Connected Vehicle Pilot Deployment Program

Driving Towards Deployment: Lessons Learned from the Design/Build/Test Phase

www.its.dot.gov/index.htm

Final – December 13, 2018
FHWA-JPO-18-712

Source: USDOT, 2018

U.S. Department of Transportation

Produced by Noblis
U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
Intelligent Transportation Systems (ITS) Joint Program Office (JPO)

Notice

Technical Report Documentation Page

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-JPO-18-712		

4. Title and Subtitle	5. Report Date
Connected Vehicle Pilot Deployment Program Driving Towards Deployment: Lessons Learned from the Design/Build/Test Phase	December 13, 2018
	6. Performing Organization Code
7. Author(s) Kathy Thompson	**8. Performing Organization Report No.**
9. Performing Organization Name and Address Noblis 600 Maryland Ave SW, Suite 700E Washington, DC 20024	**10. Work Unit No. (TRAIS)**
	11. Contract or Grant No. DTFH6116F00019
12. Sponsoring Agency Name and Address Intelligent Transportation Systems (ITS) Joint Program Office (JPO) 1200 New Jersey Ave., SE Washington, DC 20590-9898	**13. Type of Report and Period Covered** Final Report
	14. Sponsoring Agency Code HOIT-1

15. Supplementary Notes

Work performed for: Kate Hartman (CV Pilots Program Manager, ITS JPO)

16. Abstract

The Connected Vehicle Pilot Deployment (CV Pilots) Program seeks to spur innovation among early adopters of connected vehicle application concepts. Pilot deployment awards were given to three sites, New York City, Wyoming, and Tampa, FL. The CV pilot sites are expected to integrate connected vehicle research concepts into practical and effective elements, enhancing current operational capabilities. Each pilot deployment site is being developed in three distinct phases: Phase 1: Concept Development, Phase 2: Design/Build/Test, and Phase 3: Operate and Maintain.

Based on the material the CV Pilot sites presented during a workshop session at ITE Annual Meeting 2018, this report covers experiences and lessons learned from the pilot deployment sites during Phase 2 (Design/Build/Test) of the CV Pilot Program.

17. Keywords	18. Distribution Statement
Connected vehicles, Intelligent Transportation Systems, Systems Engineering, Planning, Implementation Guide, Lessons Learned	No restrictions

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
Unclassified	Unclassified	30	

Acknowledgements

This work was sponsored by ITS JPO and was performed by Noblis under contract DTFH6116F00019. Noblis would like to thank the Connected Vehicle Pilot Deployment Program reviewers listed below for the valuable input they provided for this report.

USDOT Team Members	Noblis Technical Support Team Members	CV Pilot Site Team Members
• Deborah Curtis, FHWA • Ed Fok, FHWA • Kate Hartman, ITS JPO • Govind Vadakpat, FHWA • Jonathan Walker, ITS JPO	• Justin Anderson • Barbara Staples • Meenakshy Vasudevan • Peiwei Wang • Karl Wunderlich	New York City Pilot Deployment Team • David Benevelli • Bob Rausch • Mohamed Talas Tampa Pilot Deployment Team • Bob Frey • Steven Johnson • Dave McNamara • Dave Miller • Stephen Novosad Wyoming Pilot Deployment Team • Tony English • Vince Garcia • Deepak Gopalakrishna • Ali Ragan

Table of Contents

List of Tables

1 Introduction

1.1 Background

1.1.1 Connected Vehicle Pilot Deployment Program

Connected vehicles (CVs) are poised to transform our streets, communities, and personal lives. But first, we must tackle deployment challenges head on and provide interested regions with examples of success stories and identified champions. The U.S. Department of Transportation (USDOT) is taking on this challenge by investing in a regional pilot deployment program that is not only accelerating deployment but also identifying what barriers remain and how to address them.

The USDOT awarded cooperative agreements collectively worth more than $45 million to three individual pilot sites in New York City; Wyoming; and Tampa to implement a suite of connected vehicle applications and technologies tailored to meet their region's unique transportation needs. These pilot sites are helping connected vehicles make the final leap into real-world deployment so that they can deliver on their promises to increase safety, improve personal mobility, enhance economic productivity, reduce negative environmental impacts and transform public agency operations. Moreover, these sites are laying the groundwork for even more dramatic transformations as other areas follow in their footsteps.

Following the award, each site spent 12 months preparing a comprehensive deployment concept to ensure rapid and efficient connected vehicle capability roll-out. The sites next completed a 24-month phase to design, build, and test these deployments of integrated wireless in-vehicle, mobile device, and roadside technologies. As of Fall 2018, the sites are entering a third phase of the deployment where the tested connected vehicle systems will become operational for a minimum 18-month period and will be monitored on a set of key performance measures.

1.1.1.1 Wyoming Pilot Overview

The Wyoming CV Pilot will focus on the efficient and safe movement of freight through the I-80 east-west corridor, which is critical to commercial heavy-duty vehicles moving across the northern portion of our country. Wyoming Department of Transportation (WYDOT) CV Pilot site focuses on the needs of the commercial vehicle operator in the State of Wyoming and will develop applications that use vehicle to infrastructure (V2I) and vehicle to vehicle (V2V) connectivity to support a flexible range of services from advisories including roadside alerts, parking notifications and dynamic travel guidance. This WYDOT CV Pilot is expected to reduce the number of blowover incidents and adverse weather-related incidents (including secondary incidents) in the corridor to improve safety and reduce incident-related delays. WYDOT will develop systems that support the use of CV Technology along the 402 miles of I-80 in Wyoming. WYDOT will equip around 400 vehicles, a combination of fleet vehicles and commercial trucks with on-board units (OBUs), at least 150 of which would be heavy trucks that are expected to be regular users of I-80. In addition, of the 400 equipped-vehicles, 100 WYDOT fleet vehicles, snowplows and highway patrol vehicles, will be equipped with OBUs and mobile weather sensors.

1.1.1.2 New York City Pilot Overview

The New York City Department of Transportation (NYCDOT) leads the New York City Pilot, which aims to improve the safety of travelers and pedestrians in the city through the deployment of V2V and V2I connected vehicle technologies. NYCDOT's planned deployment provides an ideal opportunity to evaluate connected vehicle technology and applications in tightly-spaced intersections typical in a dense urban transportation system and is anticipated to be the largest connected vehicle technology deployment to date. The NYCDOT CV Pilot Deployment project area encompasses three distinct areas in the boroughs of Manhattan and Brooklyn. Approximately 3,000 taxi cabs, 700 Metropolitan Transportation Authority (MTA) buses, 400 commercial fleet delivery trucks, and 3,400 City vehicles that frequent these areas will be outfitted with the CV technology. As a city bustling with pedestrians, the pilot will also focus on reducing vehicle-pedestrian conflicts through in-vehicle pedestrian warnings and an additional V2I/I2V project component that will equip approximately 100 visually challenged pedestrians with personal devices that assist them in safely crossing the street.

1.1.1.3 Tampa Pilot Overview

The Tampa Hillsborough Expressway Authority (THEA) CV Pilot will employ innovative V2V and V2I communication technology to improve safety and traffic conditions in downtown Tampa. The pilot seeks to address peak rush-hour congestion in downtown Tampa, reduce the risk of collisions by detecting and warning wrong-way drivers before they get on the expressway, enhance pedestrian safety at signalized intersections, provide transit signal priority to help keep buses on schedule, and help to reduce conflicts with streetcars by deploying devices that enable them to communicate wirelessly with other connected vehicles and pedestrians. The THEA CV Pilot will employ Dedicated Short-Range Communication (DSRC) to enable transmissions among approximately 1,600 cars, 10 buses, 10 trolleys, 500 pedestrians with smartphone applications. To support this initiative, THEA will be working with their primary partners, The City of Tampa (COT), Florida Department of Transportation (FDOT) and Hillsborough Area Regional Transit (HART) to create a region-wide Connected Vehicle Task Force.

1.2 Purpose

Given the promising future of connected vehicle deployments and the growing early deployer community, experiences and insights from the CV Pilots have been collected to serve as lessons learned and recommendations for future early deployer projects and efforts. This report represents an organized collection of these experiences across all stages of the Design/Build/Test Phase of the CV Pilots.

1.2.1 CV Pilots at ITE Annual Meeting 2018

Per the terms of each sites' cooperative agreement with USDOT, the Pilot sites agreed to present or exhibit at several trade shows and conferences throughout the duration of the deployment to inform and educate stakeholders and the public on their deployment activities. One such conference was the Institute of Transportation Engineers (ITE) Annual Meeting that occurred August 19 – 23, 2018 in Minneapolis, Minnesota. Representatives from each of the sites presented as part of a workshop on *Building Smarter Communities through Better Transportation*. The presentation, titled *Building a Checklist for a Robust CV Deployment*, focused on the pilot projects' progress as they wrapped up the Design/Build/Test Phase; the recent success of the Interoperability Testing; ongoing and planned deployment activity in response to the Signal Phase and Timing (SPaT) challenge; and available policy and technical guidance for those interested in deploying CV services. The content presented during this session serves as the primary input for this report, augmented with other challenges and successes documented throughout the Design/Build/Test Phase.

1.2.2 Relevant Resources

Each of the CV Pilot sites has created a clear set of documents outlining their design/build/test activities and processes, including: system architecture and design development; application development and integration; deployment system planning and installation; and operational readiness test planning, development and results. These technical planning documents are being posted on the CV Pilots website for public consumption as they are finalized. Additionally, the recordings and presentation materials from previously held webinars and conference presentations are archived on the CV Pilots' website.

While this report is structured as a concise narrative recounting many of the specific challenges and triumphs of the CV Pilots, readers seeking a more general guide for deploying CV technology can complement this report with USDOT's V2I Hub Deployment Guide. The V2I Hub Deployment Guide provides an outline with step-by-step instructions for deploying Vehicle-to-Infrastructure (V2I) software and hardware and provides insight into needs analysis, planning, design, procurement, field deployment, and post-deployment.

1.3 Executive Summary

The table below lists the core lessons from the Design/Build/Test Phase grouped by deployment topic area. Chapter 2 of this report expands on these lessons with specifics about the CV Pilot sites' experiences from the Design/Build/Test Phase.

Table 1: High-level Lessons Learned from the CV Pilots' Design/Build/Test Phase

Assessment of Infrastructure and Organizational Capabilities	
1.	Obtain a good understanding of legacy equipment and infrastructure
2.	Assess field equipment for capabilities that will be needed to support core Connected Vehicle (CV) components
3.	Embrace the challenges of deploying technologies still at a developmental technological readiness level
Institutional Arrangements	
4.	Have governance agreements in place to promote consistency and shared stakeholder expectations
5.	Look beyond partnerships solely with large businesses
6.	Secure the involvement of top-level decision makers to advocate for your deployment

7.	Establish good relationships with your agency's IT and Telecom groups
8.	Provide adequate incentives to attract driver participation
Supplier Relations	
9.	Utilize Requests for Proposals (RFPs) to scrutinize and select the best suppliers
10.	Utilize multi-vendor outsourcing and source suppliers early to create a collaborative environment
11.	Be mindful of nuances associated with language when working with external parties
12.	Establish contacts with traffic controller software manufacturers
Data Management/Governance	
13.	Assess data collection needs and requirements
14.	Have a plan for how the data will be handled both during and post-deployment
15.	Implement data collection procedures and techniques that reduce the burden on the communications network and account for the limitations of backhaul bandwidth
16.	Plan accordingly for data storage requirements
17.	Adopt a metadata standard that all data providers agree to and comply with
Security	
18.	Address security in all aspects of the CV and agency systems
19.	Maintain a physical separation between CV networks and any tolling networks
20.	Tap limited available vendor and supplier resources to their fullest extent when certifying devices for enrollment in a SCMS
21.	Implement a credential management misbehavior detection feature to address vulnerabilities to cyber attacks, spoofing and malfunctioning equipment
22.	Identify all Provider Service Identifiers (PSIDs) for all applications being implemented prior to enrollment in the SCMS
23.	Initiate message signing requirements for message types without pre-existing security protocols
24.	Provision vehicles with a sufficient number of pseudonym certificates
25.	Implement proper certificate change requirements to prevent vehicle tracking
26.	Refresh application certificates periodically
27.	Return devices to a secure environment for re-enrollment in the SCMS infrastructure
System Architecture/Design	
28.	Design systems using published U.S. standards

29.	Use experienced agile software developers over engineers for developing software applications
Upgrading Existing Infrastructure	
30.	Consider the location of existing ITS and line of sight when selecting sites for the installation of RSUs
31.	Account for a slower rate of installation of RSUs than OBUs as they require dispatch crews
32.	Have integration with the next generation internet standard at the TMC
33.	Apply and update standards conformance where appropriate
34.	Upgrade needed firmware and software on Advanced Transportation Controllers (ATCs)
35.	Update intersection geometry for accurate MAP message generation
Installation of In-vehicle Technology	
36.	Utilize professionals where possible for installations
37.	Recognize that different vehicle types require different hardware and installations processes
38.	Check vehicles for pre-existing safety systems that may interfere with an evaluator's ability to isolate impacts of the CV applications
39.	Be sensitive to the power drawn by in-vehicle devices to avoid vehicle power-drain
40.	Perform appropriate calibration procedures for all onboard technologies
41.	Refine proper antenna placement to reduce communications interferences
Testing	
42.	Arrange a testing location that can accommodate the necessary test runs
43.	Assess GPS accuracy of OBUs in dense urban environments to determine whether a correction is needed
44.	Assess GPS in mobile devices to see whether it is precise enough for pedestrian safety applications
45.	If using Dedicated Short-Range Communications (DSRC), consider purchasing interference tracking equipment to detect potential interference from other users in the 5.9 GHz band that can compromise data exchange
46.	Tune the applications for the proper density and speed of the environment that you are deploying in

2 Considerations for a Robust CV Deployment

2.1 Deployment Planning

This section identifies key insights from Phase 2 of the CV Pilot sites with specific examples of the challenges they faced and their corresponding resolutions. Note that it is assumed that an early deployer has completed the concept development and requirements specification phase prior to advancing to deployment planning.

2.1.1 Assessment of Infrastructure and Organizational Capabilities

The following lessons revolve around identifying the infrastructure an agency currently has versus what infrastructure they will need to deploy a robust connected vehicle environment.

Table 2: CV Pilots' Experiences Related to the Assessment of Infrastructure and Organizational Capabilities

Assessment of Infrastructure and Organizational Capabilities
1. Obtain a good understanding of legacy equipment and infrastructure Agencies are advised to first gather an understanding of what infrastructure is currently in the field before deploying cutting edge technology. Agencies should consider making existing infrastructure and legacy systems part of their traffic solution. For example, integration with existing legacy systems at the Traffic Management Center (TMC) enables the CV environment to become part of the overall management framework. A significant WYDOT pilot achievement in their connected vehicle functionality has been integrating with the WYDOT TMC and other back office systems. For example, an administrator tool was developed to allow operators to identify weather conditions in real-time and note when these results do not align with the Pikalert forecast. This information is passed to the National Center for Atmospheric Research (NCAR) to improve the Pikalert system so that accurate forecasts are used by the performance measurement team to support system evaluation. In addition to the administrator tool, a Roadside Unit (RSU) Monitor subsystem was developed to monitor and report on the status of all RSUs deployed along the I-80 corridor in Wyoming. This software code was made available on the OSADP for other state DOTs to download.
2. Assess field equipment for capabilities that will be needed to support core Connected Vehicle (CV) components The infrastructure required for Dedicated Short-Range Communications (DSRC) based CV includes but is not limited to: DSRC-based Radio Equipment (both Onboard Units (OBUs) and Roadside Units (RSUs)), advanced traffic signal controllers, backhaul communications, data management systems, and security/credential management systems. This investigation should take into account the security requirements of the existing agency systems and networks as well as their change control procedures, and network management systems. The CV infrastructure will need to be integrated with many of the existing systems.

Assessment of Infrastructure and Organizational Capabilities
3. Embrace the challenges of deploying technologies still at a developmental technological readiness level When implementing cutting edge technology, there can often be a lot of hype without follow through. Going into deployment, many of the Pilots were under the impression that the applications were deployment-ready – however this was often not the case. An abundance of time and effort was required to refine the applications. To address the non-deployment ready nature of the applications, New York City explicitly stated in their RFI that they were interested in purchasing turn-key applications, and that any necessary application development would be the responsibility of the vendors. Although WYDOT vendors were tasked with the development of the OBU and RSU applications, the WYDOT team often found themselves having to expend their own resources to trouble-shoot issues and conduct field tests.

2.1.2 Institutional Arrangements

This section describes the institutional arrangements that needs to be made to outline the expectations of partners in terms of service, outcomes and reporting.

Table 3: CV Pilots' Experiences Related to Institutional Arrangements

Institutional Arrangements
4. Have governance agreements in place to promote consistency and shared stakeholder expectations Memorandums of Understanding (MOUs) should be utilized and must clearly define a path for partnership activities, including financial viability, ability to meet delivery and installation targets, specification adherence, and similar items. To promote success, engagement of CV Pilot partners occurred early in the formation of the project design and throughout Phase 2 of the pilot.

Institutional Arrangements

5. Look beyond partnerships solely with large businesses

Many small and medium-sized businesses will be able to be more flexible with accommodating the deployment. Additionally, often in partnerships with smaller businesses, both parties having a common interest in seeing benefits for their local community. However, be cognizant of the more limited depth of staff and resources that smaller organizations may have to offer.

In Wyoming, the team found it easier to get smaller truck partners committed to the Pilot than the larger firms. For the smaller firms, even saving just one accident made participation in the Pilot worthwhile for them.

6. Secure the involvement of top-level decision makers to advocate for your deployment

Agencies should not be afraid to approach the higher-up decision makers at their organizations as they can be your biggest champions. In WYDOT's experiences, the team reached out to WYDOT Director Bill Panos who has since addressed the US Senate committee on intelligent driving systems and the Wyoming Pilot and is now a big proponent of DSRC.

7. Establish good relationships with your agency's IT and Telecom groups

The New York City team cited the NYCDOT IT department as the biggest partner they had to get involved with. As the pilot had to be integrated with NYCDOT's IT systems, NYCDOT's IT group wanted to ensure that access to their resources would be protected and thus took great interest in supporting the IT systems associated with the pilot. The WYDOT team had support not only from the WYDOT Telecommunications staff but also from a number of other WYDOT groups including GIS/ITS, Traffic Engineering, Fleet Operations, Highway patrol, Procurement Services and Program Administration.

8. Provide adequate incentives to attract driver participation

When recruitment for drivers of private vehicles was lagging, THEA updated the toll discount incentive from 30% to 50% and widened the pool of potential participants to allow non-Reversible Express Lanes (REL) drivers to participate in the study. The Tampa team did run into some challenges with participants cancelling or not showing up for their installation appointments, although most of the time these scenarios stemmed from participants simply forgetting about their appointment. Many potential participants attributed their reluctance to joining the study to the potential for the non-standard equipment the Pilot would require be installed in their vehicle to reduce the vehicle's trade-in value.

2.1.3 Supplier Relations

This section describes engaging with project partners and device vendors.

Table 4: CV Pilots' Experiences Related to Supplier Relations

Supplier Relations
9. Utilize RFPs to scrutinize and select the best suppliers It is suggested that agencies conduct multiple technical scans using request for proposal (RFP) documents that require on-the-road testing to identify promising suppliers who can meet system, cost and project timing requirements. Since this technology cannot be purchased off the shelf yet, the New York City pilot did a Request for Expression of Interest (RFEI) demonstration/evaluation, where two vendors were eventually selected as their Aftermarket Safety Device (ASD) suppliers. The winner of the New York City RSU bid resulted in award to the same vendor partnered with THEA's project from very early on in the Pilots. Although THEA did not go through an RFP process, NYC's selection of the same vendor as THEA validated THEA's up-front research. WYDOT on the other hand did not utilize RFPs in the procurement of their devices. Some of their procurements were sole-source and others were extensions of existing contracts WYDOT already had with current partners.
10. Utilize multi-vendor outsourcing and source suppliers early to create a collaborative environment Early sourcing of suppliers is key to understand how system requirements are implemented in the design and to allow for participation in developing open specifications. To reduce risk, it is wise to select more than one supplier in the event that a supplier is unable to commit to previous agreements. With multiple selected vendors, an agency can disqualify any non-performing vendors (if needed) and continue with the performing vendor for the full complement of units. During the implementation phase, both the New York City and Tampa Pilots had to deal with suppliers backing out. In New York City's case, they had originally selected two OBU suppliers, however, one of the suppliers could not sign the final contract in good conscience as they did not think they could sufficiently meet NYC's design specification requirement for the vehicle's positioning accuracy. Similarly, one of Tampa's initial vendors had to withdraw because they could not provide the support outlined in the contract.

Supplier Relations
11. Be mindful of nuances associated with language when working with external parties Not everyone has the same common understanding of terminology. In discussion with their vendors, the THEA team found that vocabulary between organizations do not always match. THEA went back and forth with their device manufacturers for six months about why they would not be able to deploy THEA's planned *Curve Speed Warning* application. It turned out that *Curve Speed Warning* meant something else to the manufacturer, so THEA ended up renaming the application *End of Ramp Deceleration* – which the vendor was in agreement with. THEA cited that if they had known all along that it was just a misunderstanding of the application name, the issue would have been resolved in a few hours and saved them six months of hassle.
12. Establish contacts with traffic controller software manufacturers As the standards for connected vehicle systems evolve overtime, the software of the traffic controllers will likely need to be updated. Having an established relationship in place with the software manufacturers will enable them to easily access the devices to make the necessary changes when needed.

2.1.4 Data Management / Governance

This section describes the sensitivities with the type and amount of data that needs to be collected and the need for a data governance framework that outlines how data will be collected, managed and archived.

Table 5: CV Pilots' Experiences Related to Data Management / Governance

Data Management / Governance
13. Assess data collection needs and requirements While the CV system can provide terrabytes of data, it is important to have a good understanding of what data is needed for what purposes and where. Data collection must be scalable and sustainable and should provide value during system operation. For example, recording and uploading every Basic Safety Message (BSM) the RSU hears when vehicles are in range in an urban environment to a TMC will typically result in over 500 BSMs from each instrumented vehicle within range of an RSU traveling at 25-30 MPH. If the goal is to compute travel times between RSUs – then a single vehicle will result in the TMC receiving on the order of 1,000 BSMs under free-flow conditions (and this can easily double or triple if the vehicle is stopped). In reality, to compute travel times, the TMC only needs a single BSM from a configured zone within each intersection to begin the matching operation and measurement of travel times. The result is a reduction in 99.8% of the network data flow, and a reduction in processing at the TMC by a similar amount. Further, consider the scalability problem with the processing for travel time data. If every vehicle were equipped, then the TMC's task is unmanageable at a reasonable cost. The NYC pilot project had to address these issues due to the expected density of CV equipped vehicles, the limitation of the backhaul bandwidth, and a limit to the processing power at the TMC. Travel times are a critical element to the City's adaptive control system, and by using the RSU to determine when the vehicle is within a small zone at the intersection makes it possible to compute the travel times. Likewise, as one looks to more sophisticated local monitoring, the combination of the RSU and the Advanced Transportation Controllers (ATC) can convert the data streams to usable information such as queue lengths such that it can share data with the TMC to improve the allocation of phase time, progression, and platoon management.

Data Management / Governance

14. Have a plan for how the data will be handled both during and post-deployment

Connected vehicle, mobile device, and infrastructure sensor data captured during the operational phase of the Pilot's was required to be shared with the independent evaluator in support of the broader evaluation. In addition, data stripped of personally identifiable information (PII) was required to be posted on the ITS Public Data Hub. However, uncertainties regarding data ownership led to sites concerns over subpoenas. After some back-and-forth around the issue, specific language was developed that clarified protections for the data. All CV data sent to the IE was sworn to protection from PII disclosures and the potential to expose privacy-related tracking information.

Regarding the fate of the data post-Pilots, the USDOT plans to follow the standard data access and retention contract language for JPO-funded projects, which states that JPO-funded data should be retained in a research data access system for two years past the date of original data collection. If there proves to be sufficient value in retaining the data past that point, it will be done on a case-by-case basis. This could include transferring the data to a more persistent operational archive.

15. Implement data collection procedures and techniques that reduce the burden on the communications network and account for the limitations of backhaul bandwidth

All municipal systems within New York City utilize the New York City Wireless Network (NYCWiN), limiting the bandwidth that the NY CV Pilot had access to. While the Tampa and Wyoming pilots are collecting vehicle data continuously, the NYC Pilot is only doing event-based data collection to address these limitations. Whenever a configurable event occurs (e.g. hard breaks, steering turns or hard accelerations), all BSMs before and after an event for a configurable amount of time are combined and encrypted into what becomes an “event” record.

CV infrastructure naturally provides the opportunity for edge processing and the aggregation of CV information to foster better mobility. NYC looked to incorporating edge computing concepts into their data management plans to further address their needs for a more scalable data collection. As opposed to having all data processing occur at the TMC, New York City designed their system architecture to have some data processing occur at “edge” devices (RSUs, OBUs). By performing local processing at the edge instead of streaming all the data to a central cloud for processing, NYC was able to reduce the amount of bandwidth used.

Data Management / Governance
16. Plan accordingly for data storage requirements Preliminary vehicle, mobile device and infrastructure data estimates should be calculated early on to determine the data storage systems needed (including CPU and disk needs). Note that the estimate for interactions between CVs is highly dependent on how often connected vehicles will be traveling within range of each other and interacting. Note that fleet vehicles may have higher daily operational hours than private passenger vehicles and produce proportionally more data. During the data collection period, the magnitude of raw and processed data volume should be closely monitored over time to anticipate and respond to any needed data storage needs, such as increasing storage at the TMC or changing the frequency at which devices upload data.
17. Adopt a metadata standard that all data providers agree to and comply with Metadata standards defining what needs to be included in the metadata associated with a data set should be adopted for all data that is uploaded for evaluation/public consumption. Uploads of preliminary sample data to USDOT's Secure Data Commons (SDC) Portal, a cloud-based analytic sandbox, was unorganized and lacked critical data dictionaries that the independent evaluator (IE) needed. To prevent further undocumented data in the SDC, the IE eventually incorporated a "form" of contextual data that the sites were required to fill out for every new table or data type uploaded to the platform.

2.1.5 Security

The section addresses changes agencies may have to make to their existing systems and/or operations to accommodate the security needs of CV technology. Emphasis is particularly placed on the utilization of a Security Credential Management System (SCMS) that uses Public Key Infrastructure (PKI) to employ encryption and certificate management to facilitate trusted communication between the vehicles and the surrounding infrastructure.

Table 6: CV Pilots' Experiences Related to Security

Security
18. Address security in all aspects of the CV and agency systems Recognize that the security requirements of the system extend to the agency's networks and computer systems and will likely require changes to existing systems and/or operations. To address the security needs of CV technology, the Pilots made numerous changes to their security procedures regarding: a. Operations – password control (strength) and expiration, physical access to facilities such as TMCs, encryption of databases b. Communications – upgrades to the ITS environment to provide increased security – especially where NTCIP is concerned; VPN tunnels, DTLS and TLS protocols using x.509 certificates; disabling local access ports without security. c. Maintenance – requiring authentication of field personnel in real time when replacing failed devices; devices have a collection of enrollment certificates; keypad interactions to use USB access to reload and re-initialize the device.
19. Maintain a physical separation between CV networks and any tolling networks For THEA, an agency that develops and owns toll highways, it was critical that the CV operations and data be kept separate from their revenue-producing toll operations and data. THEA purchased and implemented a firewall to ensure that a complete separation of the tolling network as a general standard would be maintained throughout the CV Pilot.
20. Tap limited available vendor and supplier resources to their fullest extent when certifying devices for enrollment in a SCMS One area that appeared to be more challenging and time consuming than originally envisioned was the CV certification process. Vendors supporting the CV Pilot deployments were the first group to attempt certification. As a result, there were uncertainties and risks related to certification that arose, which had to be managed and mitigated by both CV Pilot deployments and the device vendor community. To the extent that these factors were a barrier to timely progress toward deployment and operations, sites were encouraged to work with partners, suppliers, and vendors to establish clear priorities and identify critical path items and resource constraints and work holistically to maintain continued progress. In particular, dialogue with the SCMS vendor facilitated an understanding of what testing and certification-related results were critical predecessors to deployment and operations, and what items could be addressed incrementally during operations.

Security

21. Implement a credential management misbehavior detection feature to address vulnerabilities to cyber attacks, spoofing and malfunctioning equipment

The security credential management system (SCMS) does not currently have a standard Misbehavior Detection and Certificate Revocation List (CRL) distribution mechanism – both of which are essential to maintain the security of the CV infrastructures.

Recognizing the absence of Misbehavior Detection and a CRL, the New York City team chose to load only one week's worth of future certificates onto the OBUs (as opposed to the maximum three-year supply) to minimize the potential impact of compromised units.

It should be noted that USDOT is currently facilitating close coordination among device vendors and the SCMS provider to deliver the software utilities for an early, minimum viable Misbehavior Detection capability to support the CV Pilot Deployment sites.

22. Identify all Provider Service Identifiers (PSIDs) for all applications being implemented prior to enrollment in the SCMS

Each enrollment certificate is associated with a particular application that is mapped to a particular Provider Service Identifier (PSID) (enrollment certificates cannot have an empty PSID field). For this reason, users must decide on what applications the device will be supporting and their corresponding PSIDs before enlisting in enrollment. If additional applications are added later on, devices will have to go through the enrollment process again, which requires additional security mechanisms that may require bringing a device to a special secure facility. This was something that the Pilots were made aware of and have had to plan their operational deployments around.

23. Initiate message signing requirements for message types without pre-existing security protocols

The SAE V2X Security technical committee is currently working to develop Service Specific Profiles (SSPs) specifications for a number of PSIDs, however in the meantime there is currently no standard SSP guidance for a number of PSIDs including the PSIDs utilized for TIM, SPAT and MAP. Following coordination on deciding what PSIDs that they would be using, the Pilots worked to develop their own independent SSPs for those PSIDs where official guidance was missing. Those SSPs are open source and available upon request. They provide a good starting point for other deployment agencies utilizing those PSIDs.

Security

24. Provision vehicles with a sufficient number of pseudonym certificates

The sites' SCMS allocated light vehicles with just 20 certificates per week to use during their period of validity changing every 5 minutes or 2 KM – whichever came first.

The NYC Pilot was concerned that 20 certificates per week would be insufficient to ensure anonymity for their taxi fleets that are in service an average of 14 hours per day. To provide better protection against "tracking", the NYC team boosted the number of certificates provided to each device to 60 certificates per week. Note that while this is a change SCMS vendors can support, it would likely not be the default option. Deployment agencies should identify these types of use cases early and work with their SCMS vendor to address those use cases.

25. Implement proper certificate change requirements to prevent vehicle tracking

During development, the New York City Connected Vehicle Pilot Deployment team identified an issue with the SAE J2945/1 Standard's Certificate Change (CERTCHG) requirement criteria that was potentially putting the privacy of their participants at risk.

The CERTCHG requirement calls for certificates to be changed every five minutes but contains an exception involving the "absolute distance" from the previous certificate change location. The exception states that a certificate change does not occur should the System be "separated by less than 2 kilometers in absolute distance from the location at which the last certificate change occurred." Under the current absolute distance assumption, a vehicle traveling within an urban grid network (such as a taxi in NYC) may not trigger the certificate change mechanism.

The team concluded that the "absolute distance" was not the proper criteria for an exception for their Pilot, as it was still possible for a vehicle to operate in a large area for an extended time period and not be required to change its certificate. The NYC team decided to implement a change mechanism that required certificates to change every 2 KM traveled or every 5 minutes – whichever comes first.

26. Refresh application certificates periodically

Application certificates, which is what RSUs use to advertise and provide their services, are only valid for a limited time (usually one week). These types of certificates are not pre-generated for future validity periods like pseudonym certificates and must be requested on a week-to-week basis. Deployment agencies need to have mechanisms in place to allow RSUs to connect to the SCMS on at least a weekly basis in order to request and download new certificates.

Security
27. Return devices to a secure environment for re-enrollment in the SCMS infrastructure While certificates can be downloaded while a vehicle is on the go, devices must be returned to a secure environment for re-enrollment. Ideally enrollment should occur in the same environment where maintenance is being performed. Another option is to have a process in place to have the removed devices for suspected improper operation sent back to the vendor for repair and validation or replacement of the enrollment certificates.

2.2 Design/Build/Test

This section identifies components related to designing, building and testing a CV system that a deployer would need to be concerned with and the related experiences/lessons learned of the CV Pilot sites.

2.2.1 System Architecture/Design

This section summarizes the need to: build to standards, develop/enhance applications to meet deployment-specific needs and interface with existing legacy systems.

Table 7: CV Pilots' Experiences Related to System Architecture/Design

System Architecture / Design
28. Design systems using published U.S. standards Agencies considering CV deployments are highly recommended to use the most recently published ITS standards; any use of unpublished standards or standards in progress is strongly discouraged. If a U.S. standard does not exist, it is suggested to design using available international standards. In the event that no relevant standard exists, agencies are advised to use other relevant documents including USDOT's V2I Hub Deployment Guide and DSRC RSU Specifications document v4.1 as initial points of reference.

System Architecture / Design
29. Use experienced agile software developers over engineers for developing software applications While ITS systems used to be mostly hardware-based, software has been an increasingly large part of such systems for the past few decades. Software engineering greatly differs from traditional ITS engineering that focuses on long-term planning and intricate documentation. Due to the frequently changing nature of the project, the CV Pilots utilized experienced software developers that relied on agile software development processes.

2.2.2 Upgrading Existing Infrastructure

This section outlines any changes needed to prepare roadways and intersections for the installation of CV devices.

Table 8: CV Pilots' Experiences Related to Upgrading Existing Infrastructure

Upgrading Existing Infrastructure
30. Consider the location of existing ITS and line of sight when selecting sites for the installation of RSUs Wherever feasible, CV equipment should be collocated at closed-circuit television (CCTV), dynamic message sign (DMS) or traffic signal locations sites to take advantage of the existing roadside infrastructure, power and communications equipment. RSU mounting locations should also be optimized to achieve clear line of sight free of radio frequency (RF) signal path interference from trees, bridges, overpasses and other structures. In New York City, many signal poles and mast arms lay behind the building face line, therefore limiting the line-of-site. Field inventories identified 15% of the installations would require additional infrastructure changes (e.g. additional communications gear, new mast/luminaire arms, controller relocation) to place the RSU with adequate line-of-site.

Upgrading Existing Infrastructure

31. Account for a slower rate of installation of RSUs than OBUs as they require dispatch crews

For the New York City pilot, the RSU installations were performed by NYCDOT field crews at a rate of about two per day per crew, a slower rate than what the NYC team had anticipated. The installation consisted of installing the surge suppressor on the ethernet to the RSU, adding the PoE inserter, bolting on the RSU, installing the ethernet through the pole and mast arm to the bottom of the RSU – and finally powering up the units and letting the system configure and start operation.

Configuring the RSU is currently a manual process and prone to errors, however that process will eventually be automated and managed by the TMC so that it will be truly plug-and-play.

32. Have integration with the next generation internet standard at the TMC

DSRC CV deployments utilize IPv6 messaging. Though IPv6 can coexist with IPv4, IPv6 is the best answer to sufficiently address speed, security, efficiency and operational ease desired for the operation of CV systems. During transition from IPv4 to IPv6, many of the Pilots' network devices did not support IPv6. Some devices were able to apply simple firmware updates, but many others required the purchase of new hardware.

In summary, early deployers should be cognizant that the most recent version of the internet protocol is not offered on every network natively and that there may be lengths in the network that do not support IPv6 that you may have to plan around.

33. Apply and update standards conformance where appropriate

Though there is no USDOT RSU/OBU standard, all RSUs and OBUs used for deployment should conform to USDOT specifications as closely as possible wherever they exist; additionally, all messages should conform to the latest versions of SCMS, SAE J2735, SAE 2945/x, IEEE 802.11p, IEEE 1609.x, NTCIP 1202, NTCIP 1103, ISO 19091 and related standards. Vendors are expected to work with the deployer agency to determine the appropriate version for each standard/device specification that has been accepted for general use.

Upgrading Existing Infrastructure
34. Upgrade needed firmware and software on Advanced Transportation Controllers (ATCs) The RSU shall maintain a system clock based on timing information from a local positioning system. GPS typically serves as the primary time source and the Network Time Protocol (NTP) server is intended to be available as a secondary, backup time source in the event that the RSU loses GPS. To support this, it is necessary that the firmware of the ATCs be upgraded to provide SPaT and time clock information directly to the RSU.
35. Update intersection geometry for accurate MAP message generation The OBUs compare GPS location readings on the vehicle against the MAP messages' static intersection geometry data to determine a vehicle's approach. As it is critical that the vehicle have an exact reference point within the intersection, agencies must ensure the MAP data is properly coded and that the Uper Hex code is validated for field testing.

2.2.3 Installation of In-Vehicle Technology

This section describes experiences with mounting and installing CV devices along roadways and inside vehicles.

Table 9: CV Pilots' Experiences Related to Installation

Installation of In-Vehicle Technology
36. Utilize professionals where possible for installations The OBU installations should be done in a professional setting with certified vehicle mechanics to prevent unintentional modifications or damage to participants' vehicles. In particular, deployments with a large number of vehicles should utilize standardized installation and checkout procedures to ensure efficiency. • NYC used the City's mechanical installers for the installations of the OBUs on the NYCDOT fleet vehicles. NYC planned on contracting out the installation of their onboard devices for the nearly 8,000 vehicles to outside professionals after concluding that the City's mechanical installers had insufficient resources to address the fleet size within the time constraints. • The THEA team partnered with nearby Hillsborough Community College (HCC) to use their Master Mechanic Program facility and staff to install the OBUs, giving the students real-world experience and helping reduce labor costs. • WYDOT and their partner Trihydro were each responsible for installing the OBUs in their own vehicles, though Trihydro contracted with a local audio installer for the installations. WYDOT staff were used to install the OBUs in the WYDOT fleet vehicles.
37. Recognize that different vehicle types require different hardware and installations processes There is no installation methodology that applies across-the-board as each vehicle type has different needs. • NYCDOT elected to install an audio-only human-machine interface (HMI) in the participating vehicles after stakeholders indicated that they already had several other screens competing for their attention. • The THEA Pilot on the other hand included an audio and visual HMI that displayed messages on the driver's rearview mirror. The configuration in Tampa's streetcars was particularly unique as they required 2 OBUs and HMIs (one on each end) for when the streetcar reverses the direction of travel and the driver moves to the opposite side. • The WYDOT Pilot's HMI was capable of audio and visual alerts as well as displaying different messages to drivers. The semi-trucks necessitated that the OBUs and associated hardware be installed on the cab of the trucks instead of the trailer since the trailers are always changing.

Installation of In-Vehicle Technology

38. Check vehicles for pre-existing safety systems that may interfere with an evaluator's ability to isolate impacts of the CV applications

If an evaluation is being performed, it is strongly recommended that aftermarket CV technologies not be installed on vehicles that have existing safety system (such as Mobileye or Kaptyn systems) since many of the warning types will be redundant with the CV safety applications. Having redundant technologies that serve the same purpose on the CV equipped vehicles will interfere with an evaluator's ability to isolate impacts of the CV applications.

NYCDOT confirmed that their partners Metropolitan Transportation Authority (MTA) and the Taxi and Limousine Commission (TLC) had some vehicles fit with pre-existing safety systems. The NYC Pilot requested that MTA vehicles with these systems be excluded from the Pilot. However, the same blanket-ban was not able to be made for the TLC vehicles as the taxis have different owners. To address the issue of redundant safety systems in the TLC vehicles, the NYC team provided installers with a pre-install checklist that included a check item for pre-existing safety systems. If such pre-existing safety system were found during installation, an OBU was not installed on the vehicle.

39. Be sensitive to the power drawn by in-vehicle devices to avoid vehicle power-drain

Fleet vehicle owners involved in the pilot originally desired a zero quiescent current draw – though this was not feasible with the selected devices. As a result, the pilots restricted the current-draw of their OBU vendors (NYCDOT restricted their onboard unit vendors to a current draw of 25 micro-amps).

To prevent subsequent maintenance issues, it was standard operating procedure for the Pilots to first check the vehicle's electrical system (including battery and alternator/charger) before installing any CV equipment and installers would not proceed if any issues were found. Additionally, crews would cease installation when any vehicle's indicator lights (e.g. check engine) were activated.

40. Perform appropriate calibration procedures for all onboard technologies

Following the installation of the devices in private vehicles, the Tampa installation crews drove the vehicles in "figure 8s" to calibrate the accelerators in the OBUs. However, this method was not a practical approach for the NYC vehicles, especially with their MTA buses. NYC later proposed mounting an OBU on a gimbal with a known orientation for proper calibration. Additionally, NYC had their vendors provide a calibration indication to their device's system logs at each start-up.

Installation of In-Vehicle Technology
41. Refine proper antenna placement to reduce communications interferences The location of the antenna is critical to ensure continuous wireless communication without loss of signal strength. The New York City and Tampa teams found that for light-vehicles, antennas mounted near the rear-center of the rooftop was most ideal. However, large vehicles, such as the semi-trucks that the WYDOT pilot installed onboard units on, often have “self-blocking” physical elements that obstruct the vehicle’s own DSRC antennas from direct line of sight with other vehicles. This resulted in “shadows” for the Wyoming vehicles that prevented remote vehicles from properly communicating with the trucks. To alleviate this effect, the Wyoming team worked with USDOT’s communication experts to perform numerous tests in Wyoming and at the Aberdeen Proving Grounds. The testing concluded that the effect of the DSRC shadows could be best alleviated by mounting the antennas on the side mirrors of the semi-trucks.

2.2.4 Testing

This section summarizes the challenges uncovered by the sites during testing of the technology and what future deployers should be conscious of.

Table 10: CV Pilots’ Experiences Related to Testing

Testing
42. Arrange a testing location that can accommodate the necessary test runs Testing should occur in a closed-environment that is sufficiently large. • NYCDOT made available a test location within the Aqueduct Racetrack parking lot to demonstrate their CV applications. • Through partnerships, WYDOT was able to perform testing on tracks owned by the Office of Emergency Management. • THEA was able to close parts of the Selmon Expressway for the testing and demonstration of their CV technology.

Testing

43. Assess GPS accuracy of OBUs in dense urban environments to determine whether a correction is needed

New York City is known for its "urban canyons" which provide a challenging environment for GPS technology that is often limited to open sky. As a result, additional techniques were required in the OBUs positioning algorithms to provide the accuracy needed for many of the V2V and V2I safety applications to function properly. Such augmentation of vehicle positioning was needed to provide continuous access to GPS positioning data so that the safety applications could continue operating while the connected vehicles passed under bridges, elevated roadways, through tunnels etc. while navigating the typical Manhattan streetscapes and traffic environment. The NYC Pilot vendors introduced a combination of supporting techniques to improve location accuracy, including:

- Dead reckoning
- CAN bus integration for speed information
- Inertial Measurement Unit (IMU) integration
- RSU time-of-flight feature.

44. Assess GPS in mobile devices to see whether it is precise enough for pedestrian safety applications

An initial demonstration of New York’s Personal Information Device (PID) and its associated Mobile Accessible Pedestrian Signal System application in Manhattan experienced issues with the continuity of the PIDs’ GPS signal as the result of frequent loss of satellite signal. To address for the devices’ inaccurate GPS readings, NYC resorted to installing traditional ITS pedestrian detection equipment that utilized infrared cameras.

Similarly, during testing of Tampa’s Pedestrian Crossing (PED-X) smartphone application, the mobile devices were unable to determine the pedestrian’s location and speed with sufficient accuracy,.e.g. being unable to distinguish stepping into the street from standing on the sidewalk, leading to numerous false alarms. To correct this, THEA modified the vehicular side of the PED-X application to collect pedestrian location data from LIDAR sensors installed near the crosswalk that could provide more precise geo locations.

Testing

45. If using Dedicated Short-Range Communications (DSRC), consider purchasing interference tracking equipment to detect potential interference from other users in the 5.9 GHz band that can compromise data exchange

Though the FCC originally allocated the 5.9 GHz band for DSRC-based ITS applications, in 2013 the FCC proposed allowing unlicensed devices to share the spectrum with primary users as long as they were not found to be interfering with the primary DSRC users. During the deployment period, THEA detected and tracked down an interference on their DSRC communication channels coming from a local amateur radio operator.

While the ham radio could not receive DSRC radio messages due to the far lesser range of DSRC, THEA's DSRC radio would receive the ham radio messages, causing the DSRC radio to consider the channel "busy" and not "clear to send". The additional signal on THEA's channels impacted the performance of their equipment in terms of data exchange and back haul speed, with testing indicating a degradation in data uploads by up to 50%. Upon review of these findings, Florida Department of Transportation (acting as the enforcement agency) ordered the amateur radio operator to vacate the channel.

Due to the scale of the NYC deployment, the NYC team invested in the purchase of sophisticated interference checking and RF spectrum analysis equipment. This equipment will allow them to locate and quantify field interference with GNSS and DSRC and to confirm the failures of the OBU and RSUs in the event of a suspected failure.

46. Tune the applications for the proper density and speed of the environment that you are deploying in

In the absence of standard performance requirements for applications, it became evident that each CV Pilot vendor had their own interpretation and tuning of applications deployed. For NYC, it was key that the applications be tuned for urban density and speeds to balance proper alerts versus false alarms. This required:

- Consistent expectations for the drivers about the sensitivity of the applications across all vendors
- Performance tradeoffs
- Staging open sky testing (for baseline) and urban canyon testing.

3 Conclusions and Next Steps

At the time of writing (Fall 2018), the CV Pilot sites are wrapping up Phase 2 (Design/Build/Test) of the Connected Vehicle Pilot Deployment Program – though not without having experienced significant technical and non-technical challenges along the way. Phase 2 required substantial CV engineering and development, resulting from the still maturing state of key applications, a dynamic security credential management environment and challenges in radio-frequency interference.

One should keep in mind that the CV Pilot sites are "piloting" this technology – and are doing so on a scale covering all elements of the surface transportation system and involving numerous stakeholder partnerships and data captured from multiple sources. As a result, some of the challenges documented in this paper were simply the result of the low technological maturity of the systems being deployed and are expected to be mitigated in the future as connected vehicle and supporting technologies mature.

Each CV Pilot, while unique regarding size, features, and functionality to be deployed, is a prime example of a large "system of systems" entailing complex design, procurement, specification, build, integration, and testing principles. It is imperative that agencies considering CV deployment have a deep knowledge and understanding of systems engineering concepts prior to designing and building such systems. Further, data management procedures for the collection, processing and storage of data should be scalable and sustainable while still providing value during system operation. Deployers are also encouraged to compose requirements specifications for the software, firmware and hardware that will be procured outside the development team to prevent additional cost and schedule risks. Though there are many challenges associated with integrating and testing large disparate systems, addressing these needs early in the project lifecycle is guaranteed to reap significant project resource savings over the life of the system.

In the next phase of the Connected Vehicle Pilot Deployment Program, the tested connected vehicle systems will be operated and maintained for a minimum 18-month period. During this phase, the Pilot sites will measure the impacts of their deployments – including improved safety, improved personal mobility, enhanced economic productivity, reduced environmental impacts and transformations to public agencies' operations.

Appendix A. Acronym List

Acronym	Definition
ASD	Aftermarket Safety Device
ATC	Advanced Transportation Controller
BSM	Basic Safety Message
CAN	Controller Area Network
CCTV	Circuit Television
CERTCHG	Certificate Change
COT	City of Tampa
CPU	Central Processing Unit
CRL	Certificate Revocation List
DMS	Dynamic Message Signs
DOT	Department of Transportation
DSRC	Dedicated Short Range Communications
DTLS	Datagram Transport Layer Security
FCC	Federal Communications Commission
FDOT	Florida Department of Transportation
FHWA	Federal Highway Administration
GIS	Geographic Information Systems
GNSS	Global Navigation Satellite Systems
GPS	Global Positioning System
HART	Hillsborough Area Regional Transit

Acronym	Definition
HCC	Hillsborough Community College
HMI	Human Machine Interface
I-80	Interstate 80
IEEE	Institute of Electrical and Electronics Engineers
IMU	Inertial Measurement Unit
ITE	Institute of Transportation Engineers
ITS	Intelligent Transportation Systems
JPO	Joint Program Office
MAP	Metropolitan Atlanta Performance
MTA	Maryland Transit Administration
NCAR	National Center for Atmospheric Research
NTCIP	National Transportation Communications for ITS Protocol
NTP	Network Time Protocol
NYCDOT	New York City Department of Transportation
OBU	Onboard Unit
OSADP	Open Source Application Development Portal
PED-X	Pedestrian Crossing
PID	Pedestrian Information Device
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PSID	Provider Service Identifiers
REL	Reversible Express Lanes
RFEI	Request for Expressions of Interest (RFEI)

Acronym	Definition
RFI	Radio Frequency Interface
RFP	Request for Proposal
RSU	Roadside Unit
SAE	Society of Automotive Engineers
SCMS	Security Credential Management System
SDC	Secure Data Commons
SPAT	Signal Phase and Timing
SSP	Service Specific Profiles
THEA	Tampa Hillsborough Expressway Authority
TIM	Traveler Information Message
TLC	Taxi and Limousine Commission
TLS	Transport Layer Security
TMC	Transportation Management Center
USB	Universal Serial Bus
USDOT	U.S. Department of Transportation
V2I	Vehicle-to-Infrastructure
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Device
VPN	Virtual Private Network
WYDOT	Wyoming Department of Transportation

1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free “Help Line” 866-367-7487

www.its.dot.gov

FHWA-JPO-18-712

U.S. Department of Transportation