Connected Vehicle Pilot Deployment Program Phase II

Data Privacy Plan – Tampa (THEA)

www.its.dot.gov/index.htm
Final Report - Feb 2017
FHWA-JPO-17-461

U.S. Department of Transportation

Produced by Tampa Hillsborough Expressway Authority (THEA) CV Pilot Team
U.S. Department of Transportation
Intelligent Transportation Systems (ITS) Joint Program Office (JPO)

Notice

1. Report No. **FHWA-JPO-17-461**	**2. Government Accession No.**	**3. Recipient's Catalog No.**
4. Title and Subtitle Connected Vehicle Pilot Deployment Program Phase II Data Privacy Plan - Tampa Hillsborough Expressway Authority (THEA)		**5. Report Date** February 2017 **6. Performing Organization Code**
7. Author(s) Steve Johnson, HNTB, Linda Rolfes, HNTB, Victor Blue, HNTB, Stephen Reich, CUTR		**8. Performing Organization Report No.** Task 2 C Report
9. Performing Organization Name and Address **HNTB CORPORATION** One Tampa City Center, 201 N. Franklin St., Suite1200, Tampa, FL 33602 Tampa Hillsborough Expressway Authority, 1104 E Twiggs St #300, Tampa, FL 33602		**10. Work Unit No. (TRAIS)** **11. Contract or Grant No.**
12. Sponsoring Agency Name and Address U.S Department of Transportation 1200 New Jersey Ave, SE Washington, DC 20590		**13. Type of Report and Period Covered** Revised Draft **14. Sponsoring Agency Code**

15. Supplementary Notes

Govind Vadakpat (AOR), Sarah Tarpgaard (AO)

16. Abstract

The Tampa Hillsborough Expressway Authority (THEA) Connected Vehicle (CV) Pilot Deployment Program is intended to develop a suite of applications that utilize vehicle to infrastructure (V2I) and vehicle to vehicle (V2V) communication technology to reduce traffic congestion, improve safety, and decrease emissions using the authority provided by the United States Department of Transportation within the signed cooperative agreement (DTFH6116H00025). These CV applications support a flexible range of services from advisories, roadside alerts, transit mobility enhancements and pedestrian safety. The Pilot will be conducted in three Phases. Phase II includes the design, development, and testing phase.

This document presents the Data Privacy Plan (DPP).

It provides guidance material regarding security and privacy for the THEA Deployment Participant Data. The document discusses the policies and procedures required to affect the protection of PII (Personally Identifiable Information) as outlined in the Phase I Security Management Operating Concept (SMOC). It is important to note that security requirements in the DPP are developed to address privacy specifically and not security as a whole. Additional references for security analyses, V2V security, the Security Credential Management System, and connected vehicle application security needs are included in the SMOC and this document focuses on the controls to be utilized for protecting PII.

17. Key Word. Connected Vehicle Technologies, PII, SPII, Cybersecurity, Privacy, Phase II, V2I, V2V, V2X, SCMS, DPP	**18. Distribution Statement**		
19. Security Classif. (of this report) **Unclassified**	**20. Security Classif. (of this page)** **Unclassified**	**21. No. of Pages** 50	**22. Price**

Form DOT F 1700.7 (8-72)
authorized

Reproduction of completed page

Acknowledgements

We acknowledge the timely and high-quality support offered by U.S. DOT and the support contractor, Noblis.

Table of Contents

Executive Summary

The Data Privacy Plan (DPP) provides details about how to ensure the privacy of Pilot participants for the Tampa Hillsborough Expressway Authority (THEA) CV Pilot. The intended audience is USDOT, JPO; transportation researchers; Salus IRB and future CAV/SmartCities deployers.

This document applies to all registered participants including privately owned vehicle drivers and pedestrians having the application on a mobile device. The document also covers, in limited scope, the non-participant transit drivers. All Pilot team members, partners and sub-consultants are included and governed by this DPP. Where applicable, contract and other acquisition-related documents include privacy statement language.

Scope and Approach

The THEA CV DPP relies and builds upon the analyses, conclusions and guidelines established in the Phase I Security Management Operating Concept (SMOC) (THEA, Task 3, SMOC, April 2016). The THEA CV SMOC includes overviews for Vehicle-To-Everything (V2X) system security and privacy for communications, access, hardware, software, and operating systems. The SMOC also includes a V2X system threat assessment, analysis of application information flows and device classifications per Federal Information Processing Standard (FIPS) 199 and 200, and identified security controls for each device class per National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 cross checked against International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 15408 Common Criteria (CC) security controls.

The THEA team approached DPP development based on the SMOC; as well as information from (Official (ISC)² Guide to the CISSP CBK, Fourth Edition, 2015); (Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, FIPS PUB 199, 2004); (Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, FIPS PUB 200 , 2006); (National Institute of Standards and Technology, NIST Special Publication 800-60 Revision 1, 2008) and (National Institute of Standards and Technology, NIST Special Publication 800-53 Revision 4, 2013)

This Data Privacy Plan is a companion document to the SMOC created in Phase I. Whereas the SMOC sets forth a “concept” or approach to addressing security as a whole, this document provides guidelines and controls that will be used to accomplish the protection of personally identifiable data (PII).

The DPP covers the following major sections:

1. Background – Brief discussion of the existing state of affairs regarding security and privacy.
2. Data Privacy Defined – Discussion of the categories of privacy as used in this document.
3. Requirements – Discusses and validates the need to collect the participant data and other potential PII.
4. Security Controls for PII – Provides list of and info about the security controls that will be utilized for each category of data.
5. The Role of the IRB – Provides information on the IRB selected and their role in protecting participants and PII.
6. Support for the Independent Evaluator (IE) – Discusses the role of the independent evaluator, the support to be provided by the Pilot team and the processes for scrubbing PII from data prior to submittal to the IE.

1. Background

The Data Privacy Plan provides details about how to ensure the privacy of Pilot participants for the Tampa Hillsborough Expressway Authority (THEA) CV Pilot.

The DPP describes the actions that will be taken by the team during the Pilot Deployment to protect the privacy of users, guard against potential breaches of the system, and prevent unauthorized use of the participant data and other PII. The DPP outlines privacy considerations and how privacy by design is built into the Security Credentials Management System (SCMS) Proof of Concept (POC). Where privacy is not sufficiently addressed by the SCMS POC design, this DPP explains additional actions that will be taken by the Pilot team to increase privacy, such as the protection of participant data used for CV Pilot administration purposes and the use of sanitization algorithms for vehicle situation data as necessary. These sanitization algorithms are part of the filtering/scrubbing process described in Sections 3, 4 and 6, used to protect against exposure of participants' PII.

1.1. Current Internet of Things (IoT) Landscape

The Internet of Things is a term used to describe the various collection of ever expanding, everyday items that now include a wireless connection to the internet for mundane purposes. For example, home appliances often are network enabled and may access your home network to send you email when you need a new filter for the refrigerator or new heating element for the dishwasher. Your security camera most likely has an option to see a live view of your home via a smart phone. While these items can keep an eye on your pets while you are away or know which filter you need and when to order it is a great convenience, the security issues interjected are a serious concern; primarily because these types of network connections have little to no security controls. These unsecured connections for such innocuous devices create critical security openings which malicious actors can leverage to penetrate otherwise secure networks.

The CV Pilot deployment certainly won't contain appliances. However, cars made since 1988 have CPU (Central Processing Unit) capability – with the most recent models containing more "computers" than a typical small office. These include vehicle sensors, control systems and infotainment systems and most operate on LTE or similar cellular connections with little security. Such a scenario is rife with network vulnerabilities for any vehicle communications system.

In 2014 and again in 2015, a trio of white hat penetration testers successfully took control of a Jeep Grand Cherokee. The first event required the hacker team to be within line of sight and was limited to overriding control of non-essential functions like wipers and stereo volume. The second event however, occurred from several miles away and turned off the engine of the target vehicle while it was traversing a bridge on the interstate. The bridge had no emergency shoulder and the target vehicle was being followed by a semi-truck. Needless to say, the driver was a little "concerned".

The DPP addresses this vulnerability through the application of controls and requiring that security by design is a feature of the architecture. Further, the plan ensures that all OBU/RSU devices meet the requirements of the certification body (OMNIAIR, DANLAW, 7Layers) prior to being granted access via the bootstrapping and Security Credential Management System (SCMS) certificate process. While the SCMS cannot prevent all attacks on vehicle systems, it will help to prevent unauthorized access to the CV applications and CV Data within DSRC operations. Other transmission of CV and/or PII will be via encrypted and secured data networks.

1.2. CV Pilot Participant Registration Data

The CV Pilot requires registration of participants. The registration will by necessity include Sensitive PII (SPII). This creates special considerations for protecting this data. In addition to the standard safeguards for PII, this Sensitive PII must also be treated in accordance with the Code of Federal Regulations, TITLE 45, PUBLIC WELFARE DEPARTMENT OF HEALTH AND HUMAN SERVICES PART 46, PROTECTION OF HUMAN SUBJECTS and the approved documents of the THEA CV Pilot Institutional Review Board (IRB), Salus IRB.

THEA has established policies and procedures to ensure that this Sensitive PII can be protected in accordance with all of these applicable standards and documents. This DPP discusses the policies, procedures and security controls which will be used in the protection of all participant PII.

The need for collecting this information is discussed in Section 3.

1.3. NIST Special Publication 800-53 Control Categories

NIST SP 800-53 specifies a list of control categories to be included in a data privacy plan. Table 1 below illustrates how the DPP correlates to the aforementioned NIST categories.

NIST CATEGORY	DPP SECTION	NIST OBJECTIVE	VERIFICATION METHOD / OUTCOME
Authority and Purpose			
AP-1 Authority to Collect	Technical Documentation Page. Abstract	• Determine and document the legal authority that permits the collection, use, maintenance, and sharing of personally identifiable information (PII), either generally or in support of a specific program or information system need.	• Does the DPP cite its authority to collect PII data?
AP-2 Purpose Specification	Technical Documentation Page. Abstract Section 2.2	• Describe purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices.	• Does the DPP provide purpose(s) for PII usage? • Do ICDs disclose purpose(s) for which data will be used?
AR Accountability, Audit, and Risk Management			

AR-1 Governance and Privacy Program	Executive Summary / Scope and Approach	• Identify individual to monitor and enforce privacy policies and to monitor federal privacy laws and policies for changes that affect the Pilot program's privacy policies.	• Has an individual been identified to monitor and enforce privacy policies for the Pilot?
AR-2 Privacy Impact and Risk Assessment	2. Data Privacy Defined	• Verify the creation and implementation of a privacy risk management process and related Privacy Impact Assessments (PIAs)	• Has the Pilot created and implemented a privacy risk management process and related PIAs?
AR-3 Privacy Requirements for Contractors and Service Providers	Executive Summary	• Verify the establishment of privacy roles, responsibilities, and access requirements for contractors and service providers; and includes privacy requirements in contracts and other acquisition-related documents.	• Do contractor and service providers' contracts and other acquisition-related documents contain privacy requirements? • Do Pilot systems include and enforce permission-based roles for any contractor or service provider users? • Are all contractors and service providers given documentation regarding their responsibilities and access restrictions with regards to PII?

AR-4 Privacy Monitoring and Auditing	4.4.14 Independent Audits (IRB)	• To monitor and audit privacy controls and internal privacy policy to ensure effective implementation	• Internal Audits
			  ○ Is there a method for periodic Internal Audits in alignment with PMEP requirements?
			  ○ Is there budget and staff assigned for Internal Audits?
			  ○ Is there a process to resolve audit findings?
			  ○ How many Internal Audits are scheduled?
			  ○ How many Internal Audits have been performed?
			• External Audits
			  ○ Is there a method for periodic external Audits in alignment with PMEP requirements?

			○ Is there budget and resources identified for External Audits? ○ How many External Audits are scheduled? ○ How many External Audits have been performed?
AR-5 Privacy Awareness and Training	5. The Role of the IRB	• Verify the establishment and implementation of privacy protection training, along with documented staff acceptance of privacy protection responsibilities.	• Does the training provided to Pilot staff include content regarding privacy protection policies and practices as well as documented staff acceptance of appropriate responsibilities?
AR-6 Privacy Reporting	5. The Role of the IRB, Section 5.3	• The development, distribution and updating of reports which demonstrate compliance with Salus IRB	• Are reports of privacy plan changes and/or system breaches shared in all cases and within stated timeframes? • Are reports are retained in accordance with NARA requirements?
AR-7 Privacy-Enhanced System Design and Development	3. Access Requirements	• Verify that information systems support privacy by automating privacy controls	• Anonymity: ○ Is live data, accessed in the field on OBUs, RSUs or sniffers – protected according to the Pilot's stated security standards? ○ Is stored CV raw data protected against unauthorized dissemination and intrusion according to the Pilot's stated methods? • Is ID-based/role-based authorization required in order to access the following? ○ Live or stored CV data (raw and scrubbed) ○ PII or SPII data in any state • Filtering/Scrubbing ○ Has "scrubbed" CV data been cleared of data identified in the Pilot as 'sensitive'? • Need to Know

			○ For all systems collecting, transmitting or storing CV, PII, SPII or participant data – is all access restricted by an assigned system-enforced role? • Compartmentalization ○ According to Pilot standards, are data types in all systems which collect, transmit or store Pilot data properly separated from each other? (ie: raw data is not available to users of scrubbed data etc.)
AR-8 Accounting of Disclosures	3.1.2. Access to Stored CV Data Section 5.3 Reporting	• Track information disclosed from each system of record including date, nature and purpose of each disclosure as well as the name and address of the person or agency receiving the information. Also verify that this audit trail is retained for the life of the record or 5 years after the disclosure is made. Also verify that the audit trail of disclosures is made available to the person named in the record upon request.	• Are internal disclosures within the Pilot team documented and available for IRB audit? • Are unauthorized disclosures tracked and reported?
DI Data Quality and Integrity			
DI-1 Data Quality	5.1 Participant PII Data Integrity and Storage	• Verify that the Pilot program confirms the accuracy, relevance, timeliness and completeness of PII upon collection or creation, collect PII directly from the individual as much as possible, checks for and corrects as needed – any inaccurate or outdated	• Has the Pilot program provided the ability for individuals to enter their own PII directly? • Does the Pilot program provide a method by which individuals can update their PII?

		PII used by Pilot programs or systems.	
DI-2 Data Integrity and Data Integrity Board	Table 2	• Document processes to ensure the integrity of PII through existing security controls	• Does the system used to collect and store PII have controls applied to protect the integrity of the data? ○ Does it protect against unauthorized access? ○ Does it protect against unauthorized PII modification? ○ Does it a process for to validate the accuracy of PII?
DM Data Minimization and Retention			
DM-1 Minimization of Personally Identifiable Information	2.2. Collected PII/SPII Data Categories	• Identify the minimum PII that is necessary to accomplish the Pilot, limit the collection and retention of PII to those minimum elements, and conduct an initial evaluation of PII holdings and follow a regular schedule for reviewing those holdings to ensure that only PII identified as minimum required data is collected and retained, and that the PII continues to be necessary to accomplish the legally authorized purpose.	• Does the Pilot program only gather the PII identified in the DPP? • Has the Pilot program conducted an initial review of PII holdings to ensure that only PII identified as minimum required data is collected and retained? • Does the Pilot program periodically review its PII data categories to ensure that they remain required to accomplish its legally authorized purpose?
DM-2 Data Retention and Disposal	3. Access Requirements / Data Lifecycle, Maintenance and Disposal	• Verify that the Pilot program retains PII to fulfil stated purpose for the PII, that the Pilot disposes of the PII in accordance with a NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse or unauthorized access and uses identified methods to ensure secure deletion when destroying PII	• Is PII data used to exclusively fulfil its stated purpose in the Pilot? • Once the PII's usage is complete, is PII disposed of in a NARA-approved method?

DM-3 Minimization of PII Used in Testing, Training, and Research	2.2. Collected PII/SPII Data Categories	• Verify the development of policies and procedures that minimize the use of PII for testing, training and research. • Verify that controls have been implemented to protect PII used for testing, training and research.	• Do policies and procedures exist which minimize the use of PII? • Have the controls enumerated in the DPP been implemented?
IP Individual Participation and Redress			
IP-1 Consent	3. Access Requirements	• Verify that the Pilot has provided a means for individuals to authorize the collection, use, maintenance and sharing of PII prior to its collection. • Verify that Pilot has provided a means for individuals to understand the consequences of decisions to approve or decline the authorization of the collection, use dissemination and retention of PII.	• Does the method of signing up new Pilot participants include an explicit authorization from those individuals regarding PII collection? • Does the method of signing up new Pilot participants include a summary of consequences regarding either the approval or the rejection of PII collection?
IP-2 Individual Access	5.1 Participant PII Data Integrity and Storage	• Verify that the Pilot provides individuals the ability to have access to their PII maintained in its system(s) of records. • Verify that the Pilot publishes rules and regulations governing how individuals may request access to records maintained in a Privacy Act system of record as appropriate.	
IP-3 Redress	5.1 Participant PII Data Integrity and Storage	Verify that the Pilot provides a process for individuals to have inaccurate PII corrected.	• Does the Pilot provide a method for participants to correct their PII?

IP-4 Complaint Management	5.1 Participant PII Data Integrity and Storage	Verify that the Pilot has implemented a process for receiving and responding to complaints, concerns or questions from individuals about the Pilot's privacy practices.	• Does the Pilot provide a method for participants to lodge complaints, concerns or questions regarding privacy practices? • How many complaints have been received during the span of the Pilot project? • How many questions have been received during the span of the Pilot project? • Of the complaints received, what percentage have been resolved? • Of the questions that have been received, what percentage have been answered?
SE Security			
SE-1 Inventory of Personally Identifiable Information	2.2. Collected PII/SPII Data Categories	Verify that the Pilot has establishing and updating an inventory containing a listing of all programs and information systems which collect, use, maintain or share PII, and that this inventory is shared with the CIO or Information Security Official for the Pilot.	• Has the Pilot program established an inventory of all systems and programs which collect, use, maintain or share PII? • Does the Pilot program maintain that inventory on a periodic basis? • Has that inventory been shared with the individual charged with managing security for the Pilot program?
SE-2 Privacy Incident Response	3. Access Requirements	Verify that the Pilot has developed and implemented a Privacy Incident Response Plan, and does provide an organized and effective response to privacy incidents in accordance with the Plan.	• Does the Pilot program have a Privacy Incident Response Plan? • How many incidents have been logged since the inception of the Pilot program? • On average, how many days elapsed between the detection of the incident and the final response?
TR Transparency			
TR-1 Privacy Notice	3. Access Requirements	• Verify that the Pilot provides effective notice to the public and to individuals regarding its activities that impact privacy, including its	• Does the Pilot program effectively notify participants of its activities that impact privacy? • Does the Pilot program share with participants the types of

		collection use, sharing, safeguarding, maintenance and disposal of PII its authority for collecting PII, and the ability to access and have PII corrected. • Verify that the Pilot describes the PII collected and its purpose, how the Pilot uses the PII, whether the Pilot shares PII with external entities, how individuals may obtain access to PII and how the PII will be protected. • Verify that the Pilot revises its public notices to reflect changes in practice or policy that affect PII or changes in its activities that impact privacy – in a timely manner.	PII that is collected, the purpose for collection, if the PII will be shared with third parties, how the data will be secured, and how it will be eventually disposed of? • Have the Pilot program's processes or practices regarding PII changed, and have its public notices been updated accordingly?
TR-2 System of Records Notices and Privacy Act Statements	N/A		
TR-3 Dissemination of Privacy Program Information	5.1 Participant PII Data Integrity and Storage	• Verify that the Pilot ensures that the public has access to information about its privacy activities and is able to communicate with its Senior Agency Official for Privacy.	• Does the Pilot or its sponsor ensure that the public has adequate access to information with regards to PII used in the Pilot? • Does the public have access to the individual assigned to manage Privacy for the Pilot?
UL Use Limitation			
UL-1 Internal Use	4.4.7 Authorization – Role Based	Verify that the Pilot uses PII internally only for the authorized purpose identified in public notices and the Privacy Act.	• Does the Pilot use PII internally according to its stated authorized purpose?
UL-2 Information Sharing with Third Parties	3.1.2. Access to Stored CV Data	• Verify that the Pilot shares PII only for the authorized purposes. • Verify that the Pilot monitors, audits and trains its staff on the	• Does the Pilot consistently filter/scrub data prior to sharing with third parties? • Audit SCMS Certificates/CRL: do logs exist? Do they show

		authorized sharing of PII with third parties and on the consequences of unauthorized use or sharing of PII, and that the Pilot evaluates any proposed new instances of sharing PII with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.	a pattern of attempted intrusion? • Encryption: ○ Is live data encrypted? ○ Is stored raw CV data encrypted? ○ Is data in transit encrypted? ○ Is all PII or SPII data encrypted? ○ Is Electronic Participant data encrypted? • Access Control – Physical ○ Is physical access to the following devices protected according to the Pilot's stated standards? ▪ Devices collecting or transmitting CV data of any kind ▪ Devices storing raw or scrubbed CV data ▪ Devices collecting, transmitting or storing PII or SPII ○ Are all hard copy documents containing participant data under physical protection according to the Pilot's stated standards? • Access Control – Remote ○ Is remote access to the following devices protected according to the Pilot's stated standards? ▪ Devices collecting or transmitting CV data of any kind ▪ Devices storing raw or scrubbed CV data ▪ Devices collecting, transmitting or storing PII or SPII • Penetration Testing ○ What is the frequency of penetration testing:

			○ What is the number of systems tested? ○ What is the number of systems with high risk findings? ○ What is the number of findings per system? ○ What is the number of closed finding per system? • System Monitoring ○ Are systems which collect, transmit or store CV data monitored according to the Pilot program's stated practice? ○ How many systems are being monitored? ○ What is the average system availability to date? ○ How many intrusions have been logged by System Monitors to date? ○ How many blocked intrusions have been logged by System Monitors to date? • Anti-Virus ○ Do all systems which transmit or store CV or participant data have up-to-date anti-virus protection? ○ How many malware incidents have been logged by anti-virus software per system?

Table 1 NIST SP 800-53 to DPP correlation

2. Data Privacy Defined

The THEA CV Pilot will collect multiple types/classes of data prior to and over the course of Operate and Maintain Phase III. Some of this data will be pre-treatment and other baseline data will be independent of CV Data and is already public, containing no PII. This and other incidental data collected outside of the targeted scope of the Pilot may be utilized in the evaluation of performance measurement but is not covered by the policies and procedures of this document. All data utilized, however, will be handled with care as discussed in this document and in the Phase I SMOC (THEA, Task 3, SMOC, April 2016). The purpose of this section is to define and delineate those types/classes of data which will be held to the policies and procedures herein. This section also includes some terms common to the protection of PII as used in this document. The terms are presented logically rather than alphabetically for ease of comprehension.

2.1. Key Privacy Terms

Data Owner: By default, the owner is the subject of the PII Data. Informed consent of the owner must be acquired and documented prior to collection of PII. For the CV Pilot, the data owner shall be the vehicle owner who registers for participation in the Pilot. Owner/registrants receive training and sign informed consent documents to ensure they fully understand:

- The data to be collected
- The purpose for which the data will be used
- Their rights as the data owner
- Their protection from disclosure of SPII/PII
- Any additional entities with whom the data may be shared during/after the Pilot
- The owner/registrant is the participant and is responsible for informing other persons whom they may allow to operate their vehicle during the Pilot.

* In the case of HART transit buses and streetcars, HART, as the owner of the vehicles, shall sign an Informed Consent Document (ICD). An initial HART ICD was approved by the IRB (June 2016). While HART vehicles will be operated by HART employees, these employees, while not technically participants, will receive training and be extended the oversight for safety and safety equipment reviews, that other participants will receive. If an incident occurs, standard HART procedures will be followed and the Pilot Safety Manager will be informed, who will then follow the standard operating procedure outlined in the Phase I Safety Management Plan (THEA, Task 4, Safety, April 2016). No PII data will be collected on the HART drivers, except that which HART already possesses as the employer, so there will be no danger to their PII in the Pilot database. Raw CV data will not be available to HART to void the possibility of monitoring individual drivers. However, GPS and AVL equipment, already in use, can be used as the union contract allows (Hillsborough Area Regional Transit and Amalgamated Transit Union Local 1593, October 1, 2012). (See also Section 5.1.)

Privacy: Control over the extent, timing, and circumstances of sharing oneself (physically, behaviorally, or intellectually) with others.

PII: is the information that can be used to distinguish or trace an individual's identity, such as their name, Social Security number, biometric records, etc., alone, or when combined with other personal or identifying information, which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified by examining the context of use and combination of data elements. Non-PII can become PII whenever

additional information is made publicly available. This applies to any medium and any source that, when combined with other available information, could be used to identify an individual.

SPII: is a subset of PII which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Sensitive PII requires stricter handling guidelines because of the increased risk to an individual if the data are compromised. The following PII is always (de facto) sensitive, with or without any associated personal information:

- Social Security number (SSN)
- Passport number
- Driver's license number
- Vehicle Identification Number (VIN)
- Biometrics, such as finger or iris print
- Financial account number such as credit card or bank account number
- The combination of any individual identifier and date of birth, or mother's maiden name, or last four of an individual's SSN

In addition to de facto Sensitive PII, some non-sensitive data may be deemed sensitive based on context, as discussed next.

Non-sensitive Data as PII: Some information may be non-sensitive or anonymous by itself but when coupled with other available or discoverable data, can become PII and even SPII. For example, two recent decisions by the U.S. Court of Appeals for the First Circuit (In re Hulu Privacy Litig, 2014) and (Yershov v. Gannett), not only throw into question how PII may be understood, but also threaten to create a circuit split should any other circuit court tackle whether the definition of PII includes anonymous identifiers, geolocation data and elements of data that are sometimes passed from a streaming service to third parties, such as analytics providers.

CV Data: For the purposes of this document, CV Data shall mean data collected from the system pertaining to functional performance of the various components, devices and communications; and necessary for the CV Applications to successfully operate as intended. This also includes Basic Safety Messages (BSMs), Traffic Information Messages (TIM), Map (MAP) and Signal Phase and Timing (SPaT) data. This data will generally NOT contain ANY "direct" PII or SPII. However, as Non-sensitive data can be utilized to extrapolate PII, a "scrubbing" process will be applied to filter against this possibility before CV Data is shared on the RDE or other open portals.

Published Data: Industry guidelines establish that data which is "published" is de facto "public data" and therefore has no expectation of privacy or protection from exposure/exploit. The (Official (ISC)^2 Guide to the CISSP CBK, Fourth Edition, 2015) includes "broadcast communications" in the definition of published data. CV Pilot data that is "Broadcast" over DSRC channels is protected by the SCMS system and not publicly available. As such, broadcast live CV Data is not to be construed as "published" or "public" within that context.

The CIA Triad: Term for the "Big 3" tenets of information security – Confidentiality, Integrity and Availability as defined below:

- Confidentiality: Prevention of intentional or unintentional unauthorized disclosure of data
- Integrity:
  - Prevention of modification by unauthorized persons or processes
  - Prevention of unauthorized modification by authorized personnel or processes
  - Ensuring that data is internally and externally consistent
- Availability: Ensuring the timely and reliable access to data by appropriate personnel

Each category/class of data described in Section 2.2 and Table 1 will be treated and assessed for CIA.

Access Control Terms:

- Identification: The means by which users claim their identities to a system. Identity is a required precursor to authentication and authorization.
- Authentication: The testing or reconciliation of evidence of a user's identity. It establishes and verifies that a user is who they say they are.
- Authorization: The rights and privileges granted to a person or process.
- Accountability: The processes and procedures by which a system obtains its ability to determine the actions and behavior of a single individual or process within the system and to identify that individual person or process. Audit trails and logs are examples of tools supporting accountability.

2.2. Collected PII/SPII Data Categories

Data to be collected by the CV Pilot may include, based on motorist or pedestrian participant, many of the following forms of personal information about individual participants and their motor vehicle and motor vehicle use. The following data represent the minimum amount of data required for the research to be effective and statistically relevant. The occupation/affiliation type data was requested by the IE for socio-demographic analysis, and also supports the provision of anonymized data. This type of data will be distributed only in combined socio-demographic type reporting and not individually specific.

Participant Background Information (All Participants)

- Individual Identifiers;
- Full Name (First, Middle, Last);
- Socio-demographic information, including age, gender, marital status, and income;
- Driver's license number, issuing state, and qualifiers.

Vehicle Identifiers (Driver Participants Only)

- Personal VIN and registration information;
- VIN of government issued vehicles; and
- Identifiers for equipment installed by Pilot in personal or participant vehicle.

Contact Information (All Participants)

- Mailing/Residential Address;
- Phone number(s);
- Email address(es);
- Institutional or organizational affiliation;
- Work/Business related contact information; and
- Occupation and work schedule.

Eligibility Information (Driver Participants Only)

- Driver history and habits;
- Proof of insurance
- Proof of Florida vehicle registration
- Completion of Pilot participant training

Project Information (Driver Participants Only)

- Vehicle sensor information;
- Dynamic information about a vehicle, including location, heading, velocity, proximity to and interaction with other vehicles and infrastructure; and
- Data collected from drivers by means of surveys, focus groups, or interviews.

Some data categories are collected for the purpose of validating the statistical sample and are not specifically used for performance measurement directly. Examples are:

- Data related to occupation, age, driving history and habits
- Data collected from drivers by means of surveys, focus groups, or interviews

3. Access Requirements

This section discusses the underlying need for access to participant data that may include PII and the privacy requirements of the various data categories/classes, as described in Section 2.2. Section 4 details the tools and controls to be utilized for each category/class.

The following minimum control principles will be applied to all data collected throughout the Pilot.

Data Collection:

- Only data expressly permitted and consented will be collected.
- Only the minimum amount of data required for the research to be effective and statistically relevant will be collected.

Participant Notice and Informed Consent

- No data will be collected on any participant/candidate prior to documenting an "informed consent" in accordance with "IRB approved" informed consent document(s).
- The informed consent shall be predicated upon the presentation of Pilot details, data to be collected, its intended use and to whom it will be disclosed as shown in the IRB-approved ICD.
- There will be a mechanism to change or update participant information per the IRB documents.

Use and Sharing of Data

- Collected data will only be used for the intended and stated purposes as declared in the Research Protocol Document (RPD) and ICDs.
- Collected data will only be shared with those having both pre-authorization and "need to know"/appropriate role-based authorization. Subsequent downstream sharing within authorized organizations will be limited by these same requirements and controls will be in place for the parent custodian to conduct audits of compliance.
- No changes in use or sharing can occur after informed consent unless approved by the IRB. The IRB would dictate the notification to participants and new informed consent procedures.

Security of Collected Data

- Protect all PII, electric or hardcopy, in their custody from unauthorized disclosure, modification, or destruction so that the confidentiality, integrity and availability of the information are preserved.
- Store PII only on IT infrastructure employing security controls commensurate with the risk to the individual that would result from unauthorized access, disclosure, or use of the information.
- Encrypt all PII in transit or at rest.
- Encrypt all PII transmitted or downloaded to mobile computers/devices.
- Ensure that all individuals having access to PII have received training in the policies and procedures that protect PII.

Data Lifecycle, Maintenance and Disposal

- Maintain PII in accordance with the applicable National Archives and Records Administration (NARA) records schedule (available from the USDOT Contracting Officer).
- During the project, should a participant withdraw consent via a call to the Help Desk, data collected during the project for that participant will be retained. No data will be collected beyond their withdrawal date.

- After conclusion of the research project, maintain PII only as permitted by the NARA schedule and, in the case of contractor-conducted research, relevant data rights classes in the applicable contract. Retention of PII that may be necessary for continued routine operations may be permitted (e.g., registration and account information).

Privacy Documentation

- Data Custodians shall document staff and others who may access Pilot data with an indication of authorization and access level, period of access, Pilot role and to the extent technically feasible, a time/date stamp access log.

Reporting

- All staff shall be trained in the proper reporting of a breach or suspected breach to the data or the policies, procedures and protocols for the protection of privacy data.
- The Principal Investigator/Data Custodian(s) shall report all breaches or suspected breaches to the USDOT Agreement Officer's Representative within 48 hours of discovering the incident.
- Reporting requirements to the IRB (and potentially required follow-up actions) are also likely to apply in the case of any breach or violation of the approved research protocol, as mentioned in the IRB Document
- Any breach of participant PII will be reported to them as to its nature and what is being done about it.

3.1 CV Data Requirements

The requirement to collect CV Data is explicit in the NoFO and subsequent Agreement. The overarching purpose of the Pilot is to research the effectiveness and interoperability of CV applications. This requires collecting and analyzing the message formats, communications frequencies, interference, delivery/acknowledgement of these. This includes BSM, TIM, SPaT data as well as information from transit bus schedules, real time positioning, personal information devices etc. The Pilot relies on the analysis of this data to evaluate the performance measures as indicated in the proposal, Concept of Operations (ConOps), System Requirements (SyRs) and the Comprehensive Deployment Plan (CDP). Pilot

3.1.1. Access to live CV Data

Investigators on the Pilot team may need to periodically view real time live CV Data for the purposes of calibration, diagnosis, validation or other reasonable purposes. Because live CV Data has not been scrubbed for release to the RDE or other publication, this access will be limited to designated Pilot staff with explicit clearance, adequate training, and experience to ensure safe handling within this plan. Any capture of "live" data will be considered to reasonably contain PII and will classified and safeguarded as PII, including the use of approved, encrypted storage devices for the capture, storage and transfer of the data. Access would typically be required for system testing or troubleshooting issues, and an audit log will be maintained to track name, date and location of live DV data access. Live CV Data is broadcast over DSRC in an unencrypted state but access to the data requires multiple layers of requirements including a device to capture the communication, software to interpret the data and SCMS bootstrapping and valid certificates.

3.1.2. Access to Stored CV Data

For the Pilots to be of value to future deployers, fellow researchers and the general advancement of the viable implementation of CV technology, it is imperative that the research data collected and analyzed be made available to that segment. This will be accomplished through the distribution of the stored CV

Data to two Independent Evaluators (IEs) as well as the Research Data Exchange (RDE), which is the repository of CV research data from and for the collective Affiliate Test Bed Members. For this reason, "stored CV data" falls into 2 sub-categories, "Scrubbed" and "Non-Scrubbed". Non-scrubbed CV Data will be presumed to contain PII and/or SPII and will be protected as such. Once this stored data has been analyzed for relevance, validity and has had any PII removed, it will be re-classified as "scrubbed CV Data". This scrubbed data will be released to the IE and eventually to the RDE. An audit trail will be created to track who accessed the data, when it was accessed, and where the data was stored. The process implemented to created scrubbed data is referred to as "filtering" and is described in Section 4.

The IEs will only receive "scrubbed data" per PII/SPII Requirements.

3.1.3. Access to PII Data

PII Data is easily commingled with SPII in the context of the rapidly moving exchanges taking place in the DSRC system. Because of this, the THEA Pilot team will treat all PII as SPII in an abundance of caution. Because of this, PII will be discussed as one entity with SPII below and throughout the DPP.

3.1.4. Access to SPII

The CV Pilot's very existence is dependent on driver/participants. Inherent in the participation is the need to register and communicate with these participants. Much of the data collected during participant registration is unavoidably SPII. A very robust system of controls will be implemented to safeguard the PII/SPII data of the Pilot. These controls are discussed in detail in Section 4.

4. Security Controls for Pilot Data

4.1. Types of Controls

Security controls can be classified by three types and three means. The three types of controls are:

- Preventive: Are put in place to “inhibit” harmful events.
- Detective: Are put in place to “discover” harmful events
- Corrective; Are put in place to restore systems after a harmful event.

These security controls follow a progression from blind optimism (believing that prevention will eliminate ALL negative events) to the sky is falling (we can’t stop them, better prepare to pick up the pieces). The best security plans utilize a balance of the available controls to accomplish the best solution based on multiple factors including:

- Risk tolerance of data owner
- Value of data at risk
- Damage expected from loss or exposure
- Likelihood of loss or exposure
- Cost of various safeguard options compared to the level of assurance they bring and the above factors.

The Pilot will identify and manage Security Controls following the steps recommended by NIST in its FIPS SP800-53 Document, and the requirements traceability matrix (RTVM) will be constructed around these steps:

- Categorize the information system based on a FIPS Publication 199 impact assessment; (partially completed by USDOT - pre-award, preliminary re-assessment based on current state of design at point of DPP creation, and another re-assessment to follow after final design)
- Select the applicable security control baseline based on the results of the security categorization and apply tailoring guidance (including the potential use of overlays);
- Implement the security controls and document the design, development, and implementation details for the controls;
- Assess the security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system;
- Authorize information system operation based on a determination of risk to organizational operations and assets, individuals, other organizations, and the Nation resulting from the operation and use of the information system and the decision that this risk is acceptable; and
- Monitor the security controls in the information system and environment of operation on an ongoing basis to determine control effectiveness, changes to the system/environment, and compliance to legislation, Executive Orders, directives, policies, regulations, and standards.

4.2. Means of Control

There are also three means for implementing the first two types of controls

- Administrative: Includes policies and procedures; security awareness training; background checks, and levels of supervision.
- Logical or Technical: Targets the restriction of access and includes encryption, smart cards, access control lists, and biometrics.

- Physical: Incorporates security guards, alarm systems, locks etc.

4.3. Selected Controls by Data Class

Table 2 indicates the Controls selected for protection of the data classes comprising the CV Pilot.

Table 1: Controls for Protection of Data Classes Used in the CV Pilot **Data Type / Description** . . **Controls Used (Type/Means)**	**NIST SP 800-53 Table J-1 Controls**	**Live CV Data (Real-time data accessed in the field on OBUs, RSUs or sniffers)**	**Stored CV Data, Raw**	**Stored CV Data, Scrubbed**	**CV Data of any type when in Transit**	**PII/ SPII in any state**	**Hard Copy Participant Data**	**Electronic Participant Data**
SCMS Certificates/CRL **(Preventive/ Technical)**	AR, DI, SE, DM	√						
Anonymity **(Preventive/ Technical)**	AR, DI	√	√					
Encryption **(Preventive/ Technical)**	AR, DI, SE	√	√		√	√		√
Access Control-Cabinet locks etc. **(Preventive/ Physical)**	AR, DI, SE, DM	√	√	√	√	√	√	√
Access Control-remote to devices and via system (**Preventive/ Technical)**	AR, DI, SE, DM	√	√	√	√	√		√
Authorization - ID Based **(Preventive/ Technical)**	AR, DI, SE, UL, DM		√	√	√	√	√	√
Authorization - Role Based **(Preventive/ Administrative)**	AP, AR, DI, SE, UL, DM		√	√	√	√	√	√
Penetration Testing **(Preventive/ Technical)**	DI, SE	√	√	√	√	√		√
System Monitoring **(Detective/ Technical)**[1]	AR, DI, SE, UL, DM	√	√	√	√	√		√
Anti-Virus **(Detective/ Technical)**[1]	SE, DM		√	√	√	√		√

Filtering/ Scrubbing **(Preventive/ Technical)**	AR, DI, SE, UL			√				
Need to Know **(Preventive/ Administrative)**	AR, DI, SE, UL, DM	√	√	√	√	√	√	√
Compartmentali-zation (**Preventive/ Administrative)**	AR, DI, SE, UL	√	√	√	√	√	√	√
Internal Audits **Detective/ Administrative)**	AR, DI, SE, UL, DM	√	√	√	√	√	√	√
Independent Audits (IRB) **(Detective/ Administrative**	AR, SE, UL	√	√	√	√	√	√	√

Table 2 [1] This control can also be Corrective if enabled

4.4. Control Implementation Details

4.4.1. SCMS Certificates/CRL

USDOT has contracted with the Crash Avoidance Metrics Partnership (CAMP) to provide the Security Certificate Management System (SCMS) Proof of Concept (PoC) version for use throughout the CV Pilot. This SCMS will provide the "access control" and "authorization "services for allowing devices to participate in the exchange of CV Data within the Pilot area. This SCMS will provide the framework for bootstrapping, certificate generation and distribution, and certificate management including a daily broadcast of certificates which have been revoked due to device failure or misbehavior. The Pilot will use this system for authentication, authorization and an ongoing "Trust System" The SCMS system is discussed in detail in the THEA CV Pilot SMOC (THEA, Task 3, SMOC, April 2016).

4.4.2. Anonymity

According to NIST SP 800-122, anonymity can be introduced by: generalizing the data; suppressing the data; introducing noise into the data; swapping the data; and replacing the data with the average value. The THEA Pilot will utilize only one of these methods: swapping the data. This will be applied to CV Data by swapping identifying/potentially identifying data with anonymous random data. There will be a link between the swapped data and the original identifying data for the purposes of audits, controls and administrative purposes. This link information will only be available to specific staff specially trained in the protection of human research subjects. This link access process is explained in Section 4.4.7 Authorization - Role Based Access Control. The data swapping process is discussed in Section 4.4.11 Filtering.

Note it is possible during final design that additional BSM data may be identified as potential PII and be added to the list of data to be swapped with anonymous random data.

4.4.3. Encryption

Encryption will be applied to all data types except for scrubbed CV data. Because scrubbed data has already had all PII/SPII removed by the application of a technical filter, it is the only form of data permitted to be stored or transmitted in clear text.
256 bit Advanced Encryption Standard (ES) Encryption will be used for all other data types.

A log will be kept of all personnel/staff access to Cryptographic Key material and will be audited bi-annually. A cryptographic material custodian will be designated for control, inventory, storage and distribution of cryptographic key as needed.

4.4.4. Access Control - Cabinet locks etc.

The technical means of data and privacy protection are only as secure as the physical means preventing access to stored or live data. For example, requiring an extremely sophisticated password schema is of little effect if user passwords are widely known to be written and stored in an unlocked desk drawer. The THEA Pilot team will ensure that physical protection devices are fully and correctly utilized to protect against physical exposure to non-scrubbed Pilot data of any type and that Pilot staff are properly trained in their use. Example of physical devices and data include computer storage devices and hard copy paper records.

4.4.5. Access Control - Remote Electronic Access to Devices and System

All access to Pilot data via electronic means will be protected by an access control system including: Identification, Authentication, Role-based Authorization, Access and Event Logs, and Internal Audits.

4.4.6. Authorization - ID Based

Authorization occurs after authentication. Whereas the authentication establishes the identity of person requesting access, ID based authorization determines the level of access to be granted. All access to any level of Pilot data will begin at this ID based authorization.

4.4.7. Authorization - Role Based

In addition to the ID based authorization above, personnel access will be further restricted based on specific job roles within the Pilot. For example, the staff involved in the registration of participant data will not be involved in the collection or analysis of CV Data and the staff involved in analyzing CV data will not have access to participant data. This precludes staff with CV Data access from being able to extrapolate PII from CV Data via comparison with the registrant data.

Throughout the Pilot there may be situations where an examination of both CV Data and registrant data is required. One such example may be when an OBU malfunctions. When the CV System recognizes an anomaly likely due to an OBU malfunction, it will be necessary to contact the owner of the vehicle to come in for repair or replacement of the OBU. Since staff from the CV Data analysis group are forbidden access to the participant database, some means must be available to resolve the correlation of anonymous vehicle to known owner. This will be done by one of four designated staff on the Pilot project who maintain certification by NIH and the Salus IRB to be specifically responsible for the protection of human subjects throughout the Pilot. These comprise a Principal Investigator/Project Manager, and three Investigators.

4.4.8. Penetration Testing

Penetration testing is conducted by ethical hackers under the authority of Pilot Management. These ethical hackers operate outside of the sphere and influence of the system architecture design and implementation for the sole purpose of identifying vulnerabilities and exploits within the system. During and after the design and deployment of the system, the penetration testers will attempt to break down any of the three tenets of the CIA security model. By providing this type of targeted attack by friendly sources (White Hats), the team will be better positioned to prevent or mitigate malicious or even inadvertent outside attacks. Any successful exploit of the system after operational deployment will be a

reportable event without regard to whether data is actually compromised.

4.4.9. System Monitoring

Both passive and active system monitoring controls will be implemented for the CV Pilot system architecture. These monitoring applications will examine live and stored data for anomalies and other signs of improper operation or possible system exploits. These systems may have a corrective component that automatically implements safeguards to inhibit further exploit or may simply alert Pilot staff of the event so that manual action can be affected. These systems may include network monitoring, data sniffers, key loggers, Simple Network Management Protocol (SNMP) traps (send alerts to management system regarding suspicious traffic), Access Control Lists (ACL – hardware monitoring rule configuration) and others.

4.4.10. Anti-Virus and Malware Checking

Anti-Virus and malware checking software will be utilized for each system component where appropriate. Anti-virus and malware checking applications are primarily detective in nature in that they recognize and report code patterns known to be associated with potential exploits. These are most effective for open networks where access control is weak. While the CV Pilot Communication system and network will be actively secured, Anti-Virus and malware checking software will still be deployed on workstations, servers and other items where inadvertent introduction of hostile code could occur.

4.4.11. Filtering/Scrubbing

Filtering/Scrubbing is the single most important control to be utilized for safeguarding SPII/PII on the Pilot. Since the most likely scenario leading to the inappropriate identification of a participant has to do with the correlation between the registrant and his/her vehicle, the primary item to be protected is the data which can provide that correlation, vehicle identification. So, information about participating vehicles will be anonymized during access to the system by swapping the VIN with a random ID number within the BSM. This is also known as de-identification. The VIN is required for confirming insurance coverage of the participant. The ID will be re-randomized periodically on an interval to be determined during final design. The re-randomization will comply with J2945/1

Since the geolocation, direction of travel, velocity, time and date stamp, vehicle size classification and other similar data could be analyzed together to determine identity after the fact, a scrubbing process will also be applied to all data to be shared outside of the Pilot. This process filters out the anonymous ID assigned during de-identification, thus removing the means to reverse engineer the original ID. Data that has been scrubbed will still be of value to researchers as it will have been quantified and classified into meaningful outcomes prior to scrubbing. Examples include: reports, graphs, and, raw numbers without PII, etc.

The filtering/scrubbing of data will occur at the Central Systems level. The actual technologies/processes to be utilized are part of ongoing final design and will be documented upon completion.

4.4.12. Need to Know

“Need to know” further restricts access to data based on having a legitimate need to access the data for completing a requirement of one’s job. For example, Department of Defense information is classified into Confidential, Secret and Top Secret categories. But one cannot be given access to even Secret data to which they have no need to know simply by having a Top-Secret clearance. The appropriate clearance must be accompanied by need to know for access to be authorized. The Pilot will apply this policy when granting access to any data collected as part of the Pilot. The need to know will be based

upon an assessment of each data type and the authorized staff role as discussed in Section 4.4.7.

4.4.13. Compartmentalization

Compartmentalization is the partner to role-based access discussed earlier. Information is divided into compartments in order to keep any one entity from having the entire picture. In the case of the CV Pilot, this is applied to participant registration data and vehicle identification information. Pilot As discussed in role based access, the staff maintaining registrant data and those analyzing CV Data are not granted access to the data of the other team. This keeps the data compartmentalized such that only the role with access to both CV Data and PII can make the correlation, i.e., the Principal investigator and investigators.

4.4.14. Audits

- **Independent Audits (IRB)** Independent audits are the hallmark of prevention when it comes to staff misbehavior. Knowing that an independent entity will be reviewing your work and actions is a strong deterrent to cutting corners or malicious activities. In the case of the CV Pilot, the likelihood of such activities are already minimal. But due to the sheer volume of data to be amassed and the potential for human error, independent audits will be applied to reviews of both policy/procedure adherences and data integrity. One such evaluation is conducted by Salus IRB. Documents reviewed by auditors will include ICD's, security policies, access logs and recruiting/media materials. The role of the IRB is discussed in Section 5 below.

- **Internal Audits (Pilot Team)** System event logs will be generated by OBUs/RSUs and other system elements. Administrative logs will be generated for staff access and use of PII. These event logs and admin logs will be reviewed during internal audits to ensure security controls are effective in protecting PII as designed.

4.4.15. Breach Detection and Remediation

Breach detection for the Pilot falls into two categories: breach of the live CV-Data system which involves unauthorized access to the DSRC communications system, and breach of the local Pilot system which includes:

- Local cabinets housing CV devices
- ITS backhaul network
- Central System Components

Live Data Breach

An unauthorized access incident involving the live CV-Data environment may be difficult to identify in a timely manner because the SCMS was to have had a misbehavior detection component and associated certificate revocation list process.It is the current understanding that the misbehavior component may not be available during early deployment of the Pilots. This means that the Pilots will have limited means to discover misbehavior. The primary means of misbehavior detection by the Pilot will entail analysis of OBU or RSU data after the fact - and OBU data in many cases are only available after periodic physical downloading. Misbehavior comprises two categories, malicious and device fault/failure. Device fault or failure is the misbehavior caused due to faulty devices and will be discovered during data analysis.

Malicious misbehavior is the most troubling, and represents the category which is best handled by the proposed misbehavior component of the SCMS, and not within scope of the CV Pilots. Nonetheless, the risk of malicious misbehavior is considered low.

Local System Breach

The local Support System includes the ITS network that will carry CV-Data, the central system which will store and process CV-data, the physical facilities housing the devices, the servers, the physical facilities for storing participant registration data etc. There is currently an effort underway to update the THEA Security Policies to include requirements for safeguarding CV Pilot elements attached to THEA networks or housed in THEA facilities. A similar effort is ongoing in regard to the Siemens' facility and networks that will house Central System Elements. These external updated policies/procedures documents will be added to an updated version of this document as appendices when complete (during finalization of detailed design). These external documents already contain breach response plans and the CV-Data will be incorporated into those plans for consistency. General guidelines that will be included in these external documents in regard to CV Data protection are as follows:

- Network security: Separate VLANS will be setup for CV-Data; network monitoring will include ability to monitor and set alarms by VLAN; and, access to VLAN will be controlled by ID, authentication and role based authorization.
- Physical Security: Appropriate policies, procedures and locking devices will be incorporated to prevent unauthorized access.to devices, data storage etc.
- Data integrity: Policies, procedures, and security controls will be utilized to ensure that data remains safe from intentional and inadvertent unauthorized modification.
- Access: Will be limited based on ID, Authentication and role based authorization (need to know).
- Breach Discovery and Response: Detection of and response to breaches of CV data will be incorporated into the external plans mentioned above such that the existing monitoring and detection systems can be leveraged for enhanced detection and response. In regard to CV-Data breach response, CV-Pilot staff will be included in all event notification and response.
- Notification: All breach events, including unsuccessful attempts will be reported to:
    - USDOT (AO, AOR and JPO Security Technical Lead)
    - THEA management, including at a minimum, Executive Director, IT Manager, Pilot SDL and Communications Director
    - THEA Pilot Leadership and Salus IRB

5. The Role of the IRB

The Human Use Approval Summary (HUAS) (THEA, Task 8, HUA, July 2016), Participant Training and Stakeholder Education Plan (THEA, Task 9, PTSEP, August 2016), and Outreach Plan (THEA, Task 11, Outreach, Draft - July 2016) treat collecting and maintaining administrative participant data. THEA CV Pilot participant PII and human participation in general is under the oversight of Salus Institutional Review Board (IRB). Salus IRB has given approval to the Human Use plan described in the THEA CV Pilot Research Protocol Document (RPD) and the Informed Consent Documents (ICDs) for pedestrians, auto drivers and the HART transit agency's employees. The RPD and ICDS are summarized in the Task 12 HUAS report.

IRB approval is subject to ongoing and periodic review as progress advances past the Pilot Phase I Concept Development and into the details of recruitment, screening, registration, PII data storage, training and message sharing with participants in Phase II. In Phase I, Salus IRB granted the THEA CV Pilot Expedited Review status as requested in the THEA application and in the RPD. Salus IRB found that:

> "The research was determined to involve no more than minimal risk and qualified for expedited review in accordance with 21 CFR 56.110 and 45 CFR 46.110, under the following research category(ies): Category 7."

Category 7 entails: "research on individual or group characteristics or behavior … or research employing survey, interview, oral history, focus group, program evaluation, human factors evaluation, or quality assurance methodologies."

THEA will make periodic updates to Salus IRB in order to revise the RPD and ICDs as progress continues with ongoing reports on issues of interest to human use. In the context of this DPP, participant PII data integrity and storage are of particular interest.

5.1 Participant PII Data Integrity and Storage

IRB approval to-date covers the points made in this section. Participants in the CV Pilot study are to include: drivers, pedestrians, and the HART transit agency which manages a fleet of buses and streetcars. The anticipated and planned potential sample size of participants is subject to the actual recruitment response of pedestrians and drivers as well as budgetary constraints that expect to attract:

- 1500-2000 auto drivers
- 500 pedestrians (Pedestrian participation is not limited by budget or rule. 500 is the recruiting target but as many as meet the requirements and complete training may participate)
- 10 buses
- 9 streetcars.

Recruitment of pedestrians and auto drivers will require collection of the following PII in order to administer training, education and any notifications leading up to and continuing throughout the Pilot deployment.

- Name
- Date of Birth
- Contact information
    - home and work mailing addresses
    - email

  - phone number
- Copies of
  - driver licenses identification number
  - insurance card (only for auto drivers)
  - vehicle registration (only for auto drivers)
- Vehicle type data (only for auto drivers)
- Socio-demographic data (as defined by Task 5: Performance Measurement)
  - age
  - sex
  - race
  - marital status
  - income
  - language preference (English/Spanish)
  - recruitment method.

Data on age, gender, race/ethnicity, marital status, income, and recruitment method will be used only to show how effectively all groups were represented in the conduct of the study. Other socio-demographic data may be added to the study as needed with IRB approval. Socio-demographic data may be released to the IE as long as PII is withheld or protected. Socio-demographic data may be of interest to the IRB to evaluate the protection or treatment of vulnerable populations.

Socio-demographics, per se, are not an in scope requirement. However, some socio-demographic info is inherent in participant registration. While performance measurement by the team is not focused on socio-demographics, the data, which is, by necessity, collected, will be stored against the potential use for Pilot team or IE use. In the case of IE use, socio-demographic data will be scrubbed for release in a similar manner as other potential PII. For example, data on year/model/class of vehicles may be summarized for socio-demographic study, but would not be specific to any individual and, therefore, not contain a privacy risk.

Pilot

No PII will be collected by the THEA CV Pilot on the HART transit drivers (bus and streetcar). Transit drivers will be treated as employees of HART, the owner of the vehicles. This treatment corresponds to the approach taken with auto drivers in that only the owner of the vehicle needs to register and supply PII, while users of their vehicle are not required to do so. HART, thus, is the signatory and use of its vehicles is according to its contract with the Amalgamated Transit Union (Hillsborough Area Regional Transit and Amalgamated Transit Union Local 1593, October 1, 2012). HART will operate according to its standard operating procedures and will know which drivers have equipped vehicles. HART has had GPS/AVL equipment in place for ten years that tracks vehicles via CAD maps. The CV Pilot equipment will not add new capabilities to HART's current ability to monitor drivers' behavior. The performance and safety enhancements of the CV apps are what is of interest to HART.

The THEA team is preparing for Participant Recruitment of pedestrians and auto drivers to include the following methods and avenues of communication:

- Public-facing website
- Secure participant portal on the website for communications with participants
- Electronic newsletter to participants
- Email and/or SMS alert system for critical communication with participants
- User survey(s) at the end of the study by THEA and the IE which will have "blind" access to participants through THEA

These communications methods will require collection of information on participant contact information such as email address and phone number to send newsletters, emails, and/or SMS alerts. Participants may sign up for a registration appointment over the secure participant portal on the website with a username and

password. Per the ICDs for pedestrians and auto drivers, if there is a security breach related to personal information of participants, the THEA Pilot team will notify the participants of the breach, the nature of the breach, and how the team will resolve it.

In order to secure participant confidentiality, THEA will facilitate IE access to THEA's staff and stakeholders for the purposes of supporting surveys and interviews, but this will exclude the sharing of participant PII.

Per Phase I documents, stakeholders comprise three categories:

- General stakeholders: any entity having an interest or being impacted by the project;
- Partner stakeholder: any stakeholder who is also an active partner in the project (active participation or contribution) and;
- Participant stakeholders: registered users of the system. (NO ACCESS to this class of stakeholder by IE or any other 3rd party)

The participant data collected for participant management must be in an encrypted, standalone, password-protected database that is separate from all other CV traffic data that is to be used by the TMC staff, Performance Measurement team, IE or any other agency or research group accessing CV traffic data, now or in the future. The THEA Human Use team will establish a detailed IRB-approved process for handling participant data and provide a list of team personnel that have access to the participant data. The THEA CV Pilot team will limit access to those personnel who require access to the data in order to perform their administrative duties within the Pilot deployment, such as contacting drivers who do not appear to be any longer driving in the study area and so forth. These activities are well defined in the ICDs which the participants sign to give their approval before undergoing training and OBU or PID app installation. THEA personnel who are in contact with participants and participant data will have training and certification in Protecting Human Research Participants (PHRP), such as the PHRP Certification offered by the National Institutes of Health web-based training course or equivalent (National Institutes of Health, 2016).

At the registration location, the potential participant will watch a brief video explaining the Informed Consent process. A THEA staff person will present the person with an electronic ICD document (on a tablet or PC) and ask him/her to read it. (The ICD will be available in English and Spanish.) The staff person will offer to answer questions. Some staff will be bilingual (English/Spanish) to accommodate Spanish-preference participants. The participant will then sign or not sign the ICD. If the participant signs, they go on to the training and their vehicle is taken for installation of the device.

THEA will use secure software for taking of PII data when participants register. THEA will supply software for the taking of data by the registrar(s), which the participant will verify with ID – driver's license, vehicle registration and proof of insurance for drivers. The data will be uploaded to a secure database. With respect to the ICD signature there are two possibilities:

- Store paper copies of the signed ICD in a secure, locked file cabinet at the THEA registration facility.
- Store digital copies of the electronically signed ICD in the secure facility with the other registration information.

Participants will be given a paper copy or emailed a copy of their signed ICD, which will also act as a registration certificate with instructions for contacting the CV Pilot administrators if the participant has questions, sells the car, is involved in a crash, relocates, wishes to quit the study, and so forth. In order to ensure data quality and integrity for participant contact information, participants will have the ability to update their personal information via the Pilot portal, as well as access to a staffed Help Desk Center to resolve questions and complaints.

5.2. Other IRB Issues

This DPP is focused on data privacy and confidentiality. Beyond participant PII data integrity and storage, Salus IRB has general oversight of treatment of participants with respect to equity, safety, and Informed Consent. Participants must be treated fairly and equitably, fully informed of the study goals, what their participation involves, study risks, their legal rights, who to contact for questions, their ability to withdraw and the procedure to withdraw from the study at any time.These issues have been addressed in Phase I, Task 12 documents and are beyond the scope of this DPP treatment of IRB oversight of PII. Readers are referred to the HUAS, RPD and ICDs for further discussion.

5.3. Reporting

The Pilot shall report all events pertaining to privacy to the IRB and others as described below.

- Changes to privacy Plan shall be reported to Salus IRB and USDOT-JPO. Salus IRB shall determine if the change is approved and whether the change is of substantial significance to warrant notification of participants if a modified ICD must be provided to participants.
- System breaches or failures which are discovered by the Pilot and are conclusively determined to have not resulted in an unauthorized disclosure of PII will be reported to the Pilot PI, Pilot Management, Salus IRB and USDOT-JPO along with a resolution plan and status.
- System breaches or failures which are conclusively determined to have resulted in an unauthorized disclosure of PII will be reported to the Pilot PI, Pilot Management, Salus IRB and USDOT-JPO along with a resolution plan and status. Any unauthorized disclosure of privacy data will also require notification of participants and any State of Florida authority as determined in the legal compliance review by THEA counsel.
- Annual or other regularly scheduled audits shall be documented in a report of findings and shared with USDOT-JPO.
- Authorized disclosures of PII are only made to properly trained and IRB approved staff. Authorized disclosures will occur regularly throughout the process and shall not require reporting. There will however be an accounting of such disclosures and the accounting shall be made available during IRB audits.
- All of the reports in this section shall be retained in the project records according to the requirements of the applicable National Archives and Records Administration (NARA) records schedule (available from the USDOT Contracting Officer).

6. Support for the Independent Evaluator

In Phase II, a third-party site-specific independent evaluator(s) will execute USDOT-designed experimentation, data analysis, and qualitative evaluation. THEA will coordinate with and support these evaluation efforts in Phase II and Phase III. The precise nature and type of this support has been detailed in various Tasks in Phase I.

In general, there will be three types of data collected for the Pilot:

- Administrative participant data (also referred to as registrant data) (NO ACCESS by IE)
- CV application data (NO ACCESS by IE)
- Performance measurement data. (Direct access available to IE)

Participant data is necessary to track involvement, conduct training, and maintain communications. CV data is the data generated by OBUs, RSEs and mobile devices. Participant data is treated in Section 5.

CV application data is treated in other sections of the DPP.

Performance measurement data is generated from CV data as well as from additional sources, such as machine vision cameras and LIDAR installed on Pilot infrastructure (if used) and anonymous opinion surveys. Performance and other data supporting a comprehensive assessment of deployment impacts will be shared with the IE and the data needs associated with an independent evaluation effort will be supported. Data produced by the CV equipment for each Use Case will be stored in a database that is available to FHWA, the THEA team and the IE. Data will be scrubbed of all PII. The Use Case information flows are the source of data for the IE's performance measures, in whatever way the IE wishes to structure them.

6.1 Performance Data

THEA will support an IE effort as outlined in the Performance Measurement and Evaluation Support Plan (PMESP) (THEA, Task 5, PMESP, July 2016) and CDP (THEA, Task 12, CDP, August 2016), including:

- Relevant performance data and performance measure calculation procedures
- A summary of relevant analytical tools available to assist in evaluation, as well as access to and use of relevant analytical models (tool inputs), observed data for model calibration, and existing calibration/validation documents for the purpose of supporting independent evaluation
- Data related to the mitigation of confounding factors, including factors tracked, sources of available information utilized to track these factors, and mitigation approaches (if any) utilized. Examples of currently identified confounding factors include weather data, special events logs, changes in land use in the study area, changes to the street system, equipment anomalies, and participant self-selection, participant attrition and moral hazard effects. One example of moral hazard effect is the possibility that drivers may become more aggressive due to their confidence that the safety apps will protect them.

The CV Pilot will gather several types of data which will be scrubbed of potential PII and then shared with US DOT and the IE. In particular, Participant ID's will be entirely anonymized such that each trip will have a different, non-linkable anonymous ID. Only the Pilot's NIH-Certified Investigators will have access to the ability to tie anonymized data to Participant ID's for the purpose of handling technical issues. MAC addresses will only consist of the OBU MAC and no other vehicle system MACs will be collected.

Scrubbed data will be archived to the RDE for access by the research community. For each use case, a list of the data planned for sharing is listed below:

- **Morning Peak Hour Queues**
    - Normalized speed
    - Vehicle speed
    - BSMs
    - Signal timing updates
    - EEBL warnings
    - FCW warnings
    - ERDW warnings
- **Wrong Way Entries**
    - Vehicle BSMs
    - Wrong way entry warnings (the alert given to the driver via the HMI)
    - Wrong way driver warnings (the warning given to other drivers about a wrong way driver)
- **Pedestrian Safety**
    - Personal Safety Messages (PSM)
    - GPS corrected pedestrian BSMs
    - Vehicle BSMs
    - Pedestrian warnings
    - Driver warnings
- **Bus Rapid Transit Signal Priority Optimization, Trip Times and Safety**
    - Bus location
    - Bus movement
    - Bus number
    - Bus route
    - Bus schedule
    - Priority granted
    - Priority denied
    - Priority granted, then denied
- **TECO Line Streetcar Trolley Conflicts**
    - Vehicle BSMs
    - Streetcar BSMs

- PSMs
- GPS corrected Pedestrian BSMs
- Vehicle turning right in front of streetcar warnings
- Pedestrian warnings
- Vehicle warnings
- Streetcar warnings (to pedestrian only)

- **Enhanced Signal Coordination and Traffic Progression**

  - Vehicle BSMs

These data will be aggregated and cleansed into data sets. The actual aggregation and cleansing will be determined during the System Design. Raw and prepared data will be provided to the RDE once it has been stripped of all potential PII issues. If it is determined that some data cannot be completely stripped of PII issues and appropriate permissions cannot be obtained for sharing or storage, these data will not be shared and will be removed from the master server.

Once the CV Pilot is operational, the planned transmittal of data to the RDE will be on a quarterly basis, lagging by a quarter. This timeframe provides adequate time to amass an appropriate data sample and prepare the data.

6.1.1 Data Privacy

Privacy issues are considered in the context in which the collection occurs. Privacy concerns for state-owned service vehicles are different from those for data collected from private vehicles. The rules related to privacy must be communicated unambiguously.

1. Establish data ownership. As a rule, whoever owns the vehicle, owns the data generated by that vehicle. An OEM may also claim ownership of data published on the vehicle's data bus. This must be resolved.
2. Secure consent from the data owner. The owner of data must consent to providing the data in an agreement (drafted by the CV Pilot THEA team) that spells out how the data are used and by whom. This should include the re-distribution of data to third parties.
3. Protect the privacy of the data owner. Any information that reveals the identity of the data owner must be eliminated.
4. Identify data aggregation issues. In some cases, aggregating CV data over time can reveal patterns that are sensitive from the point of view of commercial, military, or other propriety information about the internal operations of firms or agencies. These situations will be handled individually as they arise. During initial data analysis, extra effort will be made to identify any new patterns which produce new PII data. No issues are anticipated for the Pilot as the study area is limited to one square mile and as such does not provide significant data to aggregated for tracking purposes which typically involves much longer trips and significant waypoints.

Prior to uploading data to any repository, necessary data sharing agreements will be obtained. These data sharing agreements will need to be approved by all entities, and/or their representatives, whose data will be included in the data sets that the CV Pilot team will be providing to the RDE.

6.1.2 Data Preparation

Within this step, the objective is to prepare the data sets for public research community consumption on the RDE. When the data are cleaned and prepared, the team can proceed with readying the data sets for posting or storing.

Some basic checks that are required in this stage are:

1. Data documentation is complete
2. Data are categorized and structured in a manner that is understandable and useful
3. Data elements are in standard formats (e.g., comma-separated value (CSV) format that enables other parties to read the data without the need of proprietary software)
4. Data conform to an appropriate ITS Standard (e. g., SAE J2735 for DSRC communications, SAE J2354 for center-to-center communications, or IEEE 1512 for incident management)
5. Data are cleared for sharing with appropriate data sharing agreements between the data providers and US DOT

These basic checks clear the data for archiving. Some special checks are required before data can be transmitted to the RDE:

1. Data are free of PII
2. Data are in a manageable size and format that is useful to the users (data are broken down into chunks that can be easily downloaded over the internet)
3. Data are tagged for efficient data queries
4. There are two types of data documentation that will accompany each data environment on the RDE (and most other repositories): 1) metadata documentation and 2) optional data handbook/dictionary documentation.
    a. Metadata documentation is in a format derived from the ASTM 2468-05 standard metadata format, so there is uniformity in content, structure, and format.
    b. The optional data handbook/dictionary document contains some of the same information as the metadata document but with additional information regarding files and data elements that were collected. In some cases, the data provider's existing documentation could serve or be slightly modified to serve as this optional data handbook/dictionary documentation. The additional information provided by the data handbook also includes:
        i. Details about how the data were collected and processed
        ii. Background information about the overall task that led to the collection of data being uploaded to the RDE
        iii. Specifics regarding how the data was structured
        iv. Supporting information as to how the aforementioned RDE requirements and procedures were completed for a particular data environment
        v. If a data handbook/dictionary document is being provided to the public via the US DOT, it must be in a Section 508 compliant format and it needs to undergo the US DOT publication process.

If all these checks are complete, the data can be cleared for transmission.

6.1.3 Transmitting Data

There are two main methods of transfer of the data to the public research users (through RDE) or to the USDOT:

1. Archived means
2. Near real-time transmission

If there are clear established purposes for either means, they will be carried out as outlined below:

- Archived data is prepared for transmission through acquiring and packaging data from the CV Pilot site over a length of time, such as over a period of hours, days or months. This form of transmission is appropriate where there is no established case for real-time communications. Also, the archived means of sharing data is appropriate in cases where sensitive data exists, like in the CV Pilot.

6.2 User Surveys

THEA will support an IE effort as outlined in the PMESP (THEA, Task 5, PMESP, July 2016), Human Use Approval Summary (HUAS) (THEA, Task 8, HUA, July 2016) and Comprehensive Deployment Plan (CDP) (THEA, Task 12, CDP, August 2016), including:

- Facilitation of IE access to site staff and non-participant stakeholders but excluding any and all contact with or access to participants
- THEA will assist the IE in developing and disseminating anonymous user opinion surveys.

THEA will facilitate IE access to THEA's staff and stakeholders to support surveys and interviews, but this effort must exclude the sharing of any and all participant personal information.THEA will work with the IE to send anonymous opinion surveys to participants without releasing PII to the IE. The use of participant data has not been permitted in any THEA reports to date and has been disallowed in numerous statements in the Phase I PMESP, SMOC and HUAS as well as the IRB-approved RPD and ICDs.

IE interaction with participants would require IRB approval and must be done separately from this Pilot and under the IE's "own" IRB approval. The IE's IRB approval and research protocol would also have to be reviewed and approved by THEA's IRB (i.e., Salus IRB) and any effort by or cost to the THEA team to provide assistance in this regard is out of scope for the Pilot.PilotPilotBy THEA's exclusive dissemination of IE user surveys to the participants without releasing PII to the IE, the need for the IE to involve another IRB is unnecessary. Only THEA will disseminate anonymous user surveys in accordance with its IRB (i.e., Salus IRB) approved RPD and ICDs. No PII will be released to the IE.

Since the participant in the transit (bus and streetcar) portion of the study is the HART agency, no participant PII is available to THEA. User surveys will be processed through HART to those who were drivers of OBU-equipped vehicles. THEA will work with the IE to deliver to HART user surveys for processing.

References

Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, FIPS PUB 199. (2004). *FIPS Pub 199.* Retrieved from http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, FIPS PUB 200 . (2006). *FIPS PUB 200.* Retrieved from http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf

Hillsborough Area Regional Transit and Amalgamated Transit Union Local 1593. (October 1, 2012). *Contract Between Hillsborough Area Regional Transit and Amalgamated Transit Union Local 1593.* Tampa, Florida.

In re Hulu Privacy Litig, No. C 11-03764 LB (U. S. Court of Appeals for the Frist Circuit April 2014).

National Institute of Standards and Technology, NIST Special Publication 800-53 Revision 4. (2013). Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-53r4

National Institute of Standards and Technology, NIST Special Publication 800-60 Revision 1. (2008). *NIST Special Publication 800-60.* Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

National Institutes of Health. (2016). *Protecting Human Research Participants (PHRP) Training web page.* https://phrp.nihtraining.com/users/login.php.

Official (ISC)² Guide to the CISSP CBK, Fourth Edition. (2015). ISC2 Press.

Technology, N. I. (2008). *NIST Special Publication 800-60.* Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v1r1.pdf

THEA. (Task 11, Outreach, Draft - July 2016). *Connected Vehicle Pilot Outreach Plan – Tampa, FHWA-JPO-16-320.* Federal Highway Administration (FHWA), USDOT.

THEA. (Task 12, CDP, August 2016). *Connected Vehicle Pilot Comprehensive Deployment Plan - Tampa, FHWA-JPO-311.* Federal Highway Administration, USDOT.

THEA. (Task 3, SMOC, April 2016). *Connected Vehicle Pilot Privacy and Security Mangement Operating Concept - Tampa, FHWA-JPO-16-312.* Federal Highway Administration, USDOT.

THEA. (Task 4, Safety, April 2016). *Connected Vehicle Pilot Safety Management Plan - Tampa, FHWA-JPO-16-313.* Federal Highway Administration, USDOT.

THEA. (Task 5, PMESP, July 2016). *Connected Vehicle Pilot Performance Measurement and Evaluation Support Plan - Tampa, FHWA-JPO-16-314.* Federal Highway Administration, USDOT.

THEA. (Task 8, HUA, July 2016). *Connected Vehicle Pilot Human Use Approval Plan - Tampa, FHWA-JPO-16-317.* Federal Highway Administration, USDOT.

THEA. (Task 9, PTSEP, August 2016). *Connected Vehicle Pilot Participant Training and Stakeholder Education Plan - Tampa, FHWA-JPO-318.* Federal Highway Administration, USDOT.

Yershov v. Gannett (U.S. Appeals Court for the First Circuit).

Acronyms

Table 2: Acronyms

ACRONYM	DEFINITION
ADP	Application Deployment Plan
AES	Advanced Encryption Standard
AOR	Agreement Officer Representative
BRT	Bus Rapid Transit
BSM	Basic Safety Message
CAMP	Crash Avoidance Metrics Partnership
CISSP	Certified Information Systems Security Professional
ConOps	Concept of Operations
CV	Connected Vehicle
DMP	Data Management Plan
DOP	Deployment Outreach Plan
DPP	Data Privacy Plan
DSRC	Dedicated Short Range Communications
EEBL	Emergency Electronic Brake Light
FCW	Forward Collision Warning
FDOT	Florida Department of Transportation
FHWA	Federal Highway Administration
FIPS	Federal Information Processing Standard
FWA	Federal Wide Assurance
HART	Hillsborough Area Regional Transit
HMI	Human Machine Interface
HHS	Health and Human Services
HPRP	Human Protection Research Protocol
HUA	Human Use Approval
HUAS	Human Use Approval Summary
ICD	Informed Consent Document
IE	Independent Evaluator
IEEE	Institute of Electrical and Electronics Engineers
IMA	Intersection Movement Assist
IRB	Institutional Review Board
(ISC)^2	International Information System Security Certification Consortium
I-SIG	Intelligent Signal Systems
ITS	Intelligent Transportation Systems
JPO	Joint Program Office
MOU	Memorandum of Understanding
OBU	On-Board Unit

OEM	Original Equipment Manufacturer
OIS	Outreach Implementation Schedule
PDETM	Probe Data Enabled Traffic Monitoring
PED-SIG	Mobile Accessible Pedestrian Signals System
PED-X	Pedestrian in a Signalized Crosswalk
PID	Personal Information Devices
PII	Personally Identifiable Information
PMESP	Performance Measurement and Evaluation Support Plan
RDE	Research Data Exchange
RFI	Request for Information
REL	Reversible Express Lanes
RLVW	Red Light Violation Warning
RSU	Road Side Unit
SAE	Society of Automotive Engineers
SCMS	Security Credential Management System
SAD	System Architecture Document
SMOC	Security Management Operating Concept
SPII	Sensitive Personally Identifiable Information
SyRS	System Requirements Specification
THEA	Tampa Hillsborough Expressway Authority
TMC	Transportation Management Center
TSP	Transit Signal Priority
UMTRI	University of Michigan Transportation Research Institute
USDOT	United States Department of Transportation
V2I	Vehicle-To-Infrastructure
V2V	Vehicle-To-Vehicle
V2X	Vehicle-To-Everything
VIN	Vehicle Identification Number
VTRFTV	Vehicle Turning Right in Front of a Transit Vehicle

Appendix 1 Architecture Diagrams w/Privacy Control Table

The following architecture diagrams are drawn from the SAD and modified to indicate the privacy controls applied to each use case. Figure A1 is an overview of the system as a whole. Figures A2-A7 represent the Use Case Diagrams. Table A1 Indicates the controls applied to each flow type from the drawings as indicated

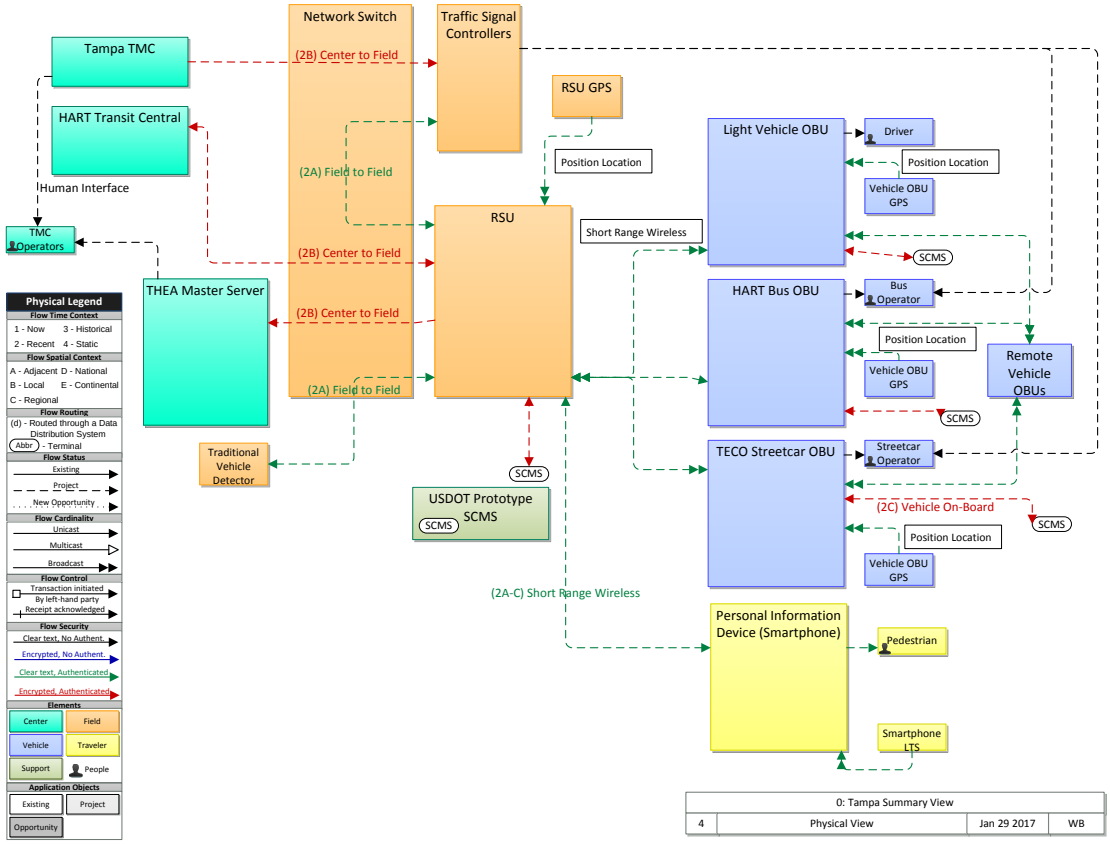

Figure A1 Physical Architecture – System-wide Overview

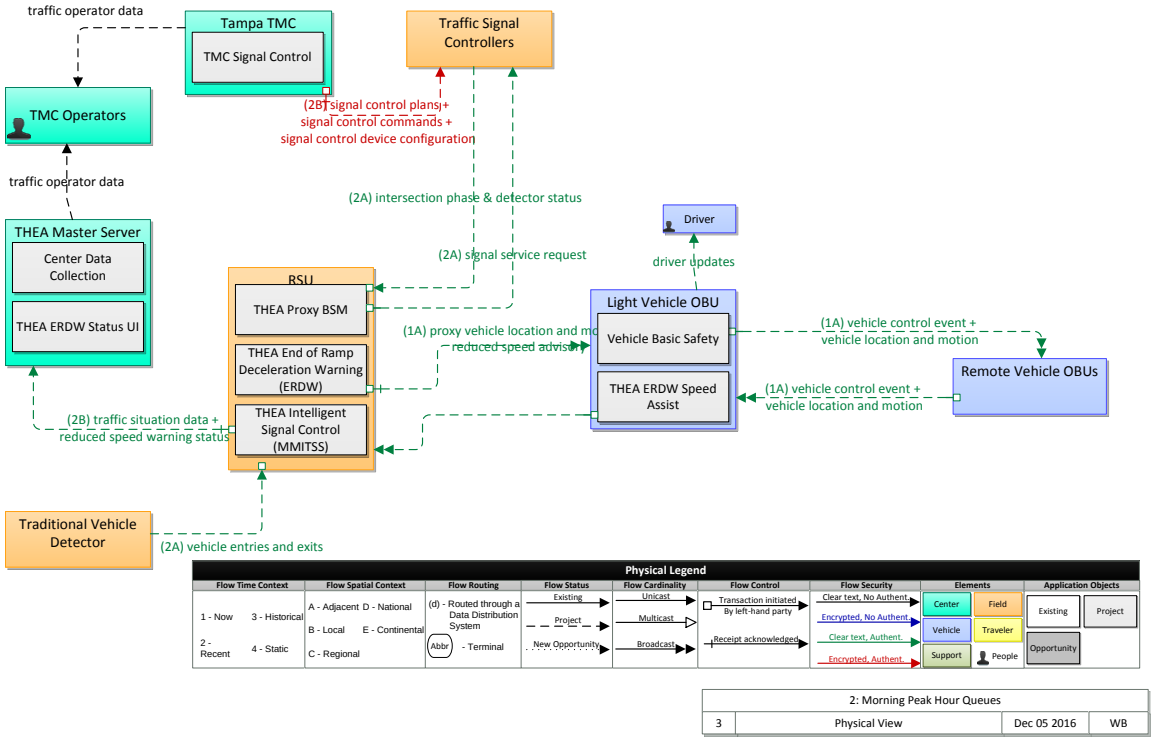

Figure A2 Use Case 1

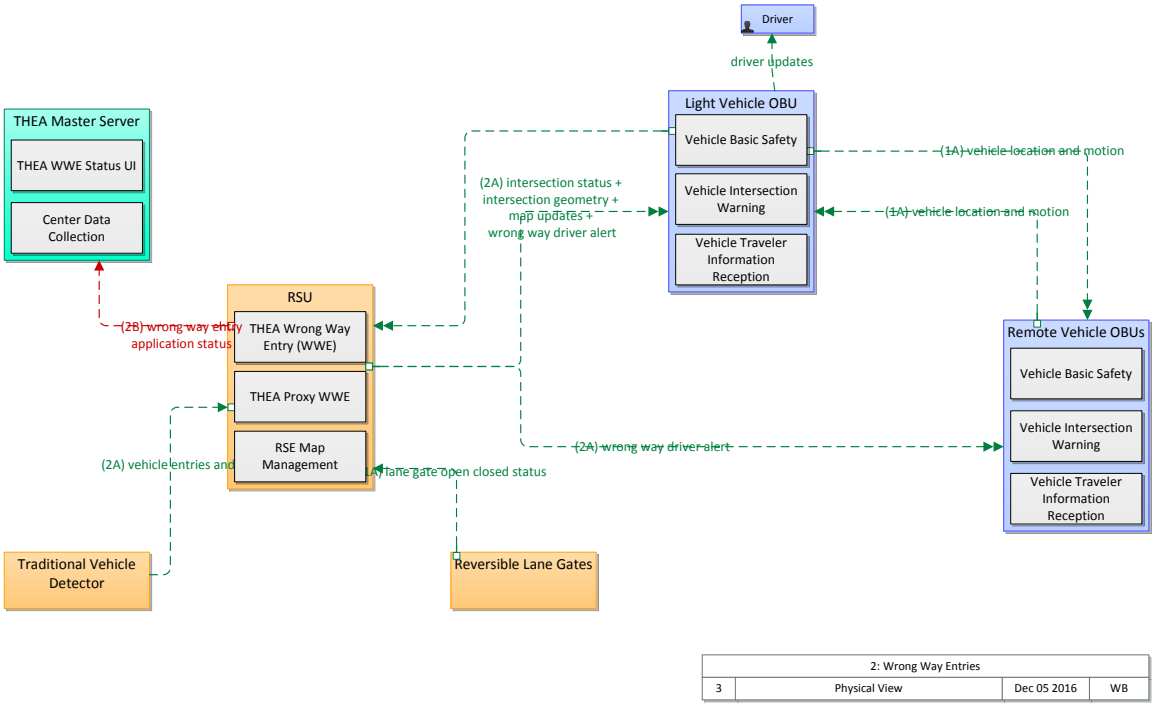

Figure A3 Use Case 2

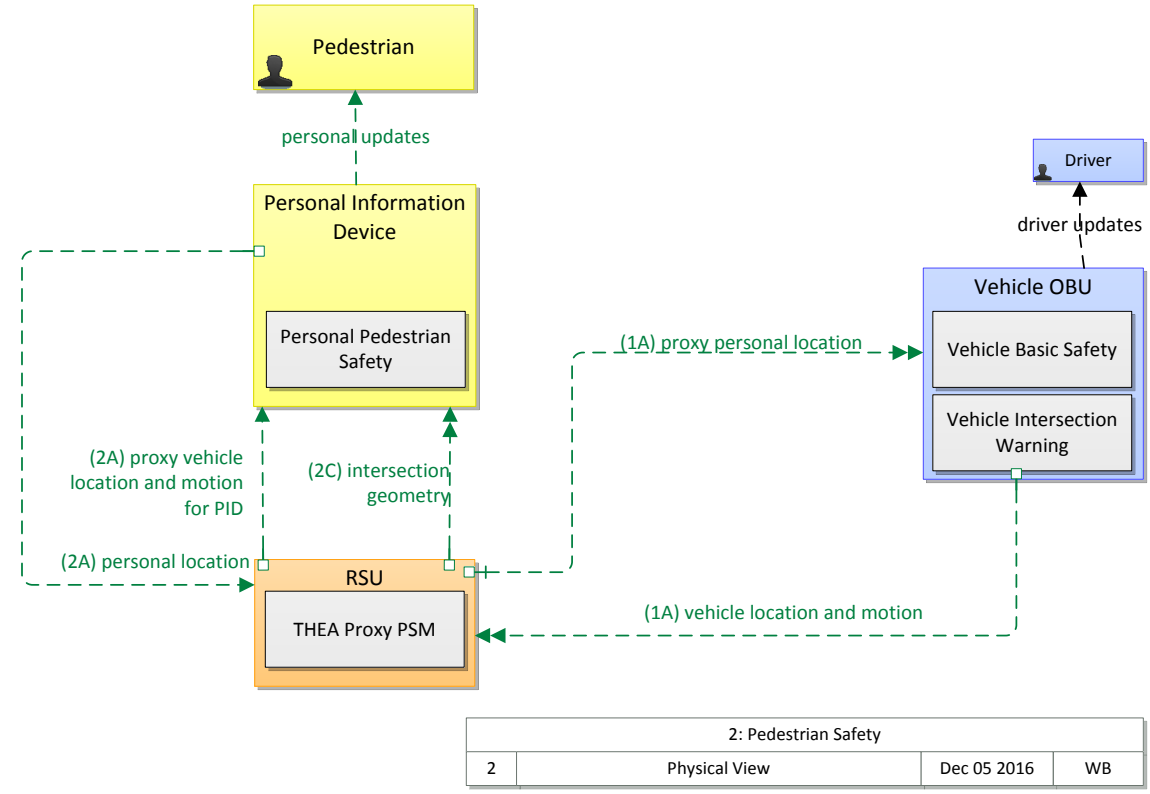

Figure A4 Use Case 3

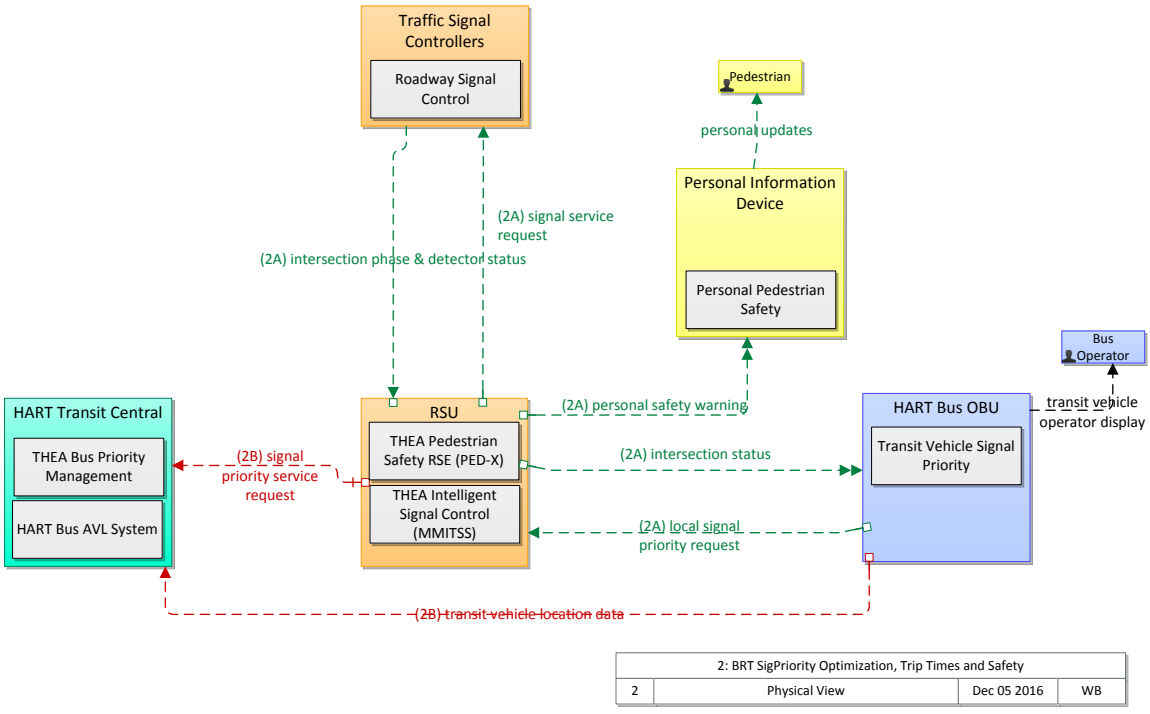

Figure A5 Use Case 4

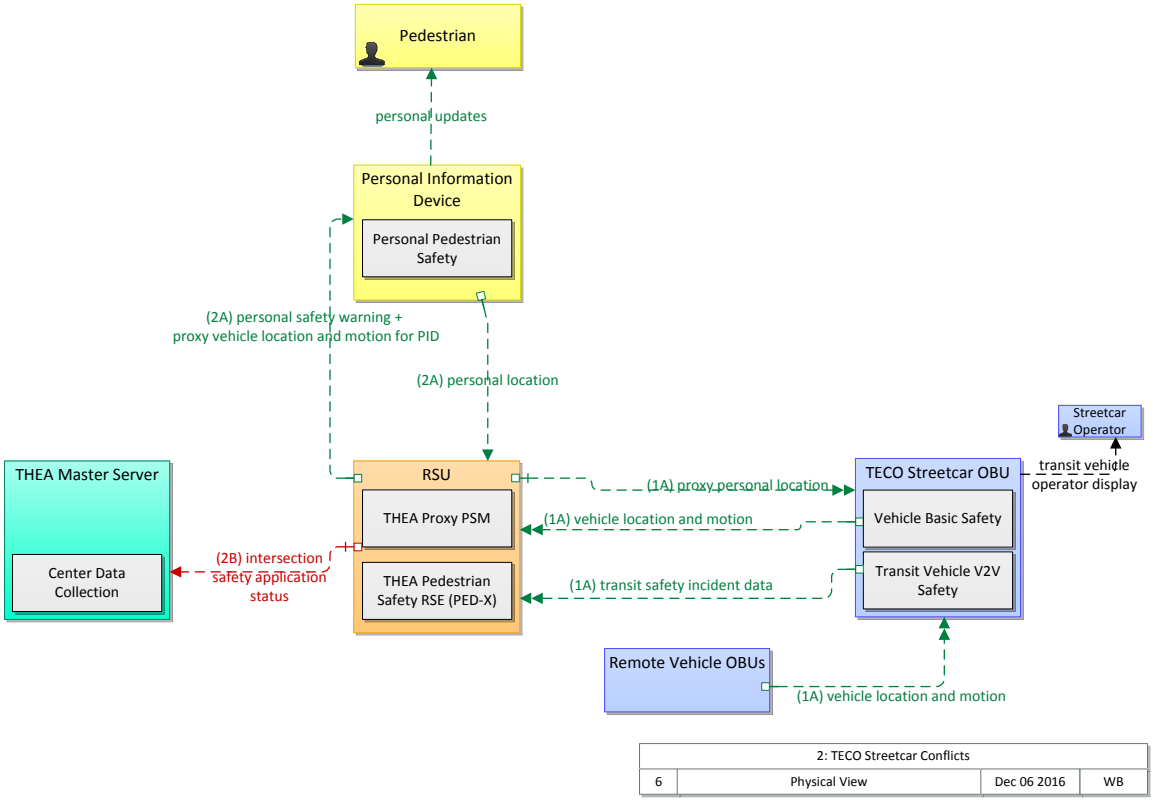

Figure A6 Use case 5

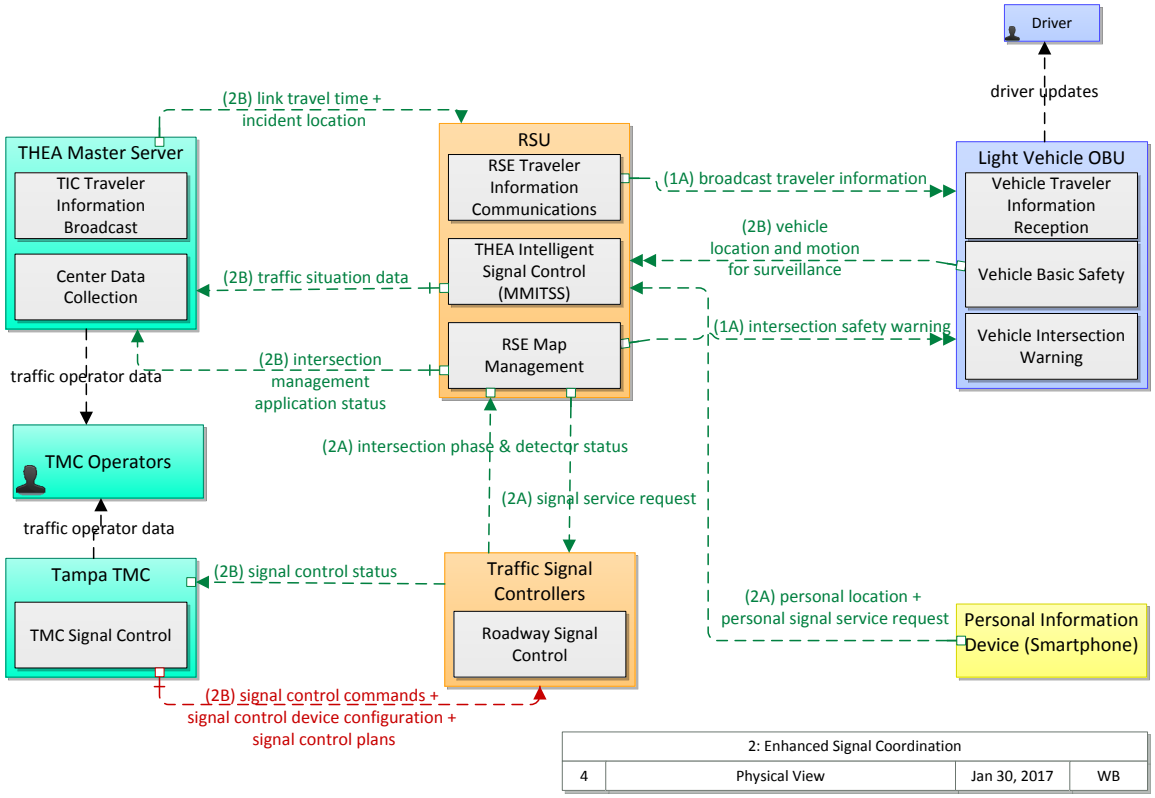

Figure A7 Use Case 6

Clear Text – No Authentication	Access Control (4.4.4 & 4.4.5); Penetration Testing (4.4.8); System Monitoring (4.4.9); Breach Detection and Remediation (4.4.15)
Encrypted No Authentication	Encryption (4.4.3); Breach Detection and remediation (4.4.15)
Clear Text Authenticated	SCMS (4.4.1); Access Control (4.4.4 & 4.4.5); Penetration Testing (4.4.8); System Monitoring (4.4.9); Breach Detection and Remediation (4.4.15)
Encrypted Authenticated	Encryption (4.4.3); Authorization (4.4.6 & 4.4.7); System Monitoring (4.4.9); Breach Detection and Remediation (4.4.15)

Table A1 Controls applied by application flow Type

U.S. Department of Transportation
ITS Joint Program Office-HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free “Help Line” 866-367-7487
www.its.dot.gov

FHWA-JPO-17-461

U.S. Department of Transportation