Connected Vehicle Pilot Deployment Program Phase 2

Security Management Operational Concept – Tampa (THEA)

www.its.dot.gov/index.htm
Final Report — December, 2018
FHWA-JPO-18-693

Source: USDOT

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

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.
The U.S. Government is not endorsing any manufacturers, products, or services cited herein and any trade name that may appear in the work has been included only because it is essential to the contents of the work.

Technical Report Documentation Page

1. Report No. **FHWA-JPO-18-693**	**2. Government Accession No.**	**3. Recipient's Catalog No.**

4. Title and Subtitle Connected Vehicle Pilot Deployment Program Phase 2 Security Management Operational Concept - Tampa Hillsborough Expressway Authority (THEA)	**5. Report Date** December/2018
	6. Performing Organization Code
7. Author(s) Joe Waggoner (THEA), Bob Frey (THEA) Steve Johnson (HNTB), Linda Rolfes (HNTB)	**8. Performing Organization Report No.**
9. Performing Organization Name And Address HNTB Corporation, 210 N. Franklin St, Suite 1200, 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. DTFH6116H00025
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** Final Security Management Operating Concept, PH2 update July 2018
	14. Sponsoring Agency Code (

15. Supplementary Notes

Govindarajan 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. 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 I includes the planning for the CV pilot including the concept of operations development. Phase II is the design, development, and testing phase. Phase III includes a real-world demonstration of the applications developed as part of this pilot).

This document presents the Security Management Operating Concept (SMOC). It provides guidance material regarding security and privacy for the THEA Deployment Phase 2. The document is presented based on identifying the impacts of security breaches regarding confidentiality, integrity, and availability along with the potential threats. It is important to note that security requirements in the SMOC are developed to address privacy by design. Additional references for security analyses, V2V security, the Security Credential Management System, and connected vehicle application security needs are included.

This document is an updated replacement of the SMOC developed in Phase I to more narrowly reflect the final design of the THEA CV Pilot as deployed in Phase 2. The original phase I SMOC has been archived under its phase I publication number and will remain available.

17. Key Word. Connected Vehicle Technologies, Cybersecurity, Privacy, DSRC V2I, V2V, V2X, SCMS	**18. Distribution Statement**

19. Security Classif. (of this report) **Unclassified**	**20. Security Classif. (of this page)** **Unclassified**	**21. No. of Pages** 61	**22. Price**

Reproduction of completed page authorized

Acknowledgements

The THEA Security Management Operating Concept (SMOC), Phase 2 development team would like to thank Joshua Kolleda, Dominie Garcia, and Tyler Polin, of Booz Allen Hamilton, for their original work on several sections of the Phase 1 SMOC. Significant changes to ultimate design vs. phase I concept indicate the need for this newly formed document for phase 2, but substantial sections are re-utilized and acknowledged here. We acknowledge the timely and high-quality support offered by USDOT and the support contractor, Noblis.

TABLE OF CONTENTS

List of Tables

List of Figures

Executive Summary

The Security Management Operating Concept (SMOC) provides a high-level view of the information security governance, policies and concepts as they will be applied to ensure the privacy of pilot participants and the overall security of the Vehicle-to-Everything (V2X) system (e.g., communications, access, hardware, software) for the Tampa Hillsborough Expressway Authority (THEA) CV Pilot.

Scope and Approach

The THEA CV SMOC includes overviews for V2X system security and privacy for communications, access, hardware, software, and operating systems. The SMOC also includes a V2X system threat assessment, incorporating local Pilot threat surfaces into the national V2X threat inventory. Discussion of guiding principles outlined in Federal and industry publications are covered and include tools that may be used in forming the subsidiary documents that will provide policies and procedures for the implementation of the principles discussed herein. These subsidiary documents consist of the Phase 2 Data Privacy Plan (DPP) (published – Feb 2017, FHWA-JPO-17-461); Data Privacy Procedures Manual (DPPM) (Confidential/Internal) and any subsequent policy or procedure change documents (Confidential/Internal).

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 is in scope for the SMOC but the controls selected and implemented are detailed in the confidential DPP and DPPM as opposed to this published document.

Application information flow analysis is limited to the applications planned to be deployed by the THEA team. The security control analysis focuses on the new devices that must be deployed in the pilot, which are primarily the Vehicle On-Board Unit (OBU), Roadside Unit (RSU) and the Central Server. However, the Intelligent Transportation Systems (ITS) Roadway Equipment (RE)[1], Transportation Management Center (TMC), and Transit Management Center (MC) information flows are considered within the analysis and for security control selections.

[1] ITS Roadway Equipment is based on the CVRIA definition "physical objects that represent all of the other ITS field equipment that interfaces with and supports the Connected Vehicle Roadside Unit (RSU). This physical object includes traffic detectors, environmental sensors, traffic signals, highway advisory radios, dynamic message signs, CCTV cameras and video image processing systems, grade crossing warning systems, and ramp metering systems. Lane management systems and barrier systems that control access to transportation infrastructure such as roadways, bridges and tunnels are also included. This object also provides environmental monitoring including sensors that measure road conditions, surface weather, and vehicle emissions. Work zone systems including work zone surveillance, traffic control, driver warning, and work crew safety systems are also included."

The THEA team approached SMOC development in four phases that combined recommendations from the U.S. Department of Transportation (USDOT) guidance documents on privacy considerations and security management with information from other related projects and reports. Our four steps are:

1) Gather and Review Existing Analyses and References
2) Categorize Information Flows and Systems based on FIPS 199
3) Select Security Controls based on FIPS 200 and NIST SP 800-53
4) Conduct Coordination/Reviews and Finalize Concept

Requirement Areas

Dedicated Short Range Communications (DSRC) Security for the THEA CV Pilot was originally planned to be largely ensured through compliance with the Security Credentials Management System (SCMS) Proof of Concept (POC) design and existing standards, such as Institute of Electrical and Electronics Engineers (IEEE) 1609.2. However, the CAMP SCMS version did not include misbehavior detection, and has been discontinued during phase 2 of the Pilots. As such, the THEA CV Pilot team contracted with a commercial SCMS provider and has presented some conceptual misbehavior detection strategies primarily based on plausibility checks[2] on incoming BSMs and implementation of a device profile which establishes baseline expectations for individual devices.

Personally Identifiable Information (PII) collected in the THEA CV pilot will be kept to the minimum necessary for the Pilot system to function effectively. The current application assessment does not directly reveal any Personally Identifiable Information (PII)[3] being collected through the deployed applications However, concerns have been raised on the overall privacy implications of a system in which vehicles broadcast location and motion information 10 times every second. This data could be merged with other data sources including CV Data Logs, telematics systems, onboard OEM data, et al; to provide information regarding specific occurrences or collisions, including potentially identifying individual devices.
Outside of V2X communications for CV applications, PII will be collected from participants for tracking equipment, conducting training, and maintaining continuous communications. This information must be protected while ensuring only limited access to the necessary THEA team personnel to complete equipment maintenance, training, and communications. The final controls selected and implemented for PII protection are detailed in the DPP.

Hardware Security for THEA pilot devices will be met by adhering to specific levels identified in FIPS 140-2: Security Requirements for Cryptographic Modules. FIPS 140-2 provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. The security requirements within these levels cover areas including cryptographic module specification, cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility; self-tests; design assurance; and mitigation of other attacks.

[2] Plausibility checks are used to validate the correctness and feasibility of the data within a BSM, such as assessing whether data parameters are realistic based on average vehicle performance and laws.
[3] NIST Special Publication 800-122 defines Personally Identifiable Information (PII) "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual‘s identity, such as name, social security number, date and place of birth, mother‘s maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

While FIPS 140-2 addresses the majority of hardware security requirements, it does not cover all software and operating system requirements. These requirements are protected through recommended architectures for the interactions between the host processor and Hardware Security Module (HSM), as well as operations such as integrity tests upon boot and secure software update procedures. OmniAir Consortium provides device certification via certified labs for DSRC equipment. Omniair DSRC device certification has been indicated by USDOT as a minimal standard for participation in the national SCMS (or approved commercial SCMS)

Authorized Access to V2X devices and data must also be managed through policies and technical strategies. The SMOC describes recommended changes to existing THEA TMC system roles and policies to manage new CV data and remote access to RSUs. Permissions to access CV data and participant specific data must be separated among various roles and entities. Those with access to raw CV data should not have access to participant data as connections could be made between participant and specific trip data. Controls selected and implemented are detailed in the DPP and DPM.

Minimum Device Requirements

The FIPS 199/200 and NIST SP 800-53 analysis (Appendix B) based on classifying application information flows between devices according to Confidentiality, Integrity, and Availability criteria resulted in the identification of one device class for the THEA Pilot.

1. Low, Moderate, Moderate (LMM) devices include the OBU, RSU and Central Server. In this case, the information flows sent or received by these devices have a Confidentiality classification of Low, Integrity classification of Moderate, and Availability classification of Moderate. These devices pose less of a security and privacy threat because their information flows are mostly broadcasted and intended to be received by any nearby devices; false information that is accepted has the potential to increase physical risk without directly causing physical harm; for information flows to be useful, they must be available a significant amount of time. Originally these devices were categorized as LHM, but because there will be measures enacted to detect misbehavior and revoke certificates as well as permissions, Integrity was downgraded to Moderate.

Based on our application information flow analysis and knowledge of the NIST SP 800-53 security controls for medium baseline devices, the team developed a list of recommended minimum security requirements (Chapter 7) for the LMM devices used in the THEA CV Pilot. These recommended requirements focus on:

Communications Security

- IEEE 1609.2 (2016) compliance
- IEEE 1609.3 (2016) compliance
- Society of Automotive Engineers (SAE) J2945/1 compliance
- SCMS Implementation EE (End Entity) Requirements and Specifications Supporting SCMS Software Release 1.0 requirements compliance
- Potential strategies to maintain (and/or increase) participant privacy
- Potential misbehavior detection strategies

Hardware Security

- FIPS 140-2 Level 2 (applicable elements) and OmniAir certification. This requirement is limited to the tamper proof elements of hardware security; specifically, the need for encryption to be automatically zeroized if the hardware is breached.

Software and Operating System (OS) Security

- Host processor: Boot, OS, and secure software and firmware requirements

- Hardware Security Module (HSM) requirements including FIPS 140-2 approved encryption and ability to interface with hardware security for automatic wiping of encryption upon detection of tampering.
- Architecture-specific requirements, depending on the architecture type selected for the host processor and HSM

Access Security

- Roles and permissions
- User name and password strategies and requirements
- Remote access requirements based on V2X device type
- Requirements for separation of data and access to that data

1. Introduction

The Security Management Operating Concept (SMOC) provides discussion of principles and controls available and considered for establishing best practices to safeguard the privacy of pilot participants and the overall security of the V2X system (e.g., communications, access, hardware, software) for the Tampa Hillsborough Expressway Authority (THEA) CV Pilot.

The SMOC describes the tools and potential actions that may be used by the team during the Pilot Deployment to protect the privacy of users, guard against potential breaches of the system, and maintain secure operations of the V2X communications system. The SMOC outlines privacy considerations and how privacy by design is built into the Security Credentials Management System (SCMS). Where privacy is not sufficiently addressed by the SCMS, this SMOC explains additional controls that may be taken by the pilot team to increase privacy, such as the protection of participant data used for CV Pilot administration purposes and using sanitization algorithms for vehicle situation data as necessary. The SMOC also defines the device and system requirements to provide reasonable assurance of communications, access, hardware, software, and operating system security.

1.1. Scope

The THEA CV SMOC includes overviews for 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 security controls. While the SMOC does not further detail the standard NIST SP 800-53 security controls, the SMOC does provide minimum recommended security requirements for pilot device classes.

Application information flow analysis is limited to the applications planned to be deployed by the THEA team. The security control analysis focuses on the new devices that must be deployed in the pilot, which are primarily Vehicle On-Board Equipment (OBU), Transit OBU, and Roadside Unit RSU). However, the Vehicle Databus, Intelligent Transportation Systems (ITS) Roadway Equipment (RE)[4], Transportation Management Center (TMC), and Transit Management Center (MC) information flows are considered within the analysis and for

[4] ITS Roadway Equipment is based on the CVRIA definition "physical objects that represent all of the other ITS field equipment that interfaces with and supports the Connected Vehicle Roadside Unit (RSU). This physical object includes traffic detectors, environmental sensors, traffic signals, highway advisory radios, dynamic message signs, CCTV cameras and video image processing systems, grade crossing warning systems, and ramp metering systems. Lane management systems and barrier systems that control access to transportation infrastructure such as roadways, bridges and tunnels are also included. This object also provides environmental monitoring including sensors that measure road conditions, surface weather, and vehicle emissions. Work zone systems including work zone surveillance, traffic control, driver warning, and work crew safety systems are also included." However, not all of these devices or systems are utilized by the Pilot.

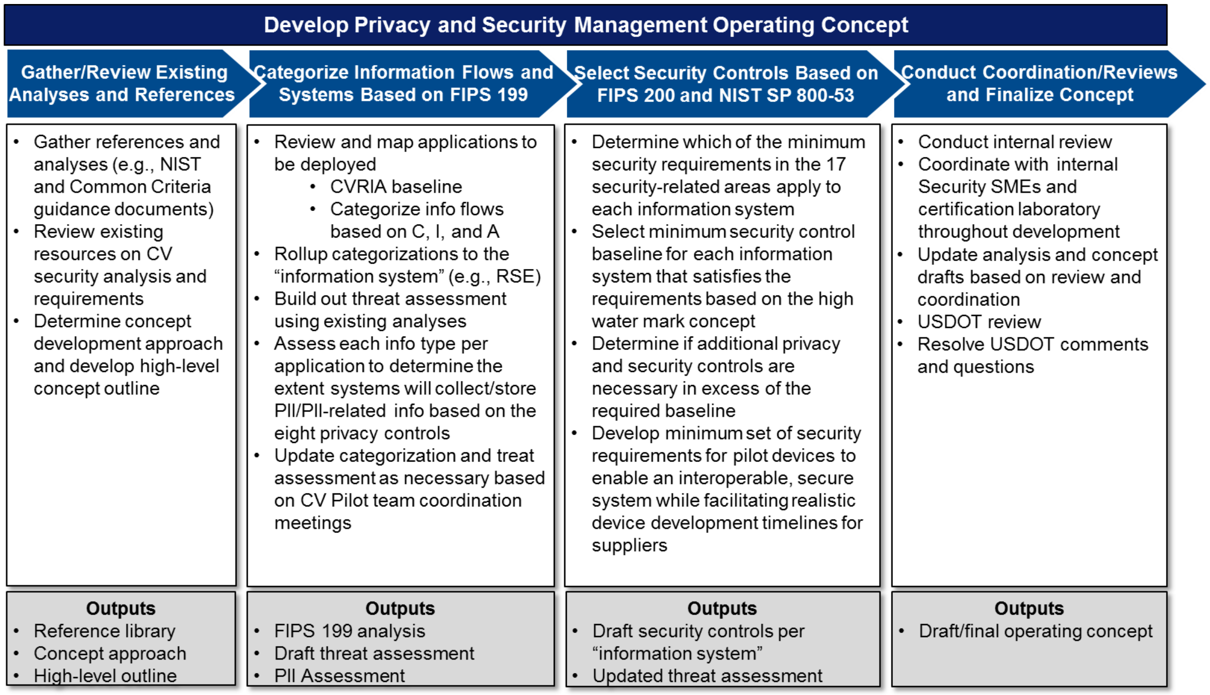
security control selections. Not all of these flows are in the final design but were considered during the analysis for future use.

1.2. Security Management Operating Concept (SMOC) Approach

The THEA team approached SMOC development in four phases that combined recommendations from the USDOT guidance documents on privacy considerations and security management with information from other related projects and reports. The four phases are:

1) Gather and Review Existing Analyses and References
2) Categorize Information Flows and Systems based on FIPS 199
3) Select Security Controls based on FIPS 200 and NIST SP 800-53
4) Conduct Coordination/Reviews and Finalize Concept

Figure 1-1. THEA CV Pilot SMOC Approach



Develop Privacy and Security Management Operating Concept

Gather/Review Existing Analyses and References	Categorize Information Flows and Systems Based on FIPS 199	Select Security Controls Based on FIPS 200 and NIST SP 800-53	Conduct Coordination/Reviews and Finalize Concept
• Gather references and analyses (e.g., NIST and Common Criteria guidance documents) • Review existing resources on CV security analysis and requirements • Determine concept development approach and develop high-level concept outline	• Review and map applications to be deployed • CVRIA baseline • Categorize info flows based on C, I, and A • Rollup categorizations to the "information system" (e.g., RSE) • Build out threat assessment using existing analyses • Assess each info type per application to determine the extent systems will collect/store PII/PII-related info based on the eight privacy controls • Update categorization and treat assessment as necessary based on CV Pilot team coordination meetings	• Determine which of the minimum security requirements in the 17 security-related areas apply to each information system • Select minimum security control baseline for each information system that satisfies the requirements based on the high water mark concept • Determine if additional privacy and security controls are necessary in excess of the required baseline • Develop minimum set of security requirements for pilot devices to enable an interoperable, secure system while facilitating realistic device development timelines for suppliers	• Conduct internal review • Coordinate with internal Security SMEs and certification laboratory throughout development • Update analysis and concept drafts based on review and coordination • USDOT review • Resolve USDOT comments and questions
Outputs • Reference library • Concept approach • High-level outline	**Outputs** • FIPS 199 analysis • Draft threat assessment • PII Assessment	**Outputs** • Draft security controls per "information system" • Updated threat assessment	**Outputs** • Draft/final operating concept

Source: BAH/HNTB

1.3. Gather and Review Existing Analyses and References

The THEA team gathered all relevant references and existing analyses to develop a reference library. This reference library, with full references listed in Appendix D, includes standards documents such as FIPS 140-2 and Common Criteria (CC) Parts 1, 2, and 3. It also includes reports and analyses from other published projects such as the CAMP V2V-Interoperability reports. We then reviewed analyses and references to determine what information could be used for the SMOC. Based on the USDOT guidance and existing references, we determined our concept approach, which is primarily focused on the first two steps of the NIST Risk Management Framework: Categorize information system (FIPS 199) and Select security controls (FIPS 200 and NIST SP 800-53). However, it also draws upon the Common Criteria methodology of security control development and other existing analyses such as the European Telecommunications Standards Institute (ETSI) Threat, Vulnerability, and Risk Analysis (TVRA). After finalizing the concept approach, the team developed a high-level outline of the SMOC.

1.3.1. Categorize Information Flows and Systems based on FIPS 199

The next phase involved categorizing information flows of the applications to be deployed in the THEA CV Pilot based on the Confidentiality, Integrity, and Availability criteria specified in FIPS 199. After the team completed the information flow classifications, the information flows were filtered by the source and destination device type. Based on the information flow classifications in which a device was a source or destination, the device was classified based on the Confidentiality, Integrity, and Availability criteria as well. The devices were classified according to the high-water mark system (i.e., the device will carry the same classification as the highest information flow). During this process, the team conducted an assessment of the information flows to determine the extent that systems collect and store PII and/or PII-related information. The team also consolidated the threat assessments of multiple existing analyses to develop a combined threat assessment for the THEA CV Pilot.

1.3.2. Select Security Controls based on FIPS 200 and NIST SP 800-53

The team reviewed and selected the security controls for each device class based on FIPS 200 and NIST SP 800-53. We further specify those controls by application and data type in the The SMOC includes a minimum set of security requirements for pilot devices, while detailed requirements developed from the Threat Definition of V2I Architecture project will be used as guidance for future devices. The SMOC focuses on a minimum set of requirements to enable an interoperable, secure system while still facilitating realistic device development timelines for device suppliers.

1.3.3. Conduct Coordination/Reviews and Finalize Concept

The final phase consisted of coordination among the teams and reviews within the THEA team and by USDOT to finalize the SMOC. Coordination among the teams occurred throughout the SMOC development. The THEA team also coordinated with internal security subject matter experts and testing labs with experience in the commercial, federal, and defense areas to review the security analysis and selected security controls.

2. Communications Security Overview

Communications security for the THEA CV Pilot is largely ensured through compliance with the SCMS design and existing standards, such as IEEE 1609.2/3. The SCMS design and existing standards are referenced in this chapter. This chapter also addresses considerations not fully covered in the SCMS and existing standards such as misbehavior detection and maintaining privacy in applications and situations unique to the THEA CV Pilot.

2.1. Communications Security Standards

This section describes the security standards to which V2X communications and devices must comply to provide communications security and privacy.

2.1.1. IEEE 1609.2

All Wireless Access in Vehicular Environments (WAVE) devices (i.e., OBU, RSU) shall comply with IEEE 1609.2: Standard for WAVE – Security Services for Applications and Management Messages. ITS RE, TMC, and Transit MC should also comply with IEEE 1609.2 and contain the necessary libraries. The current working version of the standard is IEEE 1609.2 (2016). This standard describes secure message formats and processing for use by WAVE devices, including methods to secure WAVE management messages and methods to secure application messages. It also describes administrative functions necessary to support the core security functions.

IEEE 1609.2 defines formats and methods to create, decode, sign, and verify using:

- Signed messages, which are used by all broadcast communications (e.g., BSM, SPaT, MAP, TIM)
- Encrypted messages, which are used for IPv6 based communications with back office systems
- Security test profiles, which are summaries of attributes applicable for a specific type of message
    - BSM transmission and reception security profile is covered in SAE J2945/1 V5
    - WSA security profile is covered in IEEE 1609.3 (2016)
    - SPaT, MAP, and TIM security profiles are covered in the Certification Operating Council (COC – currently OMNIAIR) System Functional and Performance Specification Ver. 0.4.0
    - Note: IPv6 security profile is TBD
- Mechanisms for peer-to-peer certificate distribution

2.1.2. Additional Standards and Protocols

While all devices and communications nodes (e.g., OBU, RSU, ITS RE, and TMC) must be compatible with IEEE 1609.2, devices must support other standards and protocols (e.g., TCP/IP, TLS) as identified in the SCMS to complete use cases such as bootstrapping, requesting certificates, etc. Devices will sign and/or encrypt data exchanged over non-DSRC IP communications (i.e., cellular, WiFi direct) interfaces with IEEE 1609.2 certificates.

2.2. Security Credentials Management System (SCMS)

This section describes the current SCMS design and how it will be used for the Tampa CV Pilot. The section references SCMS design documentation, interfaces, and process information. Within the SCMS, the THEA CV Pilot is only responsible for the Device Configuration Manager (DCM) and the V2X devices (e.g., OBU, RSU used within the deployment. For all interactions between these system elements and the other elements of the SCMS, the interface is fully specified by the SCMS Operator, who also provides functionality across fully-tested implementations of those interfaces.
NOTE: During Phase 2 of the pilot, THEA determined that the CAMP SCMS POC was not adequately positioned to service the specific needs of the pilot within the given timeframe of the cooperative agreement. The THEA CV Pilot Team, with approval from USDOT JPO, contracted with a private, commercial SCMS to replace the CAMP SCMS POC. The requirements for enrollment in the commercial SCMS remain substantially the same and as such this section remains substantially unchanged from the Phase 1 SMOC.

2.2.1. SCMS Requirements, Interfaces, and Processes

THEA CV Pilot devices must support requirements identified in the SCMS Implementation End Entity (EE) Requirements and Specifications Supporting SCMS Software Release 1.0 Appendix A and B to complete processes and use cases. Refer to the SCMS documentation for full requirements. Processes and use cases include but are not limited to:

- Core Communication
    - Universal SCMS Handshake
    - File Download Operations
    - Sending SCMS Messages
- Services
    - Provision Pseudonym Certificate Batch
    - Download.info file
    - Download Global Policy File
    - Download Pseudonym Certificate Batch
    - Retrieve Registration Authority Certificate
- Use Cases
    - OBU
        - Bootstrapping
        - Initial Provisioning of Pseudonym Certificates
        - Misbehavior Reporting (Next SCMS revision will add further requirements)
        - Certificate Revocation List (CRL) Download
        - OBU Revocation
        - Refresh Pseudonym Certificates
        - Update Pseudonym Certificate Request Parameters
    - RSU
        - RSU Bootstrapping
        - RSU Application Certificate Provisioning
        - RSU Misbehavior Reporting
        - RSU CRL Check
        - RSU Application and OBU Identification Certificate Revocation
        - Refresh RSU Application Certificates

2.2.2. Bootstrapping and Re-Bootstrapping Processes

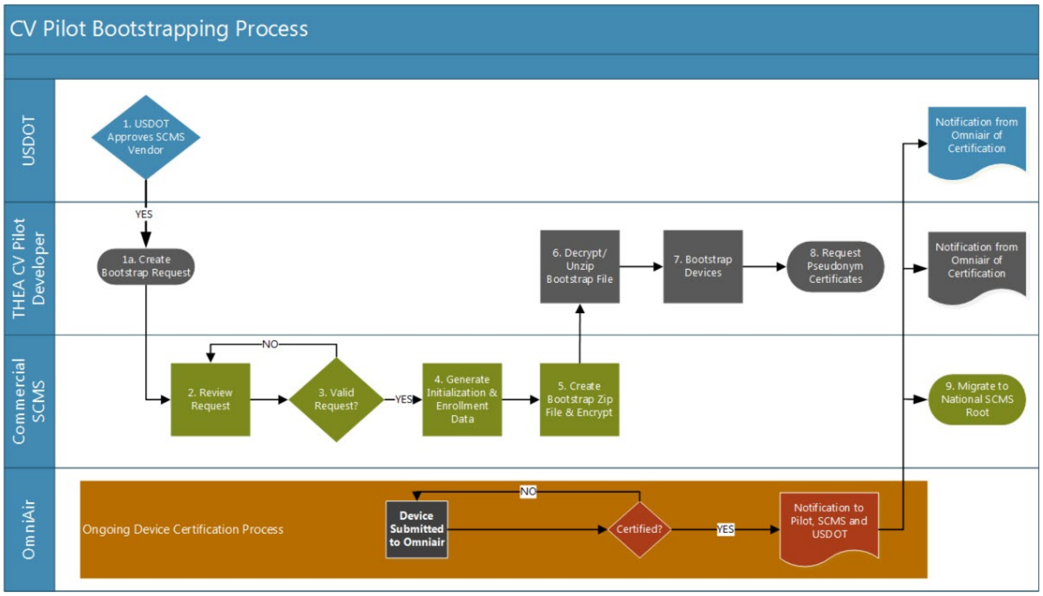
Based on the initial design, the SCMS only supported a manual bootstrapping process to support overall security requirements as described in the SCMS documentation. Latest versions of the system include an automated process. Each OBU vendor will select the manual, automated or hybrid approach based on their needs. The manual process will also be used for re-bootstrapping if a device's enrollment certificate is placed on the internal blacklist and can no longer request certificates from the SCMS.

Bootstrapping encompasses two distinct activities: initialization and enrollment. Initialization is the process by which a device receives keys that allow it to trust other SCMS components and credentials to connect to them. Enrollment is the process by which a device receives a long-term certificate which it can use in interactions with the SCMS to allow other devices to trust it. The overall security requirements for this process are:

- Process must protect device from receiving incorrect information
- Process must prevent SCMS from issuing certificates to unauthorized devices

The following process flow provides an overview of the manual bootstrapping process.

Figure 2-1. Manual Bootstrapping Process


CV Pilot Bootstrapping Process
USDOT
THEA CV Pilot Developer
Commercial SCMS
OmniAir
1. USDOT Approves SCMS Vendor
YES
1a. Create Bootstrap Request
2. Review Request
NO
3. Valid Request?
YES
4. Generate Initialization & Enrollment Data
5. Create Bootstrap Zip File & Encrypt
6. Decrypt/ Unzip Bootstrap File
7. Bootstrap Devices
8. Request Pseudonym Certificates
Notification from Omniair of Certification
Notification from Omniair of Certification
9. Migrate to National SCMS Root
Ongoing Device Certification Process
Device Submitted to Omniair
NO
Certified?
YES
Notification to Pilot, SCMS and USDOT

Source: HNTB

The THEA CV Pilot DCM has responsibility in the SCMS architecture for providing assurance that the devices that are required by the THEA CV Pilot team to obtain credentials from the SCMS are in fact eligible to receive those credentials. For devices which are provisioned by the Pilot Deployment team, the DCM will be a part of a Provisioning Center at which devices are prepared for deployment. At the DCM, devices will undergo end-of-line testing and provisioning, where OBUs are installed in vehicles. THEA will assume that devices are shipped securely from the suppliers and will provide secure storage at this location with protection against theft or modification of the devices.

The THEA CV Pilot team will have to determine how to test and certify that devices meet the requirements to be approved for initialization and enrollment. Testing for compliance with existing standards and message specifications, such as IEEE 1609.2, SCMS interfaces, and SPaT information broadcast system specification, should be handled by the testing services that will be provided, for a fee, by the Certification Operating Council that is currently working with USDOT to standardize testing processes. However, additional requirements introduced by the THEA CV Pilot team, such as specific hardware and software security requirements, will be specified and/or self-certified by equipment suppliers and the pilot team. Third-party testing of these requirements usually requires submitting the devices and design documents to an accredited certification lab which is very costly and time consuming. Given the tight timelines for developing these new devices and overall deployment, formal lab testing for additional imposed requirements is likely not realistic. Suppliers will be provided with the requirements in this document and will be required to provide written documentation indicating that the device conforms to those requirements. As requirements are refined and best practices developed during widespread deployment, it is expected that certification of devices to these types of requirements would become commonplace.

After completing the manual bootstrapping process for initialization and enrollment at the DCM, OBUs will be provisioned with pseudonym certificates and RSUs with the necessary application certificates via the Registration Authority (RA). Enrollment certificates have a validity period of 40 years for the SCMS.

OBUs will receive three years of pseudonym certificates via the RA (the PCA actually issues the certificates, but the RA provides the interface), where the validity period of each certificate is one week and 20 certificates are valid simultaneously at any time. The pseudonym certificates for consecutive time periods overlap for a period of 1 hour. The device will stop using the old batch and start using the new batch as soon as the new batch becomes available, unless the application is in a state where continuing to use the old batch is vital. If at any point connectivity is not available for requesting and receiving new certificates, the device waits until connectivity is available and requests the certificates again. After the device discards the old batch of certificates, the device requests and receives a new batch of pseudonym certificates via an RSU and the RA to top off certificates. If the device has no currently valid pseudonym certificates, it stops sending messages until it is able to contact the RA and receive more pseudonym certificates. OBUs will also be provisioned with one identification certificate per necessary application. Identification certificates are used primarily for authorization in V2I applications, such as signal preemption. As there are no pseudonymity constraints for identification certificates, an OBU has only one identification certificate valid at a time for a given application. While pseudonymity and tracking is not a concern, identity certificates still protect privacy of a user and do not contain any privacy sensitive information such as VIN or owner's name. Certificates for consecutive time periods will have a minimal overlap period to account for critical events. Revocation of identification certificates is done through CRLs.

RSUs will receive an initial set of application certificates via the RA (the PCA actually issues the certificates, but the RA provides the interface). The application certificates have a lifetime of one week + 1-hour overlap. A day before the current application certificate expires the RSU requests and receives a new application certificate via the RA. The new and the old application certificate have an overlap of one hour. The RSU will stop using the old one and start using the new one as soon as the new one becomes available, unless the application is in a state where continuing to use the old one is vital. If at any point connectivity is not available for requesting and receiving new certificates the RSU waits until connectivity is available and requests the certificates again. If the RSU has no currently valid application certificate for a given application, i.e., it has not received any application certificate or all its application certificates have expired, it stops sending messages associated with that application until it is able to contact the RA and receive more application certificates.

2.2.3. Recommended Local Misbehavior Detection and Certificate Revocation List (CRL) Strategies

While the SCMS design was originally to include established misbehavior reporting and CRL distribution processes, misbehavior detection was not included. The CRL strategy will also have to be tailored to the needs of the pilot. This section includes a discussion of local misbehavior detection strategies to ensure that the concept of misbehavior detection as ultimately designed and implemented by the USDOT and SCMS development team and device (OBU and RSU) suppliers is included, as needed, in future THEA CV Pilot planning and design documents. This section also addresses CRL questions, such as how to make use of and test the CRL when there are not established local misbehavior detection strategies.

Revocation is the process of protecting correctly-operating devices from the risks arising from trusting incorrect messages by removing compromised or seriously malfunctioned information from the system. The Pilot team will need to contact the owner of the device in order to make sure it is working properly. Revocation can in principle happen by two mechanisms:

- CRLs distributed to field devices that identify the certificates that are no longer trusted
- SCMS Internal Blacklist of revoked devices which ensures that the SCMS does not distribute pseudonym certificates to those specific devices

Before a device can be revoked, the SCMS must determine that revocation is appropriate. This can be accomplished through two processes:

- Local misbehavior detection
- External reporting

Local Misbehavior Detection Concepts

Local misbehavior detection is the act of a V2X device analyzing a message from another device to determine whether the message from the source device is valid or invalid because of equipment malfunction or a malicious attack targeting a vulnerability in the V2X communication system or device. Local misbehavior detection strategies have not been provided by the SCMS.

Local misbehavior detection strategies focus on detecting OBU misbehavior, not RSU misbehavior. Per the SCMS design documents, RSUs will have application certificates with short validity periods (e.g., daily, hourly) and require frequent certificate renewal, and hence no RSU CRL is necessary. For the CV Pilot, the TMC should be able to provide sufficient monitoring to determine if a RSU is not functioning properly or has been compromised. Due to an RSUs fixed location and remote access, the RSU could be taken offline much easier than an OBU.

While the OBU should obviously report any message that does not have a valid signature and/or certificate, the project team has included misbehavior detection concepts to ensure that the impacts of misbehavior detection and reporting are included in the remaining planning and design documents. Misbehavior detection and reporting, as is ultimately documented by the USDOT and the SCMS developer and implemented in the SCMS, may impact operations and data collection for performance monitoring and evaluation. The discussion of these strategies is intentionally left at a high-level description.

- Level 1 Plausibility: The OBU [and RSU] identifies as a suspect or implausible message any BSM for which the components of the vehicle dynamic state (position, speed, acceleration, and yaw rate) are outside the values as noted below
    - Speed: More than 70 m/s (252 kmph, 156 mph) which only excludes various supercars; well over any typical speed limits
    - Longitudinal acceleration: 0-100 kmph in under 2.3 second (Less than 12 m/s^2). Based on Ariel Atom, fastest accelerating production vehicle
    - Longitudinal deceleration: 100-0 kmph in under 95 feet (Less than -12 m/s^2). Based on Corvette Z6, fastest stopping production vehicle
    - Lateral Acceleration: More than 11 m/s^2 (1.12 G). Few production vehicles can exceed 1.0 G

  - Yaw Rate: Less than 1.5 radian/s, Rationale: 1.5 radian/sec is about equivalent to taking a 15 mph right turn at 27 mph (1G); tighter corners are not feasible (>1G), and softer corners are lower yaw rate at 1G acceleration
  - Values in BSM need to be internally consistent: Speed, lateral acceleration, and yaw rate are linked mathematically by the relation: $V^2=a_c^2/(Y')^2$. As a result, if the BSM includes speed, lateral acceleration, and yaw rate, the values in the BSM must follow this relationship within some allowable tolerance. For example, dividing the lateral acceleration value by the yaw rate should yield a speed value that is equal to (within some small tolerance) the speed value in the BSM.
- Level 2 plausibility: If a BSM would result in a positive application warning decision, the OBU identifies a message that fails level 2 plausibility any BSM for which the vehicle dynamic state (position, speed, acceleration, heading, and yaw rate) as described by the most recent BSM falls outside the 2 sigma distribution for the vehicle state as projected from the prior BSM to the time of the current BSM (i.e., the message is implausible if it is not on its expected trajectory within 2 sigma based on the received BSMs). If such a message fails the level 2 plausibility check, the OBU does not raise an alert to the driver on the basis of that message and prioritizes the message for misbehavior reporting. The misbehavior detection is a current topic of the USDOT Systems Engineering Roundtable, meaning 2-sigma and other range checks of the messages are not yet "ultimately documented". This section is correctly identified as describing "concepts" that will be implemented based on the roundtable and research of the BSMs collected during project Phase 3.
- The OBU [and RSU] logs within a misbehavior report (a) any message that (1) results in a warning or (2) would result in a warning but failed a level 2 plausibility check, or (b) any set of 10 continuous BSMs from the same vehicle that has consistently failed plausibility Level 1 checks
- The OBU [and RSU] performs intrusion detection activities and shall flag as misbehaving any message detected as intruding. If deployed, intrusion detection activities should follow best practices as implemented by suppliers

The feasibility of these plausibility strategies, especially Level 2, is dependent on vehicle sensors feeding accurate information to generate an accurate BSM. This also brings about considerations of hazard detection reliability.

Tighter error tolerances present a technical challenge but should also provide a reliable and consistent collision prediction, and thereby enable user applications to provide consistent safety benefits and support plausibility and misbehavior detection strategies. However, this is all dependent on current vehicle sensors and equipment being able to meet tighter error tolerances which may not be feasible.

Table 2-1. SAE J2945/1 BSM Parameter Accuracy Requirements

BSM Parameter	SAE J2945/1 Error Tolerance
Horizontal Position	1.5 m
Vertical Position	3 m
Speed	1 kph (0.277778 m/s)
Heading	2 to 3 deg depending on speed
Time	1 ms
Longitudinal Acceleration	1-sigma
Yaw Rate	1-sigma

Source: SAE

External Reporting

External reporting is the process of determining that a device should be revoked using some mechanism other than local misbehavior detection. For example, a maintenance engineer might determine that a device has been tampered with and the keys extracted, or an information security officer might discover that the keys from a device have been posted on the internet.

Due to incomplete local misbehavior detection strategies at the time of writing this concept, the THEA CV pilot may not support misbehavior reporting on day one of deployment.

One planned implementation of external reporting is to build over time, a device profile for each OBU that is adaptive to observed travel patterns. This device profile will contain baseline info collected over time after implementation and consist of data points such as:

- Number and days of week typically seen within the study area;
- Time of day typically observed within the study area
- Intersections/routes typically used within the study area;
- Typical periods of inactivity within the study area.

This baseline device profile will enable designated study investigators to observe anomalies in the baseline and identify potential faulty or malicious use of devices. By necessity, this type of misbehavior detection injects some PII/privacy concerns in that it requires identification over time. The methods to accomplish this and the controls put in place to offset this risk are intentionally omitted here and discussed in the classified version of the DPP, DPM and or DMP. High-level description of these controls include role based access and data segmentation; and techniques such as fuzzing, anonymizing and substitution.

Support for external reporting:

- Vehicle OBUs/: Currently, there is no maintenance cycle for these devices. Users of devices will be requested to report if physical tampering is noticed or the device is stolen.
- Transit OBUs/s: Maintenance engineers will check for physical tampering with the security module as part of the normal maintenance cycle. If they notice tampering they will escalate to an information security manager. If the information security manager determines that there is sufficient risk of the keys having been extracted they will notify the SCMS and request that the device is blacklisted. In this case, the device will be removed from the vehicle and returned to the supplier or the provisioning center for re-initialization.
- Field reporting by participants: If participants report an unusual number of false alerts, the information security manager will attempt to determine which device was involved by understanding the location of the alerts and notifying operators of devices that might have been in that location. An email address and automated telephone answering service will be provided for participants to report suspicious events.
- “Critical Incident” reporting: During early implantation in phase 2, a participant was involved in an accident that resulted in the vehicle being totaled by the insurance company. While we had planned for similar incidents, it had not been considered that an insurance company may take ownership of the vehicle thus removing the OBU from direct control of neither the Pilot nor the participant. Without a plan in place, this could expose the OBU to malicious actors without an effective method for identifying the vulnerability. As a result, both the DPPM and Safety Management Plan were modified to include procedures for gaining authorization to recover the OBU device if possible and to ensure collision center staff were contacted and briefed if not possible to safely gain access to the device. If the unit was recovered and found to be undamaged and uncompromised, it could be reutilized. If suspect, the unit would be disabled/destroyed. If a unit is found to be compromised, the SCMS operator would be

notified and included in the subsequent investigation and determination of whether the private key of the device and/or SCMS may have been subject to reverse engineering.

- Monitoring: The information security manager(s) will monitor internet security news for any indication that devices have been compromised. If a device's keys are posted online, the information security manager will coordinate with the SCMS Operator to revoke that device.

For external reporting support revocation, the SCMS must provide an interface and process for reporting enrollment and pseudonym certificates that should be revoked. This could be, for example, email to the SCMS Operator, or there could be a machine-to-machine protocol; there is a wide range of acceptable solutions, and our requirement is simply that there is a documented and operational process at the start of device deployment. The SCMS must also be able to determine the enrollment certificate to revoke from pseudonym certificates or keys that are published, and based on a device serial number.

CRL Strategies

At a basic level and per the SCMS, the device (i.e., OBU, RSU) sends a request for the current CRL to the CRL Store through the Location Obscurer Proxy (LOP) and the CRL Store responds with the current CRL. The CRL will hold a maximum of 10,000 entries at 40 bytes each. For the THEA Pilot (and the pilots as a whole), it is anticipated that the SCMS CRL will have more than enough space to capture all instances of misbehavior, especially if the team has no other choice than to use external reporting mechanisms for misbehavior detection. When a linkage seed is placed on the CRL, all the certificates associated with that linkage seed will be invalid and ignored by other devices. After a device is placed on the CRL, the participant should be notified so that their device can be replaced. After the device is replaced, the linkage seed can be removed from the CRL.

Depending on the availability of local misbehavior detection capabilities within the SCMS during pilot deployment, the team will refine CRL distribution strategies. If THEA must resort to the discussed external reporting mechanisms, the CRL will likely be generated and distributed whenever a new linkage seed is revoked. The SCMS internal blacklist will be updated in the same fashion, except whenever an enrollment certificate is revoked.

The THEA CV Pilot is also exploring the option to use Sirius XM as a CRL communications platform. Sirius XM provides a wide area alternate broadcast path to deliver the CRL. Any use of Sirius XM satellite service for CRL distribution will be secondary and provided as a means to demonstrate proof of concept for USDOT.

2.3. Privacy

This section covers the privacy considerations for administrative, V2X communications, and application data, including privacy by design aspects of the SCMS and specific application considerations where data could be construed as PII-related or there is the threat of some other privacy intrusion. In general, there will be three types of data collected for the pilot: administrative participant data, performance measurement data, and CV application data. Participant data is necessary to track involvement, conduct training, and maintain communications. CV data is the data generated by connected vehicles and/or the communications systems. Performance measurement data is generated from CV data as well as from additional sources, such as video cameras installed on REL infrastructure.

To ensure that data is appropriately protected, these data types should only be accessed and used for their intended purpose. Pilot applications and communications are formulated to protect the privacy of the users to the highest degree possible. Some applications will reveal more sensitive data than others. Therefore, it is important that applications do not reveal sensitive information if not necessary, as revealing the information within application A may allow it to be correlated with information from application B.

To address these concerns for broadcast and transactional unicast communications, the THEA CV Pilot team is implementing the following recommendations to maintain privacy:

- Authorization
  - The definition of "authorized to use the service" will be application specific.
- Privacy
  - Not require either party to reveal sensitive information unencrypted.
  - Not contain the User's location information unless this is necessary as part of service.
  - Not use identifiers that can be straightforwardly linked to the User's real-world identity (VIN, license number, etc.).

For all data that is collected and shared for further research, permissions must be obtained from the personnel that generated the data. Of course, these privacy concerns differ between state/local-owned vehicles and privately-owned vehicles. The privacy process for determining how to manage data for processing and sharing is below. These processes and rules reside within the Performance Management Plan which provides more detail on the process, which was submitted for IRB approval in phase 1, Task 8. The SMOC, and Performance Measurement Plan were updated as needed to reflect IRB requirements for approval.

1) **Establish data ownership**. As a rule, whoever owns the vehicle generally, but not always, owns the data generated by that vehicle.
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 is 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 protected. Controls selected for protection of this information is referenced in the DPP and detailed in the DPPM.
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.
5) **Obtain data sharing agreements prior to uploading data to any repository.** These data sharing agreements must 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 (ITS Public Data Hub). In no case will PII be included in the sharing of data with the ITS Public Data Hub or Independent Evaluator.

2.3.1. Participant Data

Participants in the CV Pilot study will include: drivers, pedestrians, and bus/trolley drivers. Below is potential sample size for participants.

- Up to 1200 drivers
- Pedestrians consisting of partner team members conducting focused tests during real-time monitoring.
- 10 transit buses and 8 transit streetcars.

Currently, the team anticipates that Participant Training and Stakeholder Education will require collection of the following:

- Name

- Date of Birth
- Contact information
  - home and work mailing addresses
  - email
  - phone number
- Copies of
  - driver licenses identification number
  - insurance card
  - vehicle registration
- Vehicle type data
- Demographic data (as defined by Task 5: Performance Measurement)
  - age
  - sex
  - race
  - recruitment

Data on age, gender and race/ethnicity will be used to show how all groups are represented in the conduct of the study.

The THEA team is currently planning for Participant Outreach 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

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 will also have to register for access to the secure participant portal on the website with a username and password. 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.

The participant data collected for Human Use Approval, Participant Training and Stakeholder Education, and Outreach must be in an encrypted, standalone, password protected database and kept separate from CV data used by the TMC and Performance Measurement team. There should be an established list of team personnel that have access to the data and should be physically separated from CV data. The THEA CV Pilot team will limit access to those personnel who require access to the data perform their duties within the pilot deployment.

2.3.2. Performance Measurement Data

As stated in the THEA ConOps, performance measures will ascertain the effectiveness of mobility, safety, environmental, and agency efficiency. As of now, these performance measures will utilize the data in the table below. It is important to note that in addition to application data, performance measures will incorporate other types of information such as infrastructure video camera data and survey data. Security and privacy requirements for these additional data sources will follow protocol from the THEA Network Security Policy and additional requirements as stated in this plan and the Performance Measurement Plan. Performance measure data is further refined in the Performance Management Plan.

Table 2-2. Performance Measurement Data

Pillar	Data Needs
Safety	AADT of UC1 segment
	AADT of UC3 segment
	AADT of UC4 segment
	AADT of UC6 segment
	Brake activation
	Deceleration rate
	Lateral acceleration
	Number of alerts in FCW
	Number of alerts in FCW/OBU
	Number of alerts in IMA
	Number of alerts in VTRFTV
	Number of crashes
	Pedestrian volume
	Actual Length
Mobility	Bus location time stamp (1 second)
	Bus/bus stop location
	Number of buses arriving on green
	Number of buses progressing through intersection on red
	Number of vehicles arriving on green
	Number of vehicles progressing through intersection on red
	Time Stamp (1 second)
	Vehicle Direction
	Vehicle Location
	Vehicle Location/Time Stamp
	Vehicle Speed
	Bus Location
Environment	Bus Speed
	Emission rates from MOVES
	Location/Speed
	As in Mobility
Agency Efficiency	As in Safety
	Survey/Opinion/App Feedback

The Performance Measurement Plan provides detailed procedures for data quality verification, data cleaning, PII removal, and fusion of CV data with data from other sources. The draft process is comprised of three high-level steps which are further detailed in the Performance Measurement Plan:

1) Data collection, data quality checking and cleaning

2) PII removal
3) Fusion of CV data with other sources

This process was applied to the Safety Pilot datasets collected in Ann Arbor, MI 2012-2013 and has been tailored to the THEA CV Pilot based on data generated by all sensors, OBUs, and driving data. We emphasize Step 2 for PII removal below as that is the most relevant to the SMOC. We will continue to coordinate with the Performance Measurement team throughout the Pilot to provide input and update the SMOC as necessary.

Step 1: Data collection, data quality checking and cleaning
Step 2: PII removal
Most of the collected datasets will need to undergo some form of cleansing before they are posted to the USDOT ITS hub. The BSM data from the OBUs, the RSU/sensor data, and any other driving data collected are typical candidates for cleansing. Each of these datasets may contain a number of different files, file types, and file structures so the execution of the cleansing procedure will be different from one data set to next, even if there are similar data files.
Step 3: Fusion of CV data with other sources

The four categories under which the datasets may fall, are as follows:

1. Trajectory based - Host Vehicle files – this category of files includes those that contain a host vehicle's detailed latitude and longitude data, as well as additional temporal information, that could support the uncovering of PII
2. Event Based - Host Vehicle files – these files capture details regarding the occurrence of events, such as those associated with forward collision warning or electronic emergency brake light activation, with respect to host vehicle
3. Trajectory Based - Remote Vehicle files – these files record latitude, longitude amongst other data elements from a remote vehicle that is in the vicinity of a host vehicle
4. Trip Summary files – this file type provides detailed trip level information for each trip completed by a host vehicle.

PII removal

The PII removal component in the CUTR Server will conduct PII removal in a nightly batch job before uploading Data Logs to the ITS Public Data Hub and SDC. Of particular concern is any information contained in BSM data from the OBU's, the Roadside Unit (RSU) /sensor data, and any other driving data that can be used as a unique identifier for a particular vehicle. For the purpose of the Tampa CV Pilot, the BSM of all vehicles will contain a unique ID. In keeping with security policy and best practices, the details of the unique ID, it's application, protection, and removal, are only available in the classified procedural documents. At the end of the Pilot period of performance, this unique ID will be removed and disabled from all participant vehicles. This field will be completely removed from the data available in the ITS Public Data Hub and SDC. In addition to removing the ID field, Data Logs will be investigated and evaluated early in the operations and maintenance phase to attempt to discover and remove any additional information that could support the uncovering of PII, including data elements if deemed sensitive on a case by case basis. To ensure PII removal, the Data Logs will be subject to cordon truncation to limit the data analysis to the geographic confines of the Tampa CV Pilot Study Area. This will be achieved by establishing a geofence around the CV Pilot Study Area and by eliminating all records that place the vehicles outside the cordon. All remaining records are those collected within the CV Pilot Study Area.

PII removal and Data Cleansing for Upload to the SDC

To meet the IE requirements to perform safety evaluation, the SDC Data Logs will contain a new randomly generated ID. This ID will remain constant over the study time frame to allow the IE conducting safety evaluation performance assessment.

2.3.3. SCMS Privacy by Design

Personal information collected in the THEA CV pilot will be kept to the minimum necessary for the V2X system to function effectively. CV data collected by the V2X communication system as described in the THEA CV Pilot ConOps will not contain specific PII or PII related data.

The original USDOT POC SCMS had "privacy by design" as a major tenet of the system development. The commercial SCMS selected to replace the USDOT provided one is by the same vendor and substantially unchanged in regard to "Privacy by Design" All V2X system communications will utilize the SCMS design along with the IEEE 1609.2 standard to provide communications security and protect user privacy. For vehicle OBUs, and RSUs to communicate, they must be enrolled with the SCMS which will provide certificates to prove authenticity of their BSMs and other messages. Note that the BSM does not contain personal information. It only contains the location and motion characteristics of the vehicle (e.g., speed, heading, acceleration) and certificate information. To protect privacy and prove authenticity, OBUs will use pseudonym certificates to sign all messages. Based on information provided by USDOT on the current SCMS design, the device will have a pool of 20 certificates that are valid simultaneously for only one week. Certificates for consecutive time periods (i.e., each week) are valid simultaneously for one hour. The device will rotate through certificates every five minutes to limit trackability, which is a commonly voiced concern. Also, any communication to the SCMS through the RSU, for example to replenish certificates, is encrypted and also passes through the Location Obscurer Proxy which strips the request of any device identifying information. Refer to the SCMS Implementation EE Requirements and Specifications Supporting SCMS Software Release 1.0 for complete details on the various types of certificates, uses, switching strategies, and validity periods.

2.3.4. Application Data Considerations

While the privacy of most data is protected by the SCMS design, privacy questions can arise if a person or organization manages to string together BSMs or vehicle situation data, combining various data elements from information flows, or when data could be perceived as aiding law enforcement in tracking law-abiding citizens. The team identified data and information that could raise questions, specifically vehicle situation/probe data and specific information flows used within the End of Ramp Deceleration Warning application.

Vehicle Situation/Probe Data

Even though the privacy by design elements of the SCMS should mitigate privacy concerns, the public may be concerned by vehicle situation/probe data depending on the additional data collected outside of the normal BSM and how the data is bundled and stored.

As mentioned previously, the BSM does not contain PII or personal information. Probe data structures may include data in addition to the normal BSM data, but should also not contain personal information. Common additional data include environmental data and vehicle system operational data. If supported, an application will typically take a snapshot of the data at a given interval. These snapshots will be bundled and sent to a data clearinghouse at specific intervals (or as possible based on available communications mediums). The data bundle is signed as specified in IEEE 1609.2, just like the BSM, which ensures authenticity. The use of rotating pseudonym certificates as specified in the SCMS design increases privacy and reduces the ability to track a specific vehicle especially in areas of high traffic density, but does not make vehicle tracking impossible. However, it would be easier to simply follow a vehicle rather than sniff BSMs.

Depending on the final data elements determined for collection within the Vehicle Situation/Probe data, there are multiple methods to protect the privacy of a vehicle/person generating the data. The strategies involve restricting the actual generation (not transmission) of the probe data based on certain triggers and/or constraints. By restricting generation, only the necessary data will exist. If, instead, the strategy is to manage the transmission of the data, the data may still exist and possibly be extracted from the device. There are three potential generation strategies. A strategy must be selected and refined after the exact data requirements are defined within the Performance Management and Application Deployment Plans.

- Probe data snapshots are only generated at specific intervals, such as every X meters or X seconds
- Start and stop probe data snapshots. An example is the device would stop generating probe data when the vehicle drops below a certain speed or stops and may not generate data snapshots until the vehicle reaches a defined speed
- Event based probe data snapshots, such as heavy breaking, windshield wipers engaged, etc.

It is possible to add even more privacy and randomization to probe data, as explained during the USDOT technical assistance webinar on 1 Feb 2016, “Preparing a Privacy Operational Concept for Connected Vehicle Deployments.” A potential option is for OBUs to generate and package vehicle situation/probe data in 120 second or one-kilometer increments, whichever comes last. There will then be randomized gaps in collecting and packaging vehicle situation/probed data. This gap will be 50-250 meters or 3-13 seconds. The collected segments are also randomized to further protect privacy and limit the ability to connect segments to identify the trip of a specific vehicle. This method would have to be further refined and implemented through an application on the OBU to control data generation and packaging.

The THEA CV Pilot will primarily focus on gathering vehicle situation/probe data packages transmitted to RSUs at the entrance/exit point of the Reversible Express Lanes (REL) at Meridian Avenue and Twiggs Street, area of downtown Tampa from the Selmon Express Lanes along Twiggs Avenue to Marion Street and along Meridian Avenue to Channelside Drive. Selected RSUs will issue a Wave Service Announcement (WSA) indicating that devices can upload vehicle situation/probe data stored in the vehicle. When the device receives this message, it will respond by transmitting the logged data packages on the specified channel and then purging its log after confirmation of receipt. This is expected to be a UDP transaction with acknowledgement at the application level. If not within range of a RSU and the device buffer is full, the OBU will delete the packaged data.

The concept of maintaining privacy while collecting vehicle situation/probe will continue to evolve as the system requirements are fully developed. The strategies, such as the mandatory gap concept, may change based on the methods of communication used to transmit the packages.

End of Ramp Deceleration Warning: Reduced Speed Warning Status and Speed Monitoring Information

This section will address what could potentially be a public concern that information generated from the End of Ramp Deceleration Warning application could be used for law enforcement purposes rather than strictly to provide safety warnings to vehicles and safety/traffic congestion benefits. The two information flows addressed are:

- Reduced Speed Warning Status (RSU->TMC): Speed warning application status reported by the RSU. This includes current operational state and status of the RSU and a record of measured vehicle speeds and notifications, alerts, and warnings issued
- Speed Monitoring Information (RSU->TMC): System status including current operational state and logged information including measured speeds, warning messages displayed, and violation records

Even if signature and certificate information is known to the TMC and even shared with law enforcement, this would be a difficult mechanism to use for the enforcement of speeding violations. Law enforcement would have to go through the SCMS Manager to get the information to link the certificate to a specific vehicle, which should be against SCMS policies. It would be much easier to set a speed camera or police officer on the curve to monitor speed and enforce any violations. However, if this is still a concern, certificate information that could link the vehicle to the warning/violation could possibly be stripped after authentication by the RSU and prior to bundling and sending the information from the RSU to the TMC to increase privacy of the vehicle and re-assure the public that the data is not collected for law enforcement reasons. The data will be immediately discarded by the RSU after sending to the TMC and it is no longer needed for the application. If the data is offered for analysis and research, the data will be scrubbed and sanitized of all certificate related information prior to making the data available.

3. Access Security Overview

This section addresses access security, such as the various roles that can access V2X devices, user name and password policies, and whether remote access to RSUs is permitted in the THEA CV Pilot. While this section covers the considerations necessary for the pilot, access security is covered in the NIST security controls listed for each device class later in the document and fully specified in the deliverables of the Threat Definition of V2I Architecture project. Within the NIST framework, there are relevant security control families for Access Control and Program Management.

3.1. Current THEA TMC and Access Security Policies

Current TMC operations are a combined and shared effort between THEA and the City of Tampa (CoT). THEA owns and maintains the TMC while the CoT staffs the TMC. Currently the THEA/CoT Joint TMC manages opening, closing, and directional reversing of the THEA Selmon Reversible Express Lanes (REL). The TMC also monitors traffic signals in downtown Tampa and throughout the City. The TMC implements special event timing plans for major events in downtown Tampa, Amalie Arena, and the Tampa Convention Center. Finally, the TMC dispatches Road Ranger Service Patrol vehicles in response to stalled vehicles or crashes on the REL or local lanes. However, the TMC does not currently continuously monitor traffic, transit, pedestrian crossings, or the TECO Streetcar line.

TMC operations and procedures are currently guided by the THEA Network Security Policy, THEA/CoT Joint TMC Memorandum of Understanding (MOU), and Standard Operating Procedures (SOP).

3.2. CV Pilot Policy Adjustments

THEA business systems IT department (non-CV Pilot systems) is in the process of re-defining their data collection needs and will be developing a secure system for data collection including maintenance and long-term storage to meet developing needs. Other than system logs, no data is currently collected or stored. Currently, the only openly published data from is the status of the Selmon Expressway REL which is displayed on the THEA website. However, THEA does have plans to make signal timing, vehicle count, and travel time information openly available in the future.

The THEA CV Pilot will create massive amounts of new data that must be collected, analyzed, and securely maintained, as well as publicly shared where appropriate. Access to this data will be governed by the data collection and storage policies discussed in this document, the DPP and classified procedures documents for the life of the Pilot. Functional needs will be identified and permissions controlled based on the individuals needs and responsibilities. A plan is under development for a coordinated migration of the CV Pilot data systems to the THEA IT department. This plan will ensure continued protection and availability of CV Data consistent with requirements of the CV Pilot security documents, and NARA.

3.3. IT System and Organizational Roles

Information systems shall enforce a role-based access control policy to conduct actions such as viewing collected CV data, remote access to equipment, and updating software in V2X devices. Roles within the TMC should not have access to PII or PII-related information regarding those participating in the pilot. Participant information and specific data identifying aligned devices should be maintained in a separate standalone, password protected, encrypted database managed by select members of the Human Use, Participant Training and Stakeholder Education, and Outreach teams. This data will be kept separate from CV data collected by the TMC for traffic analysis and operations.

Current TMC Access Control Central Software (ACCS) uses granular control to manage user access by creating groups as directed by THEA. Each user has a unique username/password and actions will be auditable and traceable to individual usernames. The following default access groups and permissions are included in the ACCS:

- VIS – View only
- CON1 – Control cameras only
- CON2 – Control cameras and operate REL
- CON3 – Control cameras and operate REL and configure some system elements
- ENG – Administrative functions as well as operate REL
- MGR – Administrative functions as well as operate REL
- DYNAC Admin – Administrative functions as well as operate REL

3.3.1. Additional Organizational Roles

THEA/CoT will likely have to create new organizational roles or delegate additional responsibilities to existing roles such as the IT Manager. The roles and responsibilities below should be incorporated within the THEA/CoT management organization to oversee execution of the SMOC and continued operation of the V2X security and privacy system.

- Information Security Director: responsible for overall execution of this SMOC, for setting policy on an ongoing basis, for liaison with SCMS Operator to ensure that requirements are clearly communicated and met, and for coordination with other Pilot Deployments and other field trials to share information about information security concerns, incidents and developments.
- Information Security Manager: may have day-to-day information security management activities delegated by the Information Security Director. The manager should produce a detailed report every month listing all known incidents involving suspected malfunctioning of the Pilot Deployment Applications and a high-level report every quarter providing a review of information security incidents associated with the Pilot Deployment. The manager should develop a database schema for storing information about these malfunctions and provide feedback arising from the study of information security incidents to the SCMS manager, the suppliers, USDOT, and the conformance test team at least quarterly (through the Information Security Director).
- Provisioning and Maintenance Engineers: responsible for correct execution of security-related provisioning and maintenance activities (i.e., DCM activities) according to this SMOC.
- Network Administration: in charge of backhaul operations to ensure THEA/CoT network security requirements are met.

The THEA CV Pilot team will need to provide training to personnel filling new roles, as well as the TMC and the rest of the THEA CV Pilot team in general, on new privacy and security processes and procedures.

3.4. User Name and Password

User name and password policies and procedures are outlined in the DPP and DPPM along with other access controls methods.

3.5. Device Remote Access and Network Connectivity

Currently, remote access to ITS RE is achieved through a physically isolated “stand alone” network. This network could be leveraged to add new functionality for RSU and additional ITS RE remote access.
RSUs and ITS REs (i.e., MHM devices) shall support remote access to perform maintenance and software updates, as specified in the Chapter 5: Software and Operating System Security Overview. The device shall support identity-based authentication to enable remote access. Currently, the firewall for remote access to the CV network is managed by the CV Pilot vendor. The migration plan for Pilot turnover includes coordinated handover of firewall.

OBUs shall not support remote access except that OBUs will be capable of OTA software updates which are protected via the use of SCMS certificates.

General network access is currently gained in the following ways for the following reasons and permissions.

- VPN Access thru THEA Firewall – Kapsch – Maintenance of ACCS
    - Authorized server personnel of the vendor are assigned a user ID and password to connect via PPTP (VPN) and access specific ports
    - Accounts are audited annually
    - Vendor is required to notify THEA of staff changes
- THEA Firewall - Live REL Status packets to www.tampa-xway.com
    - Server S-UTIL1 uses FTP to fetch a text file with the road gate status information
    - The public web site uses https (SSL) to fetch and process the text file for displaying the graphic on the tampa-xway.com home page
    - Web server alerts to fetch failures via email
- Connectivity to FDOT for camera sharing secured
- Connectivity to News Agencies to share live video streams through a secure transmission system
- ITS Network Monitoring – Lucent – Operations and Maintenance
    - Monitoring Server resides on local ITS network and only communicates with ITS field devices and computers
    - Authorized IT personnel of the vendor are assigned a user ID and password to connect through an SSL remote desk top to the server
    - Accounts are audited annually
    - Vendor is required to notify THEA of staff changes

The tolling network is firewalled and there is a physical separation maintained between the ITS and tolling networks. This complete separation of the tolling network as a general standard will be maintained throughout the CV Pilot.

To facilitate detection of abuse, the THEA/CoT TMC should monitor data traffic usage to detect abuse of the generic IP connection. In particular, if an RSU is generating more internet traffic than would be warranted by the number of OBUs known to be associated with logged security management related connections, the information security manager shall investigate to determine the reason. The TMC should make use of existing capabilities such as Web Application Firewalls (WAF) and Intrusion Detection Systems (IDS), or Intrusion Prevention Systems (IPS) to detect and prevent vulnerability exploits and protect against web application threats. However, full implementation of these capabilities (if not already implemented) is outside the scope of the CV Pilot.

3.6. Database Access

As stated in the THEA ConOps, the TMC will be the central location for operators receiving and sending information as well as archiving data for performance measure evaluation. This data will be collected, analyzed, and maintained primarily by the joint THEA/CoT TMC, along with contractors following the same privacy and security requirements and guidelines specified in existing policies and this SMOC. THEA and the City of Tampa make use of contractors to provide support for Ethernet communications network maintenance, DYNAC software maintenance, system hardware maintenance, and design and integration of ITS system revisions and expansion into the communication network and DYNAC. As stated in the Privacy section, there will be three types of data collected for the pilot: administrative participant data, performance management, and CV data.

At least one server with adequate disk space will be dedicated to archive the pilot data. Data collected by the Pilot will eventually become part of the USDOT ITS hub. As discussed in the Chapter 2: Communications Security Overview, the CV data collected from probe enabled vehicles and RSUs will not contain any PII or PII-related information. There will also be controls in place to limit the ability to string vehicle trips together, such as the strategy of having mandatory gaps in the vehicle situation/probe data. Even with these controls, the THEA CV Pilot team will scrub vehicle situation data to determine the effectiveness of strategies in providing privacy, not necessarily anonymity, to participants. More detailed privacy strategies for this type of data is contained within the Data Collection processes and Data Sharing Framework of the Performance Management Plan.

CV data (e.g., volume, occupancy, travel times, location, heading, speed) collected from probe vehicles, RSUs, and other devices will not be housed with PII and PII-related data on the participants, which is maintained for administrative and performance management reasons. These databases will be maintained separately and one person or role will not have access to both databases. Only TMC personnel and/or roles will have access to the CV data stored and analyzed by the TMC. Only select Human Use, Participant Training and Stakeholder Education, and Outreach personnel, or other group as specified in later concepts and plans, and/or roles will have access to participant data. Participant data will only be used for administrative purposes in tracking devices (and reconfiguring malfunctioning devices) and for performance management purposes. The THEA CV Pilot team will explore the potential to have these databases on separate networks and/or physical locations to increase privacy and security.

4. Hardware Security Overview

Security requirements for each device classification should specify hardware security control requirements. These requirements may differ among the OBU, and RSU devices. A widely accepted standard used to specify hardware security requirements is FIPS 140-2: Security Requirements for Cryptographic Modules. FIPS 140-2 covers the questions asked by the USDOT during the “Preparing a Security Operational Concept for Connected Vehicle Deployments” webinar presented on 9 December 2015, including protections to prevent device tampering such as tamper evident protections and tamper resistant protections. This section gives an overview of FIPS 140-2 and recommended FIPS 140-2 levels for each type of device.

4.1. FIPS 140-2 Overview

The FIPS 140-2 standard “specifies the security requirements that will be satisfied by a cryptographic module utilized within a security system protecting sensitive but unclassified information (hereafter referred to as sensitive information). The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification, cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.”

Note that not all FIPS 140 requirements within a specific level are necessary. However, a module rated at Level 3 must be at least Level 3 across all FIPS areas. The overall rating is the lowest area evaluation. The Cryptographic Module Validation Program (CMVP) confirms cryptographic modules meet FIPS 140-2 and other cryptography standards. In the CMVP, device vendors use independent testing laboratories accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) to perform compliance testing. According to NIST, there are 12 approved FIPS 140-2 testing labs in the U.S.

4.1.1. FIPS 140-2 Level 1

FIPS 140-2 Level 1 provides the lowest level of security. This level specifies basic security requirements for a cryptographic module. There are no security mechanisms required beyond the requirement for production-grade components. Level 1 allows a general computing system to support software and firmware components of a cryptographic module, which may be suitable when other controls such as physical security are unavailable or inadequate.

4.1.2. FIPS 140-2 Level 2

FIPS 140-2 Level 2 enhances the Level 1 physical security mechanisms. This level adds the requirement for tamper-evidence, which includes the use of tamper-evident coatings or seals, or for pick-resistant locks on removable covers or doors of the module. Level 2 also allows the software and firmware components of a cryptographic module to be executed on a general-purpose computing system operating system evaluated at Common Criteria (CC) Evaluation Assurance Level (EAL) 2 (or higher). Level 2 also adds the requirement of role-based authentication to perform a specific set of services appropriate to the role. RSUs/OBUs apply level 2 in regards to the HSM only.

4.1.3. FIPS 140-2 Level 3

FIPS 140-2 Level 3 attempts to prevent the intruder from gaining access to keys held within the cryptographic module in addition to Level 2 mechanisms. These mechanisms should detect and respond to physical access attempts, such as zeroizing all keys when the module is opened. Level 3 also allows the software and firmware components of a cryptographic module to be executed on a general-purpose computing system operating system evaluated at CC EAL 3 (or higher). Level 3 also requires identity-based authentication in addition to the role-based authentication of Level 2. Level 3 also requires that Critical Security Parameter (CSP) entry and output is executed using physically separated ports, or enter and exit in encrypted form.

Level 3 "certification" is not required as many elements are not relevant. RSU/OBU vendors however are applying "best effort" self-compliance of applicable sections such as tamper-resistance of the HSM. The exact application of these protections is proprietary and are self-certified with the SCMS manager.

4.1.4. FIPS 140-2 Level 4

FIPS 140-2 Level 4 provides the highest level of security. This level provides a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. A Level 4 device would also have controls that result in the immediate zeroization of all keys if the cryptographic module was penetrated. Level 4 also allows the software and firmware components of a cryptographic module to be executed on a general-purpose computing system operating system evaluated at CC EAL 4 (or higher). No elements of level 4 or higher apply to the CV Pilot.

Table 4-1.Summary of FIPS 140-2 Security Requirements

	Security Level 1	*Security Level 2*	*Security Level 3*	*Security Level 4*
Cryptographic Module Specification	Specification of cryptographic module, cryptographic boundary, Approved algorithms, and Approved modes of operation. Description of cryptographic module, including all hardware, software, and firmware components. Statement of module security policy.			
Cryptographic Module Ports and Interfaces	Required and optional interfaces. Specification of all interfaces and of all input and output data paths.		Data ports for unprotected critical security parameters logically or physically separated from other data ports.	
Roles, Services, and Authentication	Logical separation of required and optional roles and services.	Role-based or identity-based operator authentication.	Identity-based operator authentication.	
Finite State Model	Specification of finite state model. Required states and optional states. State transition diagram and specification of state transitions.			
Physical Security	Production grade equipment.	Locks or tamper evidence.	Tamper detection and response for covers and doors.	Tamper detection and response envelope. EFP or EFT.

	Security Level 1	***Security Level 2***	***Security Level 3***	***Security Level 4***
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced Protection Profiles (PP) evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance	CM system. Secure distribution. Functional specification.	High-level language implementation.	Formal model. Detailed explanations (informal proofs). Preconditions and post conditions.
Mitigation of Other Attacks	Specification of mitigation of attacks for which no testable requirements are currently available.			

4.2. Device Hardware Security Requirements

Different devices require different hardware security requirements depending on the cryptographic needs and threats. Requirements may also need to be downgraded based on assessed risk and development costs. The team believes that this also applies to the V2X devices in the THEA CV Pilot. The recommended FIPS 140-2 level depends on the device functionality, cost considerations, and risk. The FIPS 140-2 level 2 only applies to cryptographic elements of the RSU/OBU.

Suppliers will be provided with the requirements in this document and will be required to provide written documentation indicating that the device conforms to those requirements. If we cannot obtain devices that meet the security requirements, we will work with suppliers to establish the best possible match with the security requirements based on a more detailed risk assessment. Any residual risk will have to be acknowledged, accepted, and monitored.

If devices meet only a subset of the security requirements, there is increased risk of key compromise. We mitigate this by storing more than spares of each device, to increase our ability to swap out devices that appear to have been compromised.

4.2.1. Onboard Unit (OBU)

Based on the application information flow analysis, the OBU has a medium classification baseline which corresponds to FIPS 140-2 Level 2. . The classification and FIPS 140-2 level selection is consistent with other projects and expert recommendations, as well as SAE J 2945/1. FIPS 140-2 Level 2, as applicable, is feasible and achievable for device suppliers.

4.2.2. Roadside Unit (RSU)

Based on the application information flow analysis, the RSU has a medium classification baseline which corresponds to FIPS 140-2 Level 2. The RSU does not necessarily have to be automotive grade in that it would not need to be able to function in an environment as extreme as the OBU (i.e., vibrations, rapid temperature changes, and moisture issues due to rapid heating and cooling).

4.2.3. ITS Roadway Equipment (ITS RE)

Current ITS RE (i.e., signal controllers, CCTV, DMS, MVDS) are legacy devices and may connect to RSUs in support of CV Applications or CV Data backhaul. These devices do not operate on DSRC spectrum, interact with the SCMS, nor do they recognize or provide any encryption. As such, their level of security will be consistent with FDOT requirements and specifications. However, the Pilot team will work with the infrastructure owners to evaluate and apply additional “physical security” measures as may be prudent.

5. Software and Operating System Security Overview

While FIPS 140-2 addresses the majority of hardware security requirements, it does not cover all software and operating system requirements, which also need to be addressed. A key requirement for secure operations of the V2X safety system is that the software running within the system that sends and receives the messages cannot be modified, and that additional software cannot be installed that would allow an attacker to generate false messages using valid keying material. This section reviews software and operating system security considerations. ***This objectives and requirements stated in this section are in addition to or supersede the requirements specified based on the selected FIPS 140-2 level for the device type.***

While this section will cover the considerations necessary for the THEA CV pilot, software and operating system security are covered in the NIST security controls listed for each device class later in the document and will be fully specified in the deliverables of the Threat Definition of V2I Architecture project. Software and operating system controls are addressed in multiple control families including Configuration Management, Maintenance, Systems and Services Acquisition, System and Communications Protection, and System and Information Integrity.

The following subsections describe software, operating system, and additional hardware security requirements and objectives for systems that run DSRC applications that use cryptographic private keys and certificates in the format specified by IEEE 1609.2 (2016) and that are issued by the SCMS. While the SMOC does not require further protections such as intrusion detection, intrusion prevention, and passive OS fingerprinting, suppliers should use best practices to integrate these added protections as appropriate.

The security requirements apply to two logically distinct sets of functional blocks:

- **Privileged applications**: These are applications that run autonomously (i.e., do not require human intervention to start running) and either send or receive signed messages. They run on the **host processor**.
- **Cryptographic operations**: These are operations that use secret keys from symmetric cryptographic algorithms, or private keys from asymmetric cryptographic algorithms. They run on the **Hardware security module (HSM)**.

The goals of these requirements are:

1) Different privileged applications can have different sets of keys such that
    a. A privileged application is able to sign with its own keys
    b. A privileged application is not able to sign with keys reserved for use by a different privileged application
    c. Non-privileged applications do not have any access to keys that are reserved for use by privileged applications.
2) No application has read access to key material – all key material is execute- or write-only.
3) Keys used for verification are protected against unauthorized replacement.
4) The system supports software/firmware update in such a way that the above properties continue to hold.

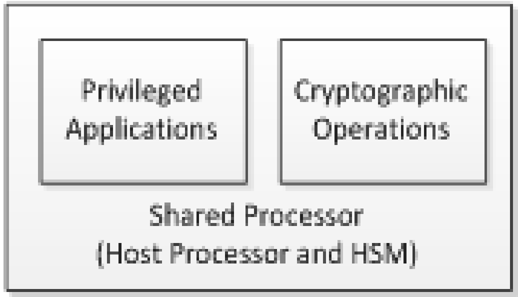
5.1. Architectures

The requirements below cover three architectures.

- **Integrated architecture** (Figure 5-1): The host processor and the HSM are the same processor.
- **Connected architecture** (Figure 5-2): The host processor and the HSM are different, but they are physically connected using a connector that connects only those two processors, such that the only way to read or write data flowing between the two processors is by physically tapping into that connector, and the only access to the HSM is via the host processor.
- **Networked architecture** (Figure 5-3): The host processor and the HSM are different and are connected over a network or bus that has other processors connected to it.

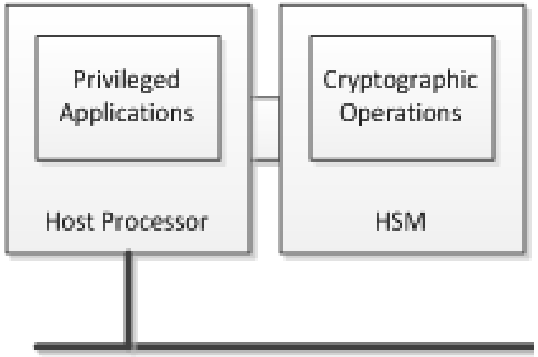
This chapter provides requirements for the host processor and the HSM separately in sections 5.2, and then provides architecture-specific requirements in section 5.3.

Figure 5-1. Integrated Architecture



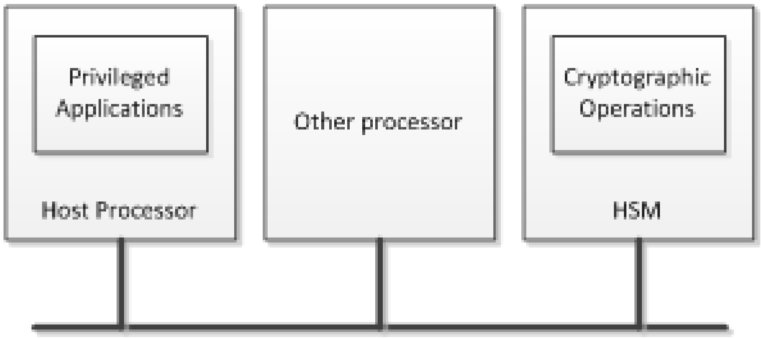
Source: BAH

Figure 5-2. Connected Architecture



Source BAH

Figure 5-3. Network Architecture



Source BAH

5.2. Host Processor

5.2.1. Manufacturing and Operational States

The host processor and its software shall be delivered in an *operational state* that implements the requirements specified in the USDOT **Specifications** for DSRC **Roadside Unit** v4.1.

5.3. Architecture-specific Requirements

5.3.1. Integrated Architecture

An integrated processor meets the complete set of requirements identified in USDOT Specifications for DSRC Roadside Unit v4.1. As both OBUs and TMC equipment interface with RSUs, the RSU v4.1 definition of an integrated architecture will apply to all DSRC devices.

5.3.2. Connected Architecture

Modifications are the following:

- Since it is assumed that the OS on the device manages process separation, the HSM need only maintain two roles:
    - User (which can execute software and firmware, write and delete cryptographic keys, and install signed software and firmware)
    - Security Officer (which can install unsigned software and firmware in the event that specialized new software and/or firmware is being tested and troubleshot – the Security Officer role must be explicitly authenticated by the device prior to installation)
- The HSM may support additional roles, either corresponding to the different privileged applications, or corresponding to non-privileged applications.
- Activities carried out by the User role need not be explicitly authenticated.

5.3.3. Networked Architecture

Modifications are the following:

- All of the Connected architecture requirements above

- In addition, the host processor must authenticate itself to the HSM with an authentication mechanism based in hardware with the same physical security level as the HSM itself.

6. Device Classifications and Selected Security Controls

This section describes the general approach to develop device classification and selecting appropriate security controls by following the beginning of the NIST Risk Management Framework of FIPS 199/200 and NIST SP 800-53. Application information flows are analyzed based on the criteria for Confidentiality, Integrity, and Availability specified in FIPS 199/200 with slight modifications to better apply to Connected Vehicles. Information flows are grouped by each device to determine the device classifications. Security controls are then selected based on the security control baselines in NIST SP 800-53 and tailored to the specific device class and needs. Refer to Data Privacy Plan (DPP) for details of selected controls.

6.1. Security Control Structure

Security controls are organized into eighteen families and have a well-defined organization and structure. Each family contains security controls related to a general security topic. Below are the eighteen families:

Table 6-1. Security Control Structure

ID	Family
AC	Access Control
AT	Awareness and Training
AU	Audit and Accountability
CA	Security Assessment and Authorization
CM	Configuration Management
CP	Contingency Planning
IA	Identification and Authorization
IR	Incident Response
MA	Maintenance
MP	Media Program
PE	Physical and Environmental Protection
PL	Planning
PS	Personnel Security
RA	Risk Assessment
SA	System and Services Acquisitions
SC	System and Communication Protection
SI	System and Information Policy
PM	Program Management

6.2. Low, Moderate, Moderate (LMM) Device Class (OBU, RSU, ITS RE and TMC)

This section covers the LMM device classification which we currently have for the OBU, RSU, ITS RE and TMC. Low Confidentially is specified for flows that are typically broadcasted and intended to be received by any nearby device. Moderate Integrity considers the consequences of a false message being accepted by a receiver. A false message being accepted can lead either to false positives or to false negatives. The false message can increase physical risk without directly causing physical harm. Moderate Availability indicates that to be useful the information flow must be available a significant amount of time. Also, wireless communications (e.g., DSRC) cannot be considered as having a higher Availability classification than moderate. Originally these devices were categorized as LHM, but because there will be measures enacted to detect misbehavior and revoke certificates as well as permissions, Integrity was downgraded to Moderate.

ITS RE is included in this section only in consideration of their potential connection to the communications network. There is potential sharing of ITS RE wireless or fiber network in the backhaul of CV data and/or detection inputs from ITS RE providing information to an RSU for use with a CV Application .

7. Minimum Security Requirements per Device Classification

This section lists the minimum, security requirements per device classification to ensure security and privacy while facilitating timely development and delivery by suppliers. Full, detailed security controls from NIST SP 800-53 was not available in time for the suppliers to modify designs, manufacturing practices, etc. as necessary. The final security controls from the Threat Definition of V2I Architecture should be used as guidelines for the next lifecycle of devices, while these requirements are used for the CV Pilots to ensure reasonable security, privacy, and interoperability.

7.1. LMM Device Minimum Security Requirements (OBU, RSU, TMC)

7.1.1. Communications

- LMM devices shall comply with IEEE 1609.2 (2016): Standard for WAVE – Security Services for Applications and Management Messages
    - LMM devices will sign and/or encrypt data exchanged over non-DSRC IP communications (i.e., cellular, WiFi direct) interfaces with IEEE 1609.2 certificates as provided by the SCMS
- LMM devices shall support requirements identified in the SCMS Implementation EE Requirements and Specifications Supporting SCMS Software Release 1.0 Appendix A and B to complete processes and use cases
- LMM devices shall support security requirements identified in SAE J2945/1 V5, such as the BSM transmission and reception security profile. Since the SAE J2945 addresses both transmission and reception, then the whole system which sends to or receives from a DSRC device in the Pilot is analyzed against these requirements and must comply where applicable to ensure the covered device or element is compliant.

7.1.2. Hardware

- LMM devices shall be equivalent with FIPS 140-2 Level 2 physical security requirements
    - There shall also be a tamper evident seal to detect tampering with the removable media. All unused media ports (e.g., USB) shall be sealed
- LMM devices shall have sufficient resources to store and process the number of certificates and CRLs stated as necessary within the SCMS Implementation EE Requirements and Specifications Supporting SCMS Software Release 1.0

7.1.3. Software and Operating System

- Refer to Chapter 5: Software and Operating System Security for LMM device requirements

7.1.4. Access

- LMM devices shall support remote access via a secure OpenVPN server/firewall application at the TMC. Devices shall support physical access in the event that re-bootstrapping is required, however the physical access shall be hidden, protected by tamper-proof seal and or approved locking mechanism. The device shall support role-based authentication to enable physical access
- LMM devices shall support the ability to reset default user names and passwords

Appendix A. Threat Assessment

Table A-2 provides a list of the threats the team identified in the system. Also identified is the impact of different threats along with the rationale for those impact levels. The impact values take into account the existing protocol designs and relevant objects but do not make any assumptions about the physical or platform security of the devices, as the devices were not selected at the time of this initial threat analysis. The impact values also assume that sending and receiving devices implement the protocol as specified, but make no other assumptions about software quality. Furthermore this table does not go into the details of how the specific threats are carried out. The purpose of this table is to have a current list of known threats independent of the V2X applications in use. UPDATE: During final design the selected devices and software/firmware were subjected to internal pen-testing, and a summary report was provided to USDOT demonstrating no significant vulnerabilities and remedial actions taken to address a few moderate ones discovered.

The team compiled a list of threats with reference to C2C-CC Protection Profile, ETSI TVRA, Sevecom Security Requirements Report, CAMP Risk Assessment and Technical Analysis Report, CAMP Misbehavior Detection Report, and the CAMP Interoperability Issues of Vehicle-to-Vehicle Base Safety Systems Project (V2V-Interoperability) Phase 2 Final Report, Volume 3 Security Research for Misbehavior Detection.

Risk Assessment of Threats

The methodology closely follows NIST SP 800-30, except for having 3 levels (as opposed to 5 levels) for both Likelihood and Impact of a threat: low, moderate, and high. Also accordingly modified is the corresponding risk matrix as shown in Table A-1 along with the rationale for those impact levels. For a system that is yet to be designed and implemented, the likelihood of an attack is largely unknown and any guestimate is very likely to be far from reality. Therefore, a slightly different approach is taken compared to the one suggested in NIST SP 800-30: first estimate the impact of all the threats, then for all the threats with moderate/high impacts, suggest countermeasures to bring the likelihood down to low/moderate, and finally carry out a full risk analysis (i.e., first estimate likelihood and impact of a threat, and then use the risk matrix of Table A-1 to calculate risk) on the system along with countermeasures. The full risk analysis was completed during early deployment of the system. It was conducted under full operational conditions but during the “silent period” before participants begin receiving alerts. An external white hat pen tester firm was used to conduct vulnerability scanning and risk assessment. No critical findings were reported. Low and moderate findings were addressed per the consultant’s recommendations, this SMOC, and other relevant references.

Table A-1. Risk Matrix showing Risk Levels for Combination of Likelihood and Impact

		Level of Impact		
		Low	**Moderate**	**High**
Level of Likelihood	**High**	Low	Moderate	High
	Moderate	Low	Moderate	Moderate
	Low	Low	Low	Low

Source: BAH

The impact of an attack is also determined as per the guidelines in NIST SP 800-30 (cf. Table H-3):

- **High**: The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
- **Moderate**: The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
- **Low**: The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.

Existing Threat Analyses

The current V2X Threat Assessment is based on analysis of existing assessments referenced in the following projects and reports.

- Sevecom Security Requirements Report- VANETS Security Requirements Final Version
- Car-to-Car Communication Consortium Protection Profile
- European Telecommunications Standards Institute Technical Report 102 893 v1.1.1 (2010-03): Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)
- CAMP Risk Assessment and Technical Analysis Report
- CAMP Interoperability Issues of Vehicle-to-Vehicle Base Safety Systems Project (V2V-Interoperability) Phase 2 Final Report, Volume 3 Security Research for Misbehavior Detection

Current V2X Threat Assessment

Table A-2. Consolidated V2X Threat Assessment

Threat ID	Description	Relevant Object	Impact	Mitigation/Notes
T.Extract.1	An attacker learns restricted information on the device/system, such as private keys, certificates, etc., using a non-invasive attack such as a side channel attack and/or cryptanalysis of algorithms and signed messages.	OBU, RSU, SCMS	High if easily scalable, moderate otherwise	Major damage to the functionality of the system: false BSMs leading to false alerts which in turn reduce the effectiveness of the system for collision avoidance, potentially also false misbehavior reports reducing ability of system to remove bad actors. Note that since vehicles have multiple certificates this attack allows an attacker to masquerade as multiple vehicles (a Sybil attack), making this attack somewhat scalable. May also be able attack or maliciously interact with RSUs, and the SCMS. Restricted information extraction is mitigated with Software and Operating System requirements, along with specified FIPS 140-2 levels based on the device type.
T.Extract.2	An attacker learns restricted information on the device/system, such as private keys, certificates, etc., using an invasive software attack such as malware (available on Internet for example) that exploits vulnerabilities in algorithms and software.	OBU, RSU, SCMS	High if easily scalable, moderate otherwise	See T.Extract.1.
T.Extract.3	An attacker learns physically protected restricted information on the device, such as private keys, using a physical attack.	OBU, RSU,	High if easily scalable, moderate otherwise	See T.Extract.1.
T.Integrity.1	An attacker replays a BSM or other system message at a different (than original) time and/or location.	OBU, RSU, PID	Low	The system protocols (e.g., IEEE 1609.2, SCMS requirements) are designed to reduce the chance that replayed messages are accepted unless there is significant clock skew between devices.
T.Integrity.2	An attacker modifies the sensor inputs on a single device before the device uses	OBU, RSU	Moderate	The effectiveness of device's primary functions, including sending/receiving BSMs with accurate information that can be

	them to generate and send a BSM or other system message.			trusted, is reduced. This is moderate rather than high impact because it is not scalable: the device under attack will still only produce the expected number of BSMs per second, and Sybil attacks are not possible. It may not be possible to fully mitigate this threat for the aftermarket devices that will be used for CV pilots. An integrated vehicle should have secure connections between components. The device within an integrated vehicle should also authenticate sensor inputs (e.g., GNSS).
T.Integrity.3	An attacker modifies the sensor inputs to multiple devices before the device uses them to generate and send a BSM or other system message. (For example, by GPS spoofing).	OBU, RSU	Moderate	The effectiveness of a device's primary functions, including sending/receiving BSMs with accurate information that can be trusted, is significantly reduced. This is moderate rather than high impact on the assumption that (a) if different units get incorrect but consistent input (e.g., with wide-area GPS spoofing) their BSMs will still be effective in avoiding collisions and (b) if different units get incorrect and inconsistent input it is the same as mounting T.Integrity.2 on each unit individually, and so has the same impact as T.Integrity.2. As with T.Integrity.2, the devices under attack will still only produce the expected number of BSMs per second. It may not be possible to fully mitigate this for the aftermarket devices that will be used for CV pilots. An integrated vehicle should have secure connections between components. The device within an integrated vehicle should also authenticate sensor inputs (e.g., GNSS).
T.Integrity.4	An attacker is able to use restricted information on the device/system to create a false BSM or other system message without actually extracting the information from the device/system (e.g., use private key to sign a message without completing one of the T.Extract attacks).	OBU, RSU	High if easily scalable, moderate otherwise	This attack essentially assumes the attacker has installed malware on the device. A scalable attack is either one where this installation is easy so large numbers of devices are affected, or one where the malware is capable of overriding the usual key tumbling and BSM scheduling mechanisms to send BSMs that appear to come from multiple different vehicles, i.e., a Sybil attack. An attacker accessing restricted information and installing malware is mitigated with Software and Operating System requirements, along with specified FIPS 140-2 levels based on the device type.

T.MBD.1	An attacker who knows about the misbehavior detection algorithms (and associated parameters) manipulates the content of the BSM to evade detection.	OBU,	High if scalable, moderate otherwise	The ability of the system to mitigate the damage caused by compromised devices is reduced. Mitigated through misbehavior reporting. System protocols (e.g., IEEE 1609.2, SCMS requirements) are designed so that messages are verified prior to taking action.
T.MBD.2	An attacker who has been reported sending invalid messages denies that those messages came from the attacker's device, thwarting the misbehavior detection process.	OBU,	Moderate	The ability of the system to mitigate the damage caused by compromised devices is reduced. This attack is unlikely to be scalable. Mitigated through system protocols (e.g., IEEE 1609.2, SCMS requirements) that implement nonrepudiation.
T.MBD.3	An attacker who knows about the misbehavior detection algorithms (and associated parameters) manipulates misbehavior reports to implicate innocent devices/systems and evade detection.	OBU,	High if scalable, moderate otherwise	The ability of the system to mitigate the damage caused by compromised devices is reduced. As misbehavior reporting will likely be limited to external reporting during the CV Pilot, this should not be a problem. This threat will need to be mitigated through SCMS global misbehavior analysis and detection strategies.
T.Track.1	An attacker uses the change pattern(s) of certificates and other BSM-relevant information to track a vehicle or other device.	OBU,	Moderate	Significant damage to device's privacy. Mitigated by using change patterns and strategies as specified in the SCMS design.
T.Track.2	An attacker uses BSM data to track a vehicle/device.	OBU,	High	Similar effects as T.Track.1, but the attack can be launched at a larger scale with little extra resources. Mitigated by using change patterns and strategies as specified in the SCMS design. Mitigated by using the vehicle situation data strategy described in the Privacy section of this document
T.TOE.1	An attacker installs malware on a device/system that prevents receiving, or making use of, or providing user interaction based on BSMs or other system messages.	OBU, RSU	High	Device is not able to perform its primary functions, such as sending/receiving BSMs. An attacker installing malware is mitigated with Software and Operating System requirements, along with specified FIPS 140-2 levels based on the device type.
T.TOE.2	An attacker uses the device as an attack vector on the rest of the vehicle/system.	OBU, RSU,	High	If the OBU is connected to the CAN bus, and an attacker is able to compromise the OBU via BSMs, severe damage can be done including loss of life, e.g., by sudden braking. It may not be possible to fully mitigate this threat for the aftermarket devices that will be used for CV pilots. An integrated vehicle

				should have secure connections between components. The device within an integrated vehicle should also authenticate information from other components (e.g., GNSS).
T.DOS.1	An attacker transmits noise and energy on the same frequency as the DSRC safety channel.	OBU, RSU,	Low	Local impact. Denial of service attacks on the channel can be detected as part of the standard medium activity sensing for channel access: a high level of channel activity, combined with a lower than expected number of successfully received application PDUs. No actual mitigation for this other than identifying the area with channel congestion, physically locating the jamming device, and turning it off
T. DOS.2	An attacker transmits messages to jam or distract. These messages may contain incorrect info but are validly signed or may appear valid but have a bad cert or signature.	OBU, RSU,	Low	Local impact. Ties up resources on the receiving device. If validly signed messages, enforcement can be carried out through misbehavior and detection. If the cert is false, there is no cryptographic identification of attacker, and may require physically locating the sending antenna.

Appendix B. Acronyms

ACRONYM	DEFINITION
ACCS	Access Control Central Software
BSM	Basic Safety Message
CA	Certificate Authority
CAMP	Crash Avoidance Metrics Partnership
CC	Common Criteria
CM	Configuration Management
CME	Certificate Management Entity
CMVP	Cryptographic Module Validation Program
COC	Certification Operating Council (Omniair)
CRL	Certificate Revocation List
CSP	Critical Security Parameter
ERDW	End of Ramp Deceleration Warning
CV	Connected Vehicle
CVRIA	Connected Vehicle Reference Implementation Architecture
DCM	Data Capture and Management (occurs only in reference table)
DCM	Device Configuration Manager
DMA	Dynamic Mobility Applications
DSRC	Dedicated Short Range Communication
EAL	Evaluation Assurance Level
EE	End Entity
EEBL	Emergency Electronic Brake Light
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
ETSI	European Telecommunications Standards Institute
EVITA	E-Safety Vehicle Intrusion Protected Applications
FCW	Forward Collision Warning
FHWA	Federal Highway Administration
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
IDS	Intrusion Detection System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMA	Intersection Movement Assist
IMEI	International Mobile Equipment Identity
IP	Internet Protocol

IPS	Intrusion Prevention Systems
I-SIG	Intelligent Traffic Signal System
ISO	International Organization for Standardization
ITS	Intelligent Transportation Systems
JPO	Joint Program Office
LMM	Low, Moderate, Moderate
LOP	Location Obscurer Proxy
MA	Misbehavior Authority
MAC	Message Authentication Code
MC	Management Center
MHM	Moderate, High, Moderate
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
OBU	On- Board Equipment
OS	Operating System
OSI	Operating System Interconnect
PCR	Platform Configuration Registry
PID	Personal Information Device
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PP	Protection Profile
RA	Registration Authority
RE	Roadway Equipment
REL	Reversible Express Lanes
RSU	Roadside Unit
RSU	Roadside Unit
SAE	Society of Automotive Engineers
SCMS	Security Credentials Management System
SMOC	Security Management Operating Concept
SOP	Standard Operating Procedures
SP	Special Publication
SSL	Site Uses Https
STOL	Saxton Transportation Operations Laboratory
TCG	Trusted Computing Group
TCP	Transmission Control Protocol
THEA	Tampa Hillsborough Expressway Authority
TMC	Transportation Management Center
TOE	Target of Evaluation
TPM	Trusted Platform Module

TSP	Transit Signal Priority
TVRA	Threat, Vulnerability and Risk Analysis
UDP	User Datagram Protocol
USDOT	U.S. Department of Transportation
V2I	Vehicle-To-Infrastructure
V2V	Vehicle-To-Vehicle
V2X	Vehicle-To-Device
VAD	Vehicle Awareness Device
VPN	Virtual Private Network
VTRFTV	Vehicle Turning Right in Front of a Transit Vehicle
WAF	Wed Application Firewalls
WAVE	Wireless Access In Vehicular Environments
WSA	WAVE Service Advertisement
WSMP	WAVE Short Message Protocol

Appendix C. Glossary

Term	Definition
Basic Safety Message (BSM)	The outgoing message sent by a vehicle that communicates information and data about its current state to a set of neighboring vehicles. That information or data is used by Vehicle-to-Vehicle (V2V) safety applications in the neighboring vehicles to warn users of crash-imminent situations.
Bootstrapping	The process of configuring and updating an uninitialized vehicle's on-board equipment (OBU), which results in the issuance of the OBU's enrollment certificate and transition to the Operating Mode.
Certificate Authority (CA)	In Public Key Infrastructure (PKI) security systems, a CA is a trusted entity authorized to create, sign, and issue public key certificates.
Certificate Management Entity (CME)	An organization that houses certain functions and activities necessary for the certificate management process.
Certificate Revocation List (CRL)	A list of certificate identifiers that the Misbehavior Authority (MA) function identifies to be misbehaving due to technical error or human malfeasance.
Common Criteria (CC)	The Common Criteria (CC) for Information Technology Security Evaluation is an international standard (ISO / International Electrotechnical Commission (IEC) 15408) for computer security certification. It is currently in version 3.1 revision 4. Common Criteria provides assurance that the process of specification, implementation and evaluation of a computer security product has been conducted in a rigorous and standard and repeatable manner at a level that is commensurate with the target environment for use. (Source: Wikipedia)
Cryptography	The combination of mathematical algorithms and computer science intended to protect users, networks, and messages sent throughout a network by encrypting messages. Only authorized users of the network have the necessary information or credentials to access the data within the network.
Dedicated Short Range Communications (DSRC)	The one-way or two-way short-to-medium range wireless communication channels specifically designed for automotive use and a corresponding set of protocols and standards. DSRC is sometimes referred to as Wireless Access in Vehicular Environments (WAVE) in other literature.
FIPS Publication 140-2 Security Requirements for Cryptographic Modules	The FIPS protocol for computer security standard used to accredit cryptographic modules.
FIPS 199 Publication Standards for Security Categorization of Federal Information and Information Systems	Standard that establishes security categories of information systems used by the Federal Government, one component of risk assessment. It assesses information systems in each of the categories of confidentiality, integrity and availability, rating each system as low, moderate or high impact in each category.

FIPS 200 Publication Minimum Security Requirements for Federal Information and Information Systems	A standard developed to first determine the security category of their information system in accordance with FIPS 199, and then apply the appropriately tailored set of baseline security controls in NIST Special Publication 800-53.
1609.2 - IEEE Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages	Secure message formats and processing for use by Wireless Access in Vehicular Environments (WAVE) devices, including methods to secure WAVE management messages and methods to secure application messages are defined in this standard. It also describes administrative functions necessary to support the core security functions.
1609.3 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services	The IEEE standard for the WAVE Networking and WAVE Short Message Protocol (WSMP) layers. Wireless Access in Vehicular Environments (WAVE) Networking Services provides services to WAVE devices and systems. Layers 3 and 4 of the open system interconnect (OSI) model and the Internet Protocol (IP), User Datagram Protocol (UDP), and Transmission Control Protocol (TCP) elements of the Internet model are represented. Management and data services within WAVE devices are provided.
IPv6 (Internet Protocol version 6)	A set of specifications from the Internet Engineering Task Force (IETF) that's essentially an upgrade of IP version 4 (IPv4). The basics of IPv6 are similar to those of IPv4 -devices can use IPv6 as source and destination addresses to pass packets over a network, and tools like ping work for network testing as they do in IPv4, with some slight variations.
ISO/IEC 15408 Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model	The international standard for Common Criteria (CC) for Information Technology Security Evaluation. establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products
Location Obscurer Proxy (LOP)	A networking entity which hides the location of the requesting device from Security Credentials Management System (SCMS) components, such as the Registration Authority (RA).
Misbehavior	The reference to technical errors and human malfeasance that have a negative impact on the effectiveness of the connected vehicle system.
Misbehavior Authority (MA)	The CME function responsible for detecting, tracking, and managing potential threats to the Security Credentials Management System (SCMS) and connected vehicle system. The MA is also responsible for CRL creation, management, and publishing through the CRL Generator sub-function.
NIST SP 800-30 Risk Management Guide for Information Technology Systems	Guidance for the development of an effective risk management program, containing both the definitions and the practical guidance necessary for assessing and mitigating risks identified within IT systems.
NIST SP 800-53 Security and Privacy Controls for Federal Information Systems and Organizations	Special Publication covers the steps in the Risk Management Framework that address security control selection for federal information systems in accordance with FIPS 200. This includes selecting an initial set of baseline security controls based on a FIPS 199 worst-case impact analysis, tailoring the baseline security controls,

	and supplementing the security controls based on an organizational assessment of risk.
On-Board Unit (OBU)	The user equipment that provides an interface to vehicular sensors for safety measures, as well as a wireless communication interface to the Location Obscurer Proxy (LOP) for Security Credentials Management System (SCMS) processes.
Personally Identifiable Information (PII)	Any form of information that can be used to identify, contact, or locate an individual person, directly or indirectly.
Private Key	In public key encryption, the key held secretly by the subject of a PKI certificate that contains a related public key. It is not made available to any other entity. In signing operations, the private key is used for generating a signature and the public key is used for validating a signature. In encryption (key agreement) operations, the sender uses the recipient's public key and the sender's private key to generate a key for encryption. The recipient uses the recipient's private key and the sender's public key to generate the same key for decryption.
Pseudonym Certificates	The implicit, short term certificates used during message exchange in the pseudonym system. These certificates do not explicitly contain the holder's public key, but contain a reconstruction value which can be combined with the CA's public key to derive the holder's public key. They are smaller than traditional certificates which contain the holder's public key explicitly and offer performance advantages when messages are verified infrequently.
Public Key Infrastructure (PKI)	A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. PKI has been chosen as the mechanism to provide integrity and authentication within the connected vehicle system. This system creates and manages digital certificates that bind an identity to its public key to certify the sources of the messages.
Roadside Unit (RSU)	An infrastructure node that serves as an intermediary in Vehicle-to-Vehicle (V2V) two-way communications between CMEs and vehicles. RSU may also send its own messages to OBU
SAE J2945/1- On-Board System Requirements for V2V Safety Communications	Specifies the minimum communication performance requirements of the DSRC Message sets, the associated data frames and data elements defined in SAE J2735 DSRC Message Set Dictionary.
Security Credentials Management System (SCMS)	The set of organizations that house the various functions and activities necessary for the certificate management process.
Signal Phase and Timing (SPaT)	A message that is used to convey the current status of a signalized intersection. The receiver of this message is able to determine the current state of each phase and when the expected next phase is to occur.

Target of Evaluation (TOE)	The Target of Evaluation (TOE) is the specific entity which is to be analyzed when taking a Common Criteria approach to developing security requirements. The selection of the boundary for the TOE can vary depending on the desired scope to be addressed in the Common Criteria Protection Profile.
Vehicle-to-Device (V2X)	The wireless communication exchange of messages and data between and among vehicles, infrastructure, and capable nomadic devices within the connected vehicle system.
Vehicle-to-Vehicle (V2V)	A dynamic wireless exchange of data between nearby vehicles that offers the opportunity for significant safety improvements.
WAVE Service Advertisement (WSA)	A message sent by DSRC Provider Terminals (e.g., Roadside Unit (RSU)) announcing service and channel information so that DSRC User Terminals can determine which services are being offered on which service channels during the service channel interval.
Wireless Access in Vehicular Environments (WAVE)	The IEEE networking, upper messaging, and security layers associated with DSRC. Defines communications conforming to the IEEE 1609 protocol suite and IEEE Standard 802.11-2012, operating outside the context of a basic service set

Appendix D. References

Booz Allen Hamilton Inc. (May 2013). Communications Data Delivery System Analysis for Connected Vehicles – Revision 5, Federal Highway Administration (FHWA), USDOT.

Booz Allen Hamilton, Inc. (January 2014). Development of DSRC Device and Communication System Performance Measures: Analysis of DSRC Operational Needs and Performance Measures. Washington, DC: NHTSA, USDOT.

Crash Avoidance Metrics Partnership. (February 2015). Interoperability Issues of Vehicle-to-Vehicle Based Safety System Project (V2V-Interoperability) Phase 2 Final Report Volume 1 – Communications Scalability for V2V Safety Development, USDOT.

Crash Avoidance Metrics Partnership. (November 2014). Interoperability Issues of Vehicle-to-Vehicle Based Safety Systems Project (V2V-Interoperability) Phase 2 Final Report Volume 3 – Security Research for Misbehavior Detection, USDOT.

Crash Avoidance Metrics Partnership. (July 2013). Vehicle Safety Communications Security Studies: Technical Design of the Security Credential Management System. USDOT.

Crash Avoidance Metrics Partnership. (July 2014). Vehicle Safety Communications Security Studies, Study 3 Final Report: Definition of Communication Protocols between SCMS Components and Specification of the Components Pseudonym Certificate Authority, Registration Authority, and Linkage Authority. USDOT.

Crash Avoidance Metrics Partnership. (January 2016). Security Credential Management System Proof-of-Concept Implementation: EE Requirements and Specifications Supporting SCMS Software Release 1.0. USDOT.

Common Criteria for Information Technology Security Evaluation 15408. (September 2012). Version 3.1 Revision 4. Part 1: Introduction and General Model. International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC).

Common Criteria for Information Technology Security Evaluation 15408. (September 2012). Version 3.1 Revision 4. Part 2: Security functional components. International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC).

Common Criteria for Information Technology Security Evaluation 15408. (September 2012).Version 3.1 Revision 4. Part 3: Security assurance components. International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC).

Connected Vehicle Data Capture and Management (DCM) and Dynamic Mobility Applications (DMA) Assessment of Relevant Standards and Gaps for Candidate Applications.(October 2012). USDOT.

Connected Vehicle Reference Implementation Architecture (CVRIA), Version 2.1, www.iteris.com/cvria.

E-safety vehicle intrusion protected applications (EVITA) project: http://www.evita-project.org/, final summary http://www.evita-project.org/Publications/EVITAD0.pdf

ETSI TR 102 893 v1.1.1 (2010-03): Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA). Available from http://www.etsi.org/deliver/etsi_tr/102800_102899/102893/01.01.01_60/tr_102893v010101p.pdf

FIPS. (2001). PUB 140-2: Security Requirements for Cryptographic Modules. NIST.

FIPS. (2004). PUB 199: Standards for Security Categorization of Federal Information and Information Systems. NIST.

FIPS. (2006). PUB 200: Minimum Security Requirements for Federal Information and Information Systems. NIST.

Harding, J., Powell, G., R., Yoon, R., Fikentscher, J., Doyle, C., Sade, D., Lukuc, M., Simons, J., & Wang, J. (August 2014). Vehicle-to-Vehicle Communications: Readiness of V2V Technology for Application. (Report No. DOT HS 812 014). Washington, DC: NHTSA, USDOT.

Leidos. (April 2014). USDOT Federal Highway Administration DSRC Roadside Unit (RSU) Specifications Document, Version 4.0, USDOT.

NIST (2012). SP 800-30: Guide for Conducting Risk Assessments. NIST.

NIST (2013). SP 800-53: Security and Privacy Controls for Federal Information Systems and Organizations. NIST.

NIST (2010). SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).NIST.

IEEE. (2016). 1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments — Security Services for Applications and Management Messages. IEEE Vehicular Technology Society.

IEEE. (2016). 1609.3-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) – Networking Services. IEEE Vehicular Technology Society.

IEEE. (2016). 1609.4-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE)--Multi-Channel Operation. IEEE Vehicular Technology Society.

Perry, F., Raboy, K., Leslie, E., Huang, Z. (October 2016) USDOT **Specifications** for DSRC **Roadside Unit** v4.1 (Project Number DTFH61-12-D-00020). USDOT

SAE. (2015a). J2735: Dedicated Short Range Communications (DSRC) Message Set Dictionary. SAE International.

SAE. (2015b). J2945.1: Dedicated Short Range Communication (DSRC) Minimum Performance Requirements. SAE International.

Sevecom VANETS Security Requirements Final Version: Deliverable 1.1. Available from http://www.transport-research.info/Upload/Documents/201306/20130605_103517_12197_Sevecom_Deliverable_D1.1_v2.0.pdf

Whyte et al., A Security Credential Management System for V2V Communications, 2013 IEEE Vehicular Networking Conference. http://www.cvt-project.ir/Admin/Files/eventAttachments/A%20Security%20Creential%20Management%20System%20for%20V2V%20Communications%20-%20VNC%20Conference%202013_514.pdf

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-18-693

U.S. Department of Transportation