MTA Procurement
333 West 34th Street, 10th Floor
New York, NY 10001

Metropolitan Transportation Authority
State of New York

December 26, 2023

Re: Request for Information (RFI) No. 0009000032
Qualified Product List (QPL) Process – Secure, Accessible & Modern Fare Gates

Dear Prospective Participants:

Please see attached Request For Information No. 0009000032 for Secure, Accessible & Modern Fare Gates.

The Metropolitan Transportation Authority ("MTA") is seeking information from firms interested in participating in the Qualified Products List ("QPL") Process during which the MTA shall identify the next generation of secure, accessible, and modern fare gates suitable for use for the MTA. The MTA intends to replace its legacy gates in the NYCT subway system, including the existing low turnstiles, and Automated Fare Access System Gates and Emergency Exit Gates with such next generation gates to meet the MTA's goals for ensuring fare compliance and preventing fare evasion, enhancing accessibility, and improving the customer experience.

Those firms interested in participating in this Phase 1 of the QPL Process should submit relevant product and other information in the form of a QPL Proposal as set forth herein. QPL Proposals will be evaluated by the MTA in this Phase 1 for participation in Phase 2 of this QPL Process, which phase shall include testing of the Gates that, in the sole discretion of the MTA, meet MTA's Technical Requirements (as defined herein) and needs as set forth herein including, but not limited to, proven commercial off-the-shelf products that have been successfully implemented in other transit agencies.

This RFI process will ultimately identify a list of qualified secure, accessible, and modern fare gates to place on the MTA's Qualified Product List (QPL) to be used for future purchases to meet MTA's needs.

Any questions regarding this RFI shall be made in writing by **January 12, 2024** via email to reggie.matela@mtahq.org. A virtual pre-RFI conference is scheduled on **January 17, 2024**. Please make sure to notify reggie.matela@mtahq.org to obtain the meeting link for this conference. All RFI responses must be submitted to reggie.matela@mtahq.org by close of business **on February 29, 2024.**

Sincerely,

Reggie Matela
Asst. Deputy Chief Procurement
Officer MTA Procurement

MTA SECURE, ACCESSIBLE, AND MODERN FARE GATES

QUALIFIED PRODUCT LIST (QPL) PROCESS
PHASE 1 - REQUEST FOR INFORMATION (RFI)

RFI NO. 0009000032

Deadline for Written Questions: January 12, 2024, 3PM EST

Virtual Pre-Proposal Conference: January 17, 2024, 2PM EST

QPL Phase 1 Proposal Due Date: February 29, 2024

I. QUALIFIED PRODUCTS LIST PROCESS

The Metropolitan Transportation Authority ("MTA") is seeking an expression of interest and product information from firms interested in participating in the Qualified Products List ("QPL") Process during which the MTA shall identify the next generation of secure, accessible, and modern fare gates suitable for use for the MTA, with initial use intended in the New York City Transit ("NYCT") public transportation system. The MTA intends to replace its legacy gates in the NYCT subway system, including the existing low turnstiles, and Automated Fare Access System Gates and Emergency Exit Gates with such next generation gates to meet the MTA's goals for ensuring fare compliance and preventing fare evasion, enhancing accessibility, and improving the customer experience. Through this multi-phased QPL Process, the MTA will prequalify viable solutions as "Qualified Products" to establish an MTA QPL for its next generation of fare gates. Submittals for the QPL must include two forms: (i) – a standard-width gate (hereby called "Wide-Aisle Gate", or "WAG") and (ii) a fully ADA-accessible wide gate (hereby called "Accessible Wide-Aisle Gate", or "AWAG"). WAG and AWAG shall collectively be referred to as "Gates". Gates can be utilized in fare arrays consisting of two (2) or more gates or as stand-alone gates.

Those firms interested in participating in this Phase 1 of the QPL Process (each, a "Participant") should submit relevant product and other information in the form of a QPL Proposal as set forth herein. QPL Proposals will be evaluated by the MTA in this Phase 1 for participation in Phase 2 of this QPL Process, which phase shall include testing of the Gates that, in the sole discretion of the MTA, meet MTA's Technical Requirements (as defined herein) and needs as set forth herein including, but not limited to, proven commercial off-the-shelf products that have been successfully implemented in other transit agencies.

Potential participants in this QPL Process are advised that this QPL Process is not a solicitation

for procurement of Gates. Any such solicitation or solicitations will take place subsequent to the establishment of the QPL. Through this QPL Process, the MTA intends only to test and evaluate Gates to establish those Gates which may be included in the QPL as eligible for future procurements.

II. BACKGROUND

NYCT serves approximately 5.6 million subway customers daily (pre-COVID-19 pandemic) across New York City. Today, most subway customers enter stations via low turnstiles ("LTs") or high entry/exit turnstiles ("HEETs"). Alternatively, at some stations, customers can access the station through the Automated Fare Access System Gate ("AFAS Gate", also known as the "AutoGate") if they are unable to use the standard LTs due to, for example, carrying luggage or using a wheelchair or stroller. And Emergency Exit Gates ("EXG"), while not intended as points of entrance, have become another point of entry for many of those evading the fare, or in some cases who are not able to use turnstiles for access.

Fare evasion has become a critical challenge for the MTA, leading to over $285 million in lost revenue for NYCT subway in 2022 alone. The loss in fare revenue can lead to significant impacts on the MTA's ability to provide reliable service for New Yorkers. With rates of fare evasion exploding in recent years, the MTA convened the Blue-Ribbon Panel on MTA Fare and Toll Evasion in 2022. The panel's final report, released in May 2023, recommended implementation of the next generation of secure fare gates to replace and modernize decades-old fare arrays.

Modern fare gates are not only solutions to the growing problem of fare evasion, but also for the MTA's goal of improving accessibility throughout the NYCT subway system. Accessible fare gates can provide a better experience for current AFAS Gate users and the larger population of customers who might have difficulty entering via existing LT or HEET. For AFAS Gate users, accessible versions of modern fare gates (or AWAGs) provide an experience more similar to the method of entry that a person without a disability uses and are less error-prone than the current AFAS Gate. The AFAS Gate also poses challenges to NYCT, both in terms of maintenance and fare evasion. A long-term, industry-proven accessible solution is needed to advance the MTA's systemwide accessibility goals.

The goal of this QPL Process is to identify a list of qualified secure, accessible, and modern fare gates to place on the MTA's Qualified Product List (QPL) for future purchases to meet the MTA's needs.

The Gates must have demonstrated capability of being widely deployable throughout the NYCT subway system, to replace the current LT (in the case of WAGs) and AFAS Gate/AutoGate and Emergency Exit Gate (in the case of AWAGs). In addition, they may be used in lieu of current gates in new stations or station renewals.

Gate design must, among other things, achieve fare evasion deterrence, accessibility, access, safety, maintenance, and cost, in order to be suitable for the MTA. During the QPL Process, the participating firm must sufficiently demonstrate, in the sole discretion of the MTA, that the Gates:

a. provide optimal customer flow and convenience for station entrance and egress;
b. minimize fare evasion, particularly in comparison to the current LT, AFAS/AutoGate, and Emergency Exit Gate;
c. are capable of being deployed at scale across the NYCT subway system;
d. are able to integrate with OMNY fare payment system and any future fare payment media to enable seamless and hassle-free paid entry;
e. are capable of withstanding in-system conditions including vandalism, steel dust, and higher levels of weather exposure and vibration at outdoor/elevated stations; and
f. minimize any slip/trip/fall, struck by/on, pinch point, or other safety hazards, and utilize parts that are modular and uniform, with minimal customization, to limit maintenance needs and complications.

In addition to these criteria, the participating firm must sufficiently demonstrate, in the sole discretion of the MTA, that AWAGs:

a. provide safe, independent system access to any customer that is unable to use a turnstile to enter or exit, due either to disability or any other need, such as pushing a stroller or transporting luggage or packages.
b. allow for entry and exit as quickly, or more quickly, than the current AFAS system. and
c. provide a code-compliant egress pathway for all emergency exit scenarios including power loss, fire/smoke condition, and other evacuation needs.

The minimum Technical Requirements for Gates are identified in Section V of this RFI.

The MTA reserves the right, in its sole discretion, to amend this document to modify the Technical Requirements, cybersecurity terms and conditions and requirements and any other requirements in this RFP to add, delete, revise, clarify and/or change such requirement. In such event, the MTA shall issue an addendum to this RFI.

III. QPL PROPOSAL REQUIREMENTS FOR FIRMS PARTICIPATING IN PHASE 1 OF THE QPL PROCESS

Firms that wish to participate in Phase 1 of this QPL Process shall submit a QPL Proposal that clearly includes the firm's legal name and address, the firm's primary point of contact name, email and telephone number. The proposal shall fully include and address the following:

a. Complies with the general submission requirements of this RFI including, but not limited to, the quality and completeness of any required written submission.
b. Demonstrates an understanding of the MTA's goals for the Gates;
c. Demonstrates an understanding of, and compliance with, the Technical Requirements (including cybersecurity requirements as set forth herein), and any revised or additional requirement(s) pursuant to any addendum to this RFI);
d. Includes an overall concept and product design, illustrated with appropriate schematics, including proposed equipment/product components and features, usability, ability to withstand the harsh NYCT operating environment, ability to ensure fare compliance, ability to be integrated with the fare payment system as well as adjacent legacy equipment, interoperability, scalability and hosting, availability, security and disaster

recovery approach.

e. Includes the firm's experience, qualifications, and technical competency in the design, manufacture, and delivery of Gates, demonstration of the firm's ability to design, manufacture, deliver, and provide technical support for Gates for a large transit property (including describing which other transit agencies have the gate in use today).
f. Demonstrates availability of, and ability to secure, relevant resources that would be committed to future procurements including the qualifications and past performance of key personnel and reliability of same.
g. Includes degree of scalability, including manufacturing capability and capacity, and raw material availability.
h. Demonstrates the firm's financial capacity and capability to provide the Gates in future procurements;
i. Includes an outline of a recommended Test Plan for MTA approval for Phase 2 and 3 (*see* below), including detailed description of the specific Gate(s) that will be tested, what should be tested, and how the testing will be performed;
j. Includes itemized, rough order of magnitude of current unit prices for Gates for the MTA to gain an understanding of costs (for informational purposes only unconnected to a procurement);
k. Includes authorized distribution network and/or resellers.
l. Identifies the standard manufacturing and delivery lead time for the Gates and any current market risks; and
m. Provides a detailed preventative maintenance program including the costs of material to maintain the Gates in a state of good repair for their useful life.
n. Provide the number of years anticipated for the useful life of the Gates and its components including any related apparatus.

IV. INSTRUCTIONS AND INFORMATION FOR FIRMS PARTICIPATING IN PHASE 1 OF THE QPL PROCESS

A. Interested firms **must submit their QPL Proposal to MTA via email or regular mail no later than close of business on February 29, 2024** (the "QPL Proposal Deadline") addressed to Reggie Matela, the designated Point of Contact for this RFI, at reggie.matela@mtahq.org or 333 West 34th Street, 10th Floor, NY, NY 10001.

B. Prospective Participants are reminded that pursuant to Sections 139-j and 139-k of New York State Finance Law, all contacts (defined as oral, written, or electronic communications with MTA) during this QPL process must be made through the designated Point of Contact only. **The Point of Contact for this procurement is Reggie Matela**. Ms. Matela can be reached by e-mail at reggie.matela@mtahq.org.

C. QPL Proposals received after the QPL Proposal Deadline may be accepted by the MTA. Firms accept sole responsibility for the timely delivery to and receipt by MTA of their QPL Proposals. MTA reserves the right to modify the QPL Proposal Deadline if considered necessary in MTA's sole and absolute discretion.

D. To assist prospective proposers in the preparation of their proposals, a virtual Pre-Proposal conference is planned for **January 17, 2024 at 2:00PM EST.** Although registration for this conference is not required, prospective proposers who desire to attend the pre-proposal conference must notify in writing to reggie.matela@mtahq.org by **4:00PM EST** of **January 16, 2024**.

Attendance to pre-proposal conference is not mandatory and shall be informal to the extent that the MTA shall not be bound by any statement made at such conference unless such statement is subsequently issued in an addendum which will be sent to prospective proposers.

E. Requests for clarification of this RFI and questions regarding this RFI and/or the QPL Process (including any questions about OMNY, OMNY System Integrator, and OMNY System Integration) shall be submitted in writing to the Point of Contact at the email address identified above. MTA will receive requests for clarification and questions through the **end of business day on January 12, 2024**. Requests submitted after that time may not be answered so firms are encouraged to submit requests in advance of the noted deadline. MTA intends to respond to written requests by **January 24, 2024.**

F. Any interpretation, correction, amendment, or additional provisions to this RFI that MTA may decide to include will be issued in writing as an addendum via email and provided to any firm that has registered with MTA for submission of a QPL Proposal; provided, however, that in Phases 2 and 3 of this QPL Process, only those firms invited to participate, and that do participate, will be entitled to receive, and will receive, addenda issued by MTA during those phases of the QPL Process. All addenda issued by MTA will be binding once sent by email and will become part of this RFI.

G. Firms who submit QPL Proposals in response to this RFI may be invited, at the sole discretion of MTA, to participate in face-to-face or virtual meetings to discuss the matters addressed in this RFI and their QPL Proposals. Firms may also be asked to provide additional information to MTA to supplement or clarify their QPL Proposals. Such discussions will assist MTA in identifying firms with Gates that may be invited to participate in Phase 2 of this QPL Process.

H. **MTA does not intend to award any contract based upon this RFI**. Responses to this RFI will be evaluated (as set forth herein) for a firm's potential further participation in this QPL Process and, ultimately, for potential qualification of a firm's Gate for inclusion on MTA's QPL. A firm's QPL Proposal and any information submitted in connection with this RFI shall not be considered bids or proposals for the procurement of Gates. Submission of a response to this RFI in no way guarantees the award of a contract in any subsequent procurement for Gates.

I. MTA, in its sole discretion, reserves the right, without liability, to modify and/or withdraw this RFI at any time without explanation, and/or to modify or waive any requirements

contained in the RFI.

V. TECHNICAL AND PERFORMANCE REQUIREMENTS FOR GATES

A. Current System Overview of Fare Array at MTA New York City Transit (NYCT)

NYCT currently operates and maintains a system of gated entry to its 474 subway stations consisting of varying types of fare control equipment. As previously noted, there are four types of fare control equipment in systemwide use: low turnstiles (including agent-operated special entry turnstiles, "SETs"), HEETs, high exit turnstiles ("HXTs"), and gates (including EXGs, agent-operated gates (AOG), and AFAS gates originally implemented for wheelchair access, both entry and exit). Since November 2021, access through the AFAS gates is no longer limited to specific customers.

MTA turnstiles are in a state of good repair, but internal electronics have exceeded their useful life. Additionally, the MTA has expanded its approach to both customer accessibility and fare evasion prevention. These new approaches create an opportunity to explore modern fare gate technologies that align with the MTA's strategic priorities while planning for new stations, station renewal, and ADA upgrade projects.

The MTA is considering the utilization of an AWAG in station projects where an AFAS gate might otherwise be installed and later, to replace existing AFAS gates. The MTA is considering utilization of WAG to replace turnstiles where access could be improved for all customers and to reduce fare evasion.

NYCT has nearly 1,000 fare arrays across the system that collectively included several thousand turnstiles, nearly 500 HEETs, more than 200 AFAS gates and an additional 1,000+ Emergency Exit Gates. A combination of AWAGs and WAGs may, over time, replace much of this legacy equipment. The MTA is currently piloting an AWAG/WAG product at several stations including Sutphin Blvd-Archer Av-JFK Airport station, a major point of connection to the airport.

B. Design Criteria and Technical Requirements for Gates

In order to participate in this QPL Process, a Participant must be able to demonstrate that it can provide both Gates (AWAG and WAG) that can readily be installed and integrated together in a fare array and meet the following design criteria and technical requirements (and collectively with the general requirements set forth in this RFI, the "Technical Requirements"):

1. **System Integration**

The Gate shall be capable of system integration with MTA's third-party OMNY validator for fare media validation, customer prompt, and gate operation and, where applicable, gate exit,

along with back-office fare payment verification. Specifically, Participants seeking to pre-qualify their Gates must be willing and able to perform and prove capacity for successful third-party integration with OMNY. This includes demonstrating that the Participant's Gates:

i. Seamlessly incorporate with existing Subway Validator with the Gate so that once a person taps for entry, the validator correctly reads the medium presented and prompts the customer accordingly.
ii. Are able to receive and respond accurately to the signals sent from existing Subway Validator to correctly allow or deny entry of the customer, including to correctly unlock gate or not unlock gate.
iii. Accepts software, firmware, and configuration downloads and updates from the NFPS Backend as provided by current system integrator.
iv. Can connect to the OMNY Backend and allow remote operations and device monitoring for maintenance.
v. Allows for local operation and service maintenance of the gate.
vi. Integrates the Subway Validator so that it also serves as an audible and visual warning system to the customer that Gate doors will open after fare collection.

2. **General Design Parameters**

i. The Gate may have a single or double paddle entry (or paddle-equivalent).
ii. The maximum width of the AWAG shall not exceed 52 inches (including a minimum clearance width of 36 inches) and the maximum length of the AWAG at floor level shall not exceed 50 inches. The distance from the floor to the underside of the entry paddles shall not exceed 14.5 inches.
iii. The maximum width of the WAG shall not exceed 36 inches (including clearance width of 24 inches) and the maximum length of the WAG at floor level shall not exceed 50 inches.
iv. Any Gate must have a minimum headroom clearance of 6-foot, 8-inches.
v. Gate must close automatically following a single customer passing through based on a configurable closing time parameter and a configurable speed of closure parameter
vi. Gate must have multiple exit sensors to support the deterrence of fare evasion and enable the collection of data for entries and exits.
vii. Gate shall not require that the MTA make any changes to its existing station flooring, including leveling. In addition, the Gate shall not be designed in a manner that requires wiring or other component parts to traverse the floor.
viii. Gate shall have a minimum throughput of 25 passengers per minute (PPM) to enter and 50 PPM to exit.
ix. AWAG shall have an equal or shorter time to enter/exit per customer, compared to both current AFAS Gate and turnstile.
x. The force required to break through the doors or paddles from the closed position must be configurable without requiring back-end software changes, capable of settings ranging from no more than 25 to no less than 150 lbs force, and adjustable to different setting for entry and exit force.

xi. Gates shall be configurable to have entry mode, exit mode, or bidirectional mode.

xii. Doors shall be capable of opening in both directions in normal use, based on the direction of customer approach. The Gate must be configurable to move in the direction of egress travel in cases of customer conflict (i.e., where customers approach from the paid and unpaid side simultaneously).

xiii. All components within the Gate shall be constructed of the highest quality materials suitable for production level use in the intended environment (i.e., NYCT). The superstructure shall be designed to provide a minimum useful life of 30 (thirty) years and the components of each gate designed to provide for each a minimum useful life of twelve (12) years.

3. **Installation and Maintenance**

i. Gate shall be capable of remote performance monitoring and signaling key metrics and potential failures utilizing ServiceNow and be integrated to NYCT's current Spear maintenance system.

ii. Gate power and communications cables must be designed to run through a dedicated Overhead Cableway System (OCS) loop connected directly to the AWAG and the WAG (power and communications shall not share the same pathway), with no ramping/cable covering or trenching required and avoiding mechanics at the base of the cabinet where possible. The OCS loop shall be designed from stainless steel type 304 with a #4 grain finish, with no plastic material on exterior cabinet, or a comparable material. The height of the OCS loop shall be adjustable.

iii. Gate shall be capable of operating on a power circuit providing a max power of 20A and designed to operate independently of other fare control equipment on the adjacent fare line (i.e. elsewhere in the station).

iv. Gate shall include conditioning equipment to regulate the NYCT supplied electrical power for use.

v. Gate shall be capable of being connected to the Fare Control Area Local Area Network or "FCALAN" switch over an ethernet connection.

vi. Materials shall be designed to withstand NYCT's harsh operating environment, including weather/elements and vibrations in an outdoor and/or elevated station environment, as well as extensive steel dust throughout the station environment (i.e., stainless steel, hardened and reinforced subassemblies, polycarbonate door, etc.), and the Participant shall submit test records and other formal and applicable documentation to confirm materials meet the following requirements, for the MTA's review and approval:

- The Gate shall resist: (i) horizontal shocks of up to 6 G and in the vertical axis of up to 1.2 G for a duration of up to 12 ms without permanent deformation or failure of such fare collection equipment. For the purposes of this requirement, "G" is the earth's gravitational constant or 9.81 meters per second squared; and (ii) half-sine shock pulse, 3 pulses/direction (where half-sine wavelength

energy is primarily used to test for responses and resonances in mechanical systems and one cycle of sine wave consists of two half cycles).

- There shall be no failure of mounts or decrease of operational characteristics of the Gate under conditions simulated by a sinusoidal sweep vibration test at a sweep rate of one-half octave per minute, from 5 Hz to 25 Hz to 5 Hz, at a peak vibratory acceleration of 0.25g for a minimum of 50 cycles when applied to each of the three axes and repeated continuously for five (5) complete cycles.

vii. All Gate components must also be vandal-resistant and "scratchitti" resistant (where scratchitti is a form of graffiti in which markings are etched into hard surfaces, including glass or plexiglass).

viii. All Gate components should be free from sharp edges or corners.

ix. PVC is not permitted in the NYCT environment. For all exposed applications, acceptable alternate materials should be utilized in lieu of PVC.

x. All Gate components shall be designed to meet or exceed International Electrotechnical Commission (IEC) Ingress Protection (IP44) requirements for water or object intrusion, and other relevant ratings such as UL certification:

- Operating Temperature -25°C to +50°C
- Relative Humidity 15% to 95% (non-condensing)
- Ingress Protection IP44
- Immunity EN61000-6-3, FCC Class B
- Flammability UL 94V-0.

xi. Gate components must be designed to maximize Mean-Cycles-Between-Failures (MCBF). MCBF shall be at least 250,000.

xii. Mean-Time-To-Repair (MTTR) for Gate components must be no greater than 0.5 hours with 90 percent of the repairs completed within 0.9 hours.

xiii. All components and materials shall be commercial off the shelf with clear documentation of sourcing and process for replacement as needed, including identification of authorized resellers. Sourcing of components will be reviewed and vetted by the MTA to verify risk, licenses, and replaceability.

xiv. All components must be self-contained within the Gate footprint such that maintenance can be performed without any impact on the function or usability of any adjacent fare control or other equipment.

xv. If doors/panels are forced open, they must be capable of being remotely reset or restarted by staff, without significant or specialized maintenance intervention.

4. Uniform Code Compliance

AWAGs and WAGs are intended to be utilized as a required emergency means of egress from the paid side to unpaid side of a subway station and, accordingly, shall meet the 2020 edition or latest of the New York State Uniform Fire Prevention and Building Code requirements including, but not limited to, the following:

i. A request to exit button that mimics the loss of power for a minimum of 30 seconds.

ii. Doors shall be held in a closed position under power. In case of power failure, doors/panels must be set to either:
    a. fail open (preferred) OR
    b. break away with a maximum of five (5) pounds force.
iii. The Gates shall have the capability to integrate with on-site systems such as fire alarms and an agent- or remote-operated switch, and to revert to the open position if triggered in case of emergency.
iv. Doors/panels must be side-hinged style (i.e., "saloon" doors), or provide a manual breakaway feature if retracting panel.
v. Is compliant with all force and time requirements of the applicable ADA and Uniform Code requirements detailed in Phase 1, Part 2.
vi. WAGs shall meet the minimum dimensional requirements of a turnstile that meets 55PPM capacity.

5. **Accessibility**

AWAGs shall meet all applicable ADA requirements in the Americans with Disabilities Act Accessibility Guidelines and the New York State Uniform Fire Prevention and Building Code including, but not limited to, the following:

i. Bottom of AWAG barriers must be no more than 27" above the walking surface.
ii. Minimum 36-inch clear width between fully opened panels/doors for AWAGs.

6. Safety, Security, and Fare Evasion

i. The Gates shall have an integrated mechanism (optical sensor or equivalent technology) to: (i) count pedestrian throughput in both directions to allow for comparison of entries and exits to paid fares, and (ii) monitor usage, fare evasion, and entry and exit time and capacity.
ii. Doors and panels must be designed to minimize opportunities to evade fare payment by reaching under, over, or in any way around while in the closed position. Maximum clearance under doors and panels and the minimum height of doors and panel must be identified by the Participant.
iii. The Gates shall use enhanced optical aisle sensors (or approved equivalent technology) to trigger door opening and closing, with remotely configurable opening and closing time and speed.
iv. The Gates shall be able to detect and provide analytics around fare non-compliance, including multiple entries (piggybacking or tail-gating). This may include built-in camera, other detection systems, and/or ability to integrate with external systems.
v. Any Gate barriers shall either be transparent or have a cutout for visibility.
vi. Gate designs shall eliminate or minimize any slip/trip/fall, struck by/on, pinch point, or other safety hazards.
vii. Demonstrate through testing that any safety hazards are either eliminated or both remote in possibility and marginal in severity.

viii. Gates shall meet the fire performance for materials as specified in NFPA-130, the Standard for Fixed Guideway Transit and Passenger Rail Systems, 2023 edition.

7. **Customer Communications/Assistance Functions**

i. The AWAG shall have an integrated two-way communications device capable of connecting to an on-site or remote voice receiver.

ii. The AWAG shall be capable of supporting two separate remote and/or button-operated opening features:

   a. An emergency opening feature in which the panels fail to the unpaid side (for egress) and stay open until the switch is released or some other action is taken to indicate the emergency is cleared; and

   b. A "customer/personnel assistance" opening feature in which the panels open to the paid side (for entrance) and the panels close after sensors are triggered detecting one entry per customer.

iii. In the case of multiple and connected AWAGs, switches shall be independent for each AWAG.

II. EVALUATION OF FARE GATES

A. Overview of Evaluation Approach

The MTA will undertake a four-phase evaluation process to develop a list of qualified fare gates to be placed on the MTA's QPL and will conduct future procurements for approved Gates in accordance with the MTA's policies and procedures.

B. Multi-step Evaluation Process

1. Phase 1: Evaluation of QPL Proposals:

Phase 1 of QPL evaluation will be a document-based review of Participants' written QPL Proposals to determine a Participant's ability to meet the stated Technical Requirements and the general requirements of this RFI. (*See* Section I above).

The MTA will evaluate, in its sole discretion, QPL Proposals based on the following criteria to determine if a Participant shall be advanced to Phase 2:

i. Participant's prior relevant experience with delivering Gates to other transit entities;

ii. Participant's prior relevant experience in integration with fare payment terminals;

iii. Participant's proven ability to design, manufacture, and deliver Gates in timely, cost-effective fashion to Participant's client's satisfaction;

iv. Participant's demonstrated ability to adapt to complex and evolving field conditions;

v. Participant's specifications and design drawings for their proposed Gates (both

WAG and AWAG) that demonstrate that the products meet the technical and performance requirements described by this RFI, or provides equivalent or better performance;

vi. Participant's proposed Test Plan including whether such plan reflects best practices and established industry practices for testing hardware and system integration; and

vii. Pricing and overall life-cycle costs including maintenance.

The evaluation shall be conducted by MTA's selection committee and technical advisory committee which will, at minimum, include representatives from:

i. NYCT Revenue Operations
ii. NYCT EMD
iii. NYCT Stations Program/Environment
iv. NYCT Operations Planning – Stations Planning
v. NYCT System Safety
vi. MTA Construction & Development FACC Services Office
vii. MTA Construction & Development Stations Business Unit
viii. MTA Construction & Development OMNY Operations & Services
ix. MTA Accessibility
x. MTA Security

Participants that meet the Phase 1 requirements, as determined in the sole discretion of the MTA, will be invited to participate in Phase 2 of this QPL Process. .

2. **Phase 2A: Lab Test:**

Phase 2 will consist of testing the Gates of Participants invited to participate including testing in the Participants' production lab to further demonstrate the Participants' ability to meet or exceed the Technical Requirements and the RFI requirements set forth herein (and in any future addendum). Participants shall ensure that their Gates, which shall be tested in Phase 2 are of production quality and are capable of installation in the NYCT system.

Lab testing shall include at least one (1) AWAG and one (1) WAG.

Participants in Phase 2 shall perform the MTA-approved Test Plan to suitably demonstrate that the Gates meet the Technical Requirements and all other requirements of this RFI. The testing shall be conducted in accordance with industry standards, this RFI, and Test Plan approved by the MTA. Generally, the tests must mimic real-world conditions (i.e., customer volumes, diversity of use cases, weather, crash conditions, emergencies, various entry and exit scenarios), which will be finalized in the Test Plan. The Participant shall compile the results of the testing in a detailed report, and shall be submitted to the MTA for review and evaluation.

The MTA's intent is to approve one Test Plan at the completion of Phase 1, which shall be used by any Participant selected to advance to Phase 2. Test Plans may require multiple rounds of testing in both Pre-Production (or Stage) and Production environments. Testing shall commence no more than 30 days after Test Plan is approved and received by any Participant invited to participate in Phase 2. Participants shall provide prior notification to

the MTA of its intent to conduct the testing to facilitate scheduling the MTA's participation in each round of testing. The MTA anticipates that Phase 2 will be conducted over approximately a two (2) month period, subject to the MTA's right to extend such time period, in its sole discretion, to ensure testing is complete for evaluation purposes. Approval to move to Production environment will be required from the MTA prior to a Participant moving from a Stage to Production phase.

The MTA reserves the right, in its sole discretion, to require retesting in whole, or in part, prior to determining whether a Phase 2A Participant shall proceed to Phase 2B of this RFI.

During Phase 2A, MTA standard contract terms and conditions will be shared with the Participants selected. In addition, Participants acknowledge and agree that they will be subject to a full financial and background check in parallel with testing and agree to provide relevant financial information requested by the MTA for evaluation.

3. Phase 2B: Lab Test with System Integration

As will be required in the Test Plan, Participants(s) that successfully pass Phase 2A must successfully integrate with OMNY and demonstrate such integration in their lab environment before their equipment can be considered for installation in the revenue environment including the integration of the OMNY subway validator. The OMNY validator(s) will be provided by the MTA.

Participants whose gates are deemed to have performed successfully against the Phase 2 Test Plan, and who pass the financial and background check, will be invited to participate in the Phase 3 of the QPL Process for In-Service and System Integration Field Testing at the sole discretion of the MTA.

The MTA reserves the option to combine Phases 2A and 2B Lab Testing.

4. Phase 3: In-Service Test with System Integration

A Participant with Gates invited to proceed to Phase 3 shall install the same AWAG and WAG in MTA-designated locations within the NYCT subway system for field testing. The designated locations may include one or more locations in any of the four (4) boroughs within the NYCT subway system. Such installations shall consist of one (1) AWAG and one (1) WAG, or a full array of an AWAG and WAGs, at the MTA's discretion. The Gates for revenue testing shall be provided by the Participant to the MTA at no cost to the MTA.

Any Gate that is selected to be installed in the field will be required to integrate with the OMNY validator to allow for field production testing of end-to-end fare payment transactions in the NYCT subway system. The OMNY validator(s) will be provided by the MTA.

At the time of Phase 3 field testing, the Gates with the integrated OMNY validator will be commissioned and placed into revenue service at location(s) of the MTA's choosing. In Phase 3, the Participant will need to demonstrate successful integration of the Gate in the

MTA fare payment system and reliable and consistent performance of the Gate in the NYCT operating environment, as defined by the Technical Requirements of this RFI. Gates will be tested in revenue service for a minimum of three (3) calendar months.

The MTA may extend the Phase 3 test period, in its sole discretion, if deemed necessary to determine whether the Gates have sufficiently demonstrated successful system integration and reliable and consistent performance in the field live environment such that it can be placed on the QPL.

During the Phase 3 evaluation period, Participants will be required to provide all maintenance for any equipment installed in the field at no cost to the MTA. Proposers may be permitted, in consultation with the MTA and with prior approval in writing, to make any modifications to gate hardware or software design required to demonstrate adherence to the Technical Requirements, provided such modifications do not, in the sole discretion of the MTA, require wholesale gate removal and replacement or other similarly disruptive activity.

Provided that the performance of the Participant's Gate satisfies the criteria in all three (3) phases of evaluation, the Gate that successfully achieves Phase 3 field testing shall be placed on the MTA's QPL. Future procurements for Gates will be conducted based on the QPL.

VI. INCLUSION OF APPROVED GATES ON QPL AND PROCUREMENT OF GATES

Once a Gate is deemed approved by the MTA for inclusion on the QPL, the Gate cannot be modified without the advance written approval of the MTA. Any modifications to the Gate without the consent of the MTA may result in removal of the Gate from the MTA QPL, in the MTA's sole discretion.

The Participant will be required to agree to the attached Qualified Products List Applicant Certification document, attached to this RFI as Attachment 2. MTA reserves its right to procure Gates from the QPL or via other permissible purchasing processes in the best interest of NYCT and other agencies.

VII. INCURRING COSTS

Except as otherwise provided herein, the MTA shall not be liable for any QPL Process activity or cost incurred by any Participant for its preparation of any QPL Proposal or participation in this QPL Process.

VIII. CONFIDENTIALITY OBLIGATIONS

All Participants are required to sign the MTA OMNY Non-Disclosure Agreement attached hereto and made a part of this RFI as Attachment 3 in order to receive certain confidential and/or sensitive information about the OMNY required for Gate testing and integration with the MTA's fare

payment system (validators and OMNY backend). No alternate forms are permitted. Participants may be required to enter into a separate confidentiality or non-disclosure agreement with the OMNY system integrator for testing purposes. Failure to enter into the MTA OMNY Non-Disclosure Agreement may prevent a Participant from advancing to Phase 2.

IX. CYBERSECURITY REQUIREMENTS – All Participants are required to certify compliance with the MTA Cybersecurity Requirements (Short Form), annexed hereto as Attachment 4.

ATTACHMENT A – DEFINITIONS

1. Turnstile: A fare control device that permits entry upon fare validation and allows for exits, with the intent of allowing one person to enter or exit at a time

2. Low turnstile (LT): NYCT's standard turnstile with rotating tripod arms at approximately waist-height. After fare payment is validated, the customer must gently push the arm to rotate in the direction of the paid zone; a similar push, without fare validation, is used to exit.in height. The tripod is designed to create a clear width below the top tripod arm to allow customers below 44" to "duck under" to enter without paying a fare. Each tripod is enclosed by two consoles. The right console is used for fare validation and to house the tripod mechanism; the left console is either another turnstile or an end console to close off the array.

3. HEET (High Entry / Exit Turnstile): A tall, circular turnstile with three sets of stacked, horizontally oriented bars. Bars are attached to a center axis that when pushed, can spin either from the paid area to the unpaid area, or from the unpaid area to the paid area. A spring mechanism above the device limits the rotation to one person per push. A separate console on the unpaid side is used for fare validation.

4. HXT (High Exit Turnstile): A device similar in design to a HEET, but that allows for exit flow only, with no associated fare validator.

5. AutoGate/Automated Farecard Access System (AFAS). Our current accessible fare control system, the AutoGate is an automatic entry/exit gate that allows customers who are accompanied by a service animal or use wheelchairs to enter and exit the subway system. The AutoGate uses the same hardware as a service gate, including a panic bar for emergency exit, enhanced with an AFAS card reader on either side of the gate. To use the AutoGate, customers must use their card/device at an AFAS reader to trigger automatic opening for both entry and exit.

ATTACHMENT 2 - Qualified Products List Applicant Certification

Provisions Governing Evaluation of Qualified Products List (QPL)

Applicant Certifies that it:

1. *Agrees to be bound by all of the provisions and terms set forth in this document.*
2. *Is the manufacturer of the product, or is an authorized agent of the manufacturer's approved branded product.*
3. *Has determined from actual tests (within the limits of test equipment commonly available, unless otherwise specified) that the product conforms to the applicable specification. (Test reports and data should be furnished with the application.)*
4. *Will supply items for test for MTA Review & Approval.*
5. *Will supply products that meet the requirements of the specification in every respect.*
6. *Will remedy deficiencies disclosed during qualification testing.*
7. *Should the original testing fail the vendor will not request an MTA retest of a product until satisfactory evidence is furnished that all defects, disclosed by previous tests have been corrected. (Test reports may be required as evidence.)*
8. *Will not state, advertise, or otherwise promote that a product(s), which has received NYC Transit qualification approval, is in any way recommended or endorsed by NYC Transit.*
9. *Will notify the appropriate NYC Transit manager of any planned change in design, materials, manufacturing processes (including quality control), plant location or point of origin after NYC Transit grants approval. The applicant will also immediately notify NYC Transit if;*
    - *a. Applicant believes the change will adversely affect the capability of the product to continue to meet the qualification test requirement, or if applicant*
    - *b. intends to submit new samples for testing or (after qualification approval) desire to have his product removed from the QPL, or if*
    - *c. The changes will affect the applicant's brand designation for the product.*
10. ***Product Identification***

BRAND NAME	*BRAND LEGAL OWNER*	*POINT OF CONTACT*

ACTUAL MANUFACTURER NAME	*ACTUAL MANUFACTURING LOCATION*	*MANUFACTURING LOCATION POINT OF CONTACT*

MANUFACTURER PART NO.	*SHELF LIFE*	*SHELF LIFE MARKER (If any)*

Qualified Products List Applicant Certification

☐ *Mark*

☐ *Trade, Logo*

☐ *Other, Specify*

_____

_____

Brand Manufacturer Quality System & Accreditation

_____

Social Compliance Review (if manufactured outside of the United States of America)

Agrees to complete applicant certificate now and upon recertification period *YES:* _____*NO*__

12 *An officer of applicant firm and a senior officer or QM representing the manufacturer (both) must endorse by signature* below.

Officer Name (Print)	*Senior Manufacturing or Quality Manager Name (Print)* At Actual Manufacturing Location
Title	*Title*
Signature	*Signature*
Date	*Date*
Company Name & Address	*Manufacturer Name & Address*

For NYCT Official Use Only

Commodity #

_____

_____

_____

_____

ATTACHMENT 3 - MTA OMNY Non-Disclosure Agreement

(QPL Participant Receipt of System Integrator Confidential Information)

This Non-Disclosure Agreement (the "**Agreement**") with an effective date as of the last signature below (the "**Effective Date**") is between (i) the Metropolitan Transportation Authority (the "**MTA** "), and (ii) the Party identified in the signature block below (the "**QPL Participant**"), (each, a "**Party**" and together the "**Parties**").

RECITALS

WHEREAS, the MTA and a systems integrator (the "**SI**") have entered into Contract A-34024 memorializing the rights and obligations of the MTA and the SI with respect to the New Fare Payment System, branded "**OMNY**" (the "**SI Contract**");

WHEREAS, the MTA has initiated a Request for Information for Wide Aisle/Accessible Fare Gates ("WAGs") to establish a Qualified Products List ("QPL"), from which QPL the MTA may solicit to purchase WAGs for integration with OMNY (the "**QPL RFI**");

WHEREAS, the SI has and/or is providing SI Confidential Information to the MTA, and the MTA in turn anticipates providing some or all of such SI Confidential Information to the QPL Participant in connection with the QPL Participant's participation in the QPL RFI;

WHEREAS, the SI requires assurances that SI Confidential Information will be protected while in the possession or under the control of the QPL Participant; and

WHEREAS, this Agreement is structured to provide such assurances, and to govern the exchange of SI Confidential Information between the MTA and the QPL Participant;

NOW THEREFORE, the Parties agree to the following:

AGREEMENT

1. Definitions.

1.1. "**Confidential Information**" means any information (in any medium) concerning the MTA and its subsidiaries and affiliates or the SI that the Disclosing Party discloses or makes available to the Receiving Party, whether orally or in writing, in connection with the QPL RFI that: (i) concerns the business, employees, customers, marketing, finance, methods, research, processes, procedures, operations, technical data, specifications, drawings, plans, diagrams, sketches, renderings, maps, surveys, photographs or other information of or about the Disclosing Party; (ii) is marked confidential, restricted or proprietary at the time of disclosure or a reasonable period thereafter; or (iii) by the nature of the information itself, or the circumstances surrounding its disclosure, should in good faith be treated as confidential.

1.2. "**Disclosing Party**" means either (i) the MTA, for MTA Confidential Information, or (ii) the SI, for SI Confidential Information.

1.3. "**Duty of Confidentiality**" means the requirements set out in Section 2 (Confidentiality) and the terms of the QPL RFI governing the QPL Participant's permitted use of Confidential Information.

1.4. "**Governmental Authority**" means any territorial, state or local governmental authority, quasi-governmental authority, instrumentality, court, government, commission, tribunal or organization or any regulatory, administrative or other agency, or any political or other subdivision, department or branch of any of the foregoing.

1.5. "**MTA Confidential Information**" means all Confidential Information that the MTA or its affiliates and subsidiaries disclose or make available to the QPL Participant that is not SI Confidential Information.

1.6. "**Person**" means an individual, a partnership, a corporation, a limited liability company, an association, a joint stock company, a trust, a joint venture, an unincorporated organization, any other business entity or a Governmental Authority (or any department, agency or political subdivision thereof).

1.7. "**Receiving Party**" means the QPL Participant.

1.8. "**SI Confidential Information**" means Confidential Information that the SI has provided to the MTA under the SI Contract. Section 2.3 (Classification of Confidential Information) shall resolve uncertainty (if any) over whether Confidential Information is SI Confidential Information or MTA Confidential Information.

1.9. "**Third Party**" means a Person other than: (i) the MTA; (ii) the SI; or (iii) the QPL Participant.

2. Confidentiality.

Confidential Information provided to the QPL Participant shall be governed as follows:

2.1. Non-Disclosure; Standard.

The QPL Participant shall not use any Confidential Information for any purpose not expressly permitted by the QPL RFI, and it shall disclose Confidential Information only to those employees, contractors, subcontractors, suppliers and agents of the QPL Participant who (i) have a need-to-know basis for access to such Confidential Information for the purpose of performing the QPL Participant's obligations or exercising the QPL Participant's rights, as set out in the QPL RFI, and (ii) are under a duty of confidentiality no less restrictive than the QPL Participant's duty hereunder and by applicable law. The QPL Participants hall protect all Confidential Information from unauthorized use, access or disclosure in the same manner as the QPL Participant protects its own confidential information, but shall in no event use less than a reasonable standard of care and diligence.

2.2. Exceptions.

The QPL Participant's obligations hereunder with respect to Confidential Information shall not apply to Confidential Information that the QPL Participant can demonstrate in writing (to the Disclosing Party's satisfaction): (i) was already known to the QPL Participant at the time of disclosure; (ii) was or becomes available to the QPL Participant on a non-confidential basis from a Third Party, provided that such Third Party is not bound by an obligation of confidentiality to the Disclosing Party with respect to such Confidential Information; (iii) is or has become generally available to the public through no fault of the QPL Participant; (iv) is independently developed by the QPL Participant without access to, or use of, the Confidential Information, as evidenced through proper documentation; or (v) is required by law to be disclosed, provided that the QPL

Participant notifies the Disclosing Party of such required disclosure promptly and in writing and cooperates with the Disclosing Party, at the Disclosing Party's reasonable request and expense, in any lawful action to contest or limit the scope of such disclosure.

2.3. Classification of Confidential Information.

Unless Confidential Information under this Agreement or the QPL RFI is clearly marked or disclosed as "MTA Confidential Information," the QPL Participant shall deem the Confidential Information "SI Confidential Information."

2.4. Entire Agreement; Order of Priority.

This Agreement supplements the QPL RFI between the MTA and the QPL Participant. This Agreement, and the terms of the QPL RFI governing the QPL Participant's permitted use of the Confidential Information, constitutes the entire agreement between the Parties regarding the Duty of Confidentiality and supersedes any prior or contemporaneous oral or written representation regarding the Duty of Confidentiality. The QPL Participant agrees that to the extent that any provision or requirement relating to the Confidential Information in the QPL RFI conflicts with the requirements set out in this Section 2 (Confidentiality), as between the MTA and the QPL Participant, the more stringent provision or requirement, from the MTA's perspective, shall apply.

3. Ownership.

Nothing contained in this Agreement shall be construed to transfer any ownership in any Confidential Information. With regard to all exchanges of Confidential Information under this Agreement, Confidential Information shall remain the property of the Disclosing Party.

4. Third Party Beneficiary.

The Parties agree that the SI is an express, intended third party beneficiary of each obligation that this Agreement places on the QPL Participant with respect to SI Confidential Information. The QPL Participant acknowledges that the SI has the right to enforce such obligations set out in this Agreement directly against the QPL Participant, if the QPL Participant is in breach of such obligations.

5. Choice of Law; Jurisdiction.

This Agreement shall be governed by and construed in accordance with the laws of the State of New York, without regard to its choice of law provisions. Each Party agrees that the state and federal courts sitting in the judicial district that includes New York, New York shall have exclusive jurisdiction over disputes arising under this Agreement, and each Party waives objections to the laying of venue in such judicial district.

6. Termination.

The MTA shall be entitled to terminate this Agreement for any reason upon ten (10) days written notice to the QPL Participant.

7. Term.

This Agreement shall commence on the Effective Date and shall continue, unless earlier terminated in accordance with Section 6 (Termination), or until the conclusion of the QPL RFI. Notwithstanding the termination or expiration of this Agreement, the QPL Participant's confidentiality obligations with respect to Confidential Information shall survive and continue in accordance with Section 9 (Cessation of Obligations).

8. Return or Destruction of Information.

Upon termination in accordance with Section 6 (Termination) or the conclusion of the QPL RFI, the QPL Participant shall, at the MTA's direction, either (i) return to the MTA all Confidential Information, including all documents and materials derived from such Confidential Information (an "**Information Return**"), or (ii) destroy all such Confidential Information and certify to such destruction in writing to the MTA (a "**Destruction Certificate**").

9. Cessation of Obligations.

The QPL Participant's obligations under this Agreement shall remain perpetually unless the Confidential Information is subject to Section 2.2 (Exceptions) at no fault of the MTA or the QPL Participant; provided, however, that the following provision shall survive: Section 3 (Ownership).

10. Defend Trade Secrets Act of 2016 Notice.

Notice is hereby given pursuant to 18 U.S.C. § 1833(b)(3)(A) as follows: (i) an individual shall not be held criminally or civilly liable under any federal or state trade secret law for the disclosure of a trade secret that: (a) is made both (1) in confidence to a federal, state or local government official, either directly or indirectly, or to an attorney, and (2) solely for the purpose of reporting or investigating a suspected violation of law; or (b) is made in a complaint or other document filed in a lawsuit or other proceeding, if such filing is made under seal, and (ii) an individual who files a lawsuit for retaliation by an employer for reporting a suspected violation of law may disclose the trade secret to the attorney of the individual and use the trade secret information in the court proceeding, if the individual both (x) files any document containing the trade secret under seal, and (y) does not disclose the trade secret, except pursuant to court order.

WHEREFORE, the Parties through their authorized agents have signed this Agreement as of the Effective Date.

[REMAINDER OF PAGE INTENTIONALLY LEFT BLANK; SIGNATURE PAGE TO FOLLOW]

Metropolitan Transportation Authority

By: _____

Print Name: _____

Title: _____

Date: _____

_____ (QPL Participant)

By: _____

Print Name: _____

Title: _____

Date: _____

Mailing Address: _____

_____

Email Contact: _____

City/State of Incorporation: _____

ATTACHMENT 4 - MTA Cybersecurity Requirements and Certification

Metropolitan Transportation Authority

CYBERSECURITY TERMS AND CONDITIONS – SHORT FORM

A. DEFINITIONS.

1. Authority: shall mean the Metropolitan Transportation Authority ("MTA") and each of its subsidiaries and affiliates.
2. Authority Data: shall mean the following regardless of whether it is contained in existing or newly created in the future physical or electronic media at rest or in motion, any and all:
   a. Personal Information as such term is defined herein;
   b. all other data, information and documentation of the Authority including current and revised technology assets and systems, procedures and methodologies for designing implementing or maintaining in general and specifically, with information technology and physical and electronic security;
   c. the Authority's owned, licensed, or subscribed inventions, ideas and designs, design documents, equipment technology and software;
   d. reports and studies whether prepared by Authority, the Contractor or a third-party and whether in development or completed; and data, information, documentation and material prepared by or for the Contractor, any subcontractor, or by their respective consultants, agents, officers or employees in connection with performance of the Work, whether prior or subsequent to execution of this Contract or Agreement; and
   e. results of the Work.
3. Contract: shall mean the agreement entered into between the Authority and the Contractor setting forth the Work, and to which these Cybersecurity Terms and Conditions are attached and made a part thereof.
4. Contractor: shall mean the vendor, contractor, individual or organization that enters into the Contract or Agreement to perform the Work pursuant to the Contract Documents.
5. Covered Contractor Information System: shall mean an information system that is owned or operated by a contractor that processes, stores, or transmits Authority information.
6. Information or information: shall mean any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.
7. Personal Information or Personal Identifiable Information (PII): shall mean any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means; information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, code, symbol, mark or other identifier) or (ii) by which the Authority or other agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors; and information permitting the physical or online contacting of a specific individual shall be deemed Personally Identifiable Information.
8. Security Incident: shall mean (i) an occurrence that actually or imminently jeopardizes, without lawful authority, the confidentiality, integrity, or availability of a Covered Contractor Information System or any Contractor system that connects to or otherwise impacts a Covered Contractor Information System; or (ii) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies that impact a Covered Contractor Information System or any Contractor system

that connects to or otherwise impacts a Covered Contractor Information System.

9. Work: shall mean all the required obligations of the Contractor under the Contract or Agreement including but not limited to, the performance of any labor or services, the supplying of any goods, materials or personnel, the furnishing of any equipment and/or supplies or any other deliverables (e.g., parts, assemblies, kits, specially manufactured items) to the Authority as required by the Contract Documents including any scope of work and any modifications to the Contract, if any.

B. NON-DISCLOSURE.

The Contractor shall not furnish or disclose or allow its employees or agents, or subcontractors or their employees or agents, to furnish or disclose to any person or entity, any Authority Data without prior, written consent of the Authority. Notwithstanding the foregoing, the Contractor may furnish or disclose Authority Data to its employees or subcontractors as necessary for the performance of the Work.

C. PROTECTION OF DATA.

1. The Contractor shall have in place dedicated personnel to work with the Authority during any Security Incident response (the "Cyber Incident Response Team"). The Cyber Incident Response Team shall be maintained by the Contractor for the duration of the Contract or Agreement.

2. The Contractor shall provide, in writing, within twenty-four hours (24) hours of the Authority's issuance of a purchase order, Notice of Award (or execution of the Contract if no Notice of Award has been issued) or modification of the Contract a list of the individual(s) on the Cyber Incident Response Team. Such list shall include the name of each team member together with a phone number and email address for each such member. In the event of any changes to team members or team member information during the term of the Contract, the Contractor shall promptly provide such new information to the Authority, to the attention of the Project Manager, in writing.

3. If the Work involves the Contractor's access to PII as defined herein, then the Contractor shall comply with the New York Stop Hacks and Improve Electronic Data Security Act (also known as the SHIELD Act), which amends section 899-aa of the New York General Business Code and adds Section 899-bb, in the performance of the Work, as applicable, which, among other things, imposes on entities identified in the SHIELD Act:

   a. particular data breach notification requirements; and
   b. data security safeguards.

D. NOTIFICATION TO MTA OF BREACH OF AUTHORITY DATA.

Unless otherwise provided by law or as further detailed in the Contract, in the event of any act, error or omission, negligence, misconduct, or breach that compromises or is suspected to compromise the security, confidentiality, or integrity of Authority Data or the physical, technical, administrative, or organizational safeguards put in place by the Contractor that relates to the protection of the security, confidentiality, or integrity of Authority Data, the Contractor shall, as applicable:

a. promptly notify (1) the Project Manager and (2) the Authority by email to ThreatIntel@mtahq.org, as well as verbally by phone at (646) 252-7300 as soon as practicable but no later than twenty-four (24) hours after initially becoming aware of such occurrence;
b. perform or take any other actions required to comply with applicable law as a result of the occurrence;
c. cooperate with the Authority in investigating the occurrence, including making available all relevant records, files, data reporting, and other materials reasonably required to comply with applicable law, in referring the occurrence to appropriate law enforcement agencies, and in issuing appropriate press releases and responding to the media;
d. provide to the Authority a detailed corrective action plan as soon as possible, but no later than within ten (10) calendar days of the occurrence unless otherwise agreed to by the Authority, such plan shall provide the following (i) explanation of how the threat actor breached the affected system; (ii) description of the measures the Contractor

will undertake to address the vulnerability; and (iii) the implementation schedule for such measures (including any compensatory controls), to both resolve the breach and prevent a future occurrence. If the Contractor is unable complete the corrective action within the required timeframe, in addition to the remedies provided herein, the Authority may contract with a third party to provide the required product, service or system until (i) corrective actions have been taken, (ii) the Authority is able to procure from the Contractor the product, service or system in a manner acceptable to the Authority, and/or (iii) until the Authority has completed a new procurement for a replacement product, service or system (the "Mitigation Efforts"). In such case, the Contractor shall reimburse the Authority for the costs related to the Mitigation Efforts following notice and demand for payment by the Authority.

E. DESTRUCTION OF DATA.

1. All Authority Data including, but not limited to, all copies and reproductions thereof and all documents and materials derived from such Authority Data including any data in electronic form (i.e. cloud hosted Authority Data, etc.) provided to, prepared by or for the Contractor or any of its employees, subcontractors, agents and representatives (collectively, the "Contractor Personnel") shall, irrespective of whether such is in writing or stored electronically, be returned to the Authority or irrevocably destroyed by the Contractor and the Contractor Personnel, at the Authority's request or until such Authority Data is no longer subject to retention pursuant to the Contractor's own internal retention policies, whichever comes first. The Contractor shall, and shall cause its Contractor Personnel to, irrevocably destroy the Authority Data by: (i) shredding physical documents; (ii) wiping clean the device memory on all equipment, machines, databases, servers, cloud storage or other electronic media on which the Authority Data is located; and (iii) sanitize storage media, as well as temporary files and backup files on which the Authority Data is stored.
2. Notwithstanding the foregoing, the Contractor may retain copies of Authority Data that are stored in backups provided that all such retained data (i) is retained in accordance with their retention policy; (ii) remains subject to the confidentiality obligations contained in Contract Documents; (iii) is not accessed by the Contractor except (a) pursuant to applicable legal requirements and/or (b) in accordance with the Contractor's disaster recovery requirements, if applicable, and (iv) is destroyed in the manner described herein at the end of the retention period pursuant to the Contractor's record retention policy.
3. The Authority may request certification that destruction has been irrevocably completed for all primary, backup and any other applicable systems or mediums from the Contractor which shall be promptly provided by the Contractor for itself and for the Contractor Personnel; but in no event, not later than fourteen (14) days following the Authority's request.

F. COMPLIANCE WITH APPLICABLE LAWS, AND AUTHORITY SECURITY POLICIES AND PROCEDURES.

The Contractor shall implement and maintain security measures that protect against the disclosure of, and unauthorized access to, Authority Data and shall ensure that Authority Data is shared in a manner to protect against disclosure of such information. Protection shall meet requirements set forth in Attachment A annexed hereto.

G. DATA PRIVACY AND INFORMATION SECURITY.

1. The Contractor shall implement and maintain security measures that meet the requirements set forth in Attachment A.
2. Should the Authority require the Contractor to make changes to its cybersecurity compliance during the term of the Contract, the Contractor shall work with the Authority to agree on the changes to the cybersecurity compliance.
3. The Contractor shall provide the Authority, upon request, with information regarding the Contractor's compliance and implementation of the requirements set forth in Attachment A.

H. NO TRANSMISSION OF AUTHORITY DATA OUTSIDE OF THE UNITED STATES.

1. The Contractor shall not transmit, transfer, or otherwise store Authority Data, Personal Information, or any MTA-provided information that is labeled "confidential" or "sensitive", outside of the United States without the Authority's prior written approval, which may be withheld for any reason.

2. Notwithstanding the generality of the foregoing, if the Contractor is currently performing any Work outside the United States and/or utilizing any third party to perform (including its own employees) any Work outside the United States, the Contractor shall:

   a. Submit a request for written approval from the Authority for the continuation the storage of such Authority Data outside the United States ("Offshore Work Request"). Such request shall be submitted, in writing, to: (1) the Project Manager and (2) the Authority by email to ThreatIntel@mtahq.org;

   b. Enforce compliance with these MTA Cybersecurity Terms and Conditions and the requirements in Attachment A on any devices that will transmit, transfer, store or print Authority Data, Personal Information, or any MTA-provided information that is labeled "confidential" or "sensitive", including but not limited to encryption standards. Notwithstanding the foregoing, should the Contractor need to print Authority Data outside the United States in connection with its Work under the Contract, the Contractor shall include a print request in the Offshore Work Request;

   c. If required by the Authority, utilize a secure virtual data room or other workshare site that complies with these MTA Cybersecurity Terms and Conditions and the requirements in Attachment A; and

   d. In the event the Authority provides virtual desktops, access Authority Data, Personal Information, or any MTA-provided information that is labeled "confidential" or "sensitive", through such virtual desktops only. The Contractor shall not transfer Authority Data between the virtual desktop and Contractor's device(s).

I. COOPERATION WITH AUTHORITY CYBERSECURITY REVIEWS.

1. The Contractor acknowledges that the Authority has a significant interest in protecting and securing Authority Data and that maintaining cybersecurity is an essential element of the Work.

2. The Contractor shall cooperate with the Authority's compliance and cybersecurity reviews during the term of the Contract or Agreement and shall provide (1) information; (2) responses to inquiries and questionnaires in written form, when requested, and (3) supporting documentation to facilitate the Authority's review(s). The Authority shall be entitled to one (1) review every twelve (12) months after award of the Contract through expiration or termination of the Contract, whichever is earlier; provided, however, that in the event of a security incident, vulnerability or other threat during the term of the Contract, the Authority shall be entitled to an additional review or reviews, as applicable.

3. Such reviews will be coordinated by the Authority's Project Manager, MTA Information Technology or such other individual(s) or department as designated by the Authority.

J. CYBERSECURITY TRAINING.

The Contractor shall ensure that any individual or individuals who have access to Authority Data under this Contract undergo cybersecurity awareness training from a reputable training source at the Contractor's cost. In the event that the Contractor is providing in-house cybersecurity awareness training, then the Contractor shall notify the Authority within ten (10) days after notice of award.

The Authority shall not be required to pay any costs related to such training.

1. The Contractor shall maintain training records during the term of the Contract and shall make such documents available to the Authority for inspection upon request of the Authority. Submission of training records shall be sufficient to enable the Authority to determine or confirm: the individuals who received the training, the nature of the training and dates of such training.

K. CONFLICT.

If there is a conflict between these MTA Cybersecurity Terms and Conditions, the Requirements in Attachment A, and the Contract Terms and Conditions, the most stringent provision shall apply.

L. REQUIREMENTS FOR SOFTWARE, HARDWARE FIRMWARE AND OTHER TECHNOLOGICAL COMPONENTS.

1. In the event the Work and/or the Covered Contractor Information System includes inventory item(s) that contain firmware or software provided by the Contractor as the manufacturer (the "OEM"), additional terms and conditions apply. The Contractor shall request from the Contract Manager, Buyer or other Procurement Officer, and shall comply with, the MTA Cybersecurity Terms and Conditions (Long Form) and MTA Cybersecurity Requirements (Long Form).

2. In the event the Work includes software, hardware, firmware (collectively, the "IT Products") provided by the Contractor as a reseller of the OEM of same, the following requirements shall apply. The Contractor shall perform due diligence with respect to (i) the IT Products; and (ii) the OEM, to ensure that the delivered IT Products and updates thereto meet or exceed the following requirements:

   a. The IT Products are developed and maintained by the OEM based upon a best practice secure development lifecycle method.

   b. The Contractor shall obtain from the OEM and promptly provide to the Authority updates that remediate newly discovered vulnerabilities.

   c. The Contractor shall obtain from the OEM and promptly provide to the Authority the OEM's recommended corrective actions, compensating security controls, mitigations, and/or procedural workarounds when the updates that remediate newly discovered vulnerabilities are not yet available for distribution by the OEM.

   d. The Contractor shall promptly disclose to the Authority the existence of any backdoors known to the Contractor.

[Intentionally Left Blank]

ATTACHMENT 4-A

CYBERSECURITY REQUIREMENTS MATURITY LEVEL 1 (SHORT FORM)

The Contractor shall apply the following basic safeguarding requirements and procedures to protect Covered Contractor Information Systems. Requirements and procedures for basic safeguarding of Covered Contractor Information Systems shall include, at a minimum, the following security controls:

1. Limit Covered Contractor Information System access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

2. Ensure that all encryption methods for data-in-motion and data-at-rest comply with the current New York State Office of Information Technology Services Security Policy Encryption Standard NYS-S14-007.

3. Limit Covered Contractor Information System access to the types of transactions and functions that authorized users are permitted to execute.

4. Verify and control/limit connections to and use of external information systems.

5. Control information posted or processed on publicly accessible information systems.

6. Identify all information system users, processes acting on behalf of users or devices.

7. Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems. Limit physical access to all information systems, equipment, and the respective operating environments to authorized individuals.

8. Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the Covered Contractor Information Systems.

9. Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

10. Identify (e.g., static analysis scans, dynamic scans, third party penetration test), report, and correct information and Covered Contractor Information System flaws and/or vulnerability in a timely manner.

11. Provide protection from malicious code at appropriate locations within all information systems.

12. Update malicious code protection mechanisms when new releases are available.

13. Perform periodic scans of the Covered Contractor Information System and real-time scans of files from external sources as files are downloaded, opened, or executed.

ATTACHMENT 4-B

CYBERSECURITY CERTIFICATION OF COMPLIANCE

PROPOSERS ARE HEREBY NOTIFIED THAT THIS SOLICITATION IS SUBJECT TO THIS CERTIFICATION OF COMPLIANCE, WHICH REQUIRES PROPOSERS TO ACKNOWLEGE AND CERTIFY COMPLIANCE WITH THE MTA CYBERSECURITY REQUIREMENTS AND THE MTA CYBERSECURUITY TERMS AND CONDITIONS (COLLECTIVELY, "CYBERSECURITY REQUIREMENTS"). THIS CERTIFICATION SHALL BE INCORPORATED HEREIN BY REFERENCE INTO THE CONTRACT DOCUMENTS UPON AWARD, OR ISSUANCE, OF THE CONTRACT.

The Proposer hereby acknowledges and agrees as follows:

1. The Proposer has read, understands and shall comply with the MTA Cybersecurity Requirements in the performance of the work under the contract resulting from this solicitation or request for quote (including, but not limited to, the performance of services and the provision of equipment, parts, commodities or other goods sold); and

2. A Proposal may not be considered for award nor shall any award be made to a Proposer who has not submitted the certification below; and

3. Where the Proposer is submitted by a corporate Proposer, such certification shall be deemed to have been authorized by the Proposer and such authorization shall be deemed to include the signing and submission of such Proposal; and

4. The successful Proposer's failure to adhere to the Cybersecurity Requirements during the Term of the Contract shall be considered an event of default pursuant to the Contract Terms and Conditions.

REQUIRED BIDDER/PROPOSER CERTIFICATION OF COMPLIANCE WITH THE CYBERSECURITY REQUIREMENTS

By submission of this Proposal, each Proposer and each person signing on behalf of any Proposer certifies, and in the case of a joint Proposal each party thereto certifies as to its own organization, under penalty of perjury, that the Proposer has read, understood and shall comply with all such Cybersecurity Requirements.

By signing below, Proposer certifies that the statements made above are complete, true, and accurate.

RFI NO. 0009000032

Proposer Name: Click here to enter Bidder name

Proposer Signature: Date: Click or tap to enter a date

Print name of signatory: Click here to enter name of signatory. Print title of signatory: Click here to enter title of signatory.