Connected Vehicle Pilot Deployment Program Phase I

Security Management Operational Concept – Tampa (THEA)

www.its.dot.gov/index.htm
Final Report — May 2016
FHWA-JPO-16-312

U.S. Department of Transportation

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

Notice

1. Report No.	2. Government Accession No.	3. Recipient's Catalog No.
FHWA-JPO-16-312		

4. Title and Subtitle	5. Report Date
Connected Vehicle Pilot Deployment Program Phase I Security Management Operational Concept - Tampa Hillsborough Expressway Authority (THEA)	May 2016
	6. Performing Organization Code
7. Author(s)	8. Performing Organization Report No.
Joshua Kolleda (BAH), Dominie Garcia (BAH), Tyler Poling (BAH)	Task 3 Report
9. Performing Organization Name And Address	10. Work Unit No. (TRAIS)
Booz Allen Hamilton, 20 M Street SE, Washington D.C., 20003 Tampa Hillsborough Expressway Authority, 1104 E Twiggs St #300, Tampa, FL 33602	
	11. Contract or Grant No.
12. Sponsoring Agency Name and Address	13. Type of Report and Period Covered
U.S Department of Transportation 1200 New Jersey Ave, SE Washington, DC 20590	Final Security Management Operating Concept, December 2015 to May 2016
	14. Sponsoring Agency Code

15. Supplementary Notes
Govind Vadakpat (COR), Sarah Khan (CO)

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 in regards to security and privacy for the THEA Deployment Phase I. 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.

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

19. Security Classif. (of this report)	20. Security Classif. (of this page)	21. No. of Pages	22. Price
		121	

Form DOT F 1700.7 (8-72) **Reproduction of completed page authorized**

Acknowledgements

The THEA Privacy and Security Management Operating Concept (SMOC) development team would like to thank the Wyoming CV Pilot team and especially the New York City CV Pilot team for their collaboration on several sections of the SMOC. The team would also like to thank everyone who was part of the biweekly conference calls as well as everyone who participated in the cross-team working session. We acknowledge the timely and high-quality support offered by U.S. DOT and the support contractor, Noblis.

Table of Contents

List of Tables

List of Figures

Executive Summary

The Privacy and Security Management Operating Concept (SMOC) provides details about how 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, analysis of application information flows and device classifications per Federal Information Processing Standard (FIPS) 199 and 200, and identified security controls for each device class per National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 cross checked against International Organization for Standardization (ISO) / International Electrotechnical Commission (IEC) 15408 Common Criteria (CC) security controls. While the SMOC does not further specify the NIST SP 800-53 security controls, the SMOC does provide minimum security requirements for pilot device classes (Chapter 7).

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 Personal Information Device (PID), Vehicle On-Board Equipment (OBE), Transit OBE, and Roadside Equipment (RSE). However, the Vehicle Databus, 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.

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

[1] ITS Roadway Equipment is based off of the CVRIA definition “physical objects that represent all of the other ITS field equipment that interfaces with and supports the Connected Vehicle Roadside Equipment (RSE). 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.”

Requirement Areas

Communications security for the THEA CV Pilot is 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. The SCMS POC has not yet finalized misbehavior detection strategies. The THEA CV Pilot team presents potential misbehavior detection strategies primarily based on plausibility checks[2] on incoming BSMs that could be tested during the THEA CV pilot.

Personal information collected in the THEA CV pilot will be kept to the minimum necessary for the V2X system to function effectively. The current application assessment does not directly reveal any Personally Identifiable Information (PII)[3] or PII-related information being collected through the deployed applications, but this assessment may change based on the requirements set for performance measurement and evaluation. 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 to provide information regarding specific occurrences or collisions, including potentially identifying individual devices. Much of these privacy concerns are addressed in the Security Credentials Management System (SCMS) Proof of Concept (POC) and associated security standards that will be implemented during the pilot. The unique cases of the PID and vehicle situation/probe data are analyzed in detail with recommended strategies to increase privacy. 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.

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.

While FIPS 140-2 addresses the majority of hardware security requirements, it does not cover all software and operating system requirements. A key requirement for secure operations of the V2V safety system is that the software running within the system that sends and receives the BSMs cannot be modified, and that additional software cannot be installed that would allow an attacker to generate false BSMs using valid BSM keying material. 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.

[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. However, implementing the potential plausibility checks is out of scope for the pilot; however, USDOT could use the THEA CV Pilot for testing and development of these strategies.

[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."

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 RSEs. 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 possibly be made between participant and specific trip data. As other plans, such as Human Use and Participant Training and Stakeholder Education, are developed, this concept will be further refined to protect the privacy of participant PII gathered by the THEA CV Pilot team.

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 two device classes for the THEA Pilot.

1. Low, Moderate, Moderate (LMM) devices include the Vehicle Awareness Device (VAD), Aftermarket Safety Device (ASD), PID, and OBE. 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[4], Integrity was downgraded to Moderate.
2. Moderate, High, Moderate (MHM) devices include the RSE, ITS RE, and TMC. In this case, the information flows sent or received by these devices have a Confidentiality classification of Moderate, Integrity classification of High, and Availability classification of Moderate. Below are two examples that justify Moderate Confidentiality and High Integrity:
    a. Example for Moderate Confidentially: If Speed Monitoring Information sent from the ITS RE to the TMC is compromised; vehicles may be identified with the speed at which they are traveling. This has the possibility to identify vehicles exceeding the speed limit. However it is important to note that this would be difficult to execute considering that multiple databases would need to be cross referenced to identify the vehicle.
    b. Example for High Integrity: The over-the-air broadcast of traffic signal timing is tampered with, resulting in an over-the-air message of the current signal status which does not match the signal status being displayed on the lights at the intersection.

    These devices pose a higher security and privacy threat because their information flows could, but not necessarily do, contain information such as personal identifiable information that the owner has a reasonable desire not be disclosed; false information could directly affect safety, mobility, and security, or cause severe financial damage; in order to be useful, information flows must be available a significant amount of time.

[4] The LMM classification assumes that misbehavior detection and reporting will be available within the SCMS POC for pilot deployment per the SCMS POC development and testing schedule. Even if full capabilities are not available, the THEA CV Pilot team will utilize external reporting mechanisms as described in Section 2.2.3.

Based on our application information flow analysis and knowledge of the NIST SP 800-53 security controls for medium and high baseline devices, the team developed a list of recommended minimum security requirements (Chapter 7) for the LMM and MHM 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 V5 compliance
- SCMS POC Implementation EE (End Entity) Requirements and Specifications Supporting SCMS Software Release 1.0 requirements compliance
- Certification Operating Council (COC) System Functional and Performance Specification Ver. 0.4.0 compliance
- Potential strategies to maintain (and/or increase) participant privacy
- Potential misbehavior detection strategies

Hardware Security

- FIPS 140-2 Level 2 (for LMM devices) and Level 3 (for MHM devices) equivalency

Software and Operating System (OS) Security

- Host processor: Boot, OS, and secure software and firmware requirements
- Hardware Security Module (HSM) requirements
- 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

Privacy and Security Management Operating Concept (SMOC) Limitations

While the THEA team took a holistic, comprehensive approach to the SMOC, there are still limitations to this concept as the overall pilot concept is still in development. The SMOC will likely have to be revisited and adjusted as pilot tasks are drafted and completed. Key limitations are listed below:

- While this draft SMOC outlines security controls for pilot V2X devices per NIST SP 800-53, the full specification of those security controls will not be complete until the final deliverables of the Threat Definition of V2I Architecture project are published. Recommended security requirements from that project will not be implemented in the pilot, as suppliers are highly unlikely to have such devices available in time for the pilots. The CV Pilot teams, in coordination with USDOT representatives, determined the best course of action was to develop a minimum set of requirements that are realistic for device suppliers to meet in time for deployment while the fully specified security controls will be used as guidance for future devices and deployments
- SCMS Proof of Concept (POC) is not yet available for testing and current interface requirements documents will continue to be updated through September 2016 as the SCMS POC is built
- Security requirements recommended by this concept may be cost prohibitive (specifically FIPS 140-2 hardware security requirements) upon further review during the development of the System Requirements Specification document in Task 6. If the THEA CV Pilot team cannot obtain devices

that meet the security requirements, the team 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

- Device suppliers may not be able to meet all recommended security requirements in time for the planned device deployment
- Full security certification testing by third parties for all recommended security requirements will not be feasible for the CV Pilots. Testing and certification for interoperability and compliance with standards such as IEEE 1609.2 will occur. However, new requirements such as equivalency with specific FIPS 140-2 levels or operating system requirements will likely be self-certified as these tests are expensive and time consuming when conducted by accredited certification labs. 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
- The concept and requirements may require updates based on the Application Deployment Plan (draft due April 2016), Human Use Approval Plan (draft due June 2016), Participant Training and Stakeholder Education Plan (draft due June 2016), Outreach Plan (draft due June 2016), Performance Measurement Plan (draft due March 2016). The Application Deployment Plan may result in changes to the ConOps and necessary security requirements. The other plans will require the collection of PII to track equipment, conduct training, and maintain communications with participants which may result in changes to privacy considerations and controls

1. Introduction

The Privacy and Security Management Operating Concept (SMOC) provides details about how to ensure 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 actions that will be taken by the team during the Pilot Deployment to protect the privacy of users, guard against potential breaches of the system, and ensure 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) Proof of Concept (POC). Where privacy is not sufficiently addressed by the SCMS POC design, this SMOC explains additional actions that will be taken by the pilot team to increase privacy, such as the protection of participant data used for CV Pilot administration purposes and using sanitation algorithms for vehicle situation data as necessary. The SMOC also defines the device and system requirements to ensure 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 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 the Personal Information Device (PID), Vehicle On-Board Equipment (OBE), Transit OBE, and Roadside Equipment (RSE). However, the Vehicle Databus, Intelligent Transportation Systems (ITS) Roadway Equipment (RE)[5], Transportation Management Center (TMC), and Transit Management Center (MC) information flows are considered within the analysis and for security control selections.

[5] ITS Roadway Equipment is based off of the CVRIA definition “physical objects that represent all of the other ITS field equipment that interfaces with and supports the Connected Vehicle Roadside Equipment (RSE). 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.”

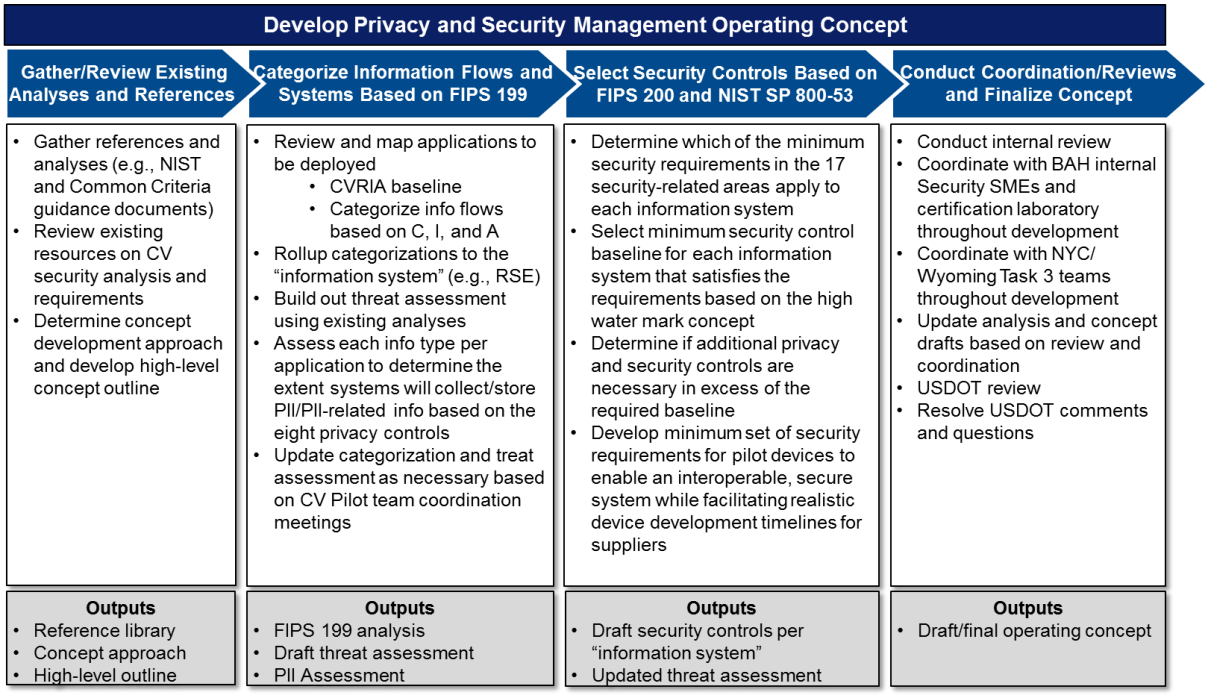
The SMOC also discusses the possible governance, policy, and audit processes for privacy and security that will be necessary to extend operations beyond the CV Pilot era.

1.2. Privacy and 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. Our 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 Task 3 Approach



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 E, 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 did not further specify those controls because the Threat Definition of V2I Architecture project[6] team, Iteris and Security Innovation, is already conducting that work. Instead, we focused on developing other aspects of the SMOC such as communications, access, hardware, software, and operating system security considerations that have not been fully addressed, such as misbehavior detection strategies and software security requirements. 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. Due to constraints listed in the SMOC Limitations section and the concurrent project focusing on detailing these security controls, 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.

[6] The Threat Definition of V2I Architecture project is a USDOT project separate from the CV Pilots. This project is managed by Iteris and Security Innovation to utilize the FIPS 199/200 and NIST SP 800-53 approach to assess the security needs for five sample V2I applications, propose device classes, and specify detailed security controls. The THEA CV Pilot team plans to update the SMOC based on the final project report.

1.4. Privacy and Security Management Operating Concept (SMOC) Limitations

While the THEA team took a holistic, comprehensive approach to the SMOC, there are still limitations to this concept as the overall pilot concept is still in the development process. As the THEA team continues to work on the remaining Pilot Deployment Concept tasks, the SMOC will likely have to be revisited and adjusted as necessary. Key limitations are listed below:

- While this draft SMOC outlines security controls for pilot V2X devices per NIST SP 800-53, the full specification of those security controls will not be complete until the final deliverables of the Threat Definition of V2I Architecture project are published. Recommended security requirements from that project will not be implemented in the pilot, as suppliers are highly unlikely to have such devices available in time for the pilots. The CV Pilot teams, in coordination with USDOT representatives, determined the best course of action was to develop a minimum set of requirements that are realistic for device suppliers to meet in time for deployment while the fully specified security controls will be used as guidance for future devices and deployments
- SCMS Proof of Concept (POC) is not yet available for testing and current interface requirements documents will continue to be updated through September 2016 as the SCMS POC is built
- Security requirements recommended by this concept may be cost prohibitive (specifically FIPS 140-2 hardware security requirements) upon further review during the development of the System Requirements Specification document in Task 6. If the THEA CV Pilot team cannot obtain devices that meet the security requirements, the team 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
- Device suppliers may not be able to meet all recommended security requirements in time for the planned device deployment
- Full security certification testing by third parties for all recommended security requirements will not be feasible for the CV Pilots. Testing and certification for interoperability and compliance with standards such as IEEE 1609.2 will occur. However, new requirements such as equivalency with specific FIPS 140-2 levels or operating system requirements will likely be self-certified as these tests are expensive and time consuming when conducted by accredited certification labs. 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
- The concept and requirements may require updates based on the Application Deployment Plan (draft due April 2016), Human Use Approval Plan (draft due June 2016), Participant Training and Stakeholder Education Plan (draft due June 2016), Outreach Plan (draft due June 2016), and the Performance Measurement Plan (draft due March 2016). The Application Deployment Plan may result in changes to the ConOps and necessary security requirements. The other plans will require the collection of PII to track equipment, conduct training, and maintain communications with participants which may result in changes to privacy considerations and controls

1.5. Connected Vehicle Pilot Team Coordination

Throughout concept development, the THEA team has coordinated with USDOT representatives and the other pilot teams to produce a broad, yet detailed security analysis and operating concept. THEA initiated and led this coordination ensuring that valuable information from current and existing projects were shared with the CV

Pilot teams. The THEA team also initiated biweekly coordination conference calls to review the status of concept development across the teams and request information from USDOT and the other pilot teams. A cross-team working session, scheduled and executed by the THEA team, was invaluable in developing a holistic concept while learning lessons and considerations from other pilot teams.

2. Communications Security Overview

Communications security for the THEA CV Pilot is largely ensured through compliance with the SCMS POC design and existing standards, such as IEEE 1609.2. The SCMS POC design and existing standards are referenced in this chapter. This chapter also addresses considerations not fully covered in the POC 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., PID, OBE, RSE) 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) 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., PID, OBE, RSE, 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 POC 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) Proof of Concept (POC)

This section describes the current SCMS POC design and how it will be used for the Tampa CV Pilot. The section references SCMS POC 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., PID, OBE, RSE) used within the deployment. For all interactions between these system elements and the other elements of the SCMS POC, the interface is fully specified by the SCMS Operator and the SCMS Operator provides functionality across fully-tested implementations of those interfaces.

2.2.1. SCMS POC Requirements, Interfaces, and Processes

THEA CV Pilot devices must support requirements identified in the SCMS POC 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 POC 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
  - OBE
    - Bootstrapping
    - Initial Provisioning of Pseudonym Certificates
    - Misbehavior Reporting (Next SCMS POC revision will add further requirements)
    - Certificate Revocation List (CRL) Download
    - OBE Revocation
    - Refresh Pseudonym Certificates
    - Update Pseudonym Certificate Request Parameters
  - RSE
    - RSE Bootstrapping
    - RSE Application Certificate Provisioning
    - RSE Misbehavior Reporting
    - RSE CRL Check
    - RSE Application and OBE Identification Certificate Revocation
    - Refresh RSE Application Certificates

2.2.2. Bootstrapping and Re-Bootstrapping Processes

Based on the current design, the SCMS POC will only support a manual bootstrapping process to support overall security requirements as described in the SCMS POC documentation. Later versions of the system will implement an automated process. The manual process will also be used for re-bootstrapping in the event that

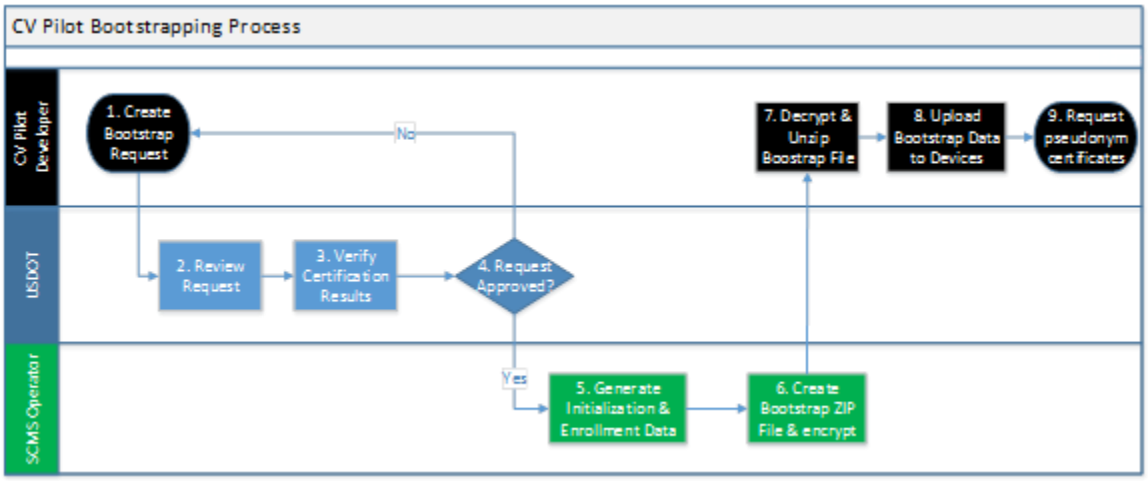
a device's enrollment certificate is placed on the internal blacklist and can no longer request certificates from the SCMS.

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



Source: 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.

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 OBEs 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 POC 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, OBEs and PIDs/ASDs will be provisioned with pseudonym certificates and RSEs with the necessary application certificates via the Registration Authority (RA). Enrollment certificates have a validity period of 40 years for the SCMS POC.

OBEs and PIDs/ASDs 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 RSE 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. OBEs and PIDs/ASDs 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 OBE has only one identification certificate valid at a time for a given application. While pseudonymity and tracking is no 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.

RSEs 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 RSE requests and receives a new application certificate via the RA. The new and the old application certificate have an overlap of one hour. The RSE 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 RSE waits until connectivity is available and requests the certificates again. If the RSE 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 POC design already has established misbehavior reporting and CRL distribution processes, misbehavior detection strategies are not complete. The CRL strategy will also have to be tailored to the needs of the pilot. This section proposes multiple local misbehavior detection strategies that could be developed with additional resources. 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 Recommendations

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 as a result of malfunction or malfeasance. Local misbehavior detection strategies have not been finalized by the SCMS POC. Based on the current SCMS POC Implementation EE Requirements and Specifications and recent USDOT technical assistance webinars, the SCMS POC is in the process of testing prototype misbehavior detection methods through 2016 and will integrate global misbehavior detection functionality from mid-2016 to mid-2017 for use in version 2.0 of the SCMS POC. Members of the current THEA team developed recommendations for potential local misbehavior detection strategies. However, testing these strategies is not within the scope of the current THEA CV Pilot. Working to develop these misbehavior checks and conduct tests would be added work that could be done with additional resources or an outside contractor.

Recommended local misbehavior detection strategies focus on detecting OBE misbehavior, not RSE misbehavior. Per the SCMS POC, RSEs will have application certificates with short validity periods (e.g., daily, hourly) and require frequent certificate renewal, and hence no RSE CRL is necessary. We do not suggest any strategies to detect RSE misbehavior at this time. The TMC should be able to provide sufficient monitoring to determine if a RSE is not functioning properly or has been compromised. Due to a RSEs fixed location and remote access, the RSE could be taken offline much easier than an OBE.

While the OBE should obviously report any message that does not have a valid signature and/or certificate, the project team also developed some strategies that could be deployed with additional resources or an outside contractor to conduct plausibility testing. The strategies are intentionally left at a high-level description to allow for additional options and ideas for misbehavior detection. These potential requirements are not part of a current device specification and would have to be developed as new capabilities.

- Level 1 Plausibility: The OBE [and RSE] 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 OBE 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 OBE does not raise an alert to the driver on the basis of that message and prioritizes the message for misbehavior reporting
- The OBE [and RSE] 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 OBE [and RSE] 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. Depending on available resources and priorities, the team believes there would be value in testing the impact of tighter BSM parameter error tolerances than those specified in SAE J2945/1 (shown in Table 2-1). Again, these tests would be outside the scope of the THEA CV Pilot and would be added work that could be done with additional resources or an outside contractor.

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

Per the SCMS POC, the format of the misbehavior report is not yet fully defined. However, a report could potentially include reported BSMs as well as the reporter's pseudonym certificate and the reporter's signature.

Global misbehavior detection strategies, which consist of analyzing misbehavior reports generated based on local misbehavior detection strategies, will be handled by the SCMS entities (i.e., SCMS Manager and Certificate Management Entities [CMEs]). Per the SCMS POC, OBE misbehavior analysis will be defined by CAMP's VSC6 Communications Research project and integrated with the yet to be awarded Misbehavior Authority Integration sub project. The global misbehavior detection strategies will determine how and when pseudonym certificates are placed on the CRL, so that messages with that associated certificate are not trusted by other devices, and enrollment certificates are placed on the internal blacklist, so that the device can no longer replenish pseudonym certificates.

External Reporting[7]

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. If a specification becomes available for misbehavior reports for any given application, and if CAMP provides a misbehavior reporting protocol, suppliers will be requested to provide support for misbehavior detection as part of the standard software support / patch / update cycle.

Support for external reporting:

- Vehicle OBEs/VADs/PIDs/ASDs: 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 OBEs/RSEs: 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 or from its mounting (if an RSE) 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.
- 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.

[7] The majority of the external reporting concept was developed by the NYC CV Pilot team. The THEA CV Pilot team modified the concept to apply to the THEA ConOps.

CRL Strategies

At a basic level and per the SCMS POC, the device (i.e., PID, OBE, RSE) 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), the SCMS POC 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 of 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 POC 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. Sirius has already been working the CAMP and USDOT to test this potential CRL distribution option during the CV pilots. As this strategy is developed and if added to the overall pilot concept, the SMOC and recommended device requirements may need to be updated.

2.3. Privacy

This section covers the privacy considerations for administrative, V2X communications, and application data, including privacy by design aspects of the SCMS POC and specific application considerations where data could be seen 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 will implement the following recommendations to maintain privacy[8]:

- Authorization
    - The definition of “authorized to use the service” will be application specific.
- Privacy

[8] These privacy recommendations were primarily developed by the Wyoming CV Pilot team.

- 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.).
- Use temporary and one-time identifiers. Separate instances of the exchange shall not use identifiers (USER MAC address, UE-ID (IMEI), IP address, certificate, temporary ID, session ID, etc.) that have been used in a previous instance of the exchange.

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.

1) **Establish data ownership**. As a general rule, whoever owns the vehicle, 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 eliminated.
4) **Identify data aggregation issues**. In some cases, aggregating CV data over time can reveal patterns that are sensitive from the point of view of commercial, military or other propriety information about the internal operations of firms or agencies.
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 Research Data Exchange (RDE) or the Saxton Transportation Operations Laboratory (STOL) repositories.

2.3.1. Participant Data

While the Human Use Approval Plan (draft due June 2016), Participant Training and Stakeholder Education Plan (draft due June 2016), and Outreach Plan (draft due June 2016) will focus on the plans for collecting and maintaining administrative participant data, the THEA CV Pilot team must consider this PII and PII-related data in developing the SMOC.

Participants in the CV Pilot study will include: drivers, pedestrians, bicyclists, and bus/trolley drivers. For purposes of this pilot, bicyclists will be grouped into pedestrians as their participation would be through using the PIDs. The recruitment of participants, their training, and involvement will be treated in detail in Tasks 8, Human Use Approval and 9 Participant Training and Stakeholder Education. Below is potential sample size for participants. It is important to note that the sample size may be adjusted or further refined in Task 8.

- 1500-2000 drivers
- 500 pedestrians
- 400 buses

Currently, the team anticipates that Participant Training and Stakeholder Education will require collection of the following PII in order to administer training and education leading up to and continuing throughout the pilot deployment.

- Name
- Date of Birth
- Contact information

    - home and work mailing addresses
    - email
    - phone number
- Copies of
    - driver licenses identification number
    - insurance card
    - 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 for will be used in Task 8 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 in order to 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 (draft due March 2016). Performance measure data will be further refined in the Performance Management Plan. The SMOC should update the content from the Performance Measurement Plan accordingly when fully developed.

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
	Break 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/Bike volume
	Pedestrian volume
Mobility	Actual Length
	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
	Pedestrian wait time
	Time Stamp (1 second)
	Vehicle Direction
	Vehicle Location
	Vehicle Location/Time Stamp
	Vehicle Speed
Environment	Bus Location
	Bus Speed
	Emission rates from MOVES
	Location/Speed
Agency Efficiency	As in Mobility
	As in Safety
	Survey/Opinion/App Feedback

The Performance Measurement Plan will provide detailed procedures (and be the master reference) 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 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 will be tailored to the THEA CV Pilot based on data generated by all sensors, OBUs, and driving data. We emphasize the current step for PII removal below as that is the most relevant to the SMOC. We will continue to coordinate with the Performance Measurement team as the plan evolves to provide input and update the SMOC as necessary.

Step 2: PII removal
Most of the collected datasets will need to undergo some form of cleansing before they are posted to the RDE. 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.

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 particular 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.

Table 2-3 outlines some of the procedures that may be adopted to remove PII from datasets, in the event that potential strategies described within the SMOC cannot be fully implemented to remove data prior to collection and storage by the TMC. These are generic procedures that are provided as examples and were previously applied to the Safety Pilot datasets collected in Ann Arbor, MI 2012-2013. These will be tailored to the THEA CV Pilot data collection system.

Table 2-3. Potential PII Removal Procedures

File to be Cleansed	Step	Purpose	Action	Output
Trajectory Based-Host Vehicle files	Test Bed Cordon Truncation	Limit data analysis to geographic confines surrounding the test bed area	Establish a 5-10 mile cordon around the test site and eliminate all records that place vehicles outside the cordon	All remaining records are those collected within the area of interest

	Distance based Trip Truncation	Protect (S)PII by establishing a distance based buffer zone around each trip's origin and destination	Eliminate host vehicle records that places a vehicle within 1-1.5km from the origin and destination of a trip	The closest coordinate pair, for a host vehicle, will be 1-1.5km away from the beginning or end of a trip, and therefore provides a layer of obscurity, protecting (S)PII
	Temporal Trip Truncation	Protect against the discovery of (S)PII for vehicles that the distance truncation step did not sufficiently obscure a trip's O/D (which is normally due to limited network / route choices around a trip's origin or destination)	Rid host vehicle trajectory file of records that were collected within 80 – 100 seconds of the start or end of a trip	Remaining records will only include those that places a vehicle sufficiently far away, both in terms of distance and time, from a vehicle's origin and destination, to provide an additional layer of security to protect (S)PII
	Adjustments of Sequential Data Element	Prevent the extrapolation of location data, with the aid of additional data elements such as speed	Reset sequentially collected data element, particularly those collected at a known and constant frequency, so that is first entry for a given trip is "1"	After truncating trip records according to distance and time, the first entries for sequentially collected data elements will be "1", which does not indicate that any other records previously were collect for a given trip
Event Based – Host Vehicle files	Truncation of event based – host vehicle files	Control the possibility of having data elements contain relevant information that may be used to deduce (S)PII	Using truncated trip records, from the above steps, deleted event records that may place a host vehicle within the distance and temporal buffer zones around a vehicle's start and end of a trip	This file will be void of records that may be combined with trajectory based records to ascertain the start and end of a host vehicle's trip
Trajectory Base – Remote Vehicle files	Truncation of trajectory based – Remote vehicle files	Guard against the deduction of the start and end of a host vehicle's trip, from a remote vehicle's location data (upon knowing range of DSRC)	Remove remote vehicle location data that were collected outside of the time period present for a host vehicle's trip as well as those that places a remote vehicle within 1-1.5km from the start or end of a host vehicle's trip	All remote vehicle records, that places a vehicle close enough to the start or end of a host vehicle's trip, will be eliminated to protect (S)PII
Trip Summary Files	Adjustment of Trip Summaries	Allow the summary of each trip to reflect the "new" reality of each truncated host vehicle trip	Mathematically edit trip summary information such as trip duration, and length, so that these summary data elements is consistent with summarized details from a host vehicle's file	Trip summary information will be consistent with the information contained in files with truncated trip information, additionally trip summaries are not able to provide data that could be used to extrapolate location data to decipher (S)PII

2.3.3. SCMS POC 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 current application assessment does not directly reveal any PII or PII-related information being collected, but this assessment may change based on the requirements set for performance measurement and evaluation. 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. Much of these privacy concerns are addressed in the Security Credentials Management System (SCMS) Proof of Concept (POC) and associated security standards that will be implemented during the pilot.

The SCMS POC being built by the USDOT and Crash Avoidance Metrics Partnership (CAMP) has "privacy by design" as a major tenet of the system development. All V2X system communications will utilize the SCMS POC design along with the IEEE 1609.2 standard to provide communications security and protect user privacy. In order for vehicle OBEs, PIDs, and RSEs 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, OBEs and PIDs will use pseudonym certificates to sign all messages. Based on information provided by USDOT on the current SCMS POC 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 RSE, 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 POC 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. Personal Information Device (PID)

While the PID will still use the SCMS POC in much the same way as a vehicle OBE to maintain privacy, the PID will likely have less physical security protection combined with potentially more attack vectors. This presents unique privacy, as well as security, questions.

Within these applications, the PID will need to communicate with the RSE to receive safety information and intersection status along with sending personal location, which is similar to a vehicle BSM and signal service request. The PID will also need to communicate with OBEs by sending personal location information and receiving BSMs. BSMs and other messages should be signed to prove authenticity. They must also support certificate change strategies to preserve privacy by design as specified in the SCMS POC. However, the device must be able to communicate with the SCMS to receive keys and certificates in order to sign messages. We have classified PIDs and OBEs as medium baseline devices based on FIPS 199 and FIPS 200 analyses which corresponds to a FIPS 140-2 Level 2 classification. The problem is that the vast majority of standard smartphones (e.g., all iPhones) are only certified to FIPS 140-2 Level 1. However, that only means that they are certified to that level across all FIPS 140-2 areas. It is possible that select smartphones are Level 2 equivalent across the majority of areas, while being only Level 1 in other areas. This would result in a certification of Level 1. The other issue is that a standard smartphone is not able to communicate via DSRC, which is a requirement based on the required functionality specified by the ConOps.

To enable the functionality of the selected applications as described in the ConOps while maintaining the recommended level of security, the THEA CV Pilot could use an ASD, such as the Arada LocoMate Me™ Mobile DSRC device, which will connect to the smartphone while using V2X applications. The ASD would be

DSRC enabled and could be built equivalent to FIPS 140-2 Level 2. Another possibility is to use specialized PIDs that are separate from the participant's personal smartphone. However, the device would have to be evaluated against FIPS 140-2 to determine if the necessary security requirement areas met FIPS 140-2 Level 2. Please refer to Chapter 4 and 5 for more information on FIPS 140-2, hardware security, and software/operating system security. Another option is to modify an existing smartphone by re-flashing its firmware to transmit over the appropriate DSRC channels; however, this usually causes additional issues such as voided warranties and the challenge of meeting hardware and software/OS requirements.

2.3.5. Application Data Considerations

While the privacy of most data is protected by the SCMS POC 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 Curve Speed Warning application.

Vehicle Situation/Probe Data

Even though the privacy by design elements of the SCMS POC 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 POC 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 OBEs 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 OBE to control data generation and packaging.

The THEA CV Pilot will primarily focus on gathering vehicle situation/probe data packages transmitted to RSEs 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, and at the gates to MacDill Air Force Base. Selected RSEs 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 RSE and the device buffer is full, the OBE 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.

Curve Speed 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 Curve Speed 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 (RSE->TMC): Speed warning application status reported by the RSE. This includes current operational state and status of the RSE and a record of measured vehicle speeds and notifications, alerts, and warnings issued
- Speed Monitoring Information (RSE->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 RSE and prior to bundling and sending the information from the RSE 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 RSE 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 RSEs 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 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. 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. Currently, the only openly published data 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 made openly available within the next year.

Future data collection procedures will be governed by the data collection and storage policies that are currently in development. Only users who are authorized by THEA and CoT TMC management will have access to the data. Functional needs will be identified and permissions controlled based on the individuals needs and responsibilities.

Access control policies will also need to be updated based on planned upgrades to the TMC software to ensure compatibility with CV applications. The THEA TMC uses proprietary software, DYNAC, to run the TMC. The DYNAC software runs the Selmon Expressway REL gates and controls the CCTV cameras. THEA and CoT are currently evaluating Cameleon and other traffic management software systems for replacement of the current control software. Software for CV Pilot equipment and TMC alert notifications will be produced

or facilitated by Siemens. Siemens will work closely with the TMC software maintenance professionals to add software modules to the TMC software that will classify, count, and distribute alerts to operators.

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 as specified in later concepts and plans (drafts due for each plan in June 2016), and preferably maintained in a database that is entirely separate from those in use at the THEA/CoT TMC. 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
- DYNACAdmin – 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. The director should ensure that
- 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.

3.4. User Name and Password

Upon receiving V2X devices (e.g., OBE, RSE, ASD, VAD) from suppliers, the team will change the default device user names and passwords to new, unique usernames and passwords. New user names and passwords to access V2X devices will be maintained by the pilot team in a database that will align specific devices (i.e., OBE, ASD, VAD) with pilot participants. Username and password should be stored based on existing TMC IT security policies containing processes and procedures for username and password management to access devices or communal type devices. Only a select group of personnel within the Human Use, Participant Training and Stakeholder Education, and Outreach teams as specified by their respective concepts and plans (drafts due June 2016), will have access to the information on pilot participants and the aligned devices to identify and contact participants that may need to have their devices reconfigured or re-bootstrapped. TMC personnel will only have access to the RSE usernames and passwords as necessary to access the devices remotely based on their assigned roles. In this way, no group has all of the information necessary to link devices to participants while also having the usernames and passwords necessary to access devices.

As of now, the THEA CV Pilot will continue to use existing TMC ACCS user name and password policies, but will modify as necessary based on USDOT guidance.

1) User accounts for the ACCS are group-based, compliant with LDAP, and Integrated with Active Directory
2) Authentication shall be Single-Sign-On
3) Group policies within Active Directory shall control user rights within the ACCS
4) The user rights management shall:
    a. Allow for the creation of groups for which permissions can be specified, with all users receiving those permissions upon joining the group
    b. User permissions shall also be individually configurable with individual configuration overriding their containing group permissions
5) All user names shall use the following taxonomy:
    a. [first initial][last name] ie: jsmith
    b. If there are multiple users with same first initial and last name, the user account shall use the following taxonomy:
        i. [first initial][middle initial][last name] ie: jdsmith
6) All passwords shall be compliant with Active Directory and allow the use of special characters (i.e., @!~)
7) All passwords shall have a minimum requirement of eight (8) characters. THEA may re-evaluate the minimum password requirement to contain more characters along with numbers and symbols
8) Users shall be allowed to change their passwords
9) Passwords do not expire
10) Account is locked out after 5 incorrect attempts and automatically resets after 120 minutes

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 RSE and additional ITS RE remote access.

RSEs 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.

OBEs, PIDs, ASDs, and VADs (i.e., LMM devices) shall not support remote access. If the THEA team uses conventional smartphones for PIDs, the V2X applications used on the PID must protect against remote access per the Software and Operations System requirements in Chapter 5. However, devices shall support physical access in the event that re-bootstrapping is required. The device shall support role-based authentication to enable physical access.

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 RSE is generating more internet traffic than would be warranted by the number of OBEs 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 RDE, and be available to Test Bed Affiliates and other independent evaluators. As discussed in the Chapter 2: Communications Security Overview, the CV data collected from probe enabled vehicles and RSEs 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. If not effective, these strategies will be supplemented by existing sanitation algorithms used by SE Michigan Testbed to remove pieces of trip data before submission to the RDE. 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, RSEs, 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 look into 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 PID, OBE, and RSE 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.

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.

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).

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.
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	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.			

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

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 THEA team has previously conducted work in this area for V2V OBEs and will leverage that knowledge to develop device recommendations.

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 Equipment (OBE), Vehicle Awareness Device (VAD), Personal Information Device (PID), Aftermarket Safety Device (ASD)

Based on the application information flow analysis, the OBE and PID have a medium classification baseline which corresponds to FIPS 140-2 Level 2. Like devices such as the VAD and ASD should also be equivalent with 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 is feasible and achievable for device suppliers.

However, as discussed in Chapter 2: Communications Security Overview, the vast majority of standard smartphones (e.g., all iPhones) are only rated to FIPS 140-2 Level 1. To enable the functionality of the selected applications as described in the ConOps while maintaining the recommended level of security, the THEA CV Pilot must use an Aftermarket Safety Device (ASD), such as the Arada LocoMate Me™ Mobile DSRC device, which will connect to the smartphone while using V2X applications. The ASD would be DSRC enabled and could be built to FIPS 140-2 Level 2. Another possibility is to use specialized PIDs that are separate from the participant's personal smartphone. A smartphone could potentially be modified to by re-flashing its firmware to transmit over the appropriate DSRC channels. However, the selected smartphone

would have to be evaluated against FIPS 140-2 to determine if the necessary security requirement areas met FIPS 140-2 Level 2.

4.2.2. Roadside Equipment (RSE)

Based on the application information flow analysis, the RSE has a high classification baseline which corresponds to FIPS 140-2 Level 3. The team will proceed with Level 3 and maintain an open dialogue with suppliers to determine the feasibility of developing and manufacturing devices at this level. Level 3 may not be feasible and achievable for device suppliers for cost reasons, not necessarily technical reasons. The RSE 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 OBE (i.e., vibrations, rapid temperature changes, and moisture issues due to rapid heating and cooling). However, designing and manufacturing the RSE to be FIPS 140-2 Level 3 equivalent will take considerably more development and testing resources than a Level 2 device. While this may be challenging in the short term context of the CV Pilots, certain manufacturers already have plans to produce Level 3 hardware in volumes that make the cost practical for US automakers and roadside infrastructure manufacturers.

Note: The USDOT FHWA DSRC Roadside Unit (RSU) Specifications Document, Version 4.0 April 15, 2014, includes basic security requirements for RSEs. One of these requirements is for the RSE to be equivalent with FIPS 140-2 Level 2, which is one level lower than our recommendation of Level 3.

4.2.3. ITS Roadway Equipment (ITS RE)

Current ITS RE (i.e., signal controllers) are legacy devices and planned to be replaced within the THEA CV Pilot deployment area to be compatible with RSEs. New ITS RE would require FIPS 140-2 Level 3 because it also has a high classification baseline based on the application information flow analysis. As additional ITS RE are acquired and signal controllers are replaced, THEA should upgrade/replace with equipment equivalent with FIPS 140-2 Level 3 and recommended requirements aligned with the MHM device class. As stated for RSEs, developing Level 3 equivalent devices is technically feasible but will result in more expensive devices. Legacy ITS RE that does not meet these requirements will be vulnerability when communicating with RSEs and other V2X devices, especially if wireless communication is involved with OBEs and PID. However, these devices are contained within locked cabinets that will have door open alarms and video monitoring and will also likely have hardwire connections to RSEs which should mitigate some of the risk if not FIPS 140-2 Level 3 equivalent.

5. Software and Operating System Security Overview[9]

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 POC. 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.

[9] The software and operating system security section and requirements were primarily developed by the NYC CV Pilot team with assistance and reviews by the THEA and Wyoming CV Pilot teams.

4) The system supports software/firmware update in such a way that the above properties continue to hold.

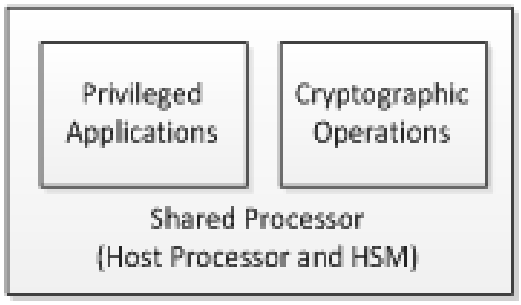
5.1. Architectures

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.

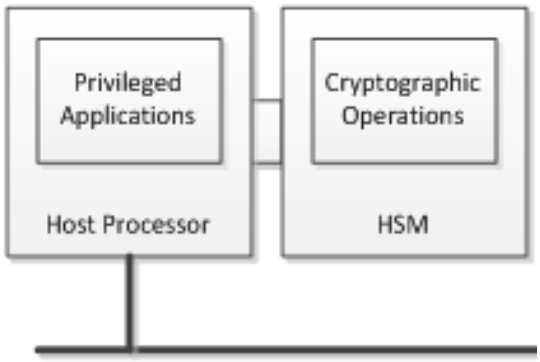
This chapter provides requirements for the host processor and the HSM separately in sections 5.2 and 5.3 respectively, and then provides architecture-specific requirements in section 5.4.

Figure 5-1. Integrated Architecture



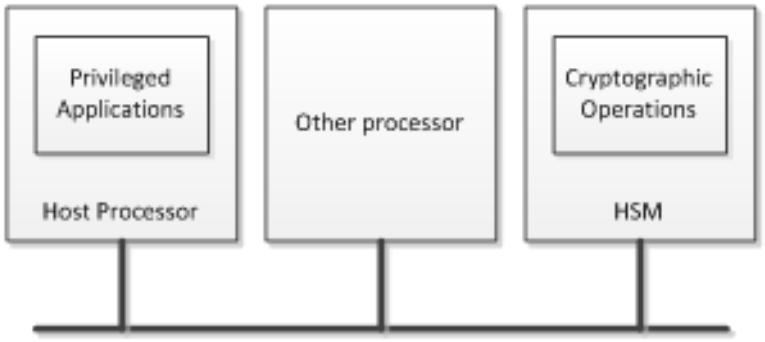
Source: NYC CV Pilot Team

Figure 5-2. Connected Architecture



Source: NYC CV Pilot Team

Figure 5-3. Network Architecture



Source: NYC CV Pilot Team

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 all the protections below.

The host processor may be initialized while in a *manufacturing state* that does not implement all the protections.

A device may be designed so it can return from the operational state to the manufacturing state. If this functionality is provided, the transition shall wipe all privileged applications from the host processor and all keys from the HSM. The device may allow a user to perform a reset to a manufacturing state without any authentication if the mechanism for a reset guarantees that the user is physically present.

5.2.2. Secure Boot

The host processor shall perform integrity checks on boot to ensure that it is in a known good software state. The integrity checks shall require the use of a hardware-protected value such that the integrity cannot be successfully compromised unless the hardware-protected value is modified. Examples of these integrity checks include signing the software such that the verification key is protected by hardware, or storing hashes via the Platform Configuration Registry (PCR) mechanism of the Trusted Computing Group (TCG)'s Trusted Platform Module (TPM).

The host processor integrity check shall verify the software and firmware configuration of the host processor such that:

- The host processor shall not allow any privileged application to request signing until the integrity checks have passed.
- If the host processor fails the integrity checks it shall not grant access for any process to private keys.
- If the host processor fails the integrity checks it shall not allow any privileged application to operate.

The host processor integrity check shall carry out a check that stored root CA certificates have not been modified since they were last accessed such that:

- If this integrity check fails, the device shall reject all incoming signed messages that chain back to those root CA certificates as invalid.

5.2.3. Operating System

The host processor operating system shall meet the following requirements (derived from FIPS 140-2 section 4.6.1):

- The operating system shall support roles which are used as specified below. Each privileged application shall map to a role.
- The discretionary access control mechanisms of the operating system shall be configured to:
  - Specify the set of roles that has execute permissions on each private key stored within the HSM
  - Specify the set of roles that can modify (i.e., write, replace, and delete) the following programs and plaintext data stored within the host processor boundary
  - Specify the set of roles that can read data stored within the host processor boundary and which data can be read by those roles
  - Specify the set of roles that can enter cryptographic keys (It is permissible for the host to require that all keys are generated on the device and that keys cannot be entered directly)
- The OS shall allow the following roles to operate without explicit authentication by a user:
  - Processes that correspond to privileged applications, i.e., applications that are intended to run without user initiation or intervention, and that have execute access to private keys
  - Processes that update private key material within the HSM, for example to implement the butterfly key process specified within the SCMS documentation.
- The OS may allow the following roles to operate without explicit authentication, or may require authentication:
  - Processes that install new software or firmware if that software or firmware is signed.
  - Processes that write private key material to the HSM. (It is permissible for the host to require that all keys are generated on the device and that keys cannot be entered directly)
- The OS may support the following roles and, if it supports them, shall require explicit authentication:
  - Processes that modify or inspect executing processes
- The OS shall not allow the following roles to exist:
  - Processes that read private cryptographic key material from the HSM (NOTE: The HSM should also not provide this functionality)

5.2.4. Secure Updates

The host processor shall use the following mechanisms to ensure that its software and firmware can be securely updated:

- The host processor requires that all software installed is signed: in other words, when requested to install software, the host processor OS ensures that the software is signed by an authority with appropriate permissions before proceeding with the installation and rejects the installation if the signature or any of the validity checks on the software or its signing certificate fail.
  - The integrity of the verification key shall be protected by local hardware, either by directly storing the key in local hardware, or by creating a chain of trust from the key to a hardware-protected key. The hardware protection shall be equivalent to FIPS 140-2 at the level appropriate to the device as a whole.
- In addition, the host processor may require that software can be installed only by an authenticated user.

The update mechanism shall include mechanisms to prevent updates being rolled back.

5.3. Hardware Security Module (HSM)

The HSM shall meet the requirements for an operating system given in FIPS 140-2 except for the audit requirements and certain additional exceptions. The baseline requirements are the following:

- All cryptographic software and firmware shall be developed and installed in a form that protects the software and firmware source and executable code from unauthorized disclosure and modification.
- A cryptographic mechanism using an Approved integrity technique (e.g., an Approved message authentication code or digital signature algorithm) shall be applied to all cryptographic software and firmware components within the HSM.
    - The message authentication code (MAC) may be used in the following circumstances only:
        - If the HSM itself calculates the MAC when the software is installed using a secret key known only to the HSM, and uses this secret key to verify the software on boot
        - If the software provider has a unique shared key with each distinct device and uses this to authenticate the software.
    - A MAC may not be used to protect the software unless the MAC key is unique to the HSM.
- All cryptographic software and firmware, cryptographic keys, and control and status information shall be under the control of an operating system that meets the functional requirements specified in the Protection Profiles listed in FIPS 140-2 Annex B and is capable of evaluation at the CC evaluation assurance level EAL2, or an equivalent trusted operating system.
- To protect plaintext data, cryptographic software and firmware, cryptographic keys, and authentication data, the discretionary access control mechanisms of the operating system shall be configured to:
    - Specify the set of roles that can execute stored cryptographic software and firmware.
    - Specify the set of roles that can modify (i.e., write, replace, and delete) the following cryptographic module software or firmware components stored within the cryptographic boundary: cryptographic programs, cryptographic data (e.g., cryptographic keys and audit data), and plaintext data.
    - Specify the set of roles that can read the following cryptographic software components stored within the cryptographic boundary: cryptographic data (e.g., cryptographic keys and audit data), and plaintext data.
    - Specify the set of roles that can enter cryptographic keys.
- The operating system shall prevent all operators and executing processes from modifying executing cryptographic processes (i.e., loaded and executing cryptographic program images). In this case, executing processes refer to all non-operating system processes (i.e., operator-initiated), cryptographic or not.
- The operating system shall prevent operators and executing processes from reading cryptographic software stored within the cryptographic boundary.

5.4. Architecture-specific Requirements

5.4.1. Integrated Architecture

An integrated processor meets the complete set of requirements identified in sections 5.2 and 5.3.

5.4.2. 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.

5.4.3. 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 Appendix B: Application Information Flow and Device Classification Analysis for full information flow and device classification analysis.

NOTE: These controls will be further developed and specified through the Threat Definition for V2I Architecture project. The THEA CV Pilot will follow minimum requirements and controls as specified in Chapter 7: Minimum Security Requirements per Device Classification.

6.1.1. 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

6.1.2. Security Control Enhancements

Security control enhancements are numbered sequentially within each control so that they can be easily identified when selected to supplement the base control. Each security control enhancement has a short subtitle to indicate the intended security capability provided by the control enhancement.[10] For example if the AC-2 first control enhancement is selected, the control designation becomes AU-2(1) (2) (3) (4). The numerical designation of a control enhancement is used only to identify the particular enhancement within the control. The designation is not indicative of either the strength of the control enhancement or any hierarchical relationship among the enhancements. Control enhancements are not intended to be selected independently (i.e., if a control enhancement is selected, then the corresponding base security control must also be selected)

6.1.3. Priority Code

The recommended priority codes are used for sequencing decisions during security control implementation and the initial allocation of security controls and control enhancements to the baselines. The priority code structure is found in Table 6.1 below.

Table 6-2. Priority Code Structure

ID	Priority Code
P1	Implement P1 security controls first
P2	Implement P2 security controls after implementation of P1 controls
P3	Implement P3 security controls after implementation of P1 and P2 controls
P0	Security control not selected in any baseline

Sequencing prioritization helps to ensure that the foundational security controls upon which other controls depend are implemented first, which will enable the THEA Pilot Team to deploy controls in a more structured and timely manner in accordance with available resources. The priority codes are intended only for implementation sequencing, not for making security control selection decisions.

6.2. Low, Moderate, Moderate (LMM) Device Class (OBE, VAD, PID, ASD)

This section covers the LMM device classification which we currently have for the OBE and PID, as well as like device such as the VAD and ASD. 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 in order 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

[10] Detailed descriptions of controls and control enhancements can be found in NIST SP 800-53.

will be measures enacted to detect misbehavior and revoke certificates as well as permissions[11], Integrity was downgraded to Moderate.

6.2.1. Classification

The initial analysis, which is presented in Appendix B, resulted in a LMM classification for the OBE, VAD, PID, and ASD. The LMM classification for these devices is consistent with other information flow and device classification projects such as the Threat Definition for V2I Architecture project.

6.2.2. Selected Security Controls

This section contains a table of the security controls selected for this device class based on the NIST SP 800-53 moderate security control baseline with justifications if a control was downgraded or upgraded. The selected controls will continue to evolve and be further specified through the Threat Definition for V2I Architecture project.

Table 6-1. LMM Device Security Controls: Moderate Baseline

No.	Control	Priority	Controls and Control Enhancements	Tailored Controls
AC-1	ACCESS CONTROL POLICY AND PROCEDURES	P1	AC-1	
AC-2	ACCOUNT MANAGEMENT	P1	AC-2 (1) (2) (3) (4)	
AC-3	ACCESS ENFORCEMENT	P1	AC-3	
AC-4	INFORMATION FLOW ENFORCEMENT	P1	AC-4	
AC-5	SEPARATION OF DUTIES	P1	AC-5	
AC-6	LEAST PRIVILEGE	P1	AC-6 (1) (2) (5) (9) (10)	
AC-7	UNSUCCESSFUL LOGON ATTEMPTS	P2	AC-7	
AC-8	SYSTEM USE NOTIFICATION	P1	AC-8	
AC-11	SESSION LOCK	P3	AC-11 (1)	
AC-12	SESSION TERMINATION	P2	AC-12	
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	P3	AC-14	
AC-17	REMOTE ACCESS	P1	AC-17 (1) (2) (3) (4)	
AC-18	WIRELESS ACCESS	P1	AC-18 (1)	

[11] The LMM classification assumes that misbehavior detection and reporting will be available within the SCMS POC for pilot deployment per the SCMS POC development and testing schedule. Even if full capabilities are not available, the THEA CV Pilot team will utilize external reporting mechanisms as described in Section 2.2.3.

AC-19	ACCESS CONTROL FOR MOBILE DEVICES	P1	AC-19 (5)	
AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	P1	AC-20 (1) (2)	
AC-21	INFORMATION SHARING	P2	AC-21	Downgraded - control focuses on access authorization to information. For systems with low confidentiality, we assume broadcast data can be read by anyone, making this control unnecessary
AC-22	PUBLICLY ACCESSIBLE CONTENT	P3	AC-22	
AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	P1	AT-1	
AT-2	SECURITY AWARENESS TRAINING	P1	AT-2 (2)	
AT-3	ROLE-BASED SECURITY TRAINING	P1	AT-3	
AT-4	SECURITY TRAINING RECORDS	P3	AT-4	
AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	P1	AU-1	
AU-2	AUDIT EVENTS	P1	AU-2 (3)	
AU-3	CONTENT OF AUDIT RECORDS	P1	AU-3 (1)	
AU-4	AUDIT STORAGE CAPACITY	P1	AU-4	
AU-5	RESPONSE TO AUDIT PROCESSING FAILURES	P1	AU-5	
AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING	P1	AU-6 (1) (3)	
AU-7	AUDIT REDUCTION AND REPORT GENERATION	P2	AU-7 (1)	
AU-8	TIME STAMPS	P1	AU-8 (1)	
AU-9	PROTECTION OF AUDIT INFORMATION	P1	AU-9 (4)	
AU-11	AUDIT RECORD RETENTION	P3	AU-11	
AU-12	AUDIT GENERATION	P1	AU-12	
CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES	P1	CA-1	
CA-2	SECURITY ASSESSMENTS	P2	CA-2 (1)	
CA-3	SYSTEM	P1	CA-3 (5)	

	INTERCONNECTIONS			
CA-5	PLAN OF ACTION AND MILESTONES	P3	CA-5	
CA-6	SECURITY AUTHORIZATION	P2	CA-6	
CA-7	CONTINUOUS MONITORING	P2	CA-7 (1)	
CA-9	INTERNAL SYSTEM CONNECTIONS	P2	CA-9	
CM-1	CONFIGURATION MANAGEMENT POLICY AND PROCEDURES	P1	CM-1	
CM-2	BASELINE CONFIGURATION	P1	CM-2 (1) (3) (7)	
CM-3	CONFIGURATION CHANGE CONTROL	P1	CM-3 (2)	
CM-4	SECURITY IMPACT ANALYSIS	P2	CM-4	
CM-5	ACCESS RESTRICTIONS FOR CHANGE	P1	CM-5	
CM-6	CONFIGURATION SETTINGS	P1	CM-6	
CM-7	LEAST FUNCTIONALITY	P1	CM-7 (1) (2) (4)	
CM-8	INFORMATION SYSTEM COMPONENT INVENTORY	P1	CM-8 (1) (3) (5)	
CM-9	CONFIGURATION MANAGEMENT PLAN	P1	CM-9	
CM-10	SOFTWARE USAGE RESTRICTIONS	P2	CM-10	
CM-11	USER-INSTALLED SOFTWARE	P1	CM-11	
CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES	P1	CP-1	
CP-2	CONTINGENCY PLAN	P1	CP-2 (1) (3) (4) (5) (8)	
CP-3	CONTINGENCY TRAINING	P2	CP-3	
CP-4	CONTINGENCY PLAN TESTING	P2	CP-4 (1)	
CP-6	ALTERNATE STORAGE SITE	P1	CP-6 (1) (3)	
CP-7	ALTERNATE PROCESSING SITE	P1	CP-7 (1) (2) (3)	
CP-8	TELECOMMUNICATIONS SERVICES	P1	CP-8 (1) (2)	
CP-9	INFORMATION SYSTEM BACKUP	P1	CP-9 (1)	

CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	P1	CP-10 (2)	
CP-12	Safe Mode	P1	CP-12	Upgraded - control requires the information system to enter a safe mode of operation under certain conditions. It focuses on mission critical/human safety application, which is relevant to V2I components
IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	P1	IA-1	
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	P1	IA-2 (1) (2) (3) (8) (11) (12)	
IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION	P1	IA-3	
IA-4	IDENTIFIER MANAGEMENT	P1	IA-4	
IA-5	AUTHENTICATOR MANAGEMENT	P1	IA-5 (1) (2) (3) (11)	
IA-6	AUTHENTICATOR FEEDBACK	P2	IA-6	
IA-7	CRYPTOGRAPHIC MODULE AUTHENTICATION	P1	IA-7	
IA-8	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	P1	IA-8 (1) (2) (3) (4)	
IA-9	Service Identification and Authentication	P1	IA-9 (1) (2)	Upgraded - control requires components to transmit their identity and authentication information. Authentication is a core tenet of the connected vehicle environment, so this control is added for that purpose. The control will be modified to not require identity for mandated applications
IA-11	Re-Authentication	P2	IA-11	Upgraded - control requires devices to re-authenticate for certain events and/or periodically. This is a core concept of how credential management is to be handled
IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES	P1	IR-1	
IR-2	INCIDENT RESPONSE TRAINING	P2	IR-2	
IR-3	INCIDENT RESPONSE TESTING	P2	IR-3 (2)	
IR-4	INCIDENT HANDLING	P1	IR-4 (1)	

IR-5	INCIDENT MONITORING	P1	IR-5	
IR-6	INCIDENT REPORTING	P1	IR-6 (1)	
IR-7	INCIDENT RESPONSE ASSISTANCE	P2	IR-7 (1)	
IR-8	INCIDENT RESPONSE PLAN	P1	IR-8	
MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES	P1	MA-1	
MA-2	CONTROLLED MAINTENANCE	P2	MA-2	
MA-3	MAINTENANCE TOOLS	P3	MA-3 (1) (2)	
MA-4	NONLOCAL MAINTENANCE	P2	MA-4 (2)	
MA-5	MAINTENANCE PERSONNEL	P2	MA-5	
MA-6	TIMELY MAINTENANCE	P2	MA-6	
MP-1	MEDIA PROTECTION POLICY AND PROCEDURES	P1	MP-1	
MP-2	MEDIA ACCESS	P1	MP-2	
MP-3	MEDIA MARKING	P2	MP-3	Downgraded - control is concerned with distribution limitations; for systems with low confidentiality, we assume broadcast data can be read by anyone, making this control unnecessary
MP-4	MEDIA STORAGE	P1	MP-4	Downgraded - Physical control and storage, sanitization controls are not relevant to data with low confidentiality requirements
MP-5	MEDIA TRANSPORT	P1	MP-5 (4)	Downgraded - control addresses the mechanisms used to share data, putting requirements on the transport mechanism to protect confidentiality, this activity is not relevant
MP-6	MEDIA SANITIZATION	P1	MP-6	
MP-7	MEDIA USE	P1	MP-7 (1)	
PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	P1	PE-1	
PE-2	PHYSICAL ACCESS AUTHORIZATIONS	P1	PE-2	
PE-3	PHYSICAL ACCESS CONTROL	P1	PE-3	

PE-4	ACCESS CONTROL FOR TRANSMISSION MEDIUM	P1	PE-4	Downgraded - Access control to physical medium would normally be required to protect unencrypted data from modification; however all data over relevant channels are assumed to be digitally signed, protecting against modification, thus making this control unnecessary. (Medium Integrity will drive digital signatures)
PE-5	ACCESS CONTROL FOR OUTPUT DEVICES	P2	PE-5	Downgraded - Access control to physical output devices is not relevant to broadcast data with low confidentiality requirements
PE-6	MONITORING PHYSICAL ACCESS	P1	PE-6 (1)	
PE-8	VISITOR ACCESS RECORDS	P3	PE-8	
PE-9	POWER EQUIPMENT AND CABLING	P1	PE-9	
PE-10	EMERGENCY SHUTOFF	P1	PE-10	
PE-11	EMERGENCY POWER	P1	PE-11	
PE-12	EMERGENCY LIGHTING	P1	PE-12	
PE-13	FIRE PROTECTION	P1	PE-13 (3)	
PE-14	TEMPERATURE AND HUMIDITY CONTROLS	P1	PE-14	
PE-15	WATER DAMAGE PROTECTION	P1	PE-15	
PE-16	DELIVERY AND REMOVAL	P2	PE-16	
PE-17	ALTERNATE WORK SITE	P2	PE-17	
PL-1	SECURITY PLANNING POLICY AND PROCEDURES	P1	PL-1	
PL-2	SYSTEM SECURITY PLAN	P1	PL-2 (3)	
PL-4	RULES OF BEHAVIOR	P2	PL-4 (1)	
PL-8	INFORMATION SECURITY ARCHITECTURE	P1	PL-8	
PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES	P1	PS-1	
PS-2	POSITION RISK DESIGNATION	P1	PS-2	
PS-3	PERSONNEL SCREENING	P1	PS-3	
PS-4	PERSONNEL TERMINATION	P1	PS-4	
PS-5	PERSONNEL TRANSFER	P2	PS-5	
PS-6	ACCESS AGREEMENTS	P3	PS-6	
PS-7	THIRD-PARTY PERSONNEL	P1	PS-7	

	SECURITY			
PS-8	PERSONNEL SANCTIONS	P3	PS-8	
RA-1	RISK ASSESSMENT POLICY AND PROCEDURES	P1	RA-1	
RA-2	SECURITY CATEGORIZATION	P1	RA-2	
RA-3	RISK ASSESSMENT	P1	RA-3	
RA-5	VULNERABILITY SCANNING	P1	RA-5 (1) (2) (5)	
SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	P1	SA-1	
SA-2	ALLOCATION OF RESOURCES	P1	SA-2	
SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	P1	SA-3	
SA-4	ACQUISITION PROCESS	P1	SA-4 (1) (2) (9) (10)	
SA-5	INFORMATION SYSTEM DOCUMENTATION	P2	SA-5	
SA-8	SECURITY ENGINEERING PRINCIPLES	P1	SA-8	
SA-9	EXTERNAL INFORMATION SYSTEM SERVICES	P1	SA-9 (2)	
SA-10	DEVELOPER CONFIGURATION MANAGEMENT	P1	SA-10	
SA-11	DEVELOPER SECURITY TESTING AND EVALUATION	P1	SA-11	
SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	P1	SC-1	
SC-2	APPLICATION PARTITIONING	P1	SC-2	
SC-4	INFORMATION IN SHARED RESOURCES	P1	SC-4	Downgraded - Unauthorized information transfer, while undesirable is not a compromise of confidentiality low broadcast data, so this control would be excessive
SC-5	DENIAL OF SERVICE PROTECTION	P1	SC-5	
SC-7	BOUNDARY PROTECTION	P1	SC-7 (3) (4) (5) (7)	
SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	P1	SC-8 (1)	

SC-10	NETWORK DISCONNECT	P2	SC-10	
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	P1	SC-12	
SC-13	CRYPTOGRAPHIC PROTECTION	P1	SC-13	
SC-15	COLLABORATIVE COMPUTING DEVICES	P1	SC-15	
SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	P1	SC-17	
SC-18	MOBILE CODE	P2	SC-18	
SC-19	VOICE OVER INTERNET PROTOCOL	P1	SC-19	
SC-20	SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	P1	SC-20	
SC-21	SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	P1	SC-21	
SC-22	ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE	P1	SC-22	
SC-23	SESSION AUTHENTICITY	P1	SC-23	
SC-28	PROTECTION OF INFORMATION AT REST	P1	SC-28	
SC-38	Operations Security	P0	SC-38	Upgraded - control focuses on protecting information throughout the system development life cycle. This control is necessary as a function of defense-in-depth, to protect management and security-related algorithms, keys and update procedures
SC-39	PROCESS ISOLATION	P1	SC-39	
SC-41	Port and I/O Device Access	P0	SC-41	Upgraded - control requires physically disabling or removing connection ports on devices that do not explicitly need them as part of their functionality, to prevent exfiltration of management or security data (e.g., keys) or injection of malicious code

SC-42	Sensor Capability and Data	P0	SC-42 (1) (2)	Upgraded - control prevents the unauthorized activation of sensors controlled by the host device. Such activation could compromise the location of the device or other data that may compromise the privacy of the device's end user
SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	P1	SI-1	
SI-2	FLAW REMEDIATION	P1	SI-2 (2)	
SI-3	MALICIOUS CODE PROTECTION	P1	SI-3 (1) (2)	
SI-4	INFORMATION SYSTEM MONITORING	P1	SI-4 (2) (4) (5)	
SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	P1	SI-5	
SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	P1	SI-7 (1) (7)	
SI-8	SPAM PROTECTION	P2	SI-8 (1) (2)	
SI-10	INFORMATION INPUT VALIDATION	P1	SI-10	
SI-11	ERROR HANDLING	P2	SI-11	
SI-12	INFORMATION HANDLING AND RETENTION	P2	SI-12	
SI-16	MEMORY PROTECTION	P1	SI-16	
	Pseudonymity	P1		Added - control requires that a set of users not be able to match the real user to a message, and is required to protect the privacy of devices with an expectation thereof. This control applies to vehicular and personal devices only
	Reversible Pseudonymity	P1		Added - control requires that a set of users not be able to match the real user to a message that includes an alias, and is required to protect the privacy of devices with an expectation thereof, while enabling authorized operators to identify and act on misbehavior and malfunction issues. This control applies to vehicular and personal devices only

	Unlinkability	P1		Added - control requires that a device be able to repeatedly access a resource without others being able to link those uses together. This control is in conflict with operational constraints of connected vehicle environment, and as such will be implemented partially; that is, partial unlinkablilty, where unlinkability is not enforced over brief operational periods, but is enforced over longer periods. This control applies to vehicular and personal devices only

6.3. Moderate, High, Moderate (MHM) Device Class (RSE, ITS RE, TMC)

3. This section describes the MHM device classification which we currently have for the RSE, ITS RE, and TMC. Moderate confidentially indicates that flows could, but not necessarily, contain information such as personal identifiable information that the owner has a reasonable desire not be disclosed; sensitive business information that would allow someone to gain some advantage; personal financial information that could lead to personal financial loss. High Integrity indicates that false information could directly affect safety, mobility, and security, or cause severe financial damage. Moderate Availability indicates that in order to be useful the information flow must be available a significant amount of time. Wireless communications (e.g., DSRC) cannot be considered as having a higher Availability classification than moderate. Below are two examples that justify Moderate Confidentially and High Integrity:

    1) Example for Moderate Confidentially: If Speed Monitoring Information sent from the ITS RE to the TMC is compromised, vehicles may be identified with the speed they are traveling at, which has the possibility to identify which vehicles are going over the speed limit. However, it is important to note that this would be difficult to execute considering the number of databases needed to gather the appropriate information.

    2) Example for High Integrity: The over-the-air broadcast of traffic signal timing is tampered with, resulting in an over-the-air message of the current signal status which does not match the signal status being displayed on the lights at the intersection.

6.3.1. Classification

The initial analysis, which is presented in Appendix B, resulted in a MHM classification for the RSE, ITS RE, and TMC. This is consistent with the Threat Definition for V2I Architecture classification for the RSE. The Threat Definition team focuses on the PID, various OBEs, and RSE which is also the focus in the THEA CV Pilot. However, we have also classified ITS RE and the TMC as also falling under the MHM device class based on the application information flow analysis.

6.3.2. Selected Security Controls

This section contains a table of the security controls selected for this device class based on the NIST SP 800-53 moderate security control baseline with justifications if a control was downgraded or upgraded. The selected controls will continue to evolve and be further specified through the Threat Definition for V2I Architecture project.

Table 6-2. MHM Device Security Controls- High Baseline

No.	Control	Priority	Controls and Control Enhancements	Tailored Controls
AC-1	ACCESS CONTROL POLICY AND PROCEDURES	P1	AC-1	
AC-2	ACCOUNT MANAGEMENT	P1	AC-2 (1) (2) (3) (4) (5) (11) (12) (13)	
AC-3	ACCESS ENFORCEMENT	P1	AC-3	
AC-4	INFORMATION FLOW ENFORCEMENT	P1	AC-4	
AC-5	SEPARATION OF DUTIES	P1	AC-5	
AC-6	LEAST PRIVILEGE	P1	AC-6 (1) (2) (3) (5) (9) (10)	
AC-7	UNSUCCESSFUL LOGON ATTEMPTS	P2	AC-7	
AC-8	SYSTEM USE NOTIFICATION	P1	AC-8	
AC-10	CONCURRENT SESSION CONTROL	P3	AC-10	
AC-11	SESSION LOCK	P3	AC-11 (1)	
AC-12	SESSION TERMINATION	P2	AC-12	
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	P3	AC-14	
AC-17	REMOTE ACCESS	P1	AC-17 (1) (2) (3) (4)	
AC-18	WIRELESS ACCESS	P1	AC-18 (1) (4) (5)	
AC-19	ACCESS CONTROL FOR MOBILE DEVICES	P1	AC-19 (5)	
AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	P1	AC-20 (1) (2)	
AC-21	INFORMATION SHARING	P2	AC-21	
AC-22	PUBLICLY ACCESSIBLE CONTENT	P3	AC-22	
AT-1	SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES	P1	AT-1	

AT-2	SECURITY AWARENESS TRAINING	P1	AT-2 (2)	
AT-3	ROLE-BASED SECURITY TRAINING	P1	AT-3	
AT-4	SECURITY TRAINING RECORDS	P3	AT-4	
AU-1	AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES	P1	AU-1	
AU-2	AUDIT EVENTS	P1	AU-2 (3)	
AU-3	CONTENT OF AUDIT RECORDS	P1	AU-3 (1) (2)	
AU-4	AUDIT STORAGE CAPACITY	P1	AU-4	
AU-5	RESPONSE TO AUDIT PROCESSING FAILURES	P1	AU-5 (1) (2)	
AU-6	AUDIT REVIEW, ANALYSIS, AND REPORTING	P1	AU-6 (1) (3) (5) (6)	
AU-7	AUDIT REDUCTION AND REPORT GENERATION	P2	AU-7 (1)	
AU-8	TIME STAMPS	P1	AU-8 (1)	
AU-9	PROTECTION OF AUDIT INFORMATION	P1	AU-9 (2) (3) (4)	
AU-10	NON-REPUDIATION	P2	AU-10	
AU-11	AUDIT RECORD RETENTION	P3	AU-11	
AU-12	AUDIT GENERATION	P1	AU-12 (1) (3)	
CA-1	SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES	P1	CA-1	
CA-2	SECURITY ASSESSMENTS	P2	CA-2 (1) (2)	
CA-3	SYSTEM INTERCONNECTIONS	P1	CA-3 (5)	
CA-5	PLAN OF ACTION AND MILESTONES	P3	CA-5	
CA-6	SECURITY AUTHORIZATION	P2	CA-6	
CA-7	CONTINUOUS MONITORING	P2	CA-7 (1)	
CA-8	PENETRATION TESTING	P2	CA-8	
CA-9	INTERNAL SYSTEM CONNECTIONS	P2	CA-9	
CM-1	CONFIGURATION MANAGEMENT POLICY	P1	CM-1	

	AND PROCEDURES			
CM-2	BASELINE CONFIGURATION	P1	CM-2 (1) (2) (3) (7)	
CM-3	CONFIGURATION CHANGE CONTROL	P1	CM-3 (1) (2)	
CM-4	SECURITY IMPACT ANALYSIS	P2	CM-4 (1)	
CM-5	ACCESS RESTRICTIONS FOR CHANGE	P1	CM-5 (1) (2) (3)	
CM-6	CONFIGURATION SETTINGS	P1	CM-6 (1) (2)	
CM-7	LEAST FUNCTIONALITY	P1	CM-7 (1) (2) (5)	
CM-8	INFORMATION SYSTEM COMPONENT INVENTORY	P1	CM-8 (1) (2) (3) (4) (5)	
CM-9	CONFIGURATION MANAGEMENT PLAN	P1	CM-9	
CM-10	SOFTWARE USAGE RESTRICTIONS	P2	CM-10	
CM-11	USER-INSTALLED SOFTWARE	P1	CM-11	
CP-1	CONTINGENCY PLANNING POLICY AND PROCEDURES	P1	CP-1	
CP-2	CONTINGENCY PLAN	P1	CP-2 (1) (2) (3) (4) (5) (8)	(2)(4)(5) Downgraded - Planning for disaster and cyberattacks is focused on the availability goals, and is not required to achieve medium availability
CP-3	CONTINGENCY TRAINING	P2	CP-3 (1)	(1) Downgraded - Simulated events as part of personnel training is focused on the availability of goals, and is not required to achieve medium availability
CP-4	CONTINGENCY PLAN TESTING	P2	CP-4 (1) (2)	(1) (2) Downgraded - Testing of contingency is focused on availability of goals, supplementary activity is not required to achieve medium availability
CP-6	ALTERNATE STORAGE SITE	P1	CP-6 (1) (2) (3)	Downgraded - Alternate Storage site planning is focused on maintaining high availability in the case of system disruption, is not necessary to achieve medium availability

CP-7	ALTERNATE PROCESSING SITE	P1	CP-7 (1) (2) (3) (4)	Downgraded - Alternate Processing site planning is focused on maintaining high availability in the case of system disruption, is not necessary to achieve medium availability
CP-8	TELECOMMUNICATIONS SERVICES	P1	CP-8 (1) (2) (3) (4)	Downgraded - Provision of alternate telecommunications mechanisms is focused on maintaining high availability in the case of system disruption, is not necessary to achieve medium availability
CP-9	INFORMATION SYSTEM BACKUP	P1	CP-9 (1) (2) (3) (5)	(5) Downgraded - Transfer of information system backups to an alternate storage site (separate from the backup site, which is itself separate from the operational site) may be necessary for high availability systems but is not for medium availability, and thus is not required
CP-10	INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	P1	CP-10 (2) (4)	
CP-12	Safe Mode	P1	CP-12	Upgraded CP-12 - control requires the information system to enter a safe mode of operation under certain conditions. It focuses on mission critical / human safety applications which is relevant to V2I components
IA-1	IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES	P1	IA-1	
IA-2	IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	P1	IA-2 (1) (2) (3) (4) (8) (9) (11) (12)	
IA-3	DEVICE IDENTIFICATION AND AUTHENTICATION	P1	IA-3	
IA-4	IDENTIFIER MANAGEMENT	P1	IA-4	
IA-5	AUTHENTICATOR MANAGEMENT	P1	IA-5 (1) (2) (3) (11)	
IA-6	AUTHENTICATOR FEEDBACK	P2	IA-6	
IA-7	CRYPTOGRAPHIC MODULE	P1	IA-7	

	AUTHENTICATION			
IA-8	IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	P1	IA-8 (1) (2) (3) (4)	
IA-9	Service Identification and Authentication	P1	IA-9 (1) (2)	Upgraded- control requires components to transmit their identity and authentication information. Authentication is a core tenet of the connected vehicle environment, so this control is added for that purpose. The control will be modified to not require identity for mandated applications
IA-11	Re-Authentication	P2	IA-11	Upgraded- control requires devices to re-authenticate for certain events and/or periodically. This is a core concept of how credential management is to be handled
IR-1	INCIDENT RESPONSE POLICY AND PROCEDURES	P1	IR-1	
IR-2	INCIDENT RESPONSE TRAINING	P2	IR-2 (1) (2)	
IR-3	INCIDENT RESPONSE TESTING	P2	IR-3 (2)	
IR-4	INCIDENT HANDLING	P1	IR-4 (1) (4)	
IR-5	INCIDENT MONITORING	P1	IR-5 (1)	
IR-6	INCIDENT REPORTING	P1	IR-6 (1)	
IR-7	INCIDENT RESPONSE ASSISTANCE	P2	IR-7 (1)	
IR-8	INCIDENT RESPONSE PLAN	P1	IR-8	
MA-1	SYSTEM MAINTENANCE POLICY AND PROCEDURES	P1	MA-1	
MA-2	CONTROLLED MAINTENANCE	P2	MA-2 (2)	
MA-3	MAINTENANCE TOOLS	P3	MA-3 (1) (2) (3)	
MA-4	NONLOCAL MAINTENANCE	P2	MA-4 (2) (3)	
MA-5	MAINTENANCE PERSONNEL	P2	MA-5 (1)	
MA-6	TIMELY MAINTENANCE	P2	MA-6	
MP-1	MEDIA PROTECTION POLICY AND PROCEDURES	P1	MP-1	

MP-2	MEDIA ACCESS	P1	MP-2	
MP-3	MEDIA MARKING	P2	MP-3	
MP-4	MEDIA STORAGE	P1	MP-4	
MP-5	MEDIA TRANSPORT	P1	MP-5 (4)	
MP-6	MEDIA SANITIZATION	P1	MP-6 (1) (2) (3)	(1) (2) Downgraded - Documenting, tracking sanitization, disposal and testing actions are unlikely to affect the integrity of information flows, and are not necessary to ensure medium confidentiality
MP-7	MEDIA USE	P1	MP-7 (1)	
PE-1	PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES	P1	PE-1	
PE-2	PHYSICAL ACCESS AUTHORIZATIONS	P1	PE-2	
PE-3	PHYSICAL ACCESS CONTROL	P1	PE-3 (1)	
PE-4	ACCESS CONTROL FOR TRANSMISSION MEDIUM	P1	PE-4	
PE-5	ACCESS CONTROL FOR OUTPUT DEVICES	P2	PE-5	
PE-6	MONITORING PHYSICAL ACCESS	P1	PE-6 (1) (4)	
PE-8	VISITOR ACCESS RECORDS	P3	PE-8 (1)	
PE-9	POWER EQUIPMENT AND CABLING	P1	PE-9	
PE-10	EMERGENCY SHUTOFF	P1	PE-10	
PE-11	EMERGENCY POWER	P1	PE-11 (1)	
PE-12	EMERGENCY LIGHTING	P1	PE-12	
PE-13	FIRE PROTECTION	P1	PE-13 (1) (2) (3)	
PE-14	TEMPERATURE AND HUMIDITY CONTROLS	P1	PE-14	
PE-15	WATER DAMAGE PROTECTION	P1	PE-15 (1)	
PE-16	DELIVERY AND REMOVAL	P2	PE-16	
PE-17	ALTERNATE WORK SITE	P2	PE-17	
PE-18	LOCATION OF INFORMATION SYSTEM COMPONENTS	P3	PE-18	
PL-1	SECURITY PLANNING POLICY AND PROCEDURES	P1	PL-1	
PL-2	SYSTEM SECURITY PLAN	P1	PL-2 (3)	

PL-4	RULES OF BEHAVIOR	P2	PL-4 (1)	
PL-8	INFORMATION SECURITY ARCHITECTURE	P1	PL-8	
PS-1	PERSONNEL SECURITY POLICY AND PROCEDURES	P1	PS-1	
PS-2	POSITION RISK DESIGNATION	P1	PS-2	
PS-3	PERSONNEL SCREENING	P1	PS-3	
PS-4	PERSONNEL TERMINATION	P1	PS-4 (2)	
PS-5	PERSONNEL TRANSFER	P2	PS-5	
PS-6	ACCESS AGREEMENTS	P3	PS-6	
PS-7	THIRD-PARTY PERSONNEL SECURITY	P1	PS-7	
PS-8	PERSONNEL SANCTIONS	P3	PS-8	
RA-1	RISK ASSESSMENT POLICY AND PROCEDURES	P1	RA-1	
RA-2	SECURITY CATEGORIZATION	P1	RA-2	
RA-3	RISK ASSESSMENT	P1	RA-3	
RA-5	VULNERABILITY SCANNING	P1	RA-5 (1) (2) (4) (5)	
RA-6	TECHNICAL SURVEILLANCE COUNTERMEASURES SURVEY	P2	RA-6	Upgraded - control requires penetration testing of devices, and provide input into risk assessments. Given the widespread deployment possibilities of V2I devices, and the attractiveness of these devices as targets, including this control will enable an at least a cognizance of potential vulnerabilities. It will not be inexpensive, however, which is why this control is applied only to those classes of devices with a 'High' in one or more categories
SA-1	SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES	P1	SA-1	
SA-2	ALLOCATION OF RESOURCES	P1	SA-2	
SA-3	SYSTEM DEVELOPMENT LIFE CYCLE	P1	SA-3	
SA-4	ACQUISITION PROCESS	P1	SA-4 (1) (2) (9) (10)	

SA-5	INFORMATION SYSTEM DOCUMENTATION	P2	SA-5	
SA-8	SECURITY ENGINEERING PRINCIPLES	P1	SA-8	
SA-9	EXTERNAL INFORMATION SYSTEM SERVICES	P1	SA-9 (2)	
SA-10	DEVELOPER CONFIGURATION MANAGEMENT	P1	SA-10	
SA-11	DEVELOPER SECURITY TESTING AND EVALUATION	P1	SA-11	
SA-12	SUPPLY CHAIN PROTECTION	P1	SA-12	
SA-15	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS	P2	SA-15	
SA-16	DEVELOPER-PROVIDED TRAINING	P2	SA-16	
SA-17	DEVELOPER SECURITY ARCHITECTURE AND DESIGN	P1	SA-17	
SA-18	Tamper Resistance and Detection	P2	SA-18 (1) (2)	Upgraded- control requires tamper resistance technology to be installed on devices, and for the organizations managing the device to periodically or on-event verify that the device has not been tampered with. The control's applicability includes all phases of the system life cycle; this is appropriate to maintaining confidence in the integrity of transmitted data, as compromised devices are more susceptible to modification which may affect the integrity of the data they provide
SA-19	Component Authenticity	P1	SA-19 (2) (3)	Upgraded- control deals with the configuration control of devices, and the handling of end-of-life devices. Improperly assigned or re-used devices (for instance, those bypassing a certification procedure) compromise the integrity of the data in V2I scenarios
SC-1	SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES	P1	SC-1	

SC-2	APPLICATION PARTITIONING	P1	SC-2	
SC-3	SECURITY FUNCTION ISOLATION	P1	SC-3	
SC-4	INFORMATION IN SHARED RESOURCES	P1	SC-4	
SC-5	DENIAL OF SERVICE PROTECTION	P1	SC-5	
SC-7	BOUNDARY PROTECTION	P1	SC-7 (3) (4) (5) (7) (8) (18) (21)	
SC-8	TRANSMISSION CONFIDENTIALITY AND INTEGRITY	P1	SC-8 (1)	
SC-10	NETWORK DISCONNECT	P2	SC-10	
SC-12	CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	P1	SC-12 (1)	
SC-13	CRYPTOGRAPHIC PROTECTION	P1	SC-13	
SC-15	COLLABORATIVE COMPUTING DEVICES	P1	SC-15	
SC-17	PUBLIC KEY INFRASTRUCTURE CERTIFICATES	P1	SC-17	
SC-18	MOBILE CODE	P2	SC-18	
SC-19	VOICE OVER INTERNET PROTOCOL	P1	SC-19	
SC-20	SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)	P1	SC-20	
SC-21	SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER)	P1	SC-21	
SC-22	ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE	P1	SC-22	
SC-23	SESSION AUTHENTICITY	P1	SC-23	
SC-24	FAIL IN KNOWN STATE	P1	SC-24	
SC-28	PROTECTION OF INFORMATION AT REST	P1	SC-28	

SC-38	Operations Security	P0	SC-38	Upgraded - control focuses on protecting information throughout the system development life cycle. This control is necessary as a function of defense-in-depth, to protect management and security-related algorithms, keys and update procedures
SC-39	PROCESS ISOLATION	P1	SC-39	
SC-41	Port and I/O Device Access	P0	SC-41	Upgraded - control requires physically disabling or removing connection ports on devices that do not explicitly need them as part of their functionality, to prevent exfiltration of management or security data (e.g., keys) or injection of malicious code
SC-42	Sensor Capability and Data	P0	SC-42 (1) (2)	Upgraded - control prevents the unauthorized activation of sensors controlled by the host device. Such activation could compromise the location of the device or other data that may compromise the privacy of the device's end user
SI-1	SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES	P1	SI-1	
SI-2	FLAW REMEDIATION	P1	SI-2 (1) (2)	
SI-3	MALICIOUS CODE PROTECTION	P1	SI-3 (1) (2)	
SI-4	INFORMATION SYSTEM MONITORING	P1	SI-4 (2) (4) (5)	
SI-5	SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	P1	SI-5 (1)	
SI-6	SECURITY FUNCTION VERIFICATION	P1	SI-6	
SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	P1	SI-7 (1) (2) (5) (7) (14)	
SI-8	SPAM PROTECTION	P2	SI-8 (1) (2)	
SI-10	INFORMATION INPUT VALIDATION	P1	SI-10	
SI-11	ERROR HANDLING	P2	SI-11	
SI-12	INFORMATION HANDLING AND RETENTION	P2	SI-12	

SI-16	MEMORY PROTECTION	P1	SI-16	
SI-17	Fail-Safe Procedures	P3	SI-17	Upgraded - control requires devices to react to failures in a predictable fashion designed to enable recovery without jeopardizing the operator. This may include operator notification. This control protects the integrity of the data in the environment by increasing awareness of failures suggesting an increase in repair rate

7. Minimum Security Requirements per Device Classification

This section will list 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 will not be 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 (OBE, VAD, PID, ASD)

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 POC
- LMM devices shall support requirements identified in the SCMS POC 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

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 POC 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 not support remote access. However, devices shall support physical access in the event that re-bootstrapping is required. The device shall support role-based authentication to enable physical access
- LMM devices shall support the ability to reset default user names and passwords

7.2. MHM Device Minimum Security Requirements (RSE, ITS RE, TMC)

Note: The USDOT FHWA DSRC Roadside Unit (RSU) Specifications Document, Version 4.0 April 15, 2014, includes basic security requirements for RSEs. All of the existing requirements should be followed as stated, except the requirement on FIPS 140-2 level. The RSE shall be equivalent with FIPS 140-2 Level 3, not Level 2 as stated within the specifications document.

7.2.1. Communications

- MHM devices shall comply with IEEE 1609.2 (2016): Standard for WAVE – Security Services for Applications and Management Messages
    - MHM 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 POC
- MHM devices shall meet the WSA security profile covered in IEEE 1609.3 (2016)
- MHM devices shall meet the SPaT, MAP, and TIM security profiles covered in the COC System Functional and Performance Specification Ver. 0.4.0
- MHM devices shall support requirements identified in the SCMS POC Implementation EE Requirements and Specifications Supporting SCMS Software Release 1.0 Appendix A and B to complete processes and use cases
    - The RSE maintains a log of security management related connections. This log is anonymized so all identifying information is removed from it. The log is provided periodically to the TMC

7.2.2. Hardware

- MHM devices shall be equivalent with FIPS 140-2 Level 3 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
- MHM devices shall have sufficient resources to store and process the number of certificates and CRLs stated as necessary within the SCMS POC Implementation EE Requirements and Specifications Supporting SCMS Software Release 1.0

7.2.3. Software and Operating System

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

7.2.4. Access

- MHM devices shall support remote access. The device shall support identity-based authentication to enable remote access
- MHM 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. 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 comprehensive list of threats independent of the V2X applications in use.

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, with the exception of 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.

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

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.	OBE, RSE, PID, VAD, ASD, 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 RSEs, PIDs, 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.	OBE, RSE, PID, VAD, ASD, 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.	OBE, RSE, PID, VAD, ASD	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.	OBE, RSE, PID	Low	The system protocols (e.g., IEEE 1609.2, SCMS POC 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	OBE, PID, VAD,	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.	ASD, RSE		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).	OBE, PID, VAD, ASD, RSE	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).	OBE, PID, VAD, ASD, RSE	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	OBE, PID, VAD,	High if scalable,	The ability of the system to mitigate the damage caused by compromised devices is reduced. Mitigated through

	associated parameters) manipulates the content of the BSM to evade detection.	ASD	moderate otherwise	misbehavior reporting. System protocols (e.g., IEEE 1609.2, SCMS POC 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.	OBE, PID, VAD, ASD	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 POC 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.	OBE, PID, VAD, ASD	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.	OBE, PID, VAD, ASD	Moderate	Significant damage to device's privacy. Mitigated by using change patterns and strategies as specified in the SCMS POC design.
T.Track.2	An attacker uses BSM data to track a vehicle/device.	OBE, PID, VAD, ASD	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 POC 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.	OBE, PID, VAD, ASD, RSE	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.	OBE, RSE, PID, VAD, ASD	High	If the OBE is connected to the CAN bus, and an attacker is able to compromise the OBE 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.	OBE, RSE, PID, VAD, ASD	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.	OBE, RSE, PID, VAD, ASD	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. Application Information Flow and Device Classification Analysis

This section describes how the THEA CV Pilot team analyzed the information flows for each application being deployed in the THEA pilot, based on the information flows, sources, destinations, definitions, etc. specified for each application per CVRIA. The FIPS 199 analysis is provided for each application. Device classifications with analysis and justifications are also provided. Selected security controls and minimum requirements within Chapters 6 and 7 respectively, are based on the final device classifications.

Application Information Flow Analysis

Application information flows were defined based off of the CIA criteria in FIPS 199. The table below summarizes the potential impacts (LOW, MODERATE, and HIGH) for each security objective- Confidentiality, Integrity, and Availability.

Table B-1. Potential Impact Definitions for Security Objectives

POTENTIAL IMPACT			
Security Objective	**LOW**	**MODERATE**	**HIGH**
***Confidentiality* -Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]**	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Integrity **-Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]**	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability **-Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]**	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations,

Further information flow analysis was conducted using the Threat Definition for V2I Architecture project, which has tailored the CIA security objectives to connected vehicles. Below summarizes the potential impacts defined by the Threat Definition for V2I Architecture project.

Table B-2. Potential Impact Definitions for Security Objectives for V2I Architecture

V2I THREAT ASSESSMENT DEFINITIONS -POTENTIAL IMPACT			
Security Objective	LOW	MODERATE	HIGH
Confidentiality**- Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]**	Flows which are intended to be received by any nearby device. These flows can typically be broadcast	Flows that contain information such as: –personal identifiable information –sensitive business information –personal financial information	Flows that contain information which if revealed would cause a substantial risk to operations, or personal life and limb
Integrity**- Guarding against improper information modification or destruction, and includes ensuring information non-**	if the receiver does not directly make use of the message, if the message contents are aggregated with many other messages such that the resulting information need	If a false message can increase physical risk without directly causing physical harm. A message contains information that cannot be obtained or verified by other	If a false message could directly affect safety, mobility, and security, or cause severe financial damage.

repudiation and authenticity. [44 U.S.C., SEC. 3542]	only be true "on average", or if the information in the message can be trivially confirmed by use of information from other sources with higher integrity.	means: for example, with intersection status, a receiver can gain assurance about the current signal state by observing traffic behavior, but only the intersection status message gives information about future signal state	
***Availability*-Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]**	If the system can operate successfully if some receivers receive no messages and most receivers receive some messages, and if there is no requirement that a receiver has availability status information. LOW also requires that the information is not acted upon immediately, and not used for real time decision making	If the receiver can operate successfully if all receivers receive some messages and most receivers receive most messages, and if availability status information is necessary for the safe operation of the application.	Where failure to receive a message could have an adverse effect on safety, or severe damage relative to the baseline of no deployment of the application. –NOTE: Many information flows in the CVRIA occur over a wireless medium where availability cannot be guaranteed; these information flows by definition cannot meet HIGH availability requirements, and so any application for which the availability requirements are HIGH must provide a different medium to support those information flows.

V2I Mobility

V2I mobility applications communicate operational data between vehicles and infrastructure, intended primarily to increase mobility and enable additional safety, mobility, and environmental benefits. Applications may use real-time data to increase safety and operational efficiency while minimizing the impact on the environment, and enabling travelers to make better-informed travel decisions. The THEA CV Pilot will deploy the following V2I Mobility applications:

- Intelligent Traffic Signal System (I-SIG)
- Pedestrian Mobility
- Transit Signal Priority (TSP)

Intelligent Traffic Signal System (I-SIG)

The Intelligent Traffic Signal System (I-SIG) application uses both vehicle location and movement information from connected vehicles as well as infrastructure measurement of non-equipped vehicles to improve the operations of traffic signal control systems. The application utilizes the vehicle information to adjust signal timing for an intersection or group of intersections in order to improve traffic flow, including allowing platoon flow through the intersection. The application serves as an over-arching system optimization application, accommodating other mobility applications such as Transit Signal Priority, Freight Signal Priority, Emergency Vehicle Preemption, and Pedestrian Mobility to maximize overall arterial network performance. In addition, the application may consider additional inputs such as environmental situation information or the interface (i.e., traffic flow) between arterial signals and ramp meters. This application will be incorporated into all THEA CV Pilot six use cases.

Table B-3. I-SIG Information Flow Analysis

Source	Destination	Information type	Controlling Condition		
ITS RE	Other ITS RE	Signal Control Data	C	low	encrypted, authenticated, proprietary; however will not cause harm if seen, traffic light information is visible
			I	high	proprietary info that should not be tampered used to configure local traffic signal controllers
			A	moderate	information should be immediately available to configure signal controllers, but it should be able to use a default configuration if necessary
ITS RE	RSE	Intersection Control Status	C	low	not encrypted and no harm should come from seeing this data
			I	high	info needs to be accurate and should not be tampered so the RSE has correct phase info, priority status, etc.; if compromised, could lead to sending inconsistent messages which would greatly increase the possibility of collisions
			A	moderate	should be immediately available so the RSE has correct phase info, priority status, etc.; however, the RSE could choose not to send out of date information
ITS RE	RSE	Conflict Monitor Status	C	low	info is not confidential or encrypted
			I	high	if compromised, the ITS RE may not be able to support failsafe operating mode in the event of a conflict between the ITS RE and RSE
			A	moderate	want this info to be available immediately but want to support wireless communication flows; the driver should also be able to see the traffic signal phases if there is a slight delay
ITS RE	TMC	Environmental Sensor Data	C	low	encrypted; but no impact if someone sees the data
			I	moderate	info should be correct to determine safe speeds, etc.
			A	moderate	want updates but slightly outdated information will not be catastrophic
ITS RE	TMC	Traffic Flow	C	low	encrypted; but no impact if someone sees the data
			I	low	only limited adverse effect if raw/processed traffic detector data is bad/compromised

			A	low	only limited adverse effect of info is not timely/readily available
ITS RE	TMC	Signal Control Status	C	low	encrypted and authenticated but no harm should come from seeing this data
			I	moderate	info needs to be accurate and should not be tampered to enable effective monitoring and control by the TMC; should be as accurate as the right of way request
			A	moderate	needs available to enable effective monitoring and control by the TMC; however if not immediately available, the app should still function
Other ITS RE	ITS RE	Signal Control Data	C	low	encrypted, authenticated, proprietary; however will not cause harm if seen, traffic light information is visible
			I	high	proprietary info that should not be tampered used to configure local traffic signal controllers
			A	moderate	information should be immediately available to configure signal controllers, but it should be able to use a default configuration if necessary
RSE	ITS RE	Signal Service Request	C	low	info is not confidential or encrypted
			I	moderate	requests should be accurate and not tampered with, otherwise incorrect or malicious requests could be granted which could lead to delays
			A	low	requests should be timely and available immediately but availability cannot be guaranteed over a wireless medium; also worst case scenario is the vehicle or pedestrian has to wait for the appropriate signal
RSE	ITS RE	Traffic Situation Data	C	low	encrypted; but no impact if someone sees the data
			I	low	only limited adverse effect if raw/processed connected vehicle data is bad/compromised
			A	low	only limited adverse effect of info is not timely/readily available
RSE	TMC	Traffic Situation Data	C	low	encrypted; but no impact if someone sees the data
			I	low	only limited adverse effect if raw/processed connected vehicle data is bad/compromised
			A	low	only limited adverse effect of info is not timely/readily available
RSE	ITS RE	Environmental Situation Data	C	low	no impact if someone sees the data
			I	low	only limited adverse effect if environmental data from vehicle safety and convenience systems is bad/compromised; can cope with some bad data
			A	low	only limited adverse effect of info is not timely/readily available
RSE	TMC	Environmental Situation Data	C	low	no impact if someone sees the data
			I	low	only limited adverse effect if environmental data from vehicle safety and convenience systems is bad/compromised; can cope with some bad data
			A	moderate	only limited adverse effect of info is not timely/readily available

RSE	ITS RE	Intersection Status Monitoring	C	low	not encrypted and no harm should come from seeing this data
			I	high	info needs to be accurate and should not be tampered so the ITS RE has correct SPaT info for all lanes to be able to detect conflicts and support failsafe operating mode
			A	moderate	should be immediately available so the ITS RE has correct SPaT info; but should be able to support wireless communication and a slight delay
RSE	Vehicle OBE	Vehicle Situation Data Parameters	C	low	not encrypted and no harm should come from seeing this data
			I	moderate	info should be accurate and should not be tampered so that the vehicle only discloses the correctly requested data
			A	moderate	parameters should be timely and readily available, but would not have severe/catastrophic consequences if not
RSE	Vehicle OBE	Intersection Status	C	low	not encrypted and no harm should come from seeing this data
			I	moderate	info needs to be accurate and should not be tampered so the vehicle OBE has correct SPaT info for all lanes; however the driver can still see the traffic signals
			A	moderate	needs to be available so the vehicle OBE has correct SPaT info; identifies signal priority and preemption status and pedestrian crossing status information, etc. However availability cannot be guaranteed over a wireless medium
RSE	TMC	Intersection Management Application Status	C	low	not encrypted; no impact if someone sees the data
			I	moderate	should be able to cope with some bad information on the status and record of alerts/warnings; aggregate info; however could cause appearance of excessive traffic violations or unnecessary maintenance caused if data is compromised (operational state, status, log); should not affect the application functionality
			A	low	0nly limited adverse effect of info is not timely/readily available
TMC	ITS RE	Signal System Configuration	C	low	encrypted, authenticated, proprietary; however, the result is directly observable from traffic lights
			I	high	proprietary info that should not be tampered with; data used to configure traffic signal systems; could cause significant delays and traffic issues if compromised
			A	moderate	should be readily available; configurations can be time
TMC	ITS RE	Signal Control Commands	C	low	encrypted, authenticated, proprietary; but the result is directly observable
			I	high	proprietary info that should not be tampered with, could enable outside control of traffic signals
			A	moderate	should be to be able to issue immediate commands but the ITS RE should be able to continue to function using the default configuration
TMC	ITS RE	Signal Control	C	low	encrypted, authenticated, proprietary; but the result is directly observable from traffic lights

		Plans	I	high	proprietary info that should not be tampered with; tampering with these plans could cause delays along with major safety issues
			A	moderate	should be timely and readily available; coordinated with other systems; however, should be able to function using a default configuration
TMC	ITS RE	Signal Control Device Configuration	C	low	encrypted, authenticated, proprietary; but the result is directly observable from traffic lights
			I	high	proprietary info that should not be tampered with; includes local controllers and system masters; tampering with configurations could cause delays along with major safety issues
			A	moderate	should be timely and readily available; however, should be able to function using a default configuration
TMC	ITS RE	Traffic Sensor Control	C	low	encrypted, authenticated, proprietary; but should not cause severe damage if seen
			I	moderate	should be accurate and not be tampered with; could enable outside control of traffic sensors but should not cause severe harm, but could cause issues with traffic sensor data received and be detrimental to operations
			A	low	want updates but delayed information will not be severe; should be able to operate from a previous/default control/config
TMC	ITS RE	Environmental Sensors Control	C	low	encrypted, authenticated, proprietary; but should not cause severe damage if seen
			I	moderate	should be accurate and not be tampered with; could enable outside control of traffic sensors but should not cause severe harm, but could cause issues with environmental sensor data received and be detrimental to operations
			A	low	want updates but delayed information will not be severe; should be able to operate from a previous/default control/config
TMC	RSE	Intersection Management Application Info	C	moderate	proprietary configuration data with warning parameters and thresholds
			I	high	should be accurate and not be tampered with; could enable outside control of application
			A	low	should be timely and readily available or may not be able to restart/reset; however, should be able to operate on a default configuration and/or stop sending messages
TMC	Other TMC	Road Network Conditions	C	low	encrypted; but no harm should come from seeing this data
			I	moderate	info needs to be accurate and should not be tampered but should be able to cope with some bad data; should be able to confirm conditions by other mechanisms
			A	moderate	condition info should be timely and readily available so that TMCs are aware of current traffic info, conditions, restrictions, etc. but should not have severe/catastrophic consequences if not
TMC	Other TMC	Device Status	C	low	encrypted; but no harm should come from seeing this data
			I	moderate	info needs to be accurate and should not be tampered but should be able to cope with

					some bad data; could delay maintenance actions or waste resources checking devices that are actually in good status
			A	low	status info should be timely and readily available, but should not have very limited consequences if not
TMC	Other TMC	Device Data	C	low	encrypted; but no harm should come from seeing this data
			I	moderate	info needs to be accurate and should not be tampered but should be able to cope with some bad data; includes inventory data which could lead to loss of assets if compromised
			A	low	data should be timely and readily available, but should not have limited consequences if not
Vehicle Databus	Vehicle OBE	Host Vehicle Status	C	low	sensor data is not confidential
			I	high	sensor data needs to be accurate and should not be tampered with
			A	high	sensor data must be consistently available to feed BSMs broadcast at 10Hz
Vehicle Databus	Vehicle OBE	Driver Input Information	C	low	Control commands and requests are not confidential. Most information will eventually be included in a broadcast message
			I	high	Control commands and requests need to be accurate and should not be tampered with
			A	high	Control commands and requests must be consistently available to feed messages
Vehicle OBE	Vehicle Databus	Driver Update Information	C	low	info provided to the DVI is not confidential
			I	high	information that provides warnings, etc. must be accurate and cannot be tampered with
			A	high	information that provides warnings, etc. must be immediately available for the driver to react
Vehicle OBE	RSE	Vehicle Situation Data	C	low	but could be moderate if this contains PII related information
			I	low	data should be accurate and not tampered with but should be able to cope with some bad data in traffic/environmental condition monitoring; aggregate data
			A	low	data should be timely and readily available, but limited adverse effect; aggregate data
Vehicle OBE	RSE	Vehicle Location & Motion for Surveillance	C	low	BSM information is not confidential
			I	high	BSM info needs to be accurate and should not be tampered with
			A	moderate	BSM must be broadcast regularly to make data available for the RSE, but availability cannot be guaranteed over a wireless medium
Vehicle OBE	RSE	Vehicle Environmental Data	C	low	but could be moderate if this contains PII related information
			I	low	data should be accurate and not tampered with but should be able to cope with some bad data in traffic/environmental condition monitoring; aggregate data; can also receive data from ITS RE
			A	low	data should be timely and readily available, but limited adverse effect; aggregate data; can

					also receive data from ITS RE

Pedestrian Mobility

This Pedestrian Mobility application will integrate traffic and pedestrian information from roadside or intersection detectors and new forms of data from wirelessly connected, pedestrian (or bicyclist) carried mobile devices (nomadic devices) to request dynamic pedestrian signals or to inform pedestrians when to cross and how to remain aligned with the crosswalk based on real-time Signal Phase and Timing (SPaT) and MAP information. In some cases, priority will be given to pedestrians, such as persons with disabilities who need additional crossing time, or in special conditions (e.g., weather) where pedestrians may warrant priority or additional crossing time. This application will enable a "pedestrian call" to be routed to the traffic controller from a nomadic device of a registered person with disabilities after confirming the direction and orientation of the roadway that this pedestrian is intending to cross. The application also provides warnings to the personal information device user of possible infringement of the crossing by approaching vehicles. This application will be used by Twiggs Street use case near the courthouse and will alert drivers and pedestrians of each other in order to reduce the potential of a pedestrian getting struck by a vehicle.

Table B-4. Pedestrian Mobility Information Flow Analysis

Source	Destination	Information type	Controlling Condition		
ITS RE	RSE	Intersection Control Status	C	low	not encrypted and no harm should come from seeing this data
			I	high	info needs to be accurate and should not be tampered so the RSE has correct phase info, priority status, etc.; if compromised, could lead to sending inconsistent messages which would greatly increase the possibility of collisions
			A	moderate	should be immediately available so the RSE has correct phase info, priority status, etc.; however, the RSE could choose not to send out of date information
ITS RE	RSE	Pedestrian Crossing Status	C	low	not encrypted and no harm should come from seeing this data
			I	high	info needs to be accurate and should not be tampered so the RSE has correct crossing status, etc.
			A	moderate	should be immediately available so the RSE has correct crossing status, etc. and can send that status to the PID; however, worst case is the RSE does not send out the information and the pedestrian waits to cross; also enables wireless communication
ITS RE	TMC	Right-of-Way Request Notification	C	low	encrypted and authenticated but no harm should come from seeing this data
			I	moderate	invalid messages could lead to an unauthorized user gaining priority which could delay traffic etc.

			A	low	not necessary for the app to work; can cope with not having immediately available data
ITS RE	TMC	Signal Control Status	C	low	encrypted and authenticated but no harm should come from seeing this data
			I	moderate	info needs to be accurate and should not be tampered to enable effective monitoring and control by the TMC; should be as accurate as the right of way request
			A	moderate	needs available to enable effective monitoring and control by the TMC; however if not immediately available, the app should still function
PID	Vehicle OBE	Personal Location	C	low	Similar to Vehicle Location and Motion. Pedestrian location within the crosswalk is not confidential or encrypted. Want to protect pedestrians against being tracked, but revealing instantaneous location is key to the application
			I	high	location needs to be accurate and should not be tampered
			A	moderate	location needs to be immediately available to enable warnings and messages from the PID to OBE but availability cannot be guaranteed over a wireless medium
PID	RSE	Personal Location	C	low	Similar to Vehicle Location and Motion. Pedestrian location within the crosswalk is not confidential or encrypted. Want to protect pedestrians against being tracked, but revealing instantaneous location is key to the application
			I	high	location needs to be accurate and should not be tampered
			A	moderate	location needs to be immediately available to enable warnings and messages from the PID to RSE but availability cannot be guaranteed over a wireless medium
PID	RSE	Personal Signal Service Request	C	low	info is not confidential or encrypted
			I	moderate	requests should be accurate and not tampered with, otherwise incorrect or malicious requests could be granted which could lead to delays
			A	low	requests should be timely and available immediately but availability cannot be guaranteed over a wireless medium; also worst case scenario is the vehicle or pedestrian has to wait for the appropriate signal
RSE	ITS RE	Pedestrian Location Information	C	low	pedestrian location within the crosswalk is not confidential or encrypted
			I	moderate	location should be accurate and should not be tampered; however, we assume the info is not able to cause the ITS RE to behave in extreme ways (i.e., there should be maximum different cycle phases)
			A	low	if down, the ITS RE should revert to default behavior which we assume is sensible
RSE	ITS RE	Signal Service Request	C	low	info is not confidential or encrypted
			I	moderate	requests should be accurate and not tampered with, otherwise incorrect or malicious requests could be granted which could lead to delays
			A	low	requests should be timely and available immediately but availability cannot be guaranteed

					over a wireless medium; also worst case scenario is the vehicle or pedestrian has to wait for the appropriate signal
RSE	PID	Intersection Status	C	low	not encrypted and no harm should come from seeing this data
			I	moderate	info needs to be accurate and should not be tampered so the vehicle OBE has correct SPaT info for all lanes; however the driver can still see the traffic signals
			A	moderate	needs to be available so the vehicle OBE has correct SPaT info; identifies signal priority and preemption status and pedestrian crossing status information, etc. However availability cannot be guaranteed over a wireless medium
RSE	PID	Pedestrian Safety Information	C	low	info is not confidential or encrypted
			I	high	info needs to be accurate and should not be tampered with (used to warn pedestrians of infringement, etc.); higher because enables accessibility; pedestrians may not be able to see/hear the information
			A	moderate	needs to be readily available to give permission to cross, time remaining, etc. but cannot guarantee wireless communication; however, worst case is the pedestrian has to wait; also cannot guarantee wireless communication
RSE	TMC	Intersection Safety Application Status	C	low	not encrypted, no harm should come from seeing this data
			I	moderate	should be able to cope with some bad information on the status and record of alerts/warnings; aggregate info; however could cause appearance of excessive traffic violations or unnecessary maintenance caused if data is compromised
			A	low	want regular updates but does not have to be immediate
TMC	ITS RE	Signal Control Commands	C	low	encrypted, authenticated, proprietary; but the result is directly observable
			I	high	proprietary info that should not be tampered with, could enable outside control of traffic signals
			A	moderate	should be to be able to issue immediate commands but the ITS RE should be able to continue to function using the default configuration
TMC	RSE	Intersection Safety Application Info	C	moderate	encrypted, authenticated, may contain proprietary information for device management
			I	high	proprietary info that should not be tampered with
			A	low	want updates but outdated information will not be serious assuming the signals are configured well to start with. Should be robust enough to go without reconfiguration for an arbitrary amount of time. However, this supports remote control of the application
Vehicle Databus	Vehicle OBE	Host Vehicle Status	C	low	sensor data is not confidential
			I	high	sensor data needs to be accurate and should not be tampered with
			A	high	sensor data must be consistently available to feed BSMs broadcast at 10Hz

Vehicle OBE	PID	Vehicle Location and Motion	C	low	BSM information is not confidential
			I	high	BSM info needs to be accurate and should not be tampered with
			A	moderate	BSM must be broadcast regularly to make data available for the PID, but availability cannot be guaranteed over a wireless medium
Vehicle OBE	RSE	Vehicle Location and Motion	C	low	BSM information is not confidential
			I	high	BSM info needs to be accurate and should not be tampered with
			A	moderate	BSM must be broadcast regularly to make data available for the RSE, but availability cannot be guaranteed over a wireless medium
Vehicle OBE	RSE	Intersection Infringement Info	C	low	Basically the same concept as Vehicle Location and Motion. BSM information is not confidential
			I	high	BSM info needs to be accurate and should not be tampered with
			A	moderate	BSM must be broadcast regularly to make data available for the RSE, but wireless communication cannot be guaranteed
Vehicle OBE	Vehicle Databus	Driver Update Information	C	low	info provided to the DVI is not confidential
			I	high	information that provides warnings must be accurate and cannot be tampered with
			A	high	information that provides warnings must be immediately available for the driver to react
Vehicle OBE	Vehicle Databus	Collision Warning Information	C	low	info provided to the databus on collision warnings is not confidential
			I	high	information that provides warnings must be accurate and cannot be tampered with
			A	high	information that provides warnings must be immediately available for the driver/control systems to react

Transit Signal Priority (TSP)

The Transit Signal Priority application uses transit vehicle to infrastructure communications to allow a transit vehicle to request a priority at one or a series of intersections. The application includes feedback to the transit driver indicating whether the signal priority has been granted or not. This application can contribute to improved operating performance of the transit vehicles by reducing the time spent stopped at a red light. This application will be used in the Marion Street use case, a primary route for buses, and where buses and traffic signals communicate. If a bus is behind schedule, the traffic signal system will either give the bus priority or flush the queue allowing the bus to reach its stop assuming there are no other higher priorities.

Table B-5. TSP Information Flow Analysis

Source	Destinati	Information	Controlling Condition

	on	type			
ITS RE	RSE	Intersection Control Status	C	low	not encrypted and no harm should come from seeing this data
			I	high	info needs to be accurate and should not be tampered so the RSE has correct phase info, priority status, etc.; if compromised, could lead to sending inconsistent messages which would greatly increase the possibility of collisions
			A	moderate	should be immediately available so the RSE has correct phase info, priority status, etc.; however, the RSE could choose not to send out of date information
ITS RE	TMC	Right-of-Way Request Notification	C	low	encrypted and authenticated but no harm should come from seeing this data
			I	moderate	invalid messages could lead to an unauthorized user gaining priority which could delay traffic etc.
			A	low	not necessary for the app to work; can cope with not having immediately available data
ITS RE	TMC	Signal Control Status	C	low	encrypted and authenticated but no harm should come from seeing this data
			I	moderate	info needs to be accurate and should not be tampered to enable effective monitoring and control by the TMC; should be as accurate as the right of way request
			A	moderate	needs available to enable effective monitoring and control by the TMC; however if not immediately available, the app should still function
RSE	TRANSIT OBE	Intersection Status	C	low	not encrypted and no harm should come from seeing this data
			I	moderate	info needs to be accurate and should not be tampered so the vehicle OBE has correct SPaT info for all lanes; however the driver can still see the traffic signals
			A	moderate	Needs to be available so the vehicle OBE has correct SPaT info; identifies signal priority and preemption status and pedestrian crossing status information, etc. However availability cannot be guaranteed over a wireless medium
RSE	ITS RE	Signal Priority Service Request	C	low	possible issues with disclosing priority level, though this should not lead to serious effects
			I	moderate	info needs to be accurate and should not be tampered to enable accurate requests; corrupted requests may lead to a transit vehicle not receiving a green light or an unapproved vehicle forging requests which could lead to delays
			A	low	needs to be immediately available so that requests are accurately issued when needed by the transit vehicle; but if not available, the worst that can happen is the vehicle waits for a green light
TMC	ITS RE	Signal Control Commands	C	low	encrypted, authenticated, proprietary; but the result is directly observable
			I	high	proprietary info that should not be tampered with, could enable outside control of traffic signals
			A	moderate	should be to be able to issue immediate commands but the ITS RE should be able to

					continue to function using the default configuration
TMC	Transit MC	Traffic Control Priority Status	C	low	encrypted but should not be an issue if anyone sees the information (status of request functions)
			I	moderate	correct status is important to function properly; could lead to routes that do not take advantage of optimizations
			A	moderate	info is necessary for the system to operate properly
Transit MC	TMC	Traffic Control Priority Request	C	low	encrypted but should not cause an issue if the request is seen
			I	moderate	requests should be accurate and not tampered with, otherwise malicious requests could be granted which could delay traffic. However, signals have controls in place to ensure there are not illegal configs
			A	moderate	requests should be timely and available immediately but if not received, the ITS RE should function in default config
Transit MC	TRANSIT OBE	Transit Schedule Information	C	low	proprietary info on current/projected schedule, performance, etc., but is generally made public and should not cause harm
			I	moderate	proprietary info that should not be tampered with, but operators should be able to notice any unusual configurations
			A	moderate	necessary for application to work correctly but is wireless communication which cannot be guaranteed
Transit Databus	TRANSIT OBE	Host Transit Vehicle Status	C	low	sensor data is not confidential; harm should not come from seeing status
			I	high	sensor data needs to be accurate and should not be tampered with
			A	high	sensor data must be consistently available to feed BSMs broadcast at 10Hz, notifications, etc.
Transit OBE	RSE	Local Signal Priority Request	C	low	should not cause an issue if the request is seen
			I	moderate	requests should be accurate and not tampered with, otherwise incorrect or malicious requests could be granted which could lead to delays
			A	low	requests should be timely and available immediately but availability cannot be guaranteed over a wireless medium; also worst case scenario is the TRANSIT has to wait for a green light
Transit OBE	Transit MC	Transit Vehicle Schedule Performance	C	low	no harm should come from seeing this information; “Estimated times of arrival and anticipated schedule deviations” should actually be regularly provided to the public
			I	moderate	information should be accurate and not tampered with but could cope with some bad data; not catastrophic
			A	low	want timely and readily available performance info; but not serious if updates are not immediate
Transit	RSE	Vehicle	C	low	BSM information is not confidential

OBE		Location & Motion	I	high	BSM info needs to be accurate and should not be tampered with
			A	moderate	BSM must be broadcast regularly to make data available for the RSE, but availability cannot be guaranteed over a wireless medium

V2I Safety

V2I Safety applications exchange critical safety and operational data between vehicles and infrastructure, intended primarily to avoid motor vehicle crashes and enable a wide range of other safety, mobility, and environmental benefits. V2I safety applications will compliment V2V safety applications, which will enable vehicles to have 360-degree awareness to inform a vehicle operator of hazards and situations they cannot see through advisories and warnings. The THEA CV Pilot will deploy the following V2I Safety applications:

- Curve Speed Warning (CSW)
- Pedestrian in Signalized Crosswalk

Curve Speed Warning (CSW)

The Curve Speed Warning application allows connected vehicles to receive information that it is approaching a curve along with the recommended speed for the curve. This capability allows the vehicle to provide a warning to the driver regarding the curve and its recommended speed. In addition, the vehicle can perform additional warning actions if the actual speed through the curve exceeds the recommended speed. This application will be used to help reduce morning traffic backups on the REL by Twiggs Street. It will inform drivers approaching the exit curve for the REL on a safe entry speed as well as the location of the end of the right turn queue.

Table B-6. CSW Information Flow Analysis

Source	Destination	Information type	Controlling Condition		
ITS RE	RSE	Environmental Sensor Data	C	low	no impact if someone sees info
			I	moderate	info should be correct to determine safe speeds, etc.
			A	moderate	want updates but slightly outdated information will not be catastrophic
ITS RE	TMC	Environmental Sensor Data	C	low	no impact if someone sees info
			I	moderate	info should be correct to determine safe speeds, etc.
			A	moderate	want updates but slightly outdated information will not be catastrophic
ITS RE	TMC	Speed	C	moderate	encrypted, authenticated, violation records included

		Monitoring Information	I	moderate	info that should not be tampered with, especially violation records and operational state but the rest is aggregate info
			A	moderate	want updates but outdated information will not be catastrophic; would want to know about the speeds, warnings, etc. to be able to reconfigure speed warning info as necessary
ITS RE	RSE	Reduced Speed Warning Info	C	low	encrypted and authenticated but the info would be observable through posted speed limits, warnings, etc.
			I	high	info needs to be correct to issue correct speed limit and warnings or could cause driver confusion and delays or unsafe speed if compromised
			A	moderate	want updates but outdated information will not be catastrophic; should be able to operate on previous or default information
RSE	TMC	Reduced Speed Warning Status	C	low	not encrypted, no harm should come from seeing this data
			I	moderate	should be able to cope with some bad information; but cannot obtain operational state, notifications, alerts, etc. by other means
			A	moderate	want regular updates but does not have to be immediate but could be used for modifying warning info
RSE	Vehicle OBE	Reduced Speed Notification	C	low	Seeing the broadcasted message on current reduced speed limit should not cause harm as this is sent to all nearby vehicles to notify of reduced speed limits
			I	moderate	message should not be tampered with; could increase physical risk to the driver and other drivers on the road if not warned with the correct information
			A	moderate	need immediate availability for the driver to react but cannot guarantee wireless communication
TMC	ITS RE	Environmental Sensors Control	C	low	encrypted, authenticated, proprietary; but should not cause severe damage if seen
			I	moderate	should be accurate and not be tampered with; could enable outside control of traffic sensors but should not cause severe harm, but could cause issues with environmental sensor data received and be detrimental to operations
			A	low	want updates but delayed information will not be severe; should be able to operate from a previous/default control/config
TMC	ITS RE	Speed Monitoring Control	C	moderate	encrypted, authenticated, proprietary but shouldn't cause substantial risk but does control speed enforcement systems
			I	high	proprietary info that should not be tampered with; could directly affect safety if compromised posting unsafe speed limits, etc.
			A	moderate	want updates but outdated information will not be catastrophic; should be able to use previous/default config
TMC	RSE	Reduced	C	low	encrypted and authenticated but the info would be observable through posted speed limits,

		Speed Warning Info			warnings, etc.
			I	high	info needs to be correct to issue correct speed limit and warnings or could cause driver confusion and delays or unsafe speed if compromised
			A	moderate	want updates but outdated information will not be catastrophic; should be able to operate on previous or default information
Vehicle Databus	Vehicle OBE	Driver Input Information	C	low	Control commands and requests are not confidential. Most information will eventually be included in a broadcast message
			I	high	Control commands and requests need to be accurate and should not be tampered with
			A	high	Control commands and requests must be consistently available to feed messages
Vehicle Databus	Vehicle OBE	Host Vehicle Status	C	low	sensor data is not confidential; harm should not come from seeing status
			I	high	sensor data needs to be accurate and should not be tampered with
			A	high	sensor data must be consistently available to feed BSMs broadcast at 10Hz
Vehicle OBE	RSE	Vehicle Location and Motion	C	low	BSM information is not confidential
			I	high	BSM info needs to be accurate and should not be tampered with
			A	moderate	BSM must be broadcast regularly to make data available for the RSE, but availability cannot be guaranteed over a wireless medium
Vehicle OBE	Vehicle Databus	Driver Update Information	C	low	info provided to the DVI is not confidential
			I	high	information that provides warnings must be accurate and cannot be tampered with
			A	high	information that provides warnings must be immediately available for the driver to react

Pedestrian in Signalized Crosswalk

The Pedestrian in Signalized Crosswalk Warning application provides the connected vehicle information from the infrastructure that indicates the possible presence of pedestrians in a crosswalk at a signalized intersection. The infrastructure based indication could include the outputs of pedestrian sensors or simply an indication that the pedestrian call button has been activated. This application has been defined for transit vehicles, but can be applicable to any class of vehicle. The application could also provide warning information to the pedestrian regarding crossing status or potential vehicle infringement into the crosswalk. This application will be used by the crosswalk on E. Twiggs Street near the courthouse. If a pedestrian decides to cross outside the cross walk, drivers will be alerted which will reduce the potential of a pedestrian getting struck by a vehicle.

Table B-7. Pedestrian in Signalized Crosswalk Information Flow Analysis

Source	Destination	Information type	Controlling Condition		
ITS RE	RSE	Intersection Control Status	C	low	not encrypted and no harm should come from seeing this data
			I	high	info needs to be accurate and should not be tampered so the RSE has correct phase info, priority status, etc.; if compromised, could lead to sending inconsistent messages which would greatly increase the possibility of collisions
			A	moderate	should be immediately available so the RSE has correct phase info, priority status, etc.; however, the RSE could choose not to send out of date information
ITS RE	RSE	Conflict Monitor Status	C	low	info is not confidential or encrypted
			I	high	if compromised, the ITS RE may not be able to support failsafe operating mode in the event of a conflict between the ITS RE and RSE
			A	moderate	want this info to be available immediately but want to support wireless communication flows; the driver should also be able to see the traffic signal phases if there is a slight delay
ITS RE	RSE	Pedestrian Crossing Status	C	low	not encrypted and no harm should come from seeing this data
			I	high	info needs to be accurate and should not be tampered so the RSE has correct crossing status, etc.
			A	moderate	should be immediately available so the RSE has correct crossing status, etc. and can send that status to the PID; however, worst case is the RSE does not send out the information and the pedestrian waits to cross; also enables wireless communication
ITS RE	TMC	Pedestrian Safety Warning Status	C	low	encrypted, but no harm should come from seeing this data; unless otherwise determined by the supplier because, for example it contains proprietary or security sensitive info
			I	moderate	should be able to cope with some bad information on the status, because it shouldn't actually impact device control
			A	low	want regular updates but does not have to be immediate; this could delay necessary maintenance but is not time critical
PID	Vehicle OBE	Personal Location	C	low	Similar to Vehicle Location and Motion. Pedestrian location within the crosswalk is not confidential or encrypted. Want to protect pedestrians against being tracked, but revealing instantaneous location is key to the application
			I	high	location needs to be accurate and should not be tampered
			A	low	location should be immediately available to enable warnings and messages from the PID to OBE but availability cannot be guaranteed over a wireless medium; also this should not be

					required to determine if a pedestrian is in an intersection. Not all pedestrians will carry a PIC
PID	RSE	Personal Location	C	low	Similar to Vehicle Location and Motion. Pedestrian location within the crosswalk is not confidential or encrypted. Want to protect pedestrians against being tracked, but revealing instantaneous location is key to the application
			I	high	location needs to be accurate and should not be tampered
			A	moderate	location needs to be immediately available to enable warnings and messages from the PID to RSE but availability cannot be guaranteed over a wireless medium
RSE	TMC	Intersection Safety Application Status	C	low	not encrypted, no harm should come from seeing this data
			I	moderate	should be able to cope with some bad information on the status and record of alerts/warnings; aggregate info; however could cause appearance of excessive traffic violations or unnecessary maintenance caused if data is compromised
			A	low	want regular updates but does not have to be immediate
RSE	Vehicle OBE	Intersection Safety Warning	C	low	warning is not confidential; no harm caused from seeing warning
			I	high	warning must be accurate and not tampered with; causes safety issues if incorrect; false positive could cause unnecessary sudden braking and collisions from behind
			A	moderate	warning information needs to be provided to vehicle OBEs immediately in the event of a red light, etc. but cannot guarantee wireless communication
RSE	Vehicle OBE	Intersection Status	C	low	not encrypted and no harm should come from seeing this data
			I	moderate	info needs to be accurate and should not be tampered so the vehicle OBE has correct SPaT info for all lanes; however the driver can still see the traffic signals
			A	moderate	needs to be available so the vehicle OBE has correct SPaT info; identifies signal priority and preemption status and pedestrian crossing status information, etc. However availability cannot be guaranteed over a wireless medium
RSE	ITS RE	Intersection Status Monitoring	C	low	not encrypted and no harm should come from seeing this data
			I	high	info needs to be accurate and should not be tampered so the ITS RE has correct SPaT info for all lanes to be able to detect conflicts and support failsafe operating mode
			A	moderate	should be immediately available so the ITS RE has correct SPaT info; but should be able to support wireless communication and a slight delay
RSE	ITS RE	Pedestrian Location Information	C	low	pedestrian location within the crosswalk is not confidential or encrypted
			I	moderate	location should be accurate and should not be tampered; however, we assume the info is not able to cause the ITS RE to behave in extreme ways (i.e., there should be maximum different cycle phases)
			A	low	if down, the ITS RE should revert to default behavior which we assume is sensible

RSE	PID	Pedestrian Safety Information	C	low	info is not confidential or encrypted
			I	high	info needs to be accurate and should not be tampered with (used to warn pedestrians of infringement, etc.); higher because enables accessibility; pedestrians may not be able to see/hear the information
			A	moderate	needs to be readily available to give permission to cross, time remaining, etc. but cannot guarantee wireless communication; however, worst case is the pedestrian has to wait; also cannot guarantee wireless communication
TMC	RSE	Intersection Safety Application Info	C	moderate	encrypted, authenticated, may contain proprietary information for device management
			I	high	proprietary info that should not be tampered with
			A	low	want updates but outdated information will not be serious assuming the signals are configured well to start with. Should be robust enough to go without reconfiguration for an arbitrary amount of time. However, this supports remote control of the application
TMC	ITS RE	Pedestrian Safety Warning Control	C	moderate	encrypted, authenticated, proprietary, but should not cause substantial risk
			I	high	proprietary info that should not be tampered with; equipment monitors and manages pedestrian crossings and provides visual displays and warnings
			A	low	System should be robust enough if it goes a while without reconfiguration
Vehicle Databus	Vehicle OBE	Host Vehicle Status	C	low	sensor data is not confidential; harm should not come from seeing status
			I	high	sensor data needs to be accurate and should not be tampered with
			A	high	sensor data must be consistently available to feed BSMs broadcast at 10Hz
Vehicle OBE	Vehicle Databus	Collision Warning Information	C	low	info provided to the databus on collision warnings is not confidential
			I	high	information that provides warnings must be accurate and cannot be tampered with
			A	high	information that provides warnings must be immediately available for the driver/control systems to react
Vehicle OBE	Vehicle Databus	Driver Update Information	C	low	info provided to the DVI is not confidential
			I	high	information that provides warnings must be accurate and cannot be tampered with
			A	high	information that provides warnings must be immediately available for the driver to react
Vehicle OBE	RSE	Intersection Infringement Info	C	low	Basically the same concept as Vehicle Location and Motion. BSM information is not confidential
			I	high	BSM info needs to be accurate and should not be tampered with
			A	moderate	BSM must be broadcast regularly to make data available for the RSE, but wireless communication cannot be guaranteed
Vehicle	RSE	Vehicle	C	low	BSM information is not confidential

OBE		Location & Motion	I	high	BSM info needs to be accurate and should not be tampered with
			A	moderate	BSM must be broadcast regularly to make data available for the RSE, but availability cannot be guaranteed over a wireless medium
Vehicle OBE	PID	Vehicle Location & Motion	C	low	BSM information is not confidential
			I	high	BSM info needs to be accurate and should not be tampered with
			A	moderate	BSM must be broadcast regularly to make data available for the RSE, but availability cannot be guaranteed over a wireless medium

V2V Safety

V2V safety applications exchange data among vehicles traveling in the same vicinity. Vehicles will communicate with one another broadcasting safety advisories, warnings, and messages that will inform a vehicle operator of hazards and situations they cannot see. The THEA CV Pilot will deploy the following V2V Safety applications:

- Emergency Electronic Brake Light (EEBL)
- Forward Collision Warning (FCW)
- Intersection Movement Assist (IMA)

Emergency Electronic Brake Light (EEBL)

The Emergency Electronic Brake Light (EEBL) application enables a vehicle to broadcast a self-generated emergency brake event to surrounding vehicles. Upon receiving the event information, the receiving vehicle determines the relevance of the event and if appropriate provides a warning to the driver in order to avoid a crash. This application is particularly useful when the driver's line of sight is obstructed by other vehicles or bad weather conditions (e.g., fog, heavy rain). This application will be used to increase safety during peak traffic hours on the REL. Backup on the REL causes exiting vehicles wanting to turn right to use the shoulder as part of the right turn lane. If a vehicle is broken down on the shoulder of the road the EEBL will application will notify other vehicles that may hit the stopped vehicle.

Table B-8. EEBL Information Flow Analysis

Source	Destination	Information type	Controlling Condition		
Remote Vehicle OBE	Vehicle OBE	Vehicle Control Event	C	low	Vehicle control event information is contained within BSM Part 2. BSM information is not confidential
			I	high	BSM info needs to be accurate and should not be tampered with

			A	moderate	BSM must be broadcast regularly to make data available for other vehicle OBEs, but cannot guarantee wireless communication
Vehicle Databus	Vehicle OBE	Host Vehicle Status	C	low	sensor data is not confidential; harm should not come from seeing status
			I	high	sensor data needs to be accurate and should not be tampered with
			A	high	sensor data must be consistently available to feed BSMs broadcast at 10Hz
Vehicle OBE	Remote Vehicle OBE	Vehicle Control Event	C	low	BSM information is not confidential
			I	high	BSM info needs to be accurate and should not be tampered with
			A	moderate	BSM must be broadcast regularly to make data available for other vehicle OBEs, but cannot guarantee wireless communication
Vehicle OBE	Vehicle Databus	Driver Update Information	C	low	info provided to the DVI is not confidential
			I	high	information that provides warnings must be accurate and cannot be tampered with
			A	high	information that provides warnings must be immediately available for the driver to react
Vehicle OBE	Vehicle Databus	Collision Warning Information	C	low	info provided to the databus on collision warnings is not confidential
			I	high	information that provides warnings must be accurate and cannot be tampered with
			A	high	information that provides warnings must be immediately available for the driver/control systems to react

Forward Collision Warning (FCW)

The Forward Collision Warning (FCW) application is intended to warn the driver of the vehicle in case of an impending rear-end collision with another vehicle ahead in traffic in the same lane and direction of travel. The application uses data received from other vehicles to determine if a forward collision is imminent. FCW is intended to advise drivers to take specific action in order to avoid or mitigate rear-end vehicle collisions in the forward path of travel. Similar to the EEBL, the FCW application will be used to increase safety by reducing accidents during peak traffic hours on the REL. As vehicles approach the REL exit, they may not be able to anticipate where the end of the queue is for the right turn lane, potentially causing them to hard brake. The FCW will send warnings to the driver if a vehicle ahead brakes suddenly.

Table B-9. FCW Information Flow Analysis

Source	Destination	Information type	Controlling Condition		
Remote	Vehicle	Vehicle	C	low	BSM information is not confidential

Vehicle OBE	OBE	Location and Motion	I	high	BSM info needs to be accurate and should not be tampered with
			A	moderate	BSM must be broadcast regularly to make data available for other vehicle OBEs, but availability cannot be guaranteed over a wireless medium
Vehicle Databus	Vehicle OBE	Host Vehicle Status	C	low	sensor data is not confidential; harm should not come from seeing status
			I	high	sensor data needs to be accurate and should not be tampered with
			A	high	sensor data must be consistently available to feed BSMs broadcast at 10Hz
Vehicle OBE	Remote Vehicle OBE	Vehicle Location and Motion	C	low	BSM information is not confidential
			I	high	BSM info needs to be accurate and should not be tampered with
			A	moderate	BSM must be broadcast regularly to make data available for other vehicle OBEs, but availability cannot be guaranteed over a wireless medium
Vehicle OBE	Vehicle Databus	Driver Update Information	C	low	info provided to the DVI is not confidential
			I	high	information that provides warnings must be accurate and cannot be tampered with
			A	high	information that provides warnings must be immediately available for the driver to react
Vehicle OBE	Vehicle Databus	Collision Warning Information	C	low	info provided to the databus on collision warnings is not confidential
			I	high	information that provides warnings must be accurate and cannot be tampered with
			A	high	information that provides warnings must be immediately available for the driver/control systems to react

Intersection Movement Assist (IMA)

The Intersection Movement Assist (IMA) application warns the driver of a vehicle when it is not safe to enter an intersection due to high collision probability with other vehicles at stop sign controlled and uncontrolled intersections. This application can provide collision warning information to the vehicle operational systems which may perform actions to reduce the likelihood of crashes at the intersections. This application will be used at the exit to the REL on East Twiggs Street. Drivers who use this exit may be easily confused and attempt to enter the REL going the wrong way. The IMA will send the driver warnings if they are about to enter the REL the wrong way.

Table B-10. IMA Information Flow Analysis

Source	Destination	Information type	Controlling Condition		
Remote	Vehicle	Vehicle	C	low	BSM information is not confidential

Vehicle OBE	OBE	Location and Motion	I	high	BSM info needs to be accurate and should not be tampered with
			A	moderate	BSM must be broadcast regularly to make data available for other vehicle OBEs, but availability cannot be guaranteed over a wireless medium
Vehicle Databus	Vehicle OBE	Host Vehicle Status	C	low	A moderate-BSM must be broadcast regularly to make data available for other vehicle OBEs, but availability cannot be guaranteed over a wireless medium. sensor data is not confidential; harm should not come from seeing status
			I	high	sensor data needs to be accurate and should not be tampered with
			A	high	sensor data must be consistently available to feed BSMs broadcast at 10Hz
Vehicle OBE	Vehicle Databus	Collision Warning Information	C	low	info provided to the databus on collision warnings is not confidential
			I	high	information that provides warnings must be accurate and cannot be tampered with
			A	high	information that provides warnings must be immediately available for the driver/control systems to react
Vehicle OBE	Vehicle Databus	Driver Update Information	C	low	info provided to the DVI is not confidential
			I	high	information that provides warnings must be accurate and cannot be tampered with
			A	high	information that provides warnings must be immediately available for the driver to react
Vehicle OBE	Remote Vehicle OBE	Vehicle Location and Motion	C	low	BSM information is not confidential
			I	high	BSM info needs to be accurate and should not be tampered with
			A	moderate	BSM must be broadcast regularly to make data available for other vehicle OBEs, but availability cannot be guaranteed over a wireless medium

V2V Transit

V2V transit applications address transit needs and priorities while providing interoperability and coexistence with connected-vehicle equipped cars and trucks. These applications communicate with other vehicles to enhance the mobility, safety, and environmental aspects of transit. The THEA CV Pilot will deploy the following V2V Transit application:

- Vehicle Turning Right in Front of a Transit Vehicle (VTRFTV)

Vehicle Turning Right in Front of a Transit Vehicle (VTRFTV)

The Vehicle Turning Right in Front of a Transit Vehicle (VTRFTV) application determines the movement of vehicles near to a transit vehicle stopped at a transit stop and provides an indication to the transit vehicle operator that a nearby vehicle is pulling in front of the transit vehicle to make a right turn. This application will help the transit vehicle determine if the area in front of it will not be occupied as it begins to pull away from a transit stop. This application

will be used in the TECO Streetcar, which runs along Channelside Drive from the Amalie Arena area up Channelside Drive, North, past the Selmon Expressway.

Table B-11. Vehicle Turning Right in Front of a Transit Vehicle Information Flow Analysis

Source	Destination	Information type	Controlling Condition		
Remote Vehicle OBE	Transit OBE	Vehicle Location and Motion	C	low	BSM information is not confidential
			I	high	BSM info needs to be accurate and should not be tampered with
			A	moderate	BSM must be broadcast regularly to make data available for other vehicle/TV OBEs, but availability cannot be guaranteed over a wireless medium
Transit Databus	Transit OBE	Host Transit Vehicle Status	C	low	sensor data is not confidential; harm should not come from seeing status
			I	high	sensor data needs to be accurate and should not be tampered with
			A	high	sensor data must be consistently available to feed BSMs broadcast at 10Hz
Transit OBE	Transit Databus	Collision Warning Information	C	low	info provided to the databus on collision warnings is not confidential
			I	high	information that provides warnings must be accurate and cannot be tampered with
			A	high	information that provides warnings must be immediately available for the driver/control systems to react
Transit OBE	Remote Vehicle OBE	Vehicle Location & Motion	C	low	BSM information is not confidential
			I	high	BSM info needs to be accurate and should not be tampered with
			A	moderate	BSM must be broadcast regularly to make data available for other vehicle/TV OBEs, but availability cannot be guaranteed over a wireless medium

Device Classification Analysis

Devices were classified based on the high water mark system. If the device was either the source or destination for an information flow identified as High for Confidentiality or Integrity, the device also takes the same classification. For Availability, the device is only assessed at the highest classification level in which it is the source. For example, if the device is the source of only information flows classified as Moderate Availability but is the destination for High Availability information follows, the device will be classified as Moderate Availability.

PID

Based on the High baseline Integrity classification, the PID would have an LHM classification. However, considering that there are measures to detect misbehavior and revoke certificates and permissions, Integrity was downgraded to Moderate. Therefore, the PID is downgraded from an LHM to LMM device, resulting in the Moderate baseline.

Information Flow Destination

Table B-12. Application Information Flows with PID as the Destination

Source	Destination	Information type	C	I	A
RSE	PID	Intersection Status	L	M	M
RSE	PID	Pedestrian Safety Information	L	H	M
Vehicle OBE	PID	Vehicle Location and Motion	L	H	M
RSE	PID	Pedestrian Safety Information	L	H	M
Vehicle OBE	PID	Vehicle Location & Motion	L	H	M

Information Flow Source

Table B-13. Application Information Flows with PID as the Source

Source	Destination	Information type	C	I	A
PID	Vehicle OBE	Personal Location	L	H	M
PID	RSE	Personal Location	L	H	M
PID	RSE	Personal Signal Service Request	L	M	L
PID	Vehicle OBE	Personal Location	L	H	L
PID	RSE	Personal Location	L	H	M

Vehicle OBE

Based on the High baseline Integrity classification, the Vehicle OBE would have an LHM classification. However, considering that there are measures to detect misbehavior and revoke certificates and permissions, Integrity was downgraded to Moderate. Therefore, the Vehicle OBE is downgraded from an LHM to LMM device, resulting in the Moderate baseline.

Information Flow Destination

Table B-14. Application Information Flows with Vehicle OBE as the Destination

Source	Destination	Information type	C	I	A
RSE	Vehicle OBE	Vehicle Situation Data Parameters	L	L	L
RSE	Vehicle OBE	Intersection Status	L	M	M
Vehicle Databus	Vehicle OBE	Host Vehicle Status	L	H	H
Vehicle Databus	Vehicle OBE	Driver Input Information	L	H	H
PID	Vehicle OBE	Personal Location	L	H	M
Vehicle Databus	Vehicle OBE	Host Vehicle Status	L	H	H
RSE	Vehicle OBE	Reduced Speed Notification	L	M	M
Vehicle Databus	Vehicle OBE	Driver Input Information	L	H	H
Vehicle Databus	Vehicle OBE	Host Vehicle Status	L	H	H
PID	Vehicle OBE	Personal Location	L	H	L
RSE	Vehicle OBE	Intersection Safety Warning	L	H	M
RSE	Vehicle OBE	Intersection Status	L	M	M
Vehicle Databus	Vehicle OBE	Host Vehicle Status	L	H	H
Remote Vehicle OBE	Vehicle OBE	Vehicle Control Event	L	H	M
Vehicle Databus	Vehicle OBE	Host Vehicle Status	L	H	H
Remote Vehicle OBE	Vehicle OBE	Vehicle Location and Motion	L	H	M
Vehicle Databus	Vehicle OBE	Host Vehicle Status	L	H	H
Remote Vehicle OBE	Vehicle OBE	Vehicle Location and Motion	L	H	M
Vehicle Databus	Vehicle OBE	Host Vehicle Status	L	H	H

Information Flow Source

Table B-15. Application Information Flows with Vehicle OBE as the Source

Source	Destination	Information type	C	I	A
Vehicle OBE	Vehicle Databus	Driver Update Information	L	H	H
Vehicle OBE	RSE	Vehicle Situation Data	L	L	L
Vehicle OBE	RSE	Vehicle Location & Motion for Surveillance	L	H	M

Vehicle OBE	RSE	Vehicle Environmental Data	L	L	L
Vehicle OBE	PID	Vehicle Location and Motion	L	H	M
Vehicle OBE	RSE	Vehicle Location and Motion	L	H	M
Vehicle OBE	RSE	Intersection Infringement Info	L	H	M
Vehicle OBE	Vehicle Databus	Driver Update Information	L	H	H
Vehicle OBE	Vehicle Databus	Collision Warning Information	L	H	H
Vehicle OBE	RSE	Vehicle Location and Motion	L	H	M
Vehicle OBE	Vehicle Databus	Driver Update Information	L	H	H
Vehicle OBE	Vehicle Databus	Collision Warning Information	L	H	H
Vehicle OBE	Vehicle Databus	Driver Update Information	L	H	H
Vehicle OBE	RSE	Intersection Infringement Info	L	H	M
Vehicle OBE	RSE	Vehicle Location & Motion	L	H	M
Vehicle OBE	PID	Vehicle Location & Motion	L	H	M
Vehicle OBE	Remote Vehicle OBE	Vehicle Control Event	L	H	M
Vehicle OBE	Vehicle Databus	Driver Update Information	L	H	H
Vehicle OBE	Vehicle Databus	Collision Warning Information	L	H	H
Vehicle OBE	Remote Vehicle OBE	Vehicle Location and Motion	L	H	M
Vehicle OBE	Vehicle Databus	Driver Update Information	L	H	H
Vehicle OBE	Vehicle Databus	Collision Warning Information	L	H	H
Vehicle OBE	Vehicle Databus	Collision Warning Information	L	H	H
Vehicle OBE	Vehicle Databus	Driver Update Information	L	H	H
Vehicle OBE	Remote Vehicle OBE	Vehicle Location and Motion	L	H	M

Remote Vehicle OBE

Based on the High baseline Integrity classification, the Remote Vehicle OBE would have an LHM classification. However, considering that there are measures to detect misbehavior and revoke certificates and permissions, Integrity was downgraded to Moderate. Therefore, the Remote Vehicle OBE is downgraded from an LHM to LMM device, resulting in the Moderate baseline.

Information Flow Destination

Table B-16. Application Information Flows with Remote Vehicle OBE as the Destination

Source	Destination	Information type	C	I	A

Vehicle OBE	Remote Vehicle OBE	Vehicle Control Event	L	H	M
Vehicle OBE	Remote Vehicle OBE	Vehicle Location and Motion	L	H	M
Vehicle OBE	Remote Vehicle OBE	Vehicle Location and Motion	L	H	M
Transit OBE	Remote Vehicle OBE	Vehicle Location & Motion	L	H	M

Information Flow Source

Table B-17. Application Information Flows with Remote Vehicle OBE as the Source

Source	Destination	Information type	C	I	A
Remote Vehicle OBE	Vehicle OBE	Vehicle Control Event	L	H	M
Remote Vehicle OBE	Vehicle OBE	Vehicle Location and Motion	L	H	M
Remote Vehicle OBE	Vehicle OBE	Vehicle Location and Motion	L	H	M
Remote Vehicle OBE	TRANSIT OBE	Vehicle Location and Motion	L	H	M

Transit OBE

Based on the High baseline Integrity classification, the Transit OBE would have an LHM classification. However, considering that there are measures to detect misbehavior and revoke certificates and permissions, Integrity was downgraded to Moderate. Therefore, the Transit OBE is downgraded from an LHM to LMM device, resulting in the Moderate baseline.

Information Flow Destination

Table B-18. Application Information Flows with Transit OBE as the Destination

Source	Destination	Information type	C	I	A
RSE	Transit OBE	Intersection Status	L	M	M
Transit MC	Transit OBE	Transit Schedule Information	L	M	M
TV Databus	Transit OBE	Host Transit Vehicle Status	L	H	H
Remote Vehicle OBE	Transit OBE	Vehicle Location and Motion	L	H	M
TV Databus	Transit OBE	Host Transit Vehicle Status	L	H	H

Information Flow Source

Table B-19. Application Information Flows with Transit OBE as the Source

Source	Destination	Information type	C	I	A
Transit OBE	RSE	Local Signal Priority Request	L	M	L
Transit OBE	Transit MC	Transit Vehicle Schedule Performance	L	M	L
Transit OBE	RSE	Vehicle Location & Motion	L	H	M
Transit OBE	TV Databus	Collision Warning Information	L	H	H
Transit OBE	Remote Vehicle OBE	Vehicle Location & Motion	L	H	M

RSE

Based on the application information flow analysis, the RSE has a classification of MHM with a High baseline for security controls.

Information Flow Destination

Table B-20. Application Information Flows with RSE as the Destination

Source	Destination	Information type	C	I	A
ITS RE	RSE	Intersection Control Status	L	H	M
ITS RE	RSE	Conflict Monitor Status	L	H	M
TMC	RSE	Intersection Management Application Info	M	H	L
Vehicle OBE	RSE	Vehicle Situation Data	L	L	L
Vehicle OBE	RSE	Vehicle Location & Motion for Surveillance	L	H	M
Vehicle OBE	RSE	Vehicle Environmental Data	L	L	L
ITS RE	RSE	Intersection Control Status	L	H	M
ITS RE	RSE	Pedestrian Crossing Status	L	H	M
PID	RSE	Personal Location	L	H	M
PID	RSE	Personal Signal Service Request	L	M	L
TMC	RSE	Intersection Safety Application Info	M	H	L
Vehicle OBE	RSE	Vehicle Location and Motion	L	H	M
Vehicle OBE	RSE	Intersection Infringement Info	L	H	M
ITS RE	RSE	Intersection Control Status	L	H	M

TRANSIT OBE	RSE	Local Signal Priority Request	L	M	L
TRANSIT OBE	RSE	Vehicle Location & Motion	L	H	M
ITS RE	RSE	Environmental Sensor Data	L	M	M
ITS RE	RSE	Reduced Speed Warning Info	L	H	M
TMC	RSE	Reduced Speed Warning Info	L	H	M
Vehicle OBE	RSE	Vehicle Location and Motion	L	H	M
ITS RE	RSE	Intersection Control Status	L	H	M
ITS RE	RSE	Conflict Monitor Status	L	H	M
ITS RE	RSE	Pedestrian Crossing Status	L	H	M
PID	RSE	Personal Location	L	H	M
TMC	RSE	Intersection Safety Application Info	M	H	L
Vehicle OBE	RSE	Intersection Infringement Info	L	H	M
Vehicle OBE	RSE	Vehicle Location & Motion	L	H	M

Information Flow Source

Table B-21. Application Information Flows with RSE as the Source

Source	Destination	Information type	C	I	A
RSE	ITS RE	Signal Service Request	L	M	L
RSE	ITS RE	Traffic Situation Data	L	L	L
RSE	TMC	Traffic Situation Data	L	L	L
RSE	ITS RE	Environmental Situation Data	L	L	L
RSE	TMC	Environmental Situation Data	L	L	L
RSE	ITS RE	Intersection Status Monitoring	L	H	M
RSE	Vehicle OBE	Vehicle Situation Data Parameters	L	M	M
RSE	Vehicle OBE	Intersection Status	L	M	M
RSE	TMC	Intersection Management Application Status	L	M	L
RSE	ITS RE	Pedestrian Location Information	L	M	L
RSE	ITS RE	Signal Service Request	L	M	L
RSE	PID	Intersection Status	L	M	M
RSE	PID	Pedestrian Safety Information	L	H	M
RSE	TMC	Intersection Safety Application Status	L	M	L

RSE	TRANSIT OBE	Intersection Status	L	M	M
RSE	ITS RE	Signal Priority Service Request	L	M	L
RSE	TMC	Reduced Speed Warning Status	L	M	M
RSE	Vehicle OBE	Reduced Speed Notification	L	M	M
RSE	TMC	Intersection Safety Application Status	L	M	L
RSE	Vehicle OBE	Intersection Safety Warning	L	H	M
RSE	Vehicle OBE	Intersection Status	L	M	M
RSE	ITS RE	Intersection Status Monitoring	L	H	M
RSE	ITS RE	Pedestrian Location Information	L	M	L
RSE	PID	Pedestrian Safety Information	L	H	M

ITS RE

Based on the application information flow analysis, the ITS RE has a classification of MHM with a High baseline for security controls.

Information Flow Destination

Table B-22. Application Information Flows with ITS RE as the Destination

Source	Destination	Information type	C	I	A
Other ITS RE	ITS RE	Signal Control Data	L	H	M
RSE	ITS RE	Signal Service Request	L	M	L
RSE	ITS RE	Traffic Situation Data	L	L	L
RSE	ITS RE	Environmental Situation Data	L	L	L
RSE	ITS RE	Intersection Status Monitoring	L	H	M
TMC	ITS RE	Signal System Configuration	L	H	M
TMC	ITS RE	Signal Control Commands	L	H	M
TMC	ITS RE	Signal Control Plans	L	H	M
TMC	ITS RE	Signal Control Device Configuration	L	H	M
TMC	ITS RE	Traffic Sensor Control	L	M	L
TMC	ITS RE	Environmental Sensors Control	L	M	L
RSE	ITS RE	Pedestrian Location Information	L	M	L
RSE	ITS RE	Signal Service Request	L	M	L

TMC	ITS RE	Signal Control Commands	L	H	M
RSE	ITS RE	Signal Priority Service Request	L	M	L
TMC	ITS RE	Signal Control Commands	L	H	M
TMC	ITS RE	Environmental Sensors Control	L	M	L
TMC	ITS RE	Speed Monitoring Control	M	H	M
RSE	ITS RE	Intersection Status Monitoring	L	H	M
RSE	ITS RE	Pedestrian Location Information	L	M	L
TMC	ITS RE	Pedestrian Safety Warning Control	M	H	L

Information Flow Source

Table B-23. Application Information Flows with ITS RE as the Source

Source	Destination	Information type	C	I	A
ITS RE	Other ITS RE	Signal Control Data	L	H	M
ITS RE	RSE	Intersection Control Status	L	H	M
ITS RE	RSE	Conflict Monitor Status	L	H	M
ITS RE	TMC	Environmental Sensor Data	L	M	M
ITS RE	TMC	Traffic Flow	L	L	L
ITS RE	TMC	Signal Control Status	L	M	M
ITS RE	RSE	Intersection Control Status	L	H	M
ITS RE	RSE	Pedestrian Crossing Status	L	H	M
ITS RE	TMC	Right-of-Way Request Notification	L	M	L
ITS RE	TMC	Signal Control Status	L	M	M
ITS RE	RSE	Intersection Control Status	L	H	M
ITS RE	TMC	Right-of-Way Request Notification	L	M	L
ITS RE	TMC	Signal Control Status	L	M	M
ITS RE	RSE	Environmental Sensor Data	L	M	M
ITS RE	TMC	Environmental Sensor Data	L	M	M
ITS RE	TMC	Speed Monitoring Information	M	M	M
ITS RE	RSE	Reduced Speed Warning Info	L	H	M
ITS RE	RSE	Intersection Control Status	L	H	M

ITS RE	RSE	Conflict Monitor Status	L	H	M
ITS RE	RSE	Pedestrian Crossing Status	L	H	M
ITS RE	TMC	Pedestrian Safety Warning Status	L	M	L

Other ITS RE

Other ITS RE has the same classification as ITS RE: MHM. This classification results in a High baseline for security controls.

Information Flow Destination

Table B-24. Application Information Flows with Other ITS RE as the Destination

Source	Destination	Information type	C	I	A
ITS RE	Other ITS RE	Signal Control Data	L	H	M

Information Flow Source

Table B-25. Application Information Flows with Other ITS RE as the Source

Source	Destination	Information type	C	I	A
Other ITS RE	ITS RE	Signal Control Data	L	H	M

TMC

Based on the application information flow analysis, the TMC has a classification of MHM with a High baseline for security controls.

Information Flow Destination

Table B-26. Application Information Flows with TMC as the Destination

Source	Destination	Information type	C	I	A
ITS RE	TMC	Environmental Sensor Data	L	M	M

ITS RE	TMC	Traffic Flow	L	L	L
ITS RE	TMC	Signal Control Status	L	M	M
RSE	TMC	Traffic Situation Data	L	L	L
RSE	TMC	Environmental Situation Data	L	L	L
RSE	TMC	Intersection Management Application Status	L	M	L
ITS RE	TMC	Right-of-Way Request Notification	L	M	L
ITS RE	TMC	Signal Control Status	L	M	M
RSE	TMC	Intersection Safety Application Status	L	M	L
ITS RE	TMC	Right-of-Way Request Notification	L	M	L
ITS RE	TMC	Signal Control Status	L	M	M
Transit MC	TMC	Traffic Control Priority Request	L	M	M
ITS RE	TMC	Environmental Sensor Data	L	M	M
ITS RE	TMC	Speed Monitoring Information	M	M	M
RSE	TMC	Reduced Speed Warning Status	L	M	M
ITS RE	TMC	Pedestrian Safety Warning Status	L	M	L
RSE	TMC	Intersection Safety Application Status	L	M	L

Information Flow Source

Table B-27. Application Information Flows with TMC as the Source

Source	Destination	Information type	C	I	A
TMC	ITS RE	Signal System Configuration	L	H	M
TMC	ITS RE	Signal Control Commands	L	H	M
TMC	ITS RE	Signal Control Plans	L	H	M
TMC	ITS RE	Signal Control Device Configuration	L	H	M
TMC	ITS RE	Traffic Sensor Control	L	M	L
TMC	ITS RE	Environmental Sensors Control	L	M	L
TMC	RSE	Intersection Management Application Info	M	H	L
TMC	Other TMC	Road Network Conditions	L	M	M
TMC	Other TMC	Device Status	L	M	L
TMC	Other TMC	Device Data	L	M	L
TMC	ITS RE	Signal Control Commands	L	H	M

TMC	RSE	Intersection Safety Application Info	M	H	L
TMC	ITS RE	Signal Control Commands	L	H	M
TMC	Transit MC	Traffic Control Priority Status	L	M	M
TMC	ITS RE	Environmental Sensors Control	L	M	L
TMC	ITS RE	Speed Monitoring Control	M	H	M
TMC	RSE	Reduced Speed Warning Info	L	H	M
TMC	RSE	Intersection Safety Application Info	M	H	L
TMC	ITS RE	Pedestrian Safety Warning Control	M	H	L

Transit MC

Based on the application information flow analysis, the Transit MC has a classification of LMM with a Moderate baseline for security controls. However, the Transit MC will have the same controls as the TMC at a MHM classification.

Information Flow Destination

Table B-28. Application Information Flows with Transit MC as the Destination

Source	Destination	Information type	C	I	A
TMC	Transit MC	Traffic Control Priority Status	L	M	M
Transit OBE	Transit MC	Transit Vehicle Schedule Performance	L	M	L

Information Flow Source

Table B-29. Application Information Flows with Transit MC as the Source

Source	Destination	Information type	C	I	A
Transit MC	TMC	Traffic Control Priority Request	L	M	M
Transit MC	Transit OBE	Transit Schedule Information	L	M	M

Transit Databus

Based on the application information flow analysis, the Transit Databus would have a classification of LHH with a High baseline for security controls. However, it is important to note that the THEA CV Pilot will not be modifying or developing a Transit Databus.

Information Flow Destination

Table B-30. Application Information Flows with Transit Databus as the Destination

Source	Destination	Information type	C	I	A
Transit OBE	Transit Databus	Collision Warning Information	L	H	H

Information Flow Source

Table B-31. Application Information Flows with Transit Databus as the Source

Source	Destination	Information type	C	I	A
Transit Databus	Transit OBE	Host Transit Vehicle Status	L	H	H
Transit Databus	Transit OBE	Host Transit Vehicle Status	L	H	H

Vehicle Databus

Based on the application information flow analysis, the Vehicle Databus would have a classification of LHH with a High baseline for security controls. However, it is important to note that the THEA CV Pilot will not be modifying or developing a Vehicle Databus.

Information Flow Destination

Table B-32. Application Information Flows with Vehicle Databus as the Destination

Source	Destination	Information type	C	I	A
Vehicle OBE	Vehicle Databus	Driver Update Information	L	H	H
Vehicle OBE	Vehicle Databus	Driver Update Information	L	H	H
Vehicle OBE	Vehicle Databus	Collision Warning Information	L	H	H

Vehicle OBE	Vehicle Databus	Driver Update Information	L	H	H
Vehicle OBE	Vehicle Databus	Collision Warning Information	L	H	H
Vehicle OBE	Vehicle Databus	Driver Update Information	L	H	H
Vehicle OBE	Vehicle Databus	Driver Update Information	L	H	H
Vehicle OBE	Vehicle Databus	Collision Warning Information	L	H	H
Vehicle OBE	Vehicle Databus	Driver Update Information	L	H	H
Vehicle OBE	Vehicle Databus	Collision Warning Information	L	H	H
Vehicle OBE	Vehicle Databus	Collision Warning Information	L	H	H
Vehicle OBE	Vehicle Databus	Driver Update Information	L	H	H

Information Flow Source

Table B-33. Application Information Flows with Vehicle Databus as the Source

Source	Destination	Information type	C	I	A
Vehicle Databus	Vehicle OBE	Host Vehicle Status	L	H	H
Vehicle Databus	Vehicle OBE	Driver Input Information	L	H	H
Vehicle Databus	Vehicle OBE	Host Vehicle Status	L	H	H
Vehicle Databus	Vehicle OBE	Driver Input Information	L	H	H
Vehicle Databus	Vehicle OBE	Host Vehicle Status	L	H	H
Vehicle Databus	Vehicle OBE	Host Vehicle Status	L	H	H
Vehicle Databus	Vehicle OBE	Host Vehicle Status	L	H	H
Vehicle Databus	Vehicle OBE	Host Vehicle Status	L	H	H
Vehicle Databus	Vehicle OBE	Host Vehicle Status	L	H	H

Appendix C. Acronyms

ACRONYM	DEFINITION
ACCS	Access Control Central Software
ASD	Aftermarket Safety Device
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
CRL	Certificate Revocation List
CSP	Critical Security Parameter
CSW	Curve Speed Warning
CVRIA	Connected Vehicle Reference Implementation Architecture
DSRC	Dedicated Short Range Communication
DSS	Data Security Standard
EAL	Evaluation Assurance Level
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
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMA	Intersection Movement Assist
I-SIG	Intelligent Traffic Signal System
ISO	International Organization For Standardization
ITS	Intelligent Transportation Systems
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
OBE	On- Board Equipment
OS	Operating System
PCI	Payment Card Industry
PCR	Platform Configuration Registry
PID	Personal Information Device
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
POC	Proof of Concept
PP	Protection Profile
PPTP	Point-to-Point Tunneling Protocol
RA	Registration Authority
RDE	Research Data Exchange
RE	Roadway Equipment
REL	Reversible Express Lanes
RSE	Roadside Equipment
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
SSC	Security Standards Council
SSL	Site Uses Https
TCG	Trusted Computing Group
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
USDOT	U.S. Department of Transportation
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
WAVE	Wireless Access In Vehicular Environments
WSA	WAVE Service Advertisement
WSMP	WAVE Short Message Protocol

Appendix D. 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 (OBE), which results in the issuance of the OBE'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 Equipment (OBE)	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 Equipment (RSE)	An infrastructure node that serves as an intermediary in Vehicle-to-Vehicle (V2V) two-way communications between CMEs and vehicles. RSE may also send its own messages to OBE
SAE J2945/1- On-Board System Requirements for V2V Safety Communications	Specifies the minimum communication performance requirements of the DSRC Message 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 Equipment (RSE)) 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 E. References

Any figures, tables, and charts that were not developed by the THEA CV Pilot Team are attributed within the report.

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.

ISO/IEC 15408

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-16-312

U.S. Department of Transportation