an affirmative responsibility determination before award — a finding that the proposed vendor has the "business integrity to justify the award of public tax dollars." Given Securus's record of constitutional violations, FCC sanctions, data breaches, and settlements, DOC must publicly explain how it arrived at a positive responsibility determination and what weight was given to this history. PPB Rules §4-01(b) further requires that performance evaluations be completed before renewal decisions.[22] There is no public record that DOC conducted such an evaluation of the prior Securus contract before initiating this new procurement.

Finally, NYC Charter §312 requires that prior to renewing a contract valued at more than $1 million for standard or professional services, the agency must submit a cost and comparative analysis to the Comptroller, the City Council, and affected collective bargaining representatives, after which the Council has thirty days, during which it may hold a hearing, before any renewal may proceed.[23] At $23.2 million, this contract is well above the threshold. There is no public record that DOC submitted the required analysis or that the Council's thirty-day review period was observed. Further, given the numerous problems posed by the use of Securus's community

---

[20] *Notice of Proposed Contract Award: Person-in-Custody Communication System*, EPIN 07224P0002002, N.Y.C. Record Online https://a856-cityrecord.nyc.gov/RequestDetail/20260220004.

[21] PPB Rules §2-08 N.Y.C. Procurement Policy Bd. R. § 2-08 (2025).

[22] PPB Rules §4-01(b) N.Y.C. Procurement Policy Bd. R. § 4-01(b) (2025).

[23] NYC Charter §312 N.Y.C. Charter § 312 (2026).

surveillance system, as detailed above, City Council should have held a hearing prior to DOC awarding Securus a new, five-year-long contract.

E. Conclusion

BDS urges DOC to cancel the proposed award to Securus Technologies and to use the time remaining before July 1, 2026 to identify an alternative approach to jail communications that does not involve the mass collection and uncontrolled sharing of biometric and personal data from tens of thousands of New Yorkers. The Comptroller should refuse to certify this contract.

At minimum, DOC must produce the solicitation notice and proposal due date and demonstrate that the twenty-day City Record publication requirement was met; publicly disclose the responsibility determination and explain how DOC weighed Securus's record of illegal and unethical conduct; demonstrate that the Charter §312 analysis was submitted to the City Council and that the thirty-day review period was observed; hold a hearing to complete and disclose a performance evaluation of the prior Securus contract.

Sincerely,

Lisa Schreibersdorf
Executive Director
Brooklyn Defender Services