New York City Connected Vehicle Pilot Deployment Project

Pedestrian Assistance Device Specification to support the visually impaired

The following document describes the requirements and specifications for the Pedestrian Information Device (PID) to provide urban navigation assistance to the visually impaired. This document contains the specification information from the previous document: *PID_1 0_12162016_1.7* titled Version 1.7 dated April 2016 which was added to the previous ASD specification. The enclosed document recognizes alternative approaches to implementing the PED applications using 4G/LTE rather than DSRC as originally intended.

Version 1.8
February 1, 2018

Table of Contents

List of Figures

List of Tables

1 NYCDOT Specification for *Personal Information Device* (PID)

1.1 General Information

1.1.1.1 The purpose of this Specification is to describe the minimum requirements of a Personal Information Device (PID) and associated application(s) that will be used for the New York City (NYC) Connected Vehicle Pilot Deployment (CVPD) Project.

1.1.1.2 The device specified in this document is a portable “smart device” with using 4G/LTE carrier communications to access the back-office servers and applications loading capability.

1.1.1.3 The PID shall also include both Blue Tooth and WIFi communications capability.

1.1.1.4 For the NYC CVPD, the pedestrian carries a PID which receives the the SPaT and MAP message contents (Signal, Phase, and Timing [SPaT] & Intersection Geometrics [MAP]) and is able to communicate with the back-office equipment (or other internet accessible locations) over a wide area wireless (WAW) service such as 3G, 4G/LTE, or equivalent.

1.1.1.5 Pedestrians are represented by the people that walk along the roadways. This project is intended to serve the visually impaired pedestrian and shall allow such pedestrians to orient themselves, determine their location, and determine the status of the pedestrian signals for their crosswalk of interest.

1.1.1.6 All parts shall be of high quality workmanship, and no part or attachment shall be substituted or applied contrary to the manufacturer's recommendations and standard practices.

1.1.1.7 The design shall be such as to prevent reversed assembly or improper installation of connectors, fasteners, etc. Each item of equipment shall be designed to protect personnel from exposure to dangerous conditions during equipment operation, adjustments, and maintenance.

1.1.1.8 The designed *Mean Time Between Failures* (MTBF) of the PID unit, operating continuously with the application operational, shall be 5 years or longer.

1.2 General Operation Description

The project seeks to provide a packaged unit (PID) for use by visually disabled pedestrians to assist in navigating signalized intersections within the City. New York City is installing Connected Vehicle (CV) technology at selected intersections (~320); as part of the CV installation, the intersection broadcasts ***signal phase and timing*** information (SPaT message) and detailed geographic information about the intersection (MAP message) in the DSRC spectrum (channel 172) in conformance to the DSRC standards (IEEE 802.11p, IEEE 1609.x, SAE J2735). The PID is expected to use this

information to “understand” the operation of the intersection and to assist the pedestrian. Refer to Appendix C below. The media to be used to receive this information was intended to be the DSRC communications in the 5.9 GHz spectrum from the RSU directly to the PID. However, that is no longer a requirement and it is recognized that a carrier media (LTE/4G) will be used to provide this information. It is up to the vendor to establish a design that provides the necessary information to the PID such that the information can be used to support the intersection crosswalk navigation function described herein.

1.3 General Contract Requirements

1.3.1 General

1.3.1.1 The vendor shall read and review the Phase 1 contract documents for the New York City Connected Vehicle Deployment project – specifically the Concept of Operations (ConOps), Security Management and Operating Concept (SMOC), Performance Measurement and Evaluation Support Plan, System Requirements Specifications (SyRS), and System Architecture Document (SAD).

1.3.1.2 The Phase 1 documents listed above are available online at the USDOT website (http://www.its.dot.gov/pilots/cv_pubs.htm) or the NYC CV Project site (TBD). The City is continuing to refine these documents and has incorporated these application requirements into these procurement specifications. However, many of the applications and data exchanges will require further adjustments and enhancements in order to meet all of the requirements stated herein.

1.3.1.3 The contractor shall comply with the existing functional specifications and safety applications in this document to the satisfaction of the City and adhere to all future releases related to hardware and software modifications included herein or jointly developed with the City.

1.3.1.4 The vendor shall also review and understand the RSU procurement document; the PID supplier will be responsible for coordinating their efforts with the RSU suppliers and the NYC CVPD Project team which is developing the TMC back-office CV support systems such that the system meets the stated goals and requirements stated therein.

1.3.1.5 Many of the design details have not been included herein for the PID; the standards do not currently support all of the functionality required for this project. This requires some flexibility on the part of the suppliers to cooperate with each other (RSU vendor) to solve and resolve major and minor technical issues including RF operation, messages, dialogs, channel usage, and application operation to build a successful system.

1.3.1.6 As noted above, there will be two (2) media for communications with the PID:

1.3.1.6.1 Optional: The DSRC communications from the RSU to the PID providing the MAP, SPaT, and RTCM message content;

1.3.1.6.2 The native WAN communications to the PID to provide access to the internet (e.g. 3G, 4G/LTE) and various applications such as navigation, data collection, and firmware updates.

1.3.2 The project plan

1.3.2.1 The CONTRACTOR shall develop ten (10) prototype PIDs as per this procurement specification. (Note: the CONTRACTOR may be required to make minor modifications to the PID design (with no change in cost) based upon City review. The CONTRACTOR is encouraged to work closely with the City to avoid unnecessary rework and un-reimbursed costs due to interpretation of the specifications.)

1.3.2.2 The ten (10) PID prototypes will be used to verify the vendor's quality (Software and Hardware operation) and develop the software for the back-office CV support systems including SCMS interfaces, data collection, data analysis, Over-the-Air (OTA) software updates, and OTA parameter changes.

1.3.2.3 The ten (10) PID installation Kits shall be used to work out the installation procedures with the service provider which will include initial installation and maintenance support.

1.3.2.4 The PID supply program shall undergo a ***prototype phase*** during which the City will work with the CONTRACTOR to verify conformance to the requirements herein, and demonstrate various aspects of the technical challenges including support for the following:

(a.) Over-the-air (OTA) software updates
(b.) Data collection (evaluation & operation)
(c.) Security system implementation (use of SCMS to insure the integrity of the SPaT and MAP information or an alternate scheme if DSRC is not used)
(d.) Software stability
(e.) Support for the MAP and RTCM messages if required by the vendor; the project plan does not plan to support the RTCM message at this time; if this is required by the PID vendor, then it must be stated within 10 days of contract initiation.
(f.) Location determination accuracy and navigation
(g.) Pedestrian interface to meet the needs of the visually impaired pedestrian.
(h.) Hardware stability for the portable environment including environmental (temperature, humidity, shock, vibration) and electrical (power interruption, surges, ESD)

1.3.2.5 If the PID uses the DSRC spectrum for any transmissions, then the PID prototypes will also be subjected to certification for standards conformance for the RF portion of device including messages which will

invoke the appropriate SAE standards, IEEE standards, NEMA standards, and NTCIP standards (e.g. J2735, J2945/x, 802.11p, 1609.x, NEMA TS2 environmental).

1.3.2.6 The vendor shall demonstrate that the location accuracy is sufficient to orient the pedestrian on the sidewalk, determine the desired crosswalk, and use the SPaT and MAP information to notify the pedestrian of the status of the specific crosswalk that the pedestrian intends to utilize at the intersection. Note that complex intersections will be part of the testing area.

1.3.2.7 Once the prototypes have been "proven" and successfully completed a field acceptance test, the City may release the delivery of the production quantity. (Note: such release will be optional; there is no assurance that the production quantity will be released when the City awards the contract.

1.3.2.8 During the prototype design and development, the CONTRACTOR shall provide timely submittals, design documents, test plans and test procedures, and message proposals for review as they proceed. These documents will be reviewed by NYCDOT and its subcontractors, USDOT and its consultants to ensure conformance to the overall requirements of the project and the requirements documents.

1.3.3 Advanced location options

1.3.4 Bid Items

1.3.4.1 Table 1 below lists the proposed items to be delivered for the PID procurement.

Table 1. Proposed Deliverable Items

Priority Order	Goods to Be Procured	Number To Be Procured	Estimated $ Each	Total
1	Portable/wearable PID Prototypes for evaluation and testing	10		
2	PID Production Quantity (on approval)	90		
3	On Site (NYC) Engineering Support Services – man weeks	4	$10,000	$40,000.00
4	Software source code and development environment	LS		

1.3.5 Preliminary Production Release

1.3.5.1 The City shall purchase a minimum of 100 production units (with software installed) as part of the Contract providing the CONTRACTOR makes the units fully conform to the procurement documents and

revisions to ensure interoperability as stated in the procurement documents.

1.3.5.2 The commitment to purchase the 90 production units will be dependent on the vendor's conformance to the schedule and the overall reliability of their device. If there are no problems with the prototype unit, the City has the option of releasing either 100 production units.

1.3.5.3 Once the prototypes have been "proven", the City may release the production quantity. Note that this will be optional – i.e. there is no assurance that the production quantity will be released when the City awards the contract. Further, the CONTRACTOR will be required to provide timely submittals, design documents, and message proposals for review as they proceed.

1.3.5.4 The City reserves the right, at its sole discretion to determine whether to release the additional 90 production units with installation kits based on the operation of the units, the accuracy of the location mechanism, the demonstrated operation of the applications, the stability of the computing platform, and the "proper operation" of the over-the-air (OTA) protocols.

1.3.5.5 By submitting a bid to supply this equipment, the vendor acknowledges that the City shall have the right to terminate the contract (or award of the contract) during the delivery of the prototypes and prior to notification of release of the production units without any further expense or obligation if it is deemed to be in the best interest of the City.

1.4 Correspondence and Contract Documents

1.4.1 Correspondence Material

1.4.1.1 All requests from the CONTRACTOR shall be submitted to the CITY in written (hard copy) form. This shall include but not be limited to requests for changes, time extensions, project submittals, drawings, requests for clarifications, schedules, etc. The number of hard copies is listed elsewhere herein.

1.4.1.2 Verbal discussions, telephone calls, etc. shall be committed to a written document if there are any issues regarding any technical aspects of the project, schedules, deliverables, performance, or costs.

1.4.1.3 The written document shall be transmitted (electronically and in hard copy) to the CITY by the CONTRACTOR within 5 business days of the verbal discussion.

1.4.1.4 The document shall clearly and concisely state what was discussed and shall clearly and concisely indicate any conclusions and all decisions made. The CITY shall review this document for accuracy.

1.4.1.5 The CITY shall have the right to make corrections to this document. Only the final CITY approved document shall be used for later reference.

1.4.1.6 If the CITY has not commented on or revised the document within 20 business days after receipt, it shall be assumed to be an accurate representation of the discussions as transmitted.

1.4.1.7 Following all meetings and teleconferences, the CONTRACTOR shall prepare detailed minutes of the meeting/teleconference including any decisions, clarifications, changes and action items. The minutes shall be submitted to the CITY for review. (Note: the CITY may make changes and adjustments to the meeting minutes and shall distribute the revised report to all parties.)

1.4.1.8 All action items shall clearly indicate the action, person responsible for the action, and the date the action is to be completed.

1.4.1.9 Only the final meeting minutes reviewed and approved by the CITY shall be used for later reference.

1.4.1.10 Meeting minutes shall be transmitted to the CITY within 5 business days of the meeting.

1.4.1.11 If the CITY has not commented on or revised the meeting minutes within 20 business days after receipt, they shall be assumed to be an accurate representation of the meeting as transmitted.

1.4.2 Contract Document Submittal

1.4.2.1 At the request of the City, the CONTRACTOR may be required to conduct periodic teleconferences and/or web conferences to review the status of design, construction, deliveries, testing, documentation, etc. if the City believes such periodic discussions are necessary. If such web conferences are requested [by the City or the contractor], the CONTRACTOR shall be responsible for providing the appropriate web conference tool and teleconferencing service.

1.4.2.2 All documents received by the CITY or the City's agent shall be date stamped upon receipt.

1.4.2.2.1 The date stamped on the received hard copy document shall be used for measuring all contract schedules and milestones.

1.4.2.2.2 The date the document is received and stamped by the CITY (and not the date sent by the CONTRACTOR) shall be used for measuring all contract schedules and milestones.

1.4.2.3 All documents transmitted by the CONTRACTOR shall be dated, numbered, and identified by the CONTRACTOR. Document numbers

shall be sequential from the start of the project; no numbers shall be skipped.

1.4.2.3.1 The CONTRACTOR shall maintain an ongoing list of all documents transmitted; the list shall include the topic of the document, date of transmission, and person(s) to whom the document was sent on a secure web site.

1.4.2.4 The CONTRACTOR shall maintain a secure web site which shall contain electronic copies of all documents transmitted to the CITY.

1.4.2.4.1 The web site shall only be accessible by personnel authorized by NYCDOT.

1.4.2.4.2 The secure web site shall maintain a log of all persons accessing the web site; this log shall note the date, time, IP Address, and person logging in and shall be accessible to the CITY.

1.4.2.5 All documents shall be transmitted to the CITY via email to expedite delivery; all such documents must be acknowledged by the City to be considered received. Note that the City may request selected documents be delivered in hard copy versions in which case the hard copy of the same document that must be received by the CITY within 5 business days.

1.4.2.6 The CONTRACTOR shall not assume that emailed documents have been received intact; thus, a confirmation that an email has been received does not constitute proof that the intended party received the email. The City must acknowledge proper receipt by appropriate email.

1.4.2.7 The delivery of all items to the CITY including but not limited to submittals, documentation, software, subassemblies, training, test equipment, Personal Information Devices, etc. shall include a memorandum of transmittal to *Mr. Mohamad Talas* identifying the specific deliverable enclosed and identifying what contract requirement is being addressed. Deliveries without such a memorandum of transmittal shall be considered informal in nature and shall not constitute completion with regard to project schedules [e.g. milestones], payments, or work items.

1.4.2.8 Each page of all multi-page documents transmitted to the CITY shall include the page number without skipping, total number of pages, and document number.

1.4.2.9 All contract documents shall be provided electronically in Adobe PDF and Microsoft Word 2010 format or as agreed by the City.

1.4.2.10 All contract documents may be shared with USDOT for their review. Documents shared with USDOT will not be made public except as required by a court or other legal action.

1.5 Testing and Product Qualification

1.5.1 General Testing Requirements

1.5.1.1 This specification includes extensive requirements for design submittals, prototypes, prototype testing, design reviews, design approval testing, and evaluations.

1.5.1.2 The CONTRACTOR shall include a Factory Acceptance Testing, Site Acceptance Testing, and 60 day site burn-in.

1.5.1.3 The CONTRACTOR shall be required to supply all product submittals as described herein

1.5.1.4 The CONTRACTOR shall include all costs associated with the design, submittals, and testing including but not limited to Prototype Testing, Design Approval Testing, Factory Acceptance Testing, Site Acceptance Testing, and 60 day burn-in testing in the cost of the items supplied under this contract. (Note: No separate payment will be made for any submittals or testing as required herein.)

1.5.1.5 For all testing, the CONTRACTOR shall develop a test plan and test procedures in accordance with IEEE 829 and be responsible for implementing the complete test environment that shall be used to verify that the equipment including all SOFTWARE to fully meet the requirements as specified herein.

1.5.1.6 The CONTRACTOR shall conduct a detailed design review with the City concurrent with their submittals for the design and operation of all hardware and software. This walk through of the design shall occur at the City offices (TBD) and shall be scheduled at least 14 days in advance. It is suggested that this design review occur early in the procurement process to avoid any necessary re-work.

1.5.2 Design Approval Testing

1.5.2.1 The contractor shall be responsible for conducting a design approval test at a location within New York City to be designated by the City prior to delivery of the prototypes.

1.5.2.2 The design approval test shall demonstrate that the ***PID*** meets all of the requirements including operational, performance, User interface, and environmental requirements as stated herein.

1.5.2.3 The contractor shall submit the proposed design acceptance test at least 30 days prior to the planned execution of the tests.

1.5.2.4 The City and its representatives will review the proposed test plan and procedures and indicate necessary changes which shall be adopted by the CONTRACTOR.

1.5.2.5 The CONTRACTOR shall schedule the design approval tests such that they can be witnessed by the City and its representatives. The contractor may be required to shift the schedule up to 7 days to accommodate conflicting personnel schedules.

1.5.2.6 The design approval tests shall be conducted on not less than 2 PID units concurrently; the failure of any unit may be cause for the suspension of further testing until the problem is repaired. In such cases, the City may require a restart of the total testing or continue the test program depending on the nature of the failure.

1.5.2.7 The CONTRACTOR shall be responsible for all aspects of the test environment at no additional cost to the City. This shall include but be limited to environmental testing equipment, simulation and measurements for processor loading and communications, and shall include both positive and negative testing representing errors which should be handled properly.

1.5.2.8 The CONTRACTOR shall be responsible for all monitoring and data collection during the testing and shall develop a detailed test report at the conclusion of the testing which shall be provided to the City for final approval within 5 days of the completion of the testing.

1.5.3 Factory Acceptance Testing

1.5.3.1 Factory acceptance testing shall verify that all inputs, outputs, sensors, and radios are operating within the required specifications.

1.5.3.2 All units shall be operated for a period of 1 week during which they shall be fully operational, continuously monitored for proper operation and subjected to temperature and voltage variations for the full range of operation.

1.5.3.3 The CONTRACTOR shall develop a factory acceptance test plan for review and approval by the City.

1.5.4 Site Acceptance Test

1.5.4.1 As each ***PID*** is d***eployed,*** it shall be activated such that it can gain access to the keys for proper authentication of the SPaT, MAP, and RTCM (if used) messages if required, and operated for a period of several minutes to verify that all sensors, interfaces, and software is fully operational.

1.5.4.2 The contractor shall work with the City to identify an appropriate test site(s) for verifying that the ***PID*** has been properly ***programme***d and is operating as specified herein

1.5.4.3 Following the initial installation test, the operation of the unit will be monitored continuously and when it completed 30 days of fault free

operation, the unit shall be declared to have passed the site acceptance test.

1.5.4.4 Any defect which is evident within this 30 day period shall either be corrected (software download), or replaced with a new unit and the defective unit will be returned to the contractor for analysis and repair.

1.5.4.5 Note that the City will attempt to retrieve the failing ***PID*** as quickly as possible, but due to limited access to the participants for privacy protection purposes, this may be delayed. Such delays shall not affect the contractor's obligation to repair this defective unit.

1.5.5 Final Acceptance

1.5.5.1 Once all of the ***PIDs*** have been d***eployed*** and passed the 30 day site test, the 36 month warranty on the individual units shall commence.

1.5.5.2 The City will keep track of the date of ***deployment***, site acceptance, and start of warranty.

1.5.5.3 During the warranty, the CONTRACTOR shall be responsible for all repairs as stated herein. Software "corrections" and updates shall be coordinated with NYCDOT such that the City determines which updates to install ***and*** when to install.

1.5.5.4 Final acceptance of the equipment and software shall occur at the end of the 36 month warranty for each unit.

1.5.6 Other Compatibility Requirements

1.5.6.1 All source code modified for and developed for use with the PID as supplied to NYCDOT shall be provided to the CITY electronically upon acceptance of the software. Further, should subsequent use discover "bugs" or require additional features and functions, the PID source code shall be updated by the CONTRACTOR to reflect the as-built versions once all changes have been completed and verified.

1.5.6.2 The vendor is required to identify prior existing intellectual property with his/her proposal since software development that is funded by this project (and included in the vendor's proposal) will be placed in the open source repository – OSADP funded by USDOT.

1.5.6.3 The vendor is also directed review the software available in the OSADP and to consider it for use in the delivery of the PID for New York City.

2 General Technical Requirements

2.1 Overview

2.1.1.1 This specification defines the minimum general technical requirements applicable to discrete electronic components, and the mechanical, electrical design, environmental conditions and construction of all assemblies and subassemblies

2.1.1.2 These requirements also describe the means and testing profiles by which the equipment as a whole and in parts shall be tested to determine compliance with these specifications.

2.1.1.3 This specification identifies the ambient conditions within which the equipment must operate satisfactorily and reliably.

2.1.1.4 Other standards invoked. Unless noted otherwise, the PID shall meet the requirements set forth in the following standards:

a. Institute of Electrical and Electronics Engineers (IEEE) 802.11p (for receive and future transmission)
b. IEEE 1609.x family where appropriate
c. Society of Automotive Engineers (SAE) J2735 – for the message sets where appropriate
d. SAE J2945 family of standards where appropriate

2.1.1.5 The equipment, materials, and installation shall conform to the applicable requirements of the Underwriters Laboratories Incorporated (UL), the Electronic Industries Association (EIA), the National Electrical Code (NEC), National Electrical Safety Council (NESC), the American Society of Testing and Materials (ASTM), the Insulated Power Cable Engineers Associates (IPCEA), Illumination Engineers Society (IES), the Institute of Transportation Engineers (ITE), the American National Standards Institute (ANSI), the Rural Electrification Administration (REA), and the National Electronic Manufacturers Association (NEMA).

2.2 Clarifications and precedence

2.2.1.1 Where there are conflicts between this specification and any other documents or standards listed above, the vendor shall bring such conflicts to the attention of the CITY for resolution at least 10 business days prior to the proposal delivery.

2.2.1.2 After award of the contract, the judgment of the CITY shall be considered final in all cases without further compensation to the CONTRACTOR.

2.2.1.3 The specific requirements of this specification shall take precedence over existing federal, state, and local standards or specifications unless otherwise noted.

2.2.1.4 Any conflicts within this specification must be brought to the attention of the CITY for resolution prior to construction.

2.3 Cooperative Development

2.3.1.1 Not all aspects of the PID requirements have been fully documented at this time; the contractor shall work cooperatively with the City and its engineers during the design and development of the PID to optimize its utility for the NY CVPD.

2.3.1.2 Such cooperation will include sharing documents with the USDOT, conducting design reviews with the project team, and review and comments on the submittals.

2.3.1.3 The contractor shall work closely with the City and its consultants to establish the operating parameters that can be modified for each of the applications.

2.3.1.4 The contractor shall work closely with the City and its consultants to establish the OTA software and parameter update procedures and protocols.

2.3.1.5 The contractor shall work closely with the City and its consultants to establish the operation and operating parameters that can be modified for the data collection and logging applications.

2.3.1.6 The contractor shall include provisions for this level of cooperation in their bid.

2.4 Definitions

2.4.1.1 Wherever used in these specifications the following interpretation shall apply:

- State - State of New York Department of Transportation (also NYS and NYSDOT)
- CITY – New York City DOT (also NYC and NYCDOT)/New York City Department of Citywide Administrative Services (also NYC and NYCDCAS).
- ENGINEER – The CITY'S representative who shall be responsible for reviewing all documents; the ENGINEER shall be responsible for interpreting this specification. The CITY may hire a consultant to act as the ENGINEER for this project.
- CONTRACTOR – the CONTRACTOR is used interchangeably in this document to refer to the single business entity that executes a contract with the CITY for the supply of the equipment and services described in this document.

2.5 Glossary of Terms

The following table defines selected project-specific terms used throughout PID Procurement Specifications document.

Table 2. Glossary of Terms

Term	Definition
Access Control	Refers to mechanisms and policies that restrict access to computer resources. An access control list (ACL), for example, specifies what operations different users can perform on specific files and directories.
Administrator	These are the operators that set control parameters, implement system policies, monitor system configuration, and make changes to the system as needed.
Aggregation	The process of combining data elements of similar format into a single data element that is a statistical representation of the original elements.
Analysis	The process of studying a system by partitioning the system into parts (functions, components, or objects) and determining how the parts relate to each other.
Anonymity	Lacking individuality, distinction, and “recognizability” within message exchanges.
Anonymous Certificate	A certificate which contains a pseudonym of the System User instead of his real identity in the subject of the certificate and thus prevents other System Users from identifying the certificate owner when the certificate is used to sign or encrypt a message in the USDOT Connected Vehicle Program. The real identity of the anonymous certificates can be traced by Authorized System Operators by using the services of Registration Authority and Certification Authority.
APID	Application Protocol Data Unit. This is a defined data structure that is transferred at a peer level between two applications.
Application	One or more pieces of software designed to perform some specific function; it is a configuration of interacting Engineering Objects. A computer software program with an interface, enabling people to use a computer as a tool to accomplish a specific task.
Application User	A user who interfaces with Application Layer software for a desired function or feature.
Assumption	A judgment about unknown factors and the future which is made in analyzing alternative courses of action.
Authenticate	The process of ensuring that an APID originated from a source identified within the message
Authentication	The process of determining the identity of a user that is attempting to access a network.
Authenticate-ability	The ability of the receiver of information to authenticate the sender’s identity or trustworthiness to send data within the domain. If required, this can be accomplished by verifying the incoming message has been digitally ‘signed’ by the sender.
Authenticity	The quality of being genuine or authentic; which is to have the origin supported by unquestionable evidence; authenticated; verified. This includes whether the software or hardware came from an authorized source.
Authorization	The process of determining what types of activities or access are permitted on a network. Usually used in the context of authentication: once you have authenticated a user, they may be authorized to have access to a specific service.
Available	Ready or able to be used
Backup	The ability of one System Element replacing another System Element’s functionality upon the failure of that System Element.
Bad Actor	A role played by a user or another system that provides false or misleading data, operates in such a fashion as to impede other users, operates outside of its authorized scope.
Boundaries	The area of management and control for a System or Object. It could be by latitude/longitude or by county or by regional jurisdictions.

Broadcast	A flow where the initiator sends information on a predefined communications channel using a protocol that enables others who know how to listen to that channel to receive the information. One-to-many communication, with no dialog.
Cardinality	The characterization of the relationship between the number of sender(s) and receiver(s) of a data exchange. (e.g. broadcast (one-to-many) unicast (one to one))
Center	An entity that provides application, management, administrative, and support functions from a fixed location not in proximity to the road network. The terms “back office” and “center” are used interchangeably. Center is a traditionally a transportation-focused term, evoking management centers to support transportation needs, while back office generally refers to commercial applications. From the perspective of this ConOps Specification these are considered the same.
Concept of Operations (ConOps)	A user-oriented document that describes a system’s operational characteristics from the end user’s viewpoint.
Confidentiality	The property of being unable to read Protocol Data Unit (PDU) contents by any listener that is not the intended receiver
Configurable Parameter	Non-static data that can be adjustable and updated when needed.
Configuration	Data that is used to customize the operational environment for a System Element or System User, or the System as a whole
Configure	The process of selecting from a set of option(s) or alternative values in order to create a specific operational environment.
Constraint	An externally imposed limitation on system requirements, design, or implementation or on the process used to develop or modify a system. A constraint is a factor that lies outside – but has a direct impact on – a system design effort. Constraints may relate to laws and regulations or technological, socio-political, financial, or operational factors.
Contract	In project management, a legally binding document agreed upon by the customer and the hardware or software developer or supplier; includes the technical, organizational, cost, and/or scheduling requirements of a project.
Control	To exercise influence over.
Coverage Area	A geographic jurisdiction within which the System provides services.
Cyber Address	The cyber or network address of a Unified Implementation of the Reference Architecture object.
Data Consumer	1) A user or system that is receiving or using data from another user or system. 2) Any Unified Implementation of the Reference Architecture object that registers with and subsequently requests and receives delivery of data from a data warehouse.
Data Provider	1) Any Unified Implementation of the Reference Architecture object that registers with and subsequently deposits data into a data warehouse 2) A System User that is supplying or transmitting data to another user or system. A data provider is likely to be an aggregator of data.
Data Warehouse	A data storage facility that supports the input (deposit) and retrieval (delivery) of clearly defined data objects. This can be design and implemented in a variety of ways, including publish/subscribe and a traditional query based database.
Decrypt	To decode or decipher data that has previously been encoded in such a way to secure its contents from unauthorized access. See Encryption.
Deployment Benefits	This term refers to the measures of effectiveness used by the NYCDOT and the Independent Evaluator on a periodic basis to assess the benefits realized from the utilization of connected vehicle technology and applications within the project’s deployment areas.

Digital Certificate or Signature	A digital certificate is an electronic "identification card" that establishes your credentials when doing business or other transactions on the Web. It is issued by a certification authority. It contains your name, a serial number, expiration dates, a copy of the certificate holder's public key (used for encrypting messages and digital signatures), and the digital signature of the certificate-issuing authority so that a recipient can verify that the certificate is real. Note: From the SysAdmin, Audit, Network, Security Institute - www.sans.org website.
DNS (Domain Name System)	The internet protocol for mapping host names, domain names and aliases to IP addresses.
Encryption	Scrambling data in such a way that it can only be unscrambled through the application of the correct cryptographic key.
End-User	The ultimate user of a product or service, especially of a computer system, application, or network.
Environment	The circumstances, objects, and conditions that surround a system to be built; includes technical, political, commercial, cultural, organizational, and physical influences as well as standards and policies that govern what a system must do or how it will do it.
Extensibility	The ability to add or modify functionality or features with little or no design changes.
Field	These are intelligent infrastructure distributed near or along the transportation network which perform surveillance (e.g. traffic detectors, cameras), traffic control (e.g. signal controllers), information provision (e.g. Dynamic Message Signs (DMS)) and local transaction (e.g., tolling, parking) functions. Typically, their operation is governed by transportation management functions running in back offices. Field also includes RSU and other non-DSRC wireless communications infrastructure that provides communications between Mobile elements and fixed infrastructure.
Forwarding	The process of forward sending data onto another entity (system user) without modifying or storing the data for any substantial length of time.
Functionality	The capabilities of the various computational, user interfaces, input, output, data management, and other features provided by a product.
Geo-Fence	An electronic set of geo reference points that form a bounded geographic region.
Geo-Referencing	The process of scaling, rotating, translating and de-skewing the image to match a particular size and position. To define something in terms of its physical location in space.
Hardware	Hardware refers to the physical parts of a computer and related devices. Internal hardware devices include motherboards, hard drives, and memory. External hardware devices include monitors, keyboards, mice, printers, and scanners.
Now (N)	Transient Data that is hyper current (relevant at the time of reporting for applications that require sub-second response).
Adjacent (A)	Data that is hyper local (relevant to a geographic area within ~1 minute travel distance)
Recent (R)	Transient Data that is current (relevant at the time of reporting for applications that do not require sub-second response).
Local (L)	Data that is local (relevant to a geographic area within 10 minute travel distance)
Historic (H)	Transient Data that is historical (relevant at the time of reporting for an indefinite interval).
Regional (R)	Data that is regional in scope (relevant to a geographic area greater than 10 minute travel distance).
National (N)	Data that is national in scope.
Continental (C)	Data that is continental in scope.
Static (S)	Data that is permanent (relevant at the time of reporting for an indefinite interval).

Identity Certificate	A certificate that uses a digital signature to bind a public key with an identity - information such as the name of a person or an organization, their address, and so forth. The certificate can be used to verify that a public key belongs to an individual.
Integrity	1) To maintain a system that is secure, complete and conforming to an acceptable conduct without being vulnerable and corruptible. 2) The property of being certain that a message's contents are the same at the receiver as at the sender.
Interconnect	The communications link between two architectural objects.
Internet	An interconnected system of networks that connects computers around the world via the TCP/IP protocol.
Issuance	For Anonymous Certificates: Blocks of certificates for a System User which are generated by the Certificate Authority (CA) with mappings between the System User's real identity and the pseudo-identity in the certificates are maintained by the Registration Authority (RA). For Identity Certificates: Blocks of certificates for a System User which are generated by the Certificate Authority (CA) with information such as the name of a person or an organization, their address, etc., maintained by the Registration Authority (RA). Both certificates are installed in the System User equipment by online (through a communication channel with encrypted communications) or offline (mechanisms such as USB download) mechanisms.
Jurisdictional Scope	The power, right, or authority to interpret and apply the law within the limits or territory which authority may be exercised.
Link	A Link is the locus of relations among Nodes. It provides interconnections between Nodes for communication and coordination. It may be implemented by a wired connection or with some radio frequency (RF) or optical communications media. Links implement the primary function of transporting data. Links connect to Nodes at a Port.
Logical Security	Safeguards that include user identification and password access, authentication, access rights and authority levels.
Misbehaving User	A user who exhibits misbehavior.
Misbehavior	The act of providing false or misleading data, operating in such a fashion as to impede other users, or to operate outside of their authorized scope. This includes suspicions behavior as in wrong message types or frequencies, invalid logins and unauthorized access, or incorrect signed or encrypted messages. etc.; either purposeful or unintended
Misbehavior Information	Includes Misbehavior Reports from System Users, as well as other improper System User acts, such as sending wrong message types, invalid logins, unauthorized access, incorrectly signed messages and other inappropriate System User behavior.
Misbehavior Report	Data from a System User identifying suspicious behavior from another System User that can be characterized as misbehavior.
Mobile	These are vehicle types (private/personal, trucks, transit, emergency, commercial, maintenance, and construction vehicles) as well as non-vehicle-based platforms including portable personal devices (smartphones, PDAs, tablets, etc.) used by travelers (vehicle operators, passengers, cyclists, pedestrians, etc.) to provide and receive transportation information
Non-repudiation	The property whereby a PID is constructed in such a way that the PID sender cannot effectively deny having been the sender of that PID; and the PID receiver cannot effectively deny having received a particular PID.
On-Board Equipment (OBE)	Computer modules, display and a DSRC radio, that is installed and embedded into vehicles which provide an interface to vehicular sensors, as well as a wireless communication interface to the roadside and back office environment.

Operational Data Environment	The ODE consist of several different USDOT developed smart data routers brokering processed data between various data sources, including the Unified Implementation of the Reference Architecture, and a variety of data users (e.g. RDE, TMCs). As a smart data router, the ODE routes data from disparate data sources to software applications (including CV applications) that have placed data subscription requests to the ODE. The ODE also performs necessary security / credential checks and, as needed, data valuation, aggregation, integration and propagation functions.
Operators	These are the day-to-day users of the System that monitor the health of the system components, adjust parameters to improve performance, and collect and report statistics of the overall system.
Permission	Authorization granted to do something. From the System's perspective, permissions are granted to System Users and Operators determining what actions they are allowed to take when interacting with the System.
Persistent Connection	A connection between two networked devices that remains open after the initial request is completed, to handle multiple requests thereafter. This reduces resource overhead of re-establishing connections for each message sent and received. This is opposite of Session-oriented Connection.
Physical Security	Safeguards to deny access to unauthorized personnel (including attackers or even accidental intruders) from physically accessing a building, facility, resource, or stored information. This can range from simply a locked door to badge entry. with armed security guards
Priority	A rank order of status, activities, or tasks. Priority is particularly important when resources are limited.
Privacy	The ability of an individual to seclude information about themselves, and thereby reveal information about themselves selectively.
Process	A series of actions, changes, or functions bringing about a result.
Protocol Data Unit (PDU)	A defined data structure that is transferred at a peer level between corresponding software entities functioning at the same layer in the OSI standard model which are operating on different computing platforms that are interconnected via communications media .
Public Key	In cryptography, a public key is a value provided by some designated authority as an encryption key that, combined with a private key derived from the public key, can be used to effectively encrypt messages and digitally sign them. The use of combined public and private keys is known as asymmetric cryptography. A system for using public keys is called a public key infrastructure (PKI).
Regional (R)	Data that is regional (relevant to a geographic area within ~30 minute travel distance)
Registry	A repository for maintaining data requester's information including the type of data they are subscribing to, their address, etc.
Reliability	Providing consistent and dependable system output or results.
Repackage Data	Data that is broken down for aggregation, parsing or sampling.
Requirement	(A) A condition or capability needed by a user to solve a problem or achieve an objective. (B) A condition or capability that must be met or possessed by a system component to satisfy a contract, standard, specification, or other formally imposed document. (C) A documented representation of a condition or capability as in definition (A) or (B). (IEEE Std 610.12-1990)
Research Data Exchange	A web-based data resource provided by the USDOT ITS-JPO's Real-Time Data Capture and Management (DCM) program which collects, manages, and provides archived and real-time multi-source and multi-modal data to support the development and testing of ITS applications.
Scalability	The capable of being easily grown, expanded or upgraded upon demand without requiring a redesign.

Scenario	A step-by-step description of a series of events that may occur concurrently or sequentially.
Secure Storage	Encrypted or protected data that requires a user or a process to authenticate itself before accessing to the data. Secure storage persists when the power is turned off.
Secure Transmission	To protect the transfer of confidential or sensitive data usually by encryption, Secure Sockets Layer (SSL), Hypertext Transfer Protocol Secure (HTTPS) or similar secure communications.
Secure/Securely	Referring to storage, which consists of both logical and physical safeguards
Session-oriented Connection	A connection between two networked devices that is established intermittently and to handle few requests thereafter. The connection is meant to be temporary lasting for minutes, hours, but likely not more than a day before it is closed. This is opposite of Persistent Connection.
Software	Software is a general term that describes computer programs. Terms such as software programs, applications, scripts, and instruction sets all fall under the category of computer software.
States	A distinct system setting in which the same user input will produce different results than it would in other settings. The System as a whole is always in one state. A state is typically commanded or placed in that state by an operator. States are Installation, Operational, Maintenance, Training, and Standby.
Status	Anomalies, actions, intermittent and other conditions used to inform the System Operator for reparation or maintenance.
Subsystem	An integrated set of components that accomplish a clearly distinguishable set of functions with similar or related uses.
Synchronization	the act or results of occurrence or operating at the same time or rate
System	(A) A collection of interacting elements organized to accomplish a specified function or set of functions within a specified environment. Typically the System Elements within the System are operationally self-contained but are interconnected and collaborate to meet the needs of the System and its Users. (B) A group of people, objects, and procedures constituted to achieve defined objectives of some operational role by performing specified functions. A complete system includes all of the associated equipment, facilities, material, computer programs, firmware, technical documentation, services, and personnel required for operations and support to the degree necessary for self-sufficient use in its intended environment.
System Element	(A) A collection of interacting components organized to accomplish a specified function or set of functions within a specified environment. (B) An object and procedures constituted to achieve defined objectives of some operational role by performing specified functions. A complete system element includes all of the associated equipment, facilities, material, computer programs, firmware, technical documentation, services, and personnel required for operations and support to the degree necessary for self-sufficient use in its intended environment. An integrated set of components that accomplish a clearly distinguishable set of functions with similar or related uses.
System Need	A capability that is identified and supported within the System to accomplish a specific goal or solve a problem
System Performance	This term refers to the measures of effectiveness used by NYCDOT traffic management operations staff on a periodic basis to manage the on-going operation of the system.
System Personnel	This represents the staff that operates and maintains the System. In addition to network managers and operations personnel, System Personnel includes the Administrators, Operators, Maintainers, Developers, Deployment teams, and Testers.
System Requirements Specification (SyRS)	A structured collection of information that embodies the requirements of the system.

System User	System Users refers to Mobile, Field, and Center Systems.
Testers	These users verify the System's operation when any changes are made to its operating hardware or software.
Time	A measurable period during which an action, process or condition occurs.
Time synchronization	Calibration adjustment of date, hour, minutes and seconds for keeping the same time within a system.
Time-of-Day	Current hours, minutes and seconds within a day.
Traceability	The identification and documentation of derivation paths (upward) and allocation or flow down paths (downward) of work products in the work product hierarchy. Important kinds of traceability include: to or from external sources to or from system requirements; to or from system requirements to or from lowest level requirements; to or from requirements to or from design; to or from design to or from implementation; to or from implementation to test; and to or from requirements to test.
Transition	A passage from one state, stage, subject, or place to another
Trust Credentials	A user's authentication information which determines permissions and/or allowed actions with a system and other users.
Unicast	The sending of a message to a single network destination identified by a unique address.
User	An individual who uses a computer, program, network, and related services of a hardware and/or software system, usually associated with granting that individual with an account and permissions.
User Need	A capability that is identified to accomplish a specific goal or solve a problem that is to be supported by the system.
Valid	When data values within a message are acceptable and logical (e.g., numbers fall within a range, numeric data are all digits).
Validate	To establish or confirm the correctness of the structure, format and/or contents of a data object.

2.6 Acronym List

The following defines selected project-specific acronyms used throughout this PID Procurement Specifications document.

Table 3. Acronym List

Acronym/Abbreviation	Definition
3G	Third Generation
3P	Third Party
4G	Fourth Generation
A	Adjacent
ACL	Access Control List
APID	Application Protocol Data Unit
API	Application Programming Interface

ASD	Aftermarket Safety Device
ASN.1	Abstract Syntax Notation.1
ASTC	Advanced Solid-state Traffic Controller (NYC standard traffic signal controller device)
ATC	Advance Traffic Controller (see ASTC)
ATIS	Advanced Traveler Information System
BAA	Basic Agency Agreement
BSM	Basic Safety Message
C	Continental
C2C	Center to Center
C2F	Center to Field
CA	Certificate Authority
CAMP	Crash Avoidance Metrics Partnership
CIA	Confidentiality/Integrity/Availability
ConOps	Concept of Operations
CRL	Certificate Revocation List
CV	Connected Vehicle
CVPD	Connected Vehicle Pilot Deployment
CVRIA	Connected Vehicle Reference Implementation Architecture
DCM	Device Configuration Manager
DD	Data Distribution
DNS	Domain Name System
DoS	Denial of Service
DSNY	New York City Department of Sanitation
DOT	Department of Transportation
DSRC	Dedicated Short Range Communications
EVSD	Enhance Vehicle Situation Data
Gbps	Gigabits per second
GHz	Gigahertz

GID	Geographic Intersection Description
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
H	Historic
HMI	Human Machine Interface
HSM	Hardware Security Module
HTTPS	Hypertext Transfer Protocol (Secured)
I2V	Infrastructure to Vehicle
IEEE	Institute of Electrical and Electronics Engineers
IP	Internet Protocol
ISD	Intersection Situation Data
ITS	Intelligent Transportation System
JPO	Joint Program office
KSI	Killed or Severally Injured
L	Local
MIB	Management Information Base
MAP	Map Data Message (a DSRC message)
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MTA	Metropolitan Transportation Authority
N	Now (context: temporal data distribution)
N	National (context: geographical data distribution)
NHTSA	National Highway Traffic Safety Administration
NOC	Network Operations Center
NTP	Network Time Protocol
NYC	New York City
NYCDOT	New York City Department of Transportation
NYCWiN	New York City Wireless Network
NYU	New York University

O&M	Operations & Maintenance
OBD	On-board Diagnostics
OBE	On-Board Equipment
OCMC	Office of Construction Mitigation and Coordination
ODE	Operational Data Environment
OEM	Office of Emergency Management
OER	Office of Emergency Response
ORDS	Object Registration & Recovery Service
OS	Operating System
OST-R	Office of the Assistant Secretary of Transportation for Research and Technology
OTA	Over-the-Air
PASS	Pedestrians for Accessible and Safe Streets
P2P	Peer-to-Peer
PDU	Protocol Data Unit
PID	Personal Information Device (e.g. SmartPhone)
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
POC	Proof of Concept
PSID	Provider Service Identifier
R	Recent (context: time domain)
R	Regional (context: geographic domain)
RA	Registration Authority
RDE	Research Data Exchange
RF	Radio Frequency
RSA	Roadside Alert
RSE	Roadside Equipment
RSU	Roadside Unit
RTCM	Radio Technical Commission for Maritime Services

S	Static
SAE	Society of Automotive Engineers International
SCM	Security & Credential Management
SCMS	Security Credential Management System/Service
SDC	Situation Data Clearinghouse
SDLC	System Development Life Cycle
SDW	Situation Data Warehouse
SET-IT	System Engineering Tool – Intelligent Transportation
SM	Service Monitor
SMS	Service Monitor System
SPaT	Signal Phase and Timing (a DSRC message)
SPMD	Safety Pilot Model Deployment
SSL	Secure Sockets Layer
SSP	Service Specific Permissions
SyRS	System Requirements Specification
TAI	International Atomic Time (French: Temps atomique international)
TBD	To Be Determined
TCP	Transmission Control Protocol
TIC	<Region> Transportation Information Center
TLC	New York City Taxi & Limousine Commission
TLS	Transport Layer Security
TMC	Traffic Management Center
TPAC	Third Party Application Center
TSD	Traveler Situation Data
UDP	User Datagram Protocol
UPS	United Parcel Service
USDOT	United States Department of Transportation
UTC	Coordinated Universal Time (French: Temps universal coordonné)

VAD	Vehicle Awareness Device
V2I (I2V)	Vehicle-to-Infrastructure (Infrastructure-to-Vehicle)
V2V	Vehicle-to-Vehicle
VPN	Virtual Private Network
VRU	Vulnerable Road User
WAID	Wide Area Information Distributor
WAVE	Wireless Access in Vehicular Environments
WAW	Wide Area Wireless
Wi-Fi	Wireless Fidelity (short to mid-range wireless network)
WiMAX	Worldwide Interoperability for Microwave Access
WSA	WAVE Service Advertisement
WSM	WAVE Short Messages
WSMP	WAVE Short Message Protocol
XML	eXtensible Markup Language

2.7 References

The following table lists the references used to develop this PID Procurement Specifications document. As some of the base standards referred to in the list are currently evolving, their identifiers have been temporarily highlighted to indicate that the version may change.

Table 4. References

#	Document (Title, source, version, date, location)
3	*Borough Pedestrian Safety Action Plans*, New York City Department of Transportation. http://www.nyc.gov/html/dot/html/pedestrians/ped-safety-action-plan.shtml
5	*Principles for a Connected Vehicle Environment*, U.S. Department of Transportation ITS Joint Program Office-HOIT, April 18, 2012 http://www.its.dot.gov/connected_vehicle/pdf/ConnectedVehiclePrinciples_final4-18-2012.pdf
6	*Connected Vehicle Reference Implementation Architecture Website*, US Department of Transportation, Office of the Assistant Secretary of Transportation for Research and Technology. http://www.iteris.com/cvria/
8	*Core System Architecture Document*, US Department of Transportation, Research and Innovative Technology Administration, October14, 2011 http://www.its.dot.gov/docs/CoreSystemArchitectureDoc_revC.pdf

9 *Core System Requirements Specification*, US Department of Transportation, Research and Innovative Technology Administration, October14, 2011
http://www.its.dot.gov/docs/CoreSystem_SE_SyRS_RevF.pdf

10 *Core System Deployment Critical Risk Assessment Report*, US Department of Transportation, Research and Innovative Technology Administration, October28, 2011
http://www.its.dot.gov/docs/CoreSystem_RiskReport_RevB.pdf

11 *Core System Standards Recommendations*, US Department of Transportation, Research and Innovative Technology Administration, October28, 2011
http://www.its.dot.gov/docs/CoreSystem_StdsRecommendations_RevA.pdf

12 *Connected Vehicle Technology - Test Bed Website*, US Department of Transportation, Office of the Assistant Secretary of Transportation for Research and Technology.
http://www.its.dot.gov/testbed.htm

13 Safety Pilot Model Deployment – "5.9GHz DSRC Aftermarket Safety" Device Specification, US Department of Transportation, Research and Innovative Technology Administration, Version 3.1, March 22, 2014

14 Safety Pilot Model Deployment – *"5.9GHz DSRC Vehicle Awareness Device" Specification*, US Department of Transportation, Research and Innovative Technology Administration, Version 3.5, December 12, 2011
http://www.its.dot.gov/safety_pilot/pdf/Vehicle_Awareness_Device_Specification-r3-5--20111202.pdf

15 *IEEE 1233 1998 – IEEE Guide for Developing System Requirements Specifications E-ISBN: 978-0-7381-1723-2*

16 *1609.0-2013 - IEEE Guide for Wireless Access in Vehicular Environments (WAVE) – Architecture*
http://standards.ieee.org/findstds/standard/1609.0-2013.html

17 *1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages*
http://standards.ieee.org/findstds/standard/1609.2-2013.html

18 *1609.3-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services, 2016*
http://standards.ieee.org/findstds/standard/1609.3-2016.html

19 *1609.4-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE)--Multi-channel Operation, 2016*
http://standards.ieee.org/findstds/standard/1609.4-2016.html

20 *SAE J2735 - Dedicated Short Range Communications (DSRC) Message Set Dictionary*™, SAE International, January 19, 2016
http://standards.sae.org/j2735_201601/

21 *SAE J3067 - Candidate Improvements to Dedicated Short Range Communications (DSRC) Message Set Dictionary [SAE J2735] Using Systems Engineering Methods*, August 26, 2014
http://standards.sae.org/j3067_201408/

21 *SAE J2945/1_201603 - Dedicated Short Range Communication (DSRC) Minimum Performance Requirements*™, March, 2016
http://www.sae.org/technical/standards/J2945/1_201603

22 *USDOT Security Credential Management System*, US Department of Transportation, Research and Innovative Technology Administration, April 13, 2012.
http://www.its.dot.gov/meetings/pdf/Security_Design20120413.pdf

24 *ITU-R TF.460-4: Standard-frequency and time-signal emissions*, International Telecommunication Union. 1986. Annex I
http://www.cl.cam.ac.uk/~mgk25/volatile/ITU-R-TF.460-4.pdf

25 *USDOT Broad Agency Announcement with New York City*, New York City Department of Transportation, September, 2015

26 *DSRC Roadside Unit (RSU) Specifications Document*, USDOT, Version 4.0, April 15, 2014 http://www.its.dot.gov/testbed/PDF/USDOT_RSUSpecification4%200_Final.pdf

28 U.S. DOT Issues Advance Notice of Proposed Rulemaking to Begin Implementation of Vehicle-to-Vehicle Communication Technology (NHTSA 34-14; dated Aug. 18, 2014)

29 *Accelerated Vehicle-to-Infrastructure (V2I) Safety Applications Concept of Operations Document*, Final Report —May 29, 2012 FHWA-JPO-13-058, www.its.dot.gov/index.htm

30 *Collision avoidance timing analysis of DSRC-based vehicles*, Accident Analysis and Prevention,2009, *www.elsevier.com*

31 *Security Credential Management System Proof–of–Concept Implementation, EE Requirements and Specifications Supporting SCMS Software Release 1.0,* CAMP

32 *Connected Vehicle Pilot Deployment Program Phase 1,Concept of Operations (ConOps) - New York* City, USDOT, FHWA-JPO-16-299, Final, 2016,

33 *Manual on Uniform Traffic Control Devices for Streets and Highways*, USDOT, 2009. http://mutcd.fhwa.dot.gov/pdfs/2009/pdf_index.htm

34 *Human Factors Design Guidelines for Advanced Traveler Information Systems (ATIS) and Commercial Vehicle Operations (CVO*), USDOT, FHWA-RD-98-057. http://www.fhwa.dot.gov/publications/research/safety/98057/toc.cfmk

39 *ISO TS 19091 Intelligent transport systems — Cooperative ITS — Using V2I and I2V communications for applications related to signalized intersections, In Ballot*

40 *Vehicle Safety Communications 0 Applications (VSC-A), USDOT National Highway Safety Administration, DOT HS 811 492 Volumes A-D, September, 2011*

41 *VPN over TLS references*

42 *Accelerated Vehicle-to-Infrastructure (V2I) Safety Applications -System Requirements Document, Final Report – July 18, 2012 FHWA-JPO-13-059*, www.its.dot.gov/index.htm

45 *Network Time Protocol* Internet Engineering Task Force RFC 5905-5908

2.8 General Requirements

2.8.1 Equipment and Accessories

2.8.1.1 The CONTRACTOR shall be responsible for all incidental accessories necessary to make the PID and all of its elements complete and ready for operation, even if not particularly specified. This shall include but not be limited to all chargers, cables for connection to ethernet ports, video ports, audio ports, cables for connection to chargers, and auxiliary power sources to ensure a minimum of 48 hours operation.

2.8.1.2 Such incidentals shall be furnished, delivered, and installed by the CONTRACTOR without additional compensation or expense to the CITY.

2.8.1.3 Minor details not usually shown or specified, but necessary for the proper installation and operation of the PID shall be included in the work in the CONTRACTOR's bid price, the same as if herein specified. (Note: By the submittal of a proposal, it is understood and agreed by the CONTRACTOR that the system description provided herein is complete

and includes all equipment necessary for the proper functioning of the PID and all equipment, even though every item may not be specifically mentioned.)

2.8.1.4 The CONTRACTOR shall not use the following parts in the design of any PID assembly/subassemblies provided under this contract:

- Obsolete components,
- Components no longer supported by the manufacturer
- Components not recommended for new designs
- Components which have been discontinued or which the CONTRACTOR should have reasonably been expected to know were discontinued,
- Components which the vendor has announced plans to discontinue at the time of the bid shall not be used in the design of any assembly/subassemblies provided under this contract.

2.8.1.5 The ongoing use of all equipment, systems, applications, and software supplied under this contract shall not require any ongoing license fees, usage fees, or other charges associated with the continued use of the ***PID*** for the applications indicated herein. The only exception to this is the ongoing monthly fee for the 4G/LTE carrier service for the communications between the PID and the NYU server. All charges for all other connections (vendors servers to internet etc.) shall be stated and included for the 3 year operation.

2.8.2 Furnished Material

2.8.2.1 All adhesives used shall have a minimum of 20 years of expected life under adverse field conditions. The CONTRACTOR shall not use 'stick-on' retention devices for any purpose unless specifically authorized by the CITY. The CONTRACTOR shall be required to show proof of the life expectancy of the adhesives proposed backed by the manufacturer of the material.

2.8.3 Serial Number

2.8.3.1 All PIDs shall have a unique serial number, which is permanently readable internally and on the unit (i.e. stored on non-volatile storage on the device in such a way that it cannot be changed once the device is in operational mode) so that it can be retrieved and added to selected data when required by the application.

2.8.3.2 The serial numbers shall include an obviously readable date of manufacture, the vendor's ID, and the subassembly or assembly ID.

2.8.3.3 The CONTRACTOR shall work with the CITY to determine an acceptable numbering scheme and starting numbers for serial numbers. (Note: the CITY tracks the serial numbers by procurement contract;

hence, the scheme used for serial numbers needs to identify the specific contract as well as the unique unit.)

2.8.3.4 The serial number of the unit shall be included in the embedded security module which can be accessed with the proper key by the PID message request to verify the specific device for the purposes of maintenance support. This serial number shall be permanent in the PID using the proper security certificates and the Service Specific Permissions (SSP) based on IEEE 1609.2. *<Note that there is no plan to use the 1609.2 certificates for the current pilot project; it is required that this capability be included in the unit for future use only and further investigation of such messages as the PSM, SRM)>*

2.8.4 Warranty

2.8.4.1 The purchasing of the PIDs shall be for "turnkey" units – with all software, hardware, certifications, and 36-month warranty – delivered to NYCDOT ready for deployment.

2.8.4.2 The warranty shall include all hardware and software supplied under this contract including installation kits.

2.8.4.3 The CONTRACTOR shall maintain a presence within the NY City jurisdiction for the repair, stocking, and ***testing/certification of the PID*** units.

2.8.4.4 According to the warranty terms, the CONTRACTOR shall test, repair, or replace the unit at their discretion within 2 business days after the City delivers the "defective" or suspect ***PID*** units to a depot point within the NY City geographic boundary.

2.8.4.5 The CONTRACTOR shall review any software "bugs" discovered during the warranty period, develop a solution, and coordinate with the City for testing and then the downloading of the software update to all units.

2.8.4.6 The CONTRACTOR shall address all software defects with a recommended correction within 30 days or less from the discovery date.

2.8.4.7 The 36-month warranty shall start at the successful completion of the site acceptance test and the 30-day initial period of operation. Failures during the 30-day period shall cause the 30 day observation period to be restarted from the beginning or continue at the discretion of the City.

2.8.4.8 Software defects noted within the 60-day "end" of the warranty period shall extend the final acceptance and warranty until the software "correction" has been installed and demonstrated reliable and proper operation for 60 days.

3 System Overview and Hardware Requirements

3.1 Functional Description

3.1.1.1 Under this Specification, the Contractor shall furnish a PID with the application for assisting the visually-challenged pedestrian in crossing the street.

3.1.1.2 The PID shall include a GNSS receiver and other accessories and sensors as necessary to determine the location of the unit sufficient for the application.

3.1.1.3 The PID shall be able to receive SPaT and MAP data from the traffic controller and other sources using a media which meet the timing, security, and accuracy requirements.

3.1.1.4 The vendor shall establish a platform for transmitting the SPaT and MAP information to the PID to support the urban navigation and crosswalk navigation support applications.

3.1.1.5 The PID shall also include a user interface and alternative internet access via commercial service. The commercial service connection shall be used for collecting the usage and performance data.

3.1.1.6 The vendor shall work with the City to determine the commercial service to be used for this project.

3.2 System Design

3.2.1.1 The Pedestrian in Signalized Crosswalk (PEDINXWALK) application stated in Section 5.1 of this document will not utilize the PID. However, new pedestrian detection equipment will be installed at 10 sample intersections in the NYC CVPD pilot area will be installed by NYCDOT. It will be capable of detecting pedestrians in the crosswalk and feed the detection data to the NYCDOT TMC for performance evaluation and post-processing. The detection area will extend to both the intersection and the road segment upstream of the crosswalk.

3.2.1.2 The PID shall have internal permanent storage capability. The Personal Information Device shall incorporate self-diagnostics that shall alert the pedestrian in case of a device failure.

3.2.1.3 The positioning requirements are currently being defined by USDOT and shall be addressed in subsequent releases of this specification. It is up to the vendor to demonstrate that their product can locate the PID with sufficient accuracy that the pedestrian assistance application provides the intended function.

3.2.1.4 The Actuated signal controller and/or the RSU will provide the SPaT and MAP “information” and the vendor shall work with the traffic controller

vendor, the RSU vendor, and the back-office systems (TransCore) to obtain and relay the information to the PID sufficient for the intended application. The status shall include pedestrian timing and traffic controller status such as preemption, priority treatment, and failure modes/status.

3.2.1.5 The intersection (RSU) also provides the geometric information (MAP message) which describes the geometric attributes of the intersection including the location of the curbs, distances to each corner, the name of each street, and the location of the cross walks.

3.2.1.6 This information shall be collected prior to the start of the NYC CVPD, used to build the MAP message, and broadcast within a radius near the RSU installation such that it can be read as the PID approaches the intersection. The MAP data will be housed in the TMC and will be made available to the PID and PID support applications as necessary.

3.2.1.7 This application shall be based on the SPaT being broadcasted at a rate of approximately 10 times per second, although the rate could be slower based on network loading and the number of equipped vehicles in the area. This message is broadcast and includes the data shown in the SAE J2735 standard for the SPaT message.

3.2.1.8 The intersection or TMC shall also transmit the MAP message, at a rate of approximately once or twice per second. The contents of the MAP message are shown in the SAE standard J2735.

3.2.1.9 **Future**[1]: The pedestrian shall be able to transmit a signal to the roadside infrastructure whenever the pedestrian is within the vehicle right-of-way at the street corner – i.e., the crosswalk. Such messages shall be on a different channel within the DSRC channel space.

3.2.1.10 **Future**[1]: Signal request message (SRM) and signal status message (SSM) are used for providing pedestrian services are for the future to allow the pedestrian to activate the cross walk signal timing and receive the signal status information through the PID.

3.3 System Layout

The Pedestrian Support Application Architecture for the NYC CVPD system is shown in Figure 1 below. This shows the functional breakdown for the support of the pedestrians applications. The PID assists the pedestrian by using a typical “Smartphone” type of device that includes navigation and receives the SPaT and MAP data for the intersection which has been outfitted with the CV technology. The PID includes a carrier based link to download the application, a carrier based link to upload the performance data collected; the SPaT and MAP data may be collected by various media including the

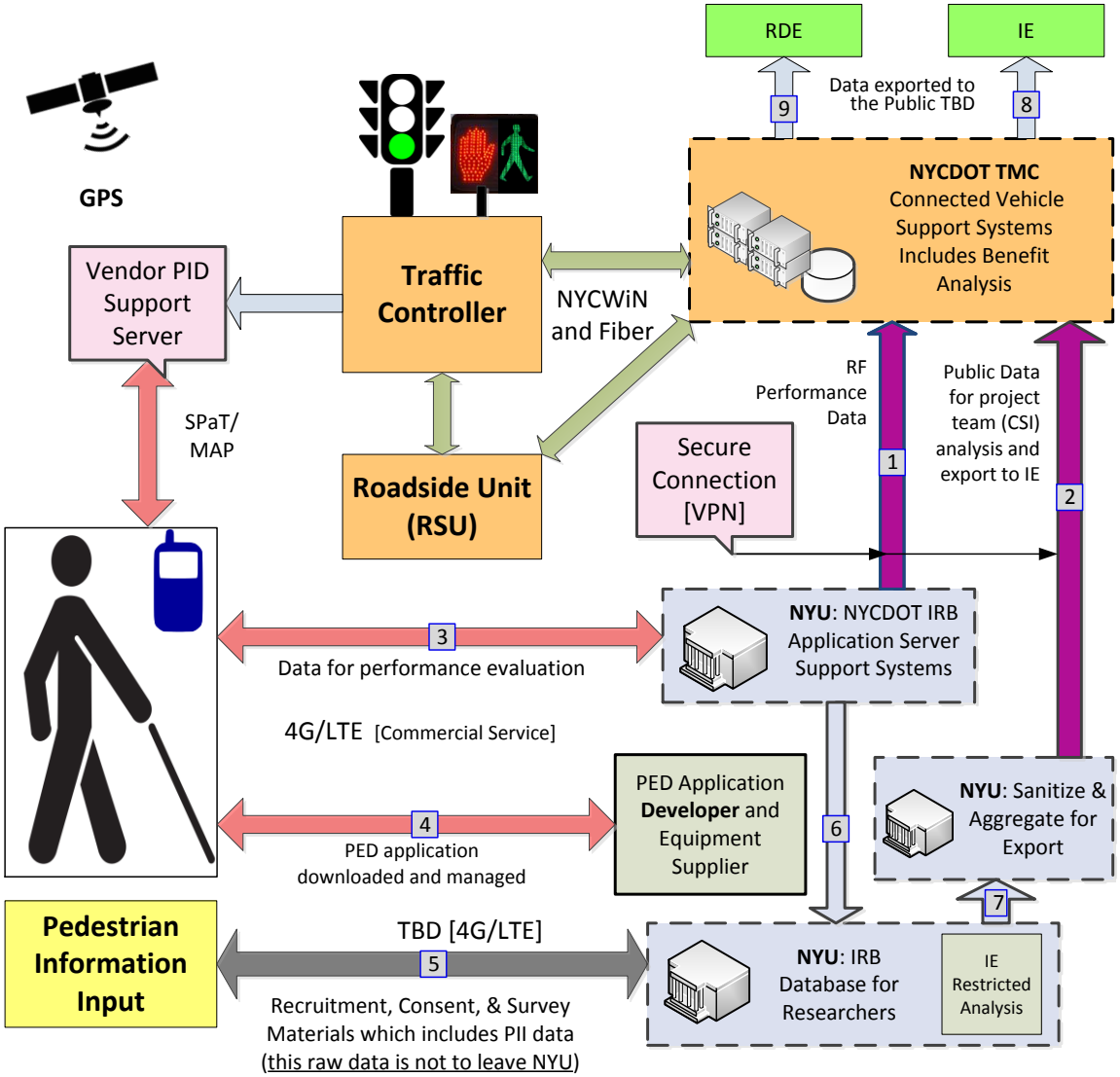
[1] These features are not required in the initial deployment; they are shown here such that the vendor can indicate whether they support this feature. The vendor’s design shall allow the use of this feature with the existing hardware and additional software.

4G/LET carrier. This data (SPaT and MAP messages) may originate at the traffic controller, the RSU, or the TMC and made available to the PID in a form and format to support the application.

Using a combination of haptic and audio feedback, the pedestrian should be able to use the PID to orient him/herself, and receive information on the signal status for the crosswalk they want to use.

The performance data will be held in a privacy protected database at NYU where it is managed by an IRB and protected from being divulged. The performance data can then be analyzed and the PII removed such that it can be exported for more detailed analysis and for operational monitoring.

Figure 1. Pedestrian Support Application Architecture



Visually Challenged Pedestrian Application Context Diagram

VisioDocument

This application should provide significant benefits to the visually challenged pedestrian by removing uncertainty of the signal status and orienting the pedestrian to the roadway network.

The diagram shows connections to a PID application server; the vendor shall identify this device and the data flow to the PID, however, the data sent to this server shall be transmitted securely over the internet and shall be limited to the data necessary for the application which shall not exceed the nominal data contained in the SPaT and MAP messages identified in SAE J2735-2016.

3.4 General Hardware Requirements

3.4.1 Hardware Procurement

3.4.1.1 The PID shall contain the following hardware:

- Optional - DSRC capabilities
- Built-in 3-axis accelerometer
- Built-in 3-axis gyroscope
- GPS
- Standard Ethernet Interface

3.4.1.2 The PID shall have one or more optional non-DSRC radios of the following types:

- 4G/LTE Cellular
- A display for use as a Human Machine Interface (HMI) (i.e. touch screen, color LCD)
- A speaker capable of playing recorded or synthesized human speech for use as a HMI.
- Vibration operation to provide feedback to the operator
- Headphone or earphone jack for audio to the user.

3.4.1.3 The PID's battery life shall be five (5) days between chargings.

3.4.1.4 The PID shall contain a removable lithium-ion battery that is capable of being charged via a separate capable and power adapter (120V). It is preferred that this be a standard USB type charger cable with mini USB or micro USB on one end and standards USB on the other for 5 Volt operation.

3.4.1.5 The PID shall be either wearable or mountable via clip.

3.4.2 Environmental Conditions and Protection

3.4.2.1 The PID shall operate at ambient temperature range of 32° to 95° F (0° to 35° C).

3.4.2.2 The PID shall stop operating at ambient temperatures below -4° and above 113° F (-20° and 45° C respectively).

3.4.2.3 The PID shall operate at a relative humidity from 5% to 95%, non-condensing.

3.4.2.4 The PID shall operate at altitudes up to 10,000 feet (3000 m).

3.5 Performance Requirements

3.5.1 Performance Characteristics

3.5.1.1 All PIDs shall utilize the same GPS time source and common accuracy configuration as the NYC CVPD Infrastructure.

3.5.1.2 The PID shall process all radio messages at maximum rates based on the message type as determined by the vendor.

3.5.2 Repair

3.5.2.1 As the NYCDOT IRB, NYU shall arrange the repair and replacement of PIDs damaged by improper maintenance, tampering, or mishap.

3.5.2.2 The PID shall be capable of being rebooted after a disruptive software glitch.

3.5.3 Adaptability

3.5.3.1 The application in the PID shall have modifiable algorithms and software parameters for tuning the system's operation.

3.5.3.2 The PID shall have upgradable hardware components for improving the device performance upon expansion of the NYC CVPD system.

4 PID Functional Requirements

4.1 Operations, Management and Control

4.1.1 Operational Modes

4.1.1.1 The PID shall communicate with other subsystems in its online state.

4.1.1.2 The PID shall stop communicating with other subsystems in its offline state.

4.1.2 Pedestrian Positioning and Crossing-Direction

4.1.2.1 The PID shall provide the pedestrian's current position information to the applications running on it. The accuracy shall be sufficient for the application.

4.1.2.2 The PID shall provide the pedestrian's intended crossing-direction to the application running on it based on the orientation of the PID.

4.1.3 Device Security

4.1.3.1 The PID shall have a Secure Non-DSRC Communications Account Password Reset

4.1.3.2 Any access over a non-DSRC communications interface shall require the use of a resettable password.

4.1.3.3 All default passwords shall be provided to and capable of being modified by NYCDOT.

4.1.3.4 Unique passwords shall be assigned to PIDs provided to each participant.

4.1.3.5 Secure passwords shall be chosen with passwords implementing an entropy of 80 bits (a random password of 13 characters in length chosen from all possible characters).

4.2 Device Communication

4.2.1 DSRC Radio Subsystem (optional)

4.2.1.1 The PID shall comply with Federal Communications Commission (FCC) 47 Code of Federal Regulations (CFR) Parts 0, 1, 2, and 95 amendments for Dedicated Short Range Communications (DSRC), mask/class type C.

4.2.1.2 The PID shall support a single DSRC radio configured to operate on a single channel or switching between channels in the 5.9 GHz (DSRC) band.

4.2.1.3 If a DSRC radio support is provided it shall meet all certification requirements and be compatible with the CV environment including the SCMS and shall be able to authenticate the DSRC messages and sign the DSRC messages as is appropriate.

4.2.1.4 It shall be the responsibility of the vendor to obtain certification for the PID such that it can receive 1609.2 certificates and participate in the CV trusted environment.

4.2.2 Secure Non-DSRC IP Communications

4.2.2.1 The onboard equipment device shall support at least one of the following secure access mechanisms for each non-DSRC communications interface configured for IP.

a. Transport Layer Security (TLS) V1.2
b. Internet Protocol Security (IPSec) for IPv4

c. Internet Protocol Security (IPSec) for IPv6
d. Secure Shell, v2 (SSH-2)
e. SSH File Transfer Protocol v6

4.2.2.2 The PID shall log an error system message for each failed access attempt to any non-DSRC communications interface configured for IP.

4.2.3 GNSS Receiver

4.2.3.1 The PID shall include a GNSS receiver that performs in accordance with GPS- Standard Positioning Service (SPS) Signal Specification*. (*See Section 6 System Interfaces of this specification.)

4.3 External WiFi or 4G/LTE carrier interactions

The PID shall include an interface to an application provider (App store) or directly to the developer which shall be used to initially load the application onto the PID and any subassemblies. Thereafter, the PID shall periodically and automatically initiate a secure communications session using either a Wifi connection or 4G/LTE connection to the NYU server for the following purposes:

4.3.1 Software Updates

4.3.1.1 This will be used when necessary to update the PID applications including the DSRC components and any security keys (or certificates) necessary to enable the PID to authenticate (or continue to authenticate) the DSRC messages received from the intersection RSU. This may include updating the user interface, map database, location algorithms, survey questions, or any other aspect of the PID operation.

4.3.1.2 Such updates shall only be permitted when authorized by NYCDOT and shall be able to target specific PID units such that software updates and changes can be tested and verified with “test” subjects.

4.3.1.3 Such software updates shall be provided to the NYU server via a secure connection where they will be held and downloaded to the PID when the PID “checks-in”. The mechanism for such updates shall be provided to NYCDOT and shall allow the project personnel to configure which PIDs will be downloaded and when. It shall be possible to download new firmware into selected PIDs or to groups of PIDs or to all PIDs.

4.3.2 Uploading Log Files

4.3.2.1 The PID application shall periodically (frequency and schedule to be determined and configured by NYCDOT) securely upload its event logs and data collected as described herein to the NYU server. Once the data has been verified as received by the NYU server, it shall be purged from the PID.

4.3.2.2 The mechanism to upload to the NYU server shall be developed by the vendor and shall be delivered to NYCDOT.

4.3.2.3 The vendor shall not provide any other means to access the PID except as listed above or by direct connection (wired) to the PID.

4.4 Data Collection

4.4.1 Data Collection Requirements

4.4.1.1 The PID shall create a record for its internal event log at 1 second intervals whenever it within a configurable[2] distance of an RSU transmitting SPaT messages. The recorded information shall include the following data:

4.4.1.1.1 The location of the PID in microdegrees

4.4.1.1.2 The PID heading at that 1 second

4.4.1.1.3 The UTC time accurate to 1 second

4.4.1.1.4 The SPaT message content from the 2 nearest RSU's; if only one is heard, then only a single entry. Note that a record is created every second – and since the SPaT message is transmitted at 10 Hz, it only needs to record the last SPaT message heard during the preceding second.

4.4.1.1.5 The MAP message content from the 2 nearest RSU's; if only one is heard, then only a single entry. Note that a record is created every second – and since the MAP message may be transmitted at more than 1 Hz, it only needs to record the last MAP message heard during the preceding second. (Note: the PID may note that a MAP message was received, but if the content is unchanged, it need not record the whole MAP message – simply the fact that one was received.)

4.4.1.1.6 BSM message from all vehicles within a configurable[2] distance of the PID (Note an alternative is to consider only those BSMs that represent a possible threat to the pedestrian.)

4.4.1.1.7 The RF level for all messages recorded as described above.

4.4.1.1.8 For each of the messages recorded – it shall note if the message was authenticated

4.4.1.1.9 For each message recorded above it shall note if the message was received with errors.

4.4.1.2 The PID shall record all operator interactions with the PID device including power changes, activation/deactivation of the application, and all interactions between the operator (pedestrian user) and the PID. This shall include the following:

[2] This shall be configurable using the over-the-air IP communications media.

4.4.1.2.1 Any messages played to the operator
4.4.1.2.2 Any screen entries by the operator
4.4.1.2.3 Actions of the operator such as steps taken
4.4.1.2.4 Any haptic output to the operator
4.4.1.2.5 Any sudden changes in the position of the operator

4.4.1.3 The PID shall be able to upload the event records to the NYU server using either wifi if available and supported or the carrier service.

4.4.1.4 Event records shall be automatically purged whenever the power is applied to the PID and the time of the last log entry is more than a configurable number of hours (example: 96 hours)

4.4.1.4.1 Any errors encountered by the orientation or instructive algorithms that prevent it from providing accurate information. This record shall include the time stamp and parameters regarding the error for analysis.

4.4.2 Additional Pedestrian (user) interactions

4.4.2.1 In addition to the dynamic data listed above, the project needs to track user feedback; the PID application shall include the ability to interact with the pedestrian to both solicit feedback and to accept pre-emptive feedback offered by the pedestrian. Examples are suggested below; it is up to the PID software developer to propose and seek approval of techniques for the solicitation and acceptance of such data.

4.4.2.2 As an example, the application could accept various possible inputs from the user such as audio, touch, and haptic feedback (shake). The user should be able to provide feedback in a way that can be captured immediately following a user's behavior and in a way that is comfortable to him or her. Thus, it may be more convenient for a user to say "I have crossed," or press a button, or shake the PID either to indicate the desired feedback or to initiate an interactive session whereby the PID may ask questions (audible) and seek feedback to select the appropriate feedback.

4.4.2.3 Examples of information needed includes whether the time allotted to cross was sufficient; were the directions adequate; was the status of the signal display (WALK/flashing DON'T WALK, steady DON'T WALK) clearly understood; was the orientation acceptable; was the street name clear. The developer shall work with NYCDOT to optimize the PID-User interface in cooperation with the application stakeholders.

4.5 System Security

The PID device shall meet all the defined security requirements in this section.

4.5.1 Security Management and Operations

The Security Management and Operations Concept (SMOC) describes how the NYC CVPD shall be employing the SCMS for the applications and the applicable physical security requirements. As of this writing, there are no established certification requirements and test procedures for the use of the SCMS and for the installation of the enrollment certificate in the PID devices.

4.5.1.1 **FUTURE** - The NYC CVPD system shall use the USDOT-specified interface to the SCMS to obtain enrollment certificates for each PID. -

4.5.1.2 **If DSRC is used**: PID vendor shall certify that their devices conform to the applicable standards for the DSRC communications (IEEE 1609.x, and IEEE 802.11p) and that their message sets conform to the SAE J2735 and J2945/x for the SPaT, MAP, and location correction (RTCM). Note that there are no expected DSRC transmissions from the PID during this initial deployment.

4.5.2 Pedestrian Security Requirements (future)

If the PID is enhanced in the future to support the transmission of PED calls to the traffic controller then the following shall apply:

4.5.2.1 The PED-SIG application on the PID shall acquire credentials from the SCMS that shall allow it to authenticate the SPaT, MAP, and SSM messages received.

4.5.2.2 The SCMS shall be able to set service specific permissions associated with the future support of pedestrian requests from the PID.

4.5.2.3 The PED-SIG application shall provide information to the pedestrian based on the content of the SPaT and MAP message at the nearest intersection

4.5.2.4 The application shall require strong passwords based on the Password Policy to devise a set of constraints before your users set their passwords with setting of passwords with expiration.

4.5.2.5 The application shall filter any input from un-trusted users before returning to the browser for rendering.

4.5.2.6 The application shall protect against attacks by inserting a token in every form and rendering the URL as protected by requesting confirmation with the API or use of the token with the URL that verifies that the token is present and valid on the response handling.

4.5.2.7 The application shall request if the security enrollment meets the criteria for processing the application request.

4.5.2.8 The application on the PID shall be able to sign messages transmitted to the RSU.

4.5.2.9 The application shall be capable of including a unique ID which shall remain stable (unchanged) throughout the PID's interaction with a single intersection.

4.5.2.10 The application shall create security requirements that shall the data can be securely transmitted or retrieved by the server at NYU.

4.5.3 SNMPv3 Agent

4.5.3.1 An SNMPv3 Agent shall support the TLS Transport Model over TCP per RFC 5953.

4.5.3.2 An SNMPv3 Agent shall support authenticating itself over TLS with an X.509 client certificate.

4.5.3.3 An SNMPv3 Agent shall support installation of an X.509 client certificate and private key at initial provisioning time.

4.5.3.4 An SNMPv3 Agent shall support installation of a whitelist of trustworthy CAs such that only CAs on the whitelist shall be trusted.

4.5.3.5 An SNMPv3 Agent shall only allow the list of trustworthy CAs to be updated as part of a device reset.

4.5.3.6 An SNMPv3 Agent shall only accept tmc.cvpd.dot.nyc.gov as the tmSecurityName.

4.5.4 TLS Client

4.5.4.1 A TLS Client shall support authenticating itself over TLS with an X.509 client certificate.

4.5.4.2 A TLS Client shall support client certificate authentication.

4.5.4.3 A TLS Client shall support session renegotiation and shall require the mechanisms specified in RFC 5746 to prevent session renegotiation attacks.

4.5.4.4 A TLS Client shall only carry out client certificate authentication within the context of renegotiating an established session.

4.5.4.5 A TLS Client shall support TLS session resumption. configurable timeout to include the following range: 1 hour to 1 week.

4.5.4.6 The TLS session resumption timeout value shall be configurable via SNMP and shall support at least the following range: 1 hour to 1 week.

4.5.4.7 A TLS Client shall support installation of an X.509 client certificate and private key at initial provisioning time.

4.5.4.8 A TLS Client shall support installation of a whitelist of trustworthy CAs such that only certificates signed by CAs on the whitelist shall be trusted.

4.5.4.9 A TLS Client shall support management of the list of trustworthy CAs via SNMP.

4.5.5 PID Configuration and Update

4.5.5.1 The PID shall support a secure OTA firmware update method using the carrier service (LTE/4G/WiFi).

4.5.5.2 The secure firmware update method supported by the PID shall use cryptographic mechanisms that provide at least 128 bits of security.

4.5.5.3 The PID firmware updates provided from the supplier to the TMC shall not be encrypted.

4.5.5.4 The PID shall connect to the TMC via mobile (e.g. 3G, 4G/LTE) IPv4 connection for downloading the new firmware images.

4.5.5.5 The PID vendor shall work with the City to optimize the mechanism for handling the OTA software updates.

4.5.5.6 The PID shall support tuning the application parameters via OTA.

4.5.6 Manufacturing State

4.5.6.1 A device shall provide functionality allowing an observer to easily determine whether it is in the operational or manufacturing state.

4.5.6.2 A device may support a manufacturing state in which it does not meet all the security requirements below. In this case it shall support the requirements identified in this requirements list by “Device security classes: manufacturing state”.

4.5.6.3 If the device allows a transition from operational to manufacturing state, it shall wipe all privileged applications (as defined in the SMOC Section 6.1.1) when that transition occurs.

4.5.6.4 If the device allows a transition from operational to manufacturing state, it shall wipe all keys from the HSM (as defined in the SMOC Section 6.1.1) when that transition occurs.

4.5.6.5 If the device allows a user to cause a transition from operational to manufacturing state without any logical authentication of the user, it shall require that the user is physically present.

4.5.6.6 The host processor on the device shall perform integrity checks on boot to ensure that it is in a known good software state.

4.5.6.7 The integrity checks performed at boot shall require the use of a hardware-protected value such that the integrity cannot be successfully compromised unless the hardware-protected value is modified.

4.5.6.8 Until all integrity checks on the software and firmware configuration of the host have passed, the device shall not allow a privileged application (as defined in the SMOC Section 6.1.1) to sign a message.

4.5.6.9 If any integrity check on the software and firmware configuration of the host fails, the device shall not allow any application to have access to stored private keys.

4.5.6.10 If any integrity check on the software and firmware configuration of the host fails, the device shall not allow any privileged application (as defined in the SMOC Section 6.1.1) to operate.

4.5.6.11 The OS on the device shall maintain an Access Control List (ACL) for which applications on the host may use each private key in the HSM

4.5.6.12 The OS on the device shall maintain an ACL for which applications can modify plaintext data stored in different locations on the device.

4.5.6.13 The OS on the device shall maintain an ACL for which applications can read plaintext data stored in different locations on the device.

4.5.6.14 The OS on the device shall maintain an ACL for which applications can enter cryptographic keys on the HSM.

4.5.6.15 The OS on the device shall maintain an ACL for which applications can modify cryptographic keys on the HSM.

4.5.6.16 The OS on the device shall allow privileged applications to operate without explicit user authentication

4.5.6.17 The OS on the device shall allow applications that update private key material within the HSM to operate without explicit user authentication

4.5.6.18 The OS on the device, if it allows processes that modify or inspect executing processes in operational mode, shall require that those processes have explicit user authentication.

4.5.6.19 The OS shall not permit keys designated as private to be read from the HSM.

4.5.6.20 When requested to install software, the host processor OS shall ensures that the software is signed by an authority with appropriate permissions and shall reject the installation if the signature or any of the validity checks on the software or its signing certificate fail.

4.5.6.21 The validation of signed software shall require use of a verification key that is protected by local hardware to a level equivalent to FIPS 140-2 at the level appropriate for the device

4.5.6.22 The device supplier shall ensure that device software has been developed according to best practices for robustness and security and shall provide documentation of how this requirement was taken into account during development.

4.5.6.23 The update mechanism shall prevent updates from being rolled back.

4.5.6.24 The HSM shall meet the requirements for an operating system given in FIPS 140-2 Level 2 except for the audit requirements and certain additional exceptions as noted below.

4.5.6.25 All cryptographic software and firmware for the HSM shall be developed and installed in a form that protects the software and firmware source and executable code from unauthorized disclosure and modification.

4.5.6.26 A cryptographic mechanism using a FIPS 140-2 Approved integrity technique (e.g., an Approved message authentication code or digital signature algorithm) shall be applied to all cryptographic software and firmware components within the HSM.

4.5.6.27 A message authentication code shall only be used to verify the integrity of the HSM software/firmware if one of the following occurs:

a. If the HSM itself calculates the MAC when the software is installed using a secret key known only to the HSM, and uses this secret key to verify the software on boot.
b. If the software/firmware provider has a unique shared key with each distinct device and uses this to authenticate the software.

4.5.6.28 All cryptographic software and firmware, cryptographic keys, and control and status information on the HSM shall be under the control of an operating system that meets the functional requirements specified in the Protection Profiles listed in FIPS 140-2 Annex B and is capable of evaluation at the CC evaluation assurance level EAL2, or an equivalent trusted operating system.

4.5.6.29 The HSM operating system shall implement role-based access control for the following activities:

a. Execute stored cryptographic software and firmware.
b. Modify (i.e., write, replace, and delete) the following cryptographic module software or firmware components stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g., cryptographic keys and audit data), and plaintext data.
c. R read the following cryptographic software components stored within the cryptographic boundary: cryptographic data (e.g., cryptographic keys and audit data), and plaintext data.

d. Enter cryptographic keys.

4.5.6.30 The HSM operating system may allow a role without explicit authorization to execute stored cryptographic software and firmware if the device follows the Integrated or Connected Architectures specified in 6.1.2. The discretionary access control mechanisms shall require explicit authorization to execute stored cryptographic software and firmware if the device follows the Networked Architecture specified in 6.1.2.

4.5.6.31 The HSM operating system shall allow an unauthenticated role to create a new cryptographic key by combining an existing key with new input.

4.5.6.32 The HSM operating system may allow automated software and firmware update if that update is carried out by a process that includes cryptographic checks to ensure the validity of the update prior to installation.

4.5.6.33 The HSM operating system shall prevent all operators and executing processes from modifying executing cryptographic processes (i.e., loaded and executing cryptographic program images). In this case, executing processes refer to all non-operating system processes (i.e., operator-initiated), cryptographic or not

4.5.6.34 The HSM operating system shall prevent operators and executing processes from reading cryptographic software stored within the cryptographic boundary

4.5.6.35 If the device has the HSM and the host processor communicate via a connection which can be accessed directly by other processors, the host processor shall authenticate itself to the HSM with an authentication mechanism based in hardware with the same physical security level as the HSM itself.

4.5.6.36 The device shall provide tamper evidence to detect tampering of the device (e.g. opening of the case).

4.5.6.37 All unused media ports (e.g. USB) on the PID shall be sealed.

4.5.6.38 There shall be no removable media on the PID.

4.5.7 1609.2 Security Management

4.5.7.1 Not all of these security requirements apply to the PID which is in listen only mode as proposed for the initial deployment for the pilot project. Where they do not apply, they may be ignored. However, in the future we hope to expand on this project to include the PSM and the SRM to request pedestrian service and to provide warning messages to approaching vehicles. Therefore, the following provisions are presented for consideration during the design.

4.5.7.2 Device suppliers shall provide written evidence demonstrating how the devices meet these security requirements

4.5.8 1609.2 Pseudonym Certificate Common Requirements

4.5.8.1 A device that uses 1609.2 pseudonym certificates shall not store the pseudonym certificates unencrypted in persistent storage. Pseudonym certificates may be stored unencrypted in volatile memory so long as that memory is not swapped unencrypted to persistent storage.

4.5.9 1609.2 Security Management Common Requirements

4.5.9.1 The devices support downloading certificates to one or two weeks in the future, either by explicit request of the short duration certificate download or by behaving stably if the SCMS only provides one or two weeks' worth of certificates.

4.5.9.2 Device suppliers shall provide written evidence of how devices have been tested for conformance with IEEE 1609.2.

4.5.9.3 Device suppliers shall provide written evidence of how devices have been tested for conformance with the SCMS interface.

4.5.10 1609.2 Verification

4.5.10.1 When verifying, the device shall require that 1609.2 signed messages are signed by a certificate that is protected from modification by, or chains back to a certificate that is protected from modification by, the secure boot process.

4.5.10.2 The 1609.2 revocation check shall not include a check for the revocation status of end-entity certificates, as these have a CrlSeries value of 0, but shall include a check for the revocation status of CA certificates

4.5.10.3 Revocation status of CA certificates shall be distributed during the certificate update process per the SCMS Interface document.

4.5.11 Encryption for TMC

4.5.11.1 Devices that encrypt for the TMC shall encrypt using IEEE 1609.2 encryption, per IEEE 1609.2-2016 section 5.3.5 with the string P1 set equal to the empty string.

4.5.11.2 Devices that encrypt for the TMC shall encrypt using an ECIES key provided for that purpose by the TMC.

4.5.11.3 Devices that encrypt for the TMC shall support updating the key via SNMPv3 per the requirements identified in this requirements list by "SNMP: Agent".

4.5.12 PSM Transmission

4.5.12.1 The PID shall sign PSMs with a 1609.2 pseudonym certificate containing the PSID for PSM signing.

4.5.12.2 The PID shall not create or transmit PSMs if they do not have a currently valid signing certificate.

4.5.12.3 The PID shall support changing the source MAC address from which PSMs are sent from time to time.

4.5.12.4 The PID shall support changing the PSM signing certificate from time to time.

4.5.12.5 The PID shall support changing the PSM temporary ID from time to time.

4.5.12.6 The PID shall change all of the source MAC address, the PSM signing certificate, and the PSM temporary ID in the same interval between PSMs.

4.5.12.7 The PID shall carry out plausibility testing on sensor data and shall not send PSMs if the sensor data fails the plausibility tests. (Note: Plausibility tests will be defined in Phase 2 design.)

4.5.13 Operations

4.5.13.1 A device with DSRC communications interfaces shall continue normal operations regardless of the number, rate, or content of the DSRC messages received.

4.5.13.2 A device with DSRC communications interfaces shall continue normal operations regardless of the number, rate, or content of the DSRC messages transmitted.

5 PID Application

The NYC CVPD will include two (2) distinctly different pedestrian oriented applications. The first is Pedestrian in Signalized Crosswalk (PEDINXWALK) application for notifying the oncoming vehicle of the pedestrian presence in the crosswalk. The second the Mobile Accessible Pedestrian Signal System (PED-SIG) for assisting the visually-impaired pedestrian in crossing the street. The PEDINXWALK application will operate on the ASD, while the PED-SIG application will reside in the PID. Note that the PEDINXWALK functional requirements are provided in this document only for reference. The ASD Procurement Specification document contains additional information on the PEDINXWALK application.

5.1 PEDINXWALK Application (For Reference Only)

5.1.1 PEDINXWALK Application Functional Requirements

5.1.1.1 The Pedestrian in Signalized Crosswalk (PEDINXWALK) application shall operate through the ASD.

5.1.1.2 The detection area for the PEDINXWALK application shall extend to both the intersection and the road segment upstream of the crosswalk.

5.1.1.3 The pedestrian presence information from the specific crosswalk for the approach roadway shall be received either by the traffic controller or the RSU included in the SPaT message transmitted by the intersection RSU.

5.1.1.4 The PEDINXWALK application shall send a combination of MAP and SPaT messages with the “pedestrian present” bit set to the ASD.

5.1.1.5 The ASD safety application shall monitor the vehicle’s location, heading, and speed.

5.1.1.6 The ASD shall issue a warning to the driver if they determine that an impact is likely.

5.1.1.7 An “event logging” mechanism shall create an “event record” which shall contain the SPaT and MAP messages heard by the ***ASD***.

5.1.1.8 The event record shall also contain any other DSRC messages from vehicles within a configurable radius and its own BSM and accelerometer information.

5.1.1.9 The event record shall reveal what the vehicle was doing before the alert and how it reacted to it.

5.1.1.10 This log shall eventually be uploaded to the New York City Department of Transportation (NYCDOT) Traffic Management Center (TMC) for analyzing the safety benefits.

5.1.1.11 The operation of the pedestrian alert mechanism on the vehicle shall be tempered to avoid continuous alerts during periods of peak pedestrian presence and very low vehicle speeds.

5.2 Mobile Accessible Pedestrian Signal System (PED-SIG) Application

5.2.1 PED-SIG Application Functional Requirements

5.2.1.1 The Mobile Accessible Pedestrian Signal (PED-SIG) application shall reside on the PID carried by the visually-impaired pedestrian and assist his or her crossing maneuvers through the SPaT and MAP message information received from the intersection RSU via DSRC. The information within the SPaT message shall allow the application to determine when the pedestrian signal displays the '**WALK'**, flashing '**DON'T WALK**', and steady '**DON'T WALK**' indications for each crosswalk (or crosswalk segment) and then transmit the appropriate audio or haptic prompts to the user (pedestrian).

5.2.1.2 The PID shall include a Global Navigation Satellite System (GNSS) receiver and any other location enhancement algorithms to interact with the pedestrian and establish the pedestrian's orientation (which crosswalk he or she intends to use). Its audio output can be used to verify the name of the crossing street and provide the current status of the pedestrian signal including the time remaining for each indication. The application could also be augmented to provide verbal information regarding the nature of the intersection such as the crosswalk distance, presence of refuge islands, diagonal crossing (Barnes dance) and other complexities. Such data shall be stored on the PID if it is not included in the MAP message. The PID is expected to use the MAP message information and its own location to determine the intersection the PED is approaching.

5.2.1.3 The basic application on the PID shall assist the pedestrians in locating their position (which corner of what intersection they are approaching), the street they are facing, and the status of the traffic signal governing that crosswalk.

5.2.1.4 As indicated above, the PED-SIG application shall acquire the following data based on the SPaT and MAP messages:

- The visually-impaired pedestrian's position (start, end) and orientation or intended crossing direction (departure range, arrival range) when they initiate an interaction with the application.
- The walk signal status in the intended crossing direction (walk time remaining, clearance time remaining, time until next walk signal is expected) – this shall be computed based on the time point information provided in the SPaT message and the time within the PID and the time stamp in the SPaT message. This should record only the data provided to the PID.

- The signal timing and controller status – this shall indicate if the traffic controller is functioning properly.
- The crosswalk geometry of the intended crossing – location of the curb/crosswalk junction (center point) and the direction and end location and type of location (refuge, sidewalk, etc.). This should record only the data provided to the PID.
- The intended crossing time from the intersection geometry (distance) and the expected pedestrian travel rate (configurable) – may be used by the application to provide additional information to the PID. This should record only the data provided to the PID.
- The intersection geometry (location of curbs, distance to each corner, name of crossing street, location of crosswalks) – this is present but need not be used – except where it is essential for the crossing (TBD). This should record only the data provided to the PID.
- Each transaction with the PED-SIG application and each intersection at which the application is invoked.

(Note: It should also record the movement of the PID during this interaction until the PID has either crossed the street or times out the action or the application recognizes that the PID has reached the end of the crosswalk.)

5.2.1.5 The PED-SIG application shall be able to communicate via DSRC.

5.2.1.6 The PED-SIG application shall be able to communicate via cloud-based mobile network (e.g. 3G, 4G/LTE).

5.2.1.7 The PED-SIG application shall collect no personally identifiable information (PII) from the user.

5.2.1.8 The PED-SIG application shall correctly discern the pedestrian's position and intended crossing direction.

5.2.1.9 The PED-SIG application shall provide status of the walk signal in the intended direction.

5.2.1.10 The PED-SIG application shall advise (via audio) the pedestrian how to use the application.

5.2.1.11 The PED-SIG application shall receive intersection geometry information from the RSU based on J2735-201603.

5.2.1.12 The PED-SIG application shall use the intersection geometry information to determine the pedestrian's orientation.

5.2.1.13 The PED-SIG application shall use the intersection geometry information provided by the MAP message to determine the crosswalk geometry of the intended crossing.

5.2.1.14 The PED-SIG application shall collect map point descriptions about the static physical geometry at intersection segments. (Note: mid-block crossings are treated identically to intersection crossings.)

5.2.1.15 The PED-SIG application shall determine the intended crossing time from the intersection geographic information (distance) and the expected pedestrian travel rate (configurable).

5.2.1.16 The PED-SIG application shall collect data on the map error status notification. (partial, unable to detect). (Note: this is intended to assist the system in troubleshooting problems; the quality of the MAP data is critical to the application and this requirement ensures that such issues are made known to the central system for correction. This assumes that the application notifies the PED whenever it encounters a geographic computation error.)

5.2.1.17 The PED-SIG application shall assist the pedestrian in determining his/her orientation. (Note: orientation refers to understanding which street crossing the pedestrian is facing.)

5.2.1.18 The PED-SIG application shall provide information to the pedestrian regarding the availability of PED support services at the intersection. (If there is an RSU and if the RSU includes the future actuation and tracking support.)

5.2.1.19 The PED-SIG application shall provide information to the pedestrian indicating the status of the pedestrian signal for the intended crossing including walk time remaining, clearance time remaining, and time until the next walk signal is expected and length of the crosswalk.

5.2.1.20 The PED-SIG application shall allow the pedestrian to configure selected parameters and characteristics such as sound volume, voice commands, and walking speeds.

5.2.1.21 The PED-SIG application shall notify the pedestrian if there is a preemption or priority change (TSP) operation taking place which may disrupt the signal timing.

5.2.1.22 The PED-SIG application shall collect DSRC RF receive levels. (Note: this is for analysis of the reliability of the RSU to PID messages and the PID to RSU messages.)

5.2.1.23 The PED-SIG application shall calculate intersection crossing information based on pedestrian's origin, destination, departure range, and arrival range. (Note: this is for coordination of signal timing phase.)

5.2.1.24 The PED-SIG application shall collect the performance data listed in listed herein.

5.2.1.25 The PED-SIG application shall have data storage capabilities for real-time and historical real-time information on intersection performance ensuring pedestrian anonymity.

5.2.1.26 The PED-SIG application shall collect metadata that includes the date and time when system information was generated.

5.2.1.27 The PED-SIG application shall receive signal timing and controller status from the RSU through the SPaT and SSM[3] messages.

5.2.1.28 All data transmitted between the PID and the NYU server shall be encrypted to protect any personal information.

5.2.1.29 The PID shall use the channel assignments defined in Table 5.

5.2.1.30 The PID shall send PSMs to the RSU per J2945/9.

5.2.1.31 The PID device shall be able to function in a communication-saturated environment.

5.2.2 Navigation Aid

5.2.2.1 The PID shall include an integrated navigation aid (pedestrian navigation application) which can assist in guiding the visually challenged pedestrian along a route on the city streets.

5.2.2.2 This application shall include a database which includes the intersection locations and intersection ID's; the purpose of the CV PED-SIG application is to assist by integrating the information about the intersection timing with the pedestrian navigation aid so that the pedestrian can determine what street they are facing and what the PED signal condition is for that crossing.

5.2.3 PED-SIG Application Non-Functional Requirements

5.2.3.1 The PED-SIG application shall load within 10 second in order for the pedestrian to feel that the system is reacting instantaneously, meaning that no special feedback is necessary except to display the result.

5.2.3.2 The PED-SIG application shall continuously notify the user in some manner that it is operating.

5.2.3.3 The PED-SIG (on the PID) application shall be able to provide requested information within 2 seconds. Note that the PID shall continuously monitor the SPaT and MAP message content around it so that it can respond quickly to any information requests of the user.

5.2.3.4 The PED-SIG application shall be developed using reactive component development metrics.

[3] Future

5.2.3.5 The PED-SIG application shall specify that the response times shall allow for workload scaling.

5.2.3.6 The PED-SIG application shall use hardware that is exclusively for the system so that there is no competition for resources.

5.2.4 PED-SIG Application Accessibility Requirements

5.2.4.1 The PED-SIG application shall provide information and sensory experience to be communicated to the user by means of a user agent, including code or markup that defines the content's structure, presentation, and interactions.

5.2.4.2 The PED-SIG application shall conform if non-text content is a control or accepts user input, then it has a name that describes its purpose.

5.2.4.3 The PED-SIG application shall not disrupt or disable activated features of other products that are identified as accessibility features, where those features are developed and documented according to industry standards.

5.2.4.4 The PED-SIG application shall create alternative versions when the application does not need to have a matched page for page with the original.

5.2.4.5 The conforming alternative version may consist of multiple pages.

5.2.5 PED-SIG Application Privacy Requirements

5.2.5.1 The PED-SIG application shall ensure that sharing data is used strictly for intended application processing.

5.2.5.2 The PED-SIG application shall ensure geo-location information is used for application processing only.

5.3 Performance Monitoring

5.3.1.1 The performance monitoring subsystem shall post-process the data surrounding the PED-SIG application events.

5.3.1.2 The performance monitoring subsystem shall utilize the post-processed event data and measure the number of pedestrian crossing violation reductions.

5.3.1.3 The performance monitoring subsystem shall utilize the post-processed event data and measure the visually-impaired pedestrian-related crash counts and rates.

5.3.1.4 The performance monitoring subsystem shall utilize the post-processed event data and measure the conflicts with visually-impaired pedestrians.

5.3.1.5 The performance monitoring subsystem shall utilize the post-processed event data and measure the wait time for crossing at the intersections.

5.3.1.6 The performance monitoring subsystem shall evaluate the change in the number of reported crashes involving visually-impaired pedestrians from the ‘Before’ period to the ‘Pilot’ period.

5.4 Safety Requirements

5.4.1.1 The PED-SIG application in the mobile device shall communicate app walk indicators to visually impaired pedestrians.

5.4.1.2 The PED-SIG application shall correctly discern the pedestrian's position and intended crossing direction.

5.4.1.3 The PED-SIG application shall provide status of the walk signal in the intended direction.

5.4.1.4 In the PED-SIG application, all subsystems and interfaces shall have independent verification and validation processes.

5.4.1.5 The PED-SIG application shall advise (via audio) the pedestrian how to use the application.

6 System Interfaces

This section contains the interface requirements of the NYC CVPD components and their external capabilities. Not all the following requirements apply to all types or approaches to the implementation of the PID. For example, if the PID uses 4G/LTE for receipt of the SPaT and MAP data from a central server, then the discussion of DSRC communications does not apply.

6.1 Global Navigation Satellite System (GNSS)

6.1.1.1 Each DSRC device shall obtain its time and position from the GNSS per the requirements of J2945/1 Section 6.2.

6.2 Wide Area Augmentation System (WAAS) [Location Correction]

6.2.1.1 Each DSRC device shall use WAAS corrections per J2945/1 Section 6.2.2.

6.3 Network Time Reference

6.3.1.1 Devices unable to receive timing information per J2945/1 Section 6.2 shall set their time from an authenticated time reference using the Network Time Protocol Version 4 per Internet Engineering Task Force RFC 5905-5908.

6.3.1.2 Regardless of the media chosen or technique used for transmitting the SPaT and MAP data to the PID or collection of data from the PID, the internal clock of the PID shall be synchronized to the local time (UTC) within 10 ms of a NIST based time reference such as the GPS time after adjustment for leap seconds. This time reference shall be used for all logging such that analysis can associate actions of the pedestrian with the actions of the traffic controller or surrounding vehicles.

7 Test Requirements

7.1 Radio Transmission

The PID transmission of DSRC messages is desired for future use but is not required; however, the following provisions shall govern if DSRC is supported by the PID.

7.1.1 Transmission Measurement

7.1.1.1 the PID provided under this contract shall include the ability to transmit DSRC signals as described herein. In the future, it is expected that the PID will be used to broadcast PSM and SRM and to further enhance the challenged pedestrian's safety and mobility.

7.1.1.2 The ***PID*** shall support a DSRC radio transmission pattern 360 degrees around the specified vehicle types (as called out in SRD-USDOTOBE-003-SYS002v001) throughout a range of 1m to 300m, with a maximum Packet Error Rate of 10.0%, in an open field under the following conditions:

a. When transmitting in an 802.11p Regulatory class 17 (even 10MHz channels in the range 172 to 184) channel.
b. With a PSM Transmission Rate of 10 Hz – configurable and adjustable based on channel saturation
c. 6 Mbps data rate

7.1.2 Pattern Measurement Location

7.1.2.1 Measurements of the radio transmission pattern shall be made in the middle of an open field with no man-made or natural structures that would reflect 5.9 GHz radiation within 2.5 kilometers (km) of the test vehicle(s).

7.2 Pedestrian Location

7.2.1 Data Elements Measurement

7.2.1.1 The ***PID*** shall provide ***pedestrian*** location data elements of the PSM to within the required values of ground truth (defined as predetermined geographic coordinates for a fixed point or points in the test area) based on the ***pedestrian***'s position and travel speed.

Appendix A. DSRC Devices –

Table 5 below identifies the details of each DSRC channel to be used in the NYC CVPD system infrastructure. This shall apply only if the PID includes a DSRC radio.

Table 5. DSRC Channel Assignment

DSRC Channel	Purpose
172	For transmission of the SPaT, MAP, BSM, and RTCM messages
174	Service channel for WAVE Short Message Protocols (WSMP) or IPv6 Infrastructure to Vehicle
176	Service channel for WAVE Short Message Protocols (WSMP) or IPv6 Vehicle to Infrastructure
178	Control channel for WAVE Service Advertisements that announce the device supports specific additional services for PED applications, parameter changes, OTA software updates, credential acquisition, and uploading of log files collected
180	Service channel for WAVE Short Message Protocols (WSMP) or IPv6 Vehicle to Infrastructure
182	Service channel for WAVE Short Message Protocols (WSMP) or IPv6 Infrastructure to Vehicle

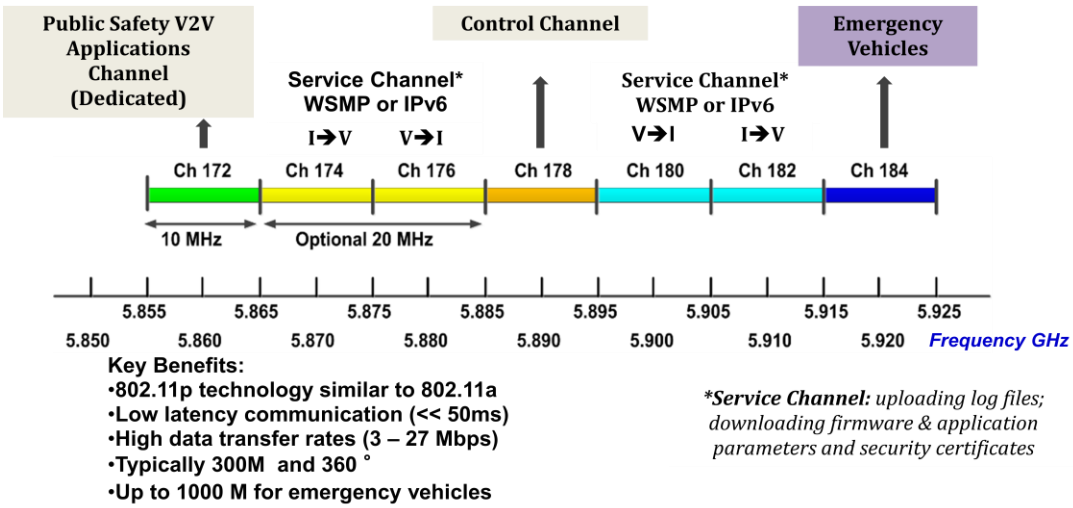


Figure 2 Channel Utilization Chart (derived from J2945/0)

Table 6 below describes the potential device fail modes in the NYC CVPD system.

Table 6. Device Fail Modes (Preliminary)

Fail Mode	Description
Mechanical	Corrosion, shock
Electrical	Electrostatic discharge, short circuit
Location Accuracy Loss	Device's location accuracy estimates exceeds the minimum performance ranges established by standards.
Certificates Unavailable	The device has been refused additional operational certificates.

Appendix B. Data Tables

Table 7 below lists the preliminary list of the performance data for the PED-SIG application.

Table 7. Preliminary PED-SIG Application Performance Data

PED-SIG Application Performance Data
number of pedestrian crossing violation reductions
visually-impaired pedestrian-related crash counts, by severity
conflicts with visually-impaired pedestrians
time to collision (vehicle to pedestrian)
waiting time at intersection for crossing

Appendix C. Functional Description Overview

1 Introduction

The connected vehicle pilot deployment project for New York City will include two distinctly different pedestrian oriented applications: one to alert oncoming vehicle(s) of the presence of a pedestrian in the crosswalk, and the second for assisting the visually challenged pedestrian in crossing the street. The following is an overview of the application to support the visually challenged pedestrian. The PED in crosswalk warning to approaching vehicles does not require any interaction with the pedestrian; pedestrian detection equipment will be installed at the intersection for the application to notify approaching vehicles of pedestrians in the roadway.

2 Fundamental Assumptions

The Personal Information Device (PID) is expected to receive SPaT and MAP information either from DSRC broadcasts from the RSU and other media and services (cellular). The PID will also include a user interface and alternative internet access via commercial service. The commercial service connection will be used for collecting the usage and performance data. Note that intersections equipped with an RSU within the project area (~320) will be broadcasting the Signal Phase and Timing (SPaT) and geometric information (MAP) messages using DSRC and this information can also be made available through alternative channels to PID servers. Data flow #11 in Figure 3 below indicates that the SPaT and MAP information may be exported by any number of devices and made available to the PID via alternative media.

The Mobile Accessible Pedestrian Signal (PED-SIG) application will reside on the PID carried by the pedestrian and use the MAP and SPaT message content to assist the pedestrian to maneuver across the street. The information within the SPaT message will allow the application to determine when the pedestrian signal displays the '**WALK'**, flashing '**DON'T WALK**', and steady '**DON'T WALK**' indications for each crosswalk (or crosswalk segment).

The MAP message describes the intersection geometry including the crosswalk location (centerline), approach streets' names (63 characters max), intersection ID, intersection location (center-point latitude/longitude), and intersection name (63 Characters max) among other attributes based on the Society of Automotive Engineers (SAE) J2735-201603 standard.

The PID shall include a Global Navigation Satellite System (GNSS) receiver and other location enhancement algorithms to interact with the pedestrian and establish the pedestrian's orientation (which crosswalk he or she intends to use). The PID is expected to use the MAP message information and its own location database to determine the intersection the pedestrian is approaching. Thus, the basic application on the PID will assist the pedestrians in locating their position (which corner of what intersection they are approaching), the street they are facing, and the status of the traffic signal governing that crosswalk.

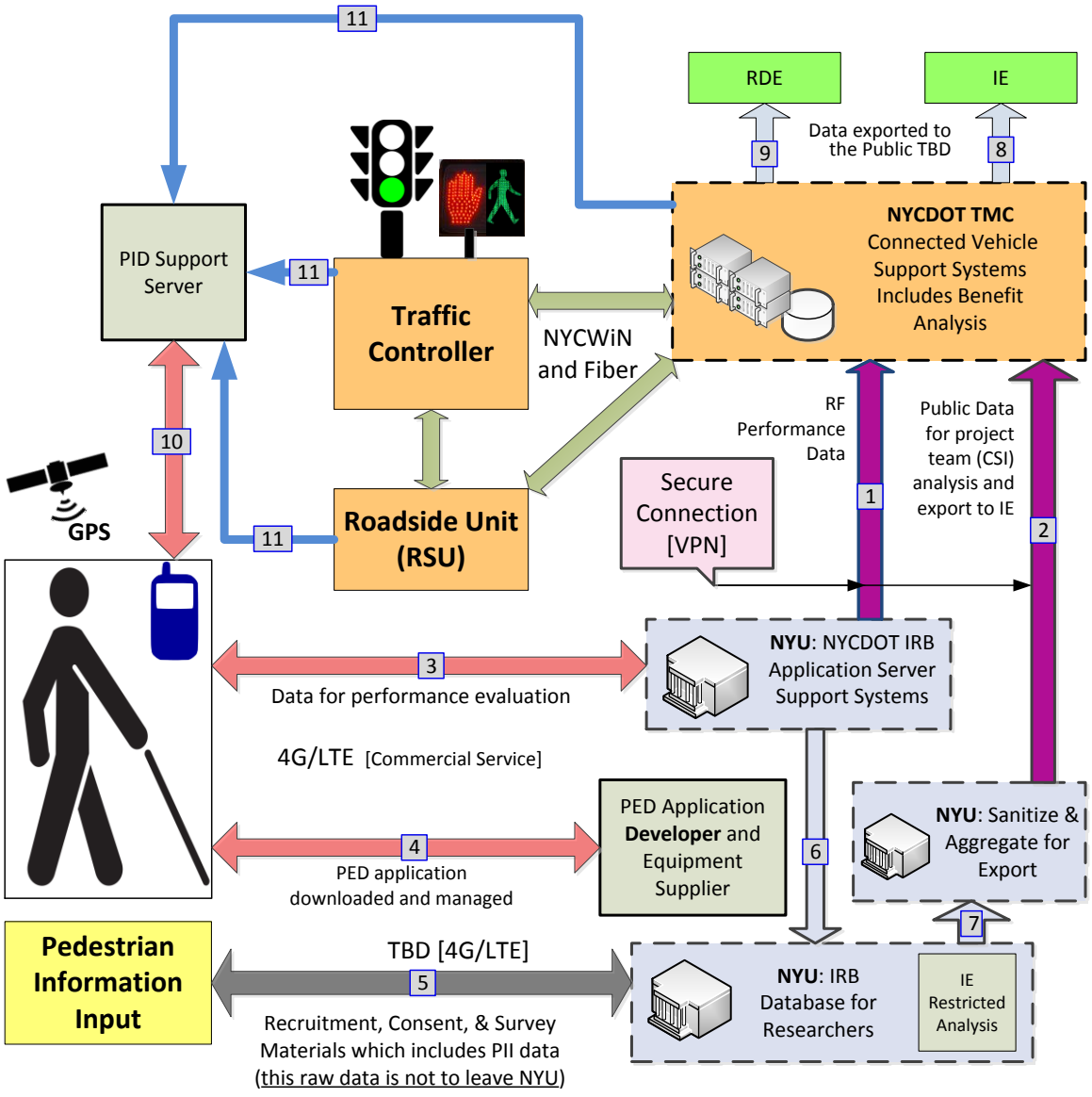
To aid the pedestrian, the PID's audio output can be used to verify the name of the crossing street and provide the current status of the pedestrian signal including the time remaining for each indication. The application could also be augmented to provide verbal information regarding the nature of the intersection such as the crosswalk distance, presence of refuge islands, diagonal crossing (Barnes dance) and other complexities. Such data must be stored on the PID if it is not included in the MAP message. Note that this may also be provided through a navigation service if the map information is not stored locally. These are design issues and it is expected that the application software on the PID will be adjusted to optimize the utility to the visually challenged pedestrian and use the features of the PID to support their disability.

The PED-SIG application's software and PID's hardware designs will be up to the selected vendor.

As indicated above, the PID will collect the following data using the SPaT and MAP messages and the onboard database:

- Pedestrian's position (start, end) and orientation or intended crossing direction (departure range, arrival range)
- Walk signal status in the intended crossing direction (walk time remaining, clearance time remaining, time until next walk signal is expected)
- Signal timing and controller status (operational, flashing, TSP, EVP, transitioning)
- Crosswalk geometry of the intended crossing
- Intended crossing time from the intersection geometry (distance) and the expected pedestrian travel rate (configurable)
- Intersection geometry (location of curbs, distance to each corner, name of crossing street, location of crosswalks)

Figure 3 Application Context Diagram



Visually Challenged Pedestrian Application Context Diagram

VisioDocument

The PID will collect the following data along with other evaluation data not listed here for assessing the device performance in the NYC CVPD system:

- Map error status notification (partial, unable to detect) for assisting the system in troubleshooting and correcting issues regarding the MAP data quality
- DSRC radio frequency (RF) receive levels for assessing the reliability of the communication between the PID and RSU or the media used.

For safety performance evaluation, the PID will collect the following pedestrian behavior data before the pedestrian application is fully activated to assist the pedestrian and after activation when it provides pedestrian support for the crossing:

- Number of pedestrian crossing violations [4]
- Visually-impaired pedestrian-related crash counts, by severity
- Conflicts with visually-impaired pedestrians
- Time to collision (vehicle to pedestrian)
- Waiting time at intersection for crossing

The data indicated above will be stored on the device. The PID will initiate a secure communication session (e.g. FTP) with the NYU on a periodic basis (configurable) to upload its log data to the NYU server for analysis [3]. Once uploaded, it will be purged from the PID. The data will contain the device serial number. The data shall be encrypted on the device and transmitted to the NYU server in encrypted form where it will be passed to the NYU pedestrian application database for controlled analysis [6]. NYU shall decrypt the data upon receipt and transmit usage information to the TMC [1] for the purpose of tracking the operations and maintenance characteristics. Note that the TMC system needs to determine which PIDs are operational and which PIDs are suspect because of a lack of data.

In order to be able to trust the data being received from the intersection, the PID needs to be configured with verification keys; however, if the intent is to allow the PID to eventually[5] transmit PED service requests or Pedestrian Safety Messages (PSM) then it will need an enrollment certificate which will be used to acquire the operating certificates to be able to sign messages transmitted to the intersection. The Security Credential Management Systems (SCMS) will support requests for verification certificates without an enrollment certificate.

Since the PID will not be transmitting DSRC messages during the initial system testing, it will not be necessary to receive operating certificates for the purpose of transmitting Pedestrian Safety Messages (PSM) or for making any service requests from the intersection.

The software shall also support a navigation application such that the PED can use the PID to select their route from start to finish.

When the software for the PID is loaded on the device [4], it needs to be activated by the agency making the devices available to the selected users.

The IDs of the users shall be collected in a database to match them with the PIDs' serial numbers. This data [3] shall be encrypted and held at the NYU server while being protected from external use.

3 Future directions

Section 2 above describes the first application envisioned for the NYC CV Pilot deployment. Future additions include the following:

[4] Note that some of this data will be collected by interviewing the selected pedestrians or through feedback using the PID – TBD.

[5] Future capability – not included in this contract

a. Pedestrian call requests for service: This will require that the PID receive certificates with special service permissions (SSP) to make such requests to the traffic signal. Since the PID will be transmitting DSRC messages, it will need to be certified with different enrollment certificate that denote its permission to transmit. The SSP can be managed by NYCDOT under a special program for the visually challenged users much like other similar services. In this case, the PID will transmit a service request message (SRM) and receive a Service Status Message (SSM) which will indicate that the request has been received, acknowledged, and processed by the intersection.

b. Pedestrian Safety Message (PSM): This message is similar to the BSM used by the vehicles and provides pedestrian travel information to surrounding PIDs, vehicles, and intersections. This message can be used to alert the traffic controller or notify the vehicles of the pedestrian presence. This can also be used in conjunction with the pedestrian call request to extend the PED timing and replace the existing ITS adaptable PED detection equipment. However, the location accuracy of the PID must be on the order of a few centimeters. Otherwise, the pedestrian's location will be too unreliable for such uses.

These future considerations are beyond the current scope of the NYC CVPD project.

Appendix D. Design Issues to be Reviewed and Resolved

Visually Challenged Pedestrian Assist

The reader is directed to the ConOps and specification for the pedestrian application developed during Phase 1 and Phase 2 of the project. This memorandum is intended for discussion purposes and does not eliminate any of the requirements contained in the previous documents.

Requirements

For this application, the vendor will develop a pedestrian application which provides urban navigation assistance for the visually challenged. There are 2 parts to this application: (A) urban navigation – getting from point A to point B and (B) intersection navigation assistance - understanding the pedestrian signal operation and the user's orientation.

A Urban navigation

This is expected to be an existing application that assists the visually challenged in generally navigating the roadway network on foot. It will provide haptic and/or verbal instructions and accept spoken or some other input means to request a route and to interact with the program. It is assumed that the intersection navigation assistance (below) will be added to this application.

B Intersection navigation assistance

This application will rely on the MAP message and the Intersection Timing information (SPaT message) to assist the user in orienting themselves for crossing the street and to understand the characteristics of the PED crossing and PED signal operation. It is expected that this portion of the application will provide information regarding the length of the crosswalk, any specific angle where it is diagonal, and other important information such as refuge areas. It should also provide information regarding the current state of the pedestrian signal which regulates the desired crosswalk; this might include seconds until **WALK** appears, remaining seconds for the **WALK** display, start of the flashing **DON'T WALK** display (e.g. pedestrian clearance), remaining time for the **FLASHING DON'T WALK** display and the start of the **STEADY STATE DON'T WALK** indication. It might also include distance to curb or distance to refuge or sidewalk as the pedestrian is progressing. The exact final user interface needs to be developed in cooperation with the user community.

Communications

The original intent of the specifications and ConOps was that the intersection Roadside Unit (RSU) would transmit (broadcast) the SPaT and MAP messages using DSRC 5.9 GHz (channel 172) in accordance with SAE J2735 and the hand-held pedestrian device (PID) would receive this information and use it in conjunction with the intersection navigation application to assist the visually challenged pedestrian in crossing the intersection. Since the MAP message provides the geometric details for the intersection layout and the SPaT Message provides the pedestrian signal timing information, this contains all the information necessary to support the application. Unfortunately, the vendor(s) have been unable to obtain chipsets that will run on both the cellular bands and DSRC 5.9 GHz and the City is now faced with the need to use some other media to broadcast the SPaT and MAP information to the PID for the pedestrian crossing assist application.

Note that cellular service is required to support data collection for the evaluation (to be uploaded on request to the NYU protected server) and OTA application loading and updating most probably

from the app store. It is also likely that a cellular data service is required for the general pedestrian urban navigation applications (how to get from “here” to “there” following the street network or a combination of public transport and walking.

SPaT and MAP data

The options for communicating the SPaT and MAP data include:

a) Wifi locally between the PID and the RSU at the intersection, or
b) 4G/LTE data exchanges between the PID and a server which provides the SPaT and MAP information interactively with the PID application.

Option (a) requires a change order for the RSU to support local wifi operation and changes to the RSU software to broadcast the SPaT and MAP on both DSRC and wifi. It will also require that the PID automatically detect the presence of the wifi signal based on the navigation application and switch to using the wifi media for the localized navigation based on the location of the PID and the nearest intersection. This will require that the SSID for the wifi signal include a uniquely identifiable ID that includes the application ID and the intersection ID. The PID could then use this media to assist in the street crossing and the 4G/LTE media to continue with the urban navigation application. However, this will only work for those locations which deploy a modified RSU which supports the Wifi option.

Option (b) requires that the real time SPaT and MAP information be transmitted from the RSU to a visually challenged pedestrian application server (i.e. AWS cloud service) where it is processed and passed in some form cooperatively to the PID to support the crosswalk navigation aid. At present, several options exist for the transmission of the SPaT and MAP message content as follows:

i. The network could open a channel from the RSU through the backhaul directly to the AWS cloud; this would require opening a portal in the firewalls and will add considerable bandwidth requirements to both the backhaul and the costs of the AWS cloud services. There would be 11 blocks per second transmitted from the RSU to the AWS Cloud from each of the instrumented intersections. This would also require a change to the RSU software to support transmission of the SPaT and MAP messages to both the DSRC radio and back through the Traffic Control Backhaul (NYCWiN) to the AWS server.
ii. The RSU could be configured with an additional 4G/LTE radio and the RSU could be modified to transmit this information to both the cellular port and the DSRC port at the same time. This would require the purchase and installation of a cellular modem within the RSU and a monthly fee for the data transmission for 40-50GB/month aggregate for all 10 sites.
iii. The ASTC could be modified (negligible) to transmit the SPaT information (not message) to the TMC at 10 HZ where it could be filtered to include only the pedestrian signal timing information and aggregated from all 10 sites for one second boundaries and transmitted once per second to the AWS server. This would significantly reduce the data transmitted since the SPaT data from the ASTC to the RSU or the TMC contains only the time tick and the data that has changed. There are issues with this approach because the ASTC expects an acknowledgement within 10 ms for the transmission – and this is unlikely over NYCWiN. Alternatively, each transmission could be filtered at the ASTC to include only the PED timing information and broadcast at once per second.

There are many assumptions and options with the above that need to be clarified. Since Savari is the PID provider and has demonstrated a portion of the application using their RSU, they may require that their RSU be installed to provide “special” data to the AWS cloud. This should not be the case, and there should be no need for a second RSU at the location just to support the PID application. They may also require the use of 4G/LTE directly from the RSU to the AWS server – which needs further discussion.

If the data is sent through the TMC, the software development in the TMC should be minimal as it must simply receive the 10 Hz SPaT data (over the secure DTLS channel), strip off the unneeded signal timing, and aggregate the PED timing for once per second. Then it can package the data for bulk once per second transmission to the AWS cloud which would contain the MAP data content (already stored at the TMC) and the filtered SPaT content. Since the SPaT content from the ASTC only contains that data which has changed, this greatly reduces the amount of data

transferred to the AWS cloud while still containing all the data necessary to drive the PID application. This approach requires minimal changes to the ASTC software because Peek has already indicated the same SPaT data could be easily sent to multiple locations.

We should be able to avoid the necessity of installing multiple RSUs at these locations; this means that the installed RSU must be fully compliant with the RSU specification and support all the NY required functionality – which necessitates considerable software development for the RSU vendor and testing by both NYC and the vendor.

Another consideration: if the TMC takes the broadcast SPaT data directly from the ASTC, then in effect, this PID application could be made to work anywhere in the City – not just where RSU infrastructure is installed. The City could simply install the new ASTC firmware at any location of interest and configure it to transmit the SPaT information to the TMC where it would be aggregated and transmitted to the AWS cloud. However, the City would be required to develop the MAP message (with the crosswalk information) for each intersection and communications must be operational between the ASTC and the TMC. This would also require that the CCS be upgraded to support the DTLS 1.2 secure exchanges for all intersections to be included in the PED application. This type of deployment will need careful financial/cost analysis to determine the internet access costs for the AWS cloud and the AWS cloud services costs, as well as the monthly cellphone charges for the users of this service. However, because it could encompass the whole City, it may be attractive to PASS and the administration.