Connected Vehicle Pilot Deployment Program Phase 1, Security Management Operational Concept – ICF/Wyoming

www.its.dot.gov/index.htm
Final Report — March 14, 2016
FHWA-JPO-16-288

U.S. Department of Transportation

Produced by DTFH6115C00038
U.S. Department of Transportation

Notice

Technical Report Documentation Page

1. Report No. FHWA-JPO-16-288	**2. Government Accession No.**	**3. Recipient's Catalog No.**
4. Title and Subtitle Connected Vehicle Pilot Deployment Program Phase 1, Security Management Operational Concept – ICF/Wyoming		**5. Report Date** **3/14/2016** **6. Performing Organization Code**
7. Author(s) Deepak Gopalakrishna (ICF), Vince Garcia (Wyoming DOT), Ali Ragan (Wyoming DOT), Tony English (Trihydro), Shane Zumpf (Trihydro), Rhonda Young (University of Wyoming), Mohamed Ahmed (University of Wyoming), Fred Kitchener (McFarland Management), Nayel Ureña Serulle (ICF), Eva Hsu (ICF)		**8. Performing Organization Report No.** Task 3 Report
9. Performing Organization Name and Address ICF International, 1725 Eye St NW, Washington DC, 20006 Wyoming DOT, 5300 Bishop Boulevard, Cheyenne, WY 82009 Trihydro Corporation, 1252 Commerce Drive, Laramie, WY 82070 McFarland Management, 1015 W. Hays Street, Boise, ID 83702 University of Wyoming, 1000 E University Avenue, Laramie, WY 82071		**10. Work Unit No. (TRAIS)** **11. Contract or Grant No.** DTFH6115C00038
12. Sponsoring Agency Name and Address U.S Department of Transportation 1200 New Jersey Ave, SE Washington, DC 20590		**13. Type of Report and Period Covered** Security Management Operating Concept, 12/14/2015 to 3/14/2016 **14. Sponsoring Agency Code**
15. Supplementary Notes Kate Hartman (COR), Sarah Khan (CO)		

16. Abstract

The Wyoming Department of Transportation's (WYDOT) 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 the impact of adverse weather on truck travel in the I-80 corridor. These applications support a flexible range of services from advisories, roadside alerts, parking notifications and dynamic travel guidance. Information from these applications are made available directly to the equipped fleets or through data connections to fleet management centers (who will then communicate it to their trucks using their own systems). 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. This document provides guidance material and operating concept in regards to security and privacy for the ICF/Wyoming Deployment Pilot. The document is presented based on identifying the impacts of security breaches regarding confidentiality, integrity, and availability along with the potential threats. Additional security analyses are included to cover V2V security, the SCMS, and CV application security needs. Major challenges such as SCMS integration and security for a complex system of systems are described.

17. Key Words Connected Vehicle Technology, I-80 Corridor, Road Weather, Truck Safety	**18. Distribution Statement** This document is available to the public through the National Technical Information Service, Springfield, Virginia 22161		
19. Security Classif. (of this report) None	**20. Security Classif. (of this page)** None	**21. No. of Pages** 71	**22. Price** NA

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

Acknowledgements

The ICF/Wyoming SMOC development team would like to thank the Tampa Hillsborough Expressway Authority (THEA) team for guidance and assistance with the information presented in the biweekly conference calls, shared documents as well as organizing and leading the cross-team working session. We would also like to thank the New York City DOT team for all the work and guidance on the software and operating system security. We acknowledge the timely and high-quality support offered by USDOT, and the support contractor Noblis throughout Phase I.

Table of Contents

List of Figures

List of Tables

1 Scope

1.1 Project Scope

Wyoming Department of Transportation (WYDOT) is one of the first wave of Connect Vehicle (CV) Pilot sites selected to showcase the value of and spur the adoption of CV Technology in the United States. CV Technology is a broad term to describe the applications and the systems that take advantage of vehicle to vehicle (V2V) and vehicle to infrastructure (V2I) communications to improve safety, mobility and productivity of the users of the nation's transportation system.

As one of the three selected pilots, WYDOT is focusing on improving safety and mobility by creating new ways to communicate road and travel information to commercial truck drivers and fleet managers along the 402 miles of Interstate 80 (I-80 henceforth) in the State. For the pilot project, WYDOT will work in a planning phase through September 2016. The deployment process will happen in the second phase (ending in September 2017) followed by an eighteen-month demonstration period in the third phase (starting in October 2017).

Systems and applications developed in the pilot will enable drivers to have 360-degree awareness of hazards and situations they cannot even see. Specifically, WYDOT hopes to improve operations on the corridor especially during periods of adverse weather and when work zones are present. Through the anticipated outcomes of the pilot, fleet managers will be able to make better decisions regarding their freight operations on I-80, truckers will be made aware of downstream conditions and provided guidance on parking options as they travel the corridor, and automobile travelers will receive improved road condition and incident information through various existing and new information outlets.

1.2 Security Management Operating Concept Introduction

The Security Management Operating Concept for the ICF/Wyoming CV Pilot is a companion document to the ConOps that is a key element in ensuring the privacy of pilot participants and the security of the pilot data and communications.

This document complies with the Broad Agency Announcement and describes the underlying needs of the ICF/Wyoming Pilot Deployment to protect the privacy of users, ensure secure operations, and outline a concept that addresses these needs. The concept determines and documents the extent to which this system will collect and store Personally Identifiable Information (PII) and PII-related information, and ensures that there is a legitimate need for this information in order to meet the goals of the system and that the data is only accessible for and used for these legitimate purposes. The concept describes, at a high level, the elements to be implemented to meet system security and address how this pilot will use the Security Credential Management System (SCMS) for proposed applications.

1.3 Document Overview

This document is an overview of the security and privacy elements utilized in this pilot. It analyzes security and privacy threats and mitigations of these threats for users, data at rest and in motion, applications, networking, and hardware. With the recent highly publicized breaches of advanced automotive systems and personal information breaches in financial network security by hackers the public awareness is heightened. As a pilot for CVs the security and privacy needs to be structured as part of the design rather than an afterthought. The success of this pilot depends on the public's acceptance that PII are protected and safety information and warnings can be trusted.

1.4 Document Organization

This document will cover five components to protect security and privacy. The first section will cover application communication and data security. The second section will cover software and operating system (OS) security for pilot devices. The third section will cover protection of hardware devices. The fourth section will cover network, database and center security to include organizational procedures and processes for data access and protection. The final section will be dedicated to user privacy protection of PII. The analysis of security for application information flows will be based on Federal Information Processing Standard (FIPS) 199, device class security controls will be based on FIPS 200 and National Institute of Standards and Technology Special Publication (NIST SP) 800-53. The device categories and requirements for security that will defined by this analysis and utilized in this pilot are Vehicle Onboard Equipment (OBE) for Snow Plows, Highway Patrol, and Commercial Vehicles; Roadside Equipment (RSE); and Personal Information Devices (PIDs).

1.5 System Overview

The pilot is intended to develop a suite of applications that utilize V2V and V2I technology to improve truck safety and reduce the impact of adverse weather on, but not limited to, truck travel on I-80. Specifically, this pilot will target the 402 mile stretch of I-80 that passes through Wyoming's Maintenance Districts 1 and 3 and will be demonstrated for an 18 month period in 2017-2018.

Through the pilot, relevant information are made available directly and shared between equipped fleets. Information is also shared through linkages with fleet management centers (who will then communicate it to their trucks using their own communication systems). Supporting the applications and the CV environment of roadside, vehicle and back-office infrastructure are core services that allow safe, secure, reliable operations of the system.

1.5.1 System Objects

The following objects are of interest to the system and will be the focus on various security and privacy-related elements:

- Vehicles – Four categories of vehicles will play a role in the pilot.

  - WYDOT Fleet –This group represents vehicles owned by WYDOT (such as snow plows, highway patrol vehicles and other state-owned vehicles) that will be equipped with OBE with Dedicated Short Range Communications (DSRC) connectivity. The OBE will support communications, generate safety messages, collect and report vehicle, weather and road condition data, store data and provide an interface to communicate safety alerts and advisories. Some vehicles in the WYDOT fleet also have cellular connectivity with WYDOT centers to support operations.
  - Connected Truck – This group represents vehicles owned by commercial vehicle operators that are participating in the pilot. These trucks will be equipped with an OBE with similar functions and capabilities as described for the WYDOT fleet. Similar to WYDOT fleets, connected trucks may have cellular or satellite connectivity to their fleet management centers.
  - Private Vehicle – This group of vehicles represent private vehicles that have access to third-party applications on their PID.
  - Truck – This group of vehicles represent trucks that are connected to fleet management centers but are not equipped with an OBE for this project.
- Infrastructure – Two infrastructure elements are part of the pilot
  - WYDOT Traditional Intelligent Transportation System (ITS) – This object group includes the existing ITS program devices like pre-trip information systems and roadside systems, such as Dynamic Message Signs (DMS), and Highway Advisory Radios (HAR).
  - WYDOT RSE – This object describes the RSE that will be deployed as part of the system. RSEs include DSRC connectivity, application support, data storage, and other support services to enable CV applications. WYDOT RSEs can be either fixed or portable equipment depending on the use-case.
- Centers/Systems – Three major centers and systems are part of the pilot.
  - WYDOT Transportation Management Center (TMC) – The TMC is planned to be the hub of operations for the CV Pilot collecting information from WYDOT fleet and partnering fleet management centers. The TMC supports the integration and fusion of CV and non-CV data to develop warnings and advisories. The TMC also provides traveler information services back to the general public and fleet management centers via various means. The TMC is also responsible for various system services that are necessary for the pilot.
  - Fleet Management Centers – This object represents the partnering fleet management centers that both receive and send real-time information to the WYDOT TMC about their firm's truck operations and corridor conditions.
  - Data Warehouse – A data warehouse capability is planned for the pilot to collect, manage and make available the data collected as part of the pilot for performance management and evaluation.
- External Systems
  - Third Party Information Service Providers (ISPs) – This object represents third-party developers of data and information products for both WYDOT and the end-consumer. These may include weather products that are used by WYDOT TMC and driver-focused applications that use data from the TMC.

- WYDOT Maintenance Management – This object represents the WYDOT maintenance management systems and functions carried out in the corridor including winter maintenance, work zone management and other non-winter maintenance activities.
- WYDOT Commercial Vehicle Enforcement– This object represents WYDOT commercial vehicle operations enforcement in the corridor including Port of Entry operations, permitting, and oversize/overweight enforcement.
- Truck Parking Services – This object represents the public and private parking services available in the corridor.
- National Weather Service (NWS) – This object represents the systems and personnel of the NWS offices in Wyoming for the I-80 corridor.
- Adjacent State DOT TMCs – This object represents the systems and personnel at adjacent State DOTs (Colorado, Utah and Nebraska) necessary for coordinated response to conditions on I-80.

1.5.2 Proposed System Functionality

System capabilities are organized by two categories – the pilot system which describes the center-related capabilities and the mobile distribution system which describes the capabilities relating to field to vehicle and V2V interactions. The system, comprising of the pilot system and the mobile distribution element provides the following capabilities.

- Pilot System – Collect Road and Weather Data- The system shall collect road and weather data from a variety of sources including connected trucks, connected WYDOT fleets, fixed infrastructure sensors like Road Weather Information Systems (RWIS), NWS, maintenance personnel and adjacent State DOTs. The data collected include both directly observed road and weather conditions or other data (such as vehicle telematics) that will help estimate the conditions of road segments along I-80.
- Pilot System – Collect Work Zone Information- The system shall collect work zone information including location, duration and nature of activity reported by maintenance personnel and centers
- Pilot System – Collect Dynamic Travel Information - The system shall collect dynamic travel information such as travel speeds, parking availability, and incident notifications
- Pilot System – Share Integrated and Fused Advisories - The system shall fuse travel information, road condition data and weather data to generate segment-level advisories along I-80. The system shall share advisories with CVs, fleet management centers, traditional ITS channels like DMS/HAR/511 and to partners like truck parking facilities and adjacent State DOTs
- Pilot System – Provide Dynamic Travel Information - The system shall provide dynamic travel information to both vehicles on-road as well as over a wide area to support travel decisions. Dynamic travel information may relate to variable speed limits, road closures, and truck parking availabilities.

- Mobile Distribution – Share Safety and Road Condition Messages - The mobile distribution aspect of the system shall share safety and road condition messages between CVs and between vehicles and the roadside infrastructure. Safety and road condition information shared by CVs to other CVs include situational awareness of downstream conditions, speeds, information on slowing traffic or queues. This information will also be relayed to RSE when CVs pass them in the corridor.
- Mobile Distribution – Collect Messages from Other CVs - Connected vehicles shall collect messages from other CVs about situational awareness of conditions and provide the information to the driver in a meaningful format.
- Mobile Distribution – Collect Messages from Infrastructure - Connected vehicles and the pilot system shall collect messages from infrastructure about advisories and alerts including speeds, parking availability, upcoming travel conditions and provide the information to the driver in a meaningful format.
- Mobile Distribution – Generate Emergency Message - Connected vehicles shall have the capability to generate an emergency message while on travel on the I-80 corridor when conditions warrant such a message from that vehicle or about other emergency conditions on the corridor observed by the vehicle.

Where necessary, DSRC will be used to support localized warnings to equipped vehicles as part of the mobile distribution system. This means when connected trucks or WYDOT fleet vehicles approach slowed or stopped traffic, they can receive messages in their vehicle from other equipped vehicles ahead of them to give more reaction time. Or if equipped vehicles pass roadside devices, drivers can receive messages alerting them to hazardous road conditions, crashes ahead, construction zone information, parking recommendations, or other road and travel information. If the equipped vehicle is stranded, the vehicle can send out an emergency notification to the appropriate center for assistance. The use of DSRC technology in the pilot will be guided by the IEEE 1609.2, 1609.3, and 1609.4 standards for Security, Network Services and Multi-Channel Operation, the SAE J2735 Message Set Dictionary (SAE, 2016), the emerging SAE J2945/1 V5 Communication Minimum Performance Requirements standard (SAE, 2016). Relevant sections from SAE J3067 (SAE 2014) Information Report will also be reviewed as part of systems development. Weather data collection will also be guided by NTCIP 1204.

The system capabilities and functions described in the previous paragraphs are implemented through the following seven applications:

- Road Weather Advisories for Trucks - This application provides the capability of collecting road weather data from WYDOT Fleets and Connected Trucks and using that data to develop short term warnings or advisories that can be provided to individual commercial vehicles or to commercial vehicle dispatchers.
- Automatic Alerts for Emergency Responders - This application provides the capability for connected trucks to transmit an emergency message when the vehicle has been involved in a crash or other distress situation.
- CV-enabled Weather-Responsive Variable Speed Limits (VSLs) - This application uses road weather information from connected trucks and WYDOT Fleet vehicles as well as current and

historical data from multiple sources to determine the appropriate current safe speed and other traffic management strategies.

- Spot Weather Impact Warning (SWIW) - This application will alert drivers to unsafe conditions or road closure at specific points on the downstream roadway as a result of weather-related impacts (e.g., high winds, flood conditions, ice, and fog).
- Work Zone Warnings - This application provides information about the conditions that exist in a work zone to vehicles that are approaching the work zone.
- Situational Awareness - The application determines if the road conditions measured by other vehicles represent a potential safety hazard for the vehicle containing the application.
- Freight-Specific Dynamic Travel Planning- This application provides both pre-trip and en-route travel planning, routing, and commercial vehicle related traveler information for fleet management center.

1.6 Security Overview

The following diagram (Figure 1-1) provides an overview of the communication security between physical objects. The data in motion is protected by SCMS signing for all DSRC communications and encryption for non-broadcast communications. The data that connects third parties to the WYDOT data center will be done over encrypted Secured Socket Layer (SSL) tunnels. This will be for access to the Commercial Vehicle Operator Portal (CVOP), REST service end points and other web sites that need protection (not for general public access). For back haul connections from RSE's and traditional ITS equipment, data will be protected with Internet Protocol Security (IPSEC) Virtual Private Networks (VPN) or private networks. Figure 1-1 below graphically shows these connections.

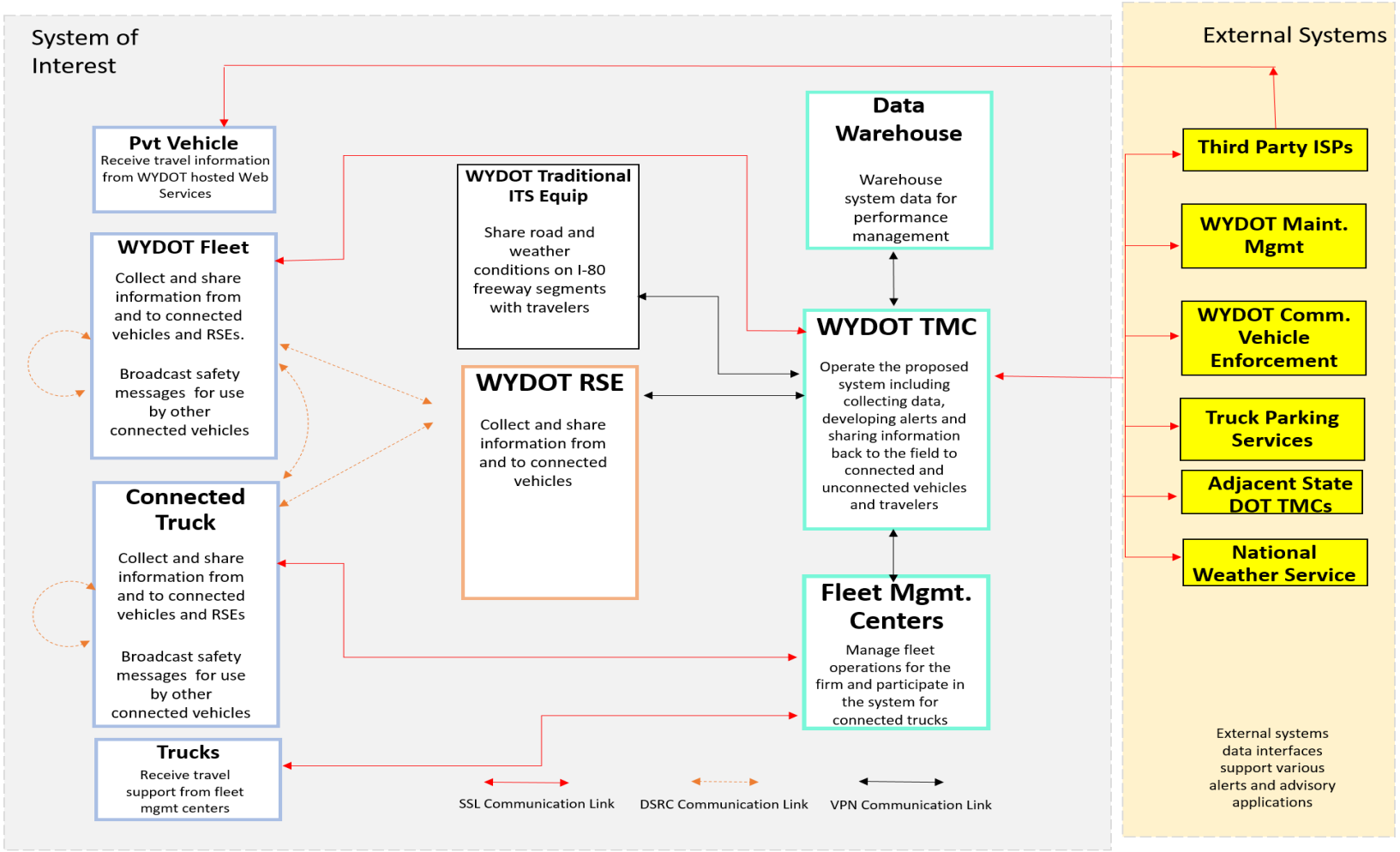

Figure 1-1. Communication Security Diagram for the CV Pilot (Source: ICF/Wyoming)

2 References

The following table lists the documents, sources and tools used to develop the concepts in this document.

Table 2-1. References

#	Documents, Sources Referenced
1	CV Reference Implementation Architecture (CVRIA), Version 2.1, www.iteris.com/cvria.
2	Systems Engineering Tool for Intelligent Transportation (SET-IT) Version 2.1.
3	Deliverable Task 2.1 Stakeholder Registry and ConOps Review Panel Roster.
4	Deliverable Task 2.2 Draft User Needs.
5	IEEE. (2016). *1609.2-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Security Services for Applications and Management Messages.* IEEE Vehicular Technology Society.
6	IEEE. (2016). *1609.3-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Networking Services.* IEEE Vehicular Technology Society.
7	IEEE. (2016). *1609.4-2016 - IEEE Standard for Wireless Access in Vehicular Environments (WAVE) - Multi-Channel Operation.* IEEE Vehicular Technology Society.
8	SAE. (2016). *J2735: Dedicated Short Range Communications (DSRC) Message Set Dictionary.* SAE International .
9	SAE. (2016). J2945/1: *Dedicated Short Range Communication (DSRC) Minimum Performance Requirements.* SAE International.
	SAE. (2014). J3067: *Candidate Improvements to Dedicated Short Range Communications (DSRC) Message Set Dictionary [SAE J2735] Using Systems Engineering Methods.* SAE International.
10	FIPS. (2004). PUB 199: *Standards for Security Categorization of Federal Information and Information Systems.* NIST.
11	FIPS. (2006). PUB 200: *Minimum Security Requirements for Federal Information and Information Systems.* NIST.

12	NIST (2013). 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations.* NIST.
13	NIST (2012). SP 800-30: Guide for Conducting Risk Assessments. NIST.
13	Deepak Gopalakrishna, et al. (2015a). *CV Pilot Deployment Program Phase 1, Concept of Operations (ConOps), ICF/Wyoming*. U.S Department of Transportation.

3 Application Communication and Data Security

Application communication and data security is critical for public confidence and acceptance of this CV pilot. Data will be collected in an environment built on preserving privacy by design. The flows that are used for each application are, where possible, based on CVRIA for V2I and V2V communication. United States Department of Transportation (USDOT) will be hosting a SCMS Proof-of-Concept that will be leveraged to support a subset of the security needs (such as IEEE 1609.2) for this CV Pilot.

3.1 Background

In order to protect pilot users' privacy and data security each application used by the pilot has been reviewed for confidentiality, integrity and availability (CIA) requirements. This is done by reviewing the individual flows that make up each application and assigning a low, medium or high ranking in each area. The CIA assessment defines the level of hardware, encryption, authentication and signature requirements for the data communications of each device.

3.1.1 Security Assessment

The information, information systems, and communications systems that form components of this pilot project must be assessed in order to determine the security requirements for the various components. The approach used by the Federal Government for classifying potential impacts and resulting security requirements, as defined in FIPS PUBS 199 and 200, are used in the assessment of CIA impacts. FIPS PUBS 199 defines these as:

- CONFIDENTIALITY: "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information..." [44 U.S.C., Sec. 3542] A loss of confidentiality is the unauthorized disclosure of information.
- INTEGRITY: "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity..." [44 U.S.C., Sec. 3542] A loss of integrity is the unauthorized modification or destruction of information. Non-repudiation is preventing users from denying their actions, e.g., the ability to prove a given user took a given action, such as sending a message. Authentication is verifying the user's identity or authorization, e.g., that the message sender is authorized to send that message.
- AVAILABILITY: "Ensuring timely and reliable access to and use of information..." [44 U.S.C., SEC. 3542] A loss of availability is the disruption of access to or use of information or an information system.

The impact assessment looks at multiple types of security threats:

- Intentional threats: both internal and external
- Accidental threats: both internal and external
- Acts of nature

The approach defined in FIPS PUBS 199 then assigns a low, medium, or high impact assessment rating for each set of information in each of the three impact areas. An impact of "not applicable" may also apply for confidentiality. For example, basic safety messages (BSM) are designed to be received by any and all neighboring equipped vehicles as well as by roadside equipment. There is no confidentiality requirement for BSM messages. The definitions of these impact levels are provided in FIPS PUBS 199.

The impact assessment for a system is then the highest impact for any information handled by the system, scored separately for each impact area. Because some confidentiality of internal information is needed to provide integrity and availability, a system, unlike information, cannot have a confidentiality assessment of "not applicable." So, for example, a server used as part of the pilot might have a rating of confidentiality: low, integrity: medium, and availability: medium. In theory, this means that a system could fall into one of 27 different combinations of security levels. The Threat Definition of V2I Architecture (still under development by Iteris and Security Innovation): Confidentiality, Integrity, Availability Analysis of Sample CVRIA Information Flows report proposes a smaller subset to reduce the need to develop security requirements for 27 different combinations.

3.1.2 Security Requirements

FIPS PUBS 200 defines an approach for identifying the appropriate types of security controls (high level requirements) for each security level in the three impact areas defined in FIPS PUBS 199. The document defines minimum requirements for Federal information and information processing systems.

The first step is to identify the specific security and privacy controls of each type that the system will require. These are defined in Security and Privacy Controls for Federal Information Systems and Organizations.

3.1.3 Risk Assessment of Threats

The methodology used for risk assessment of threats closely follows the NIST SP 800-30, with the exception of having three levels (as opposed to five levels) for both Likelihood and Impact of a threat: low, moderate, and high. This is done by rolling the lowest level into low and the highest level into high. The main reason for this action is to simplify the risk assessment, while maintaining adequate definitions for risk in the pilot given the number of types of devices that will be used. As such, three levels, rather than five, are utilized to define a reasonable set of device categories for vendors to develop that will meet or exceed the security requirement. Also, accordingly modified is the corresponding risk matrix as shown in Table 3-1 along with the rationale for those impact levels. As with any new and public system, attacks are inevitable. The approach to defining and protecting the system and software is to: first estimate the impact of all the threats, then suggest counter-measures for all the threats with moderate/high impacts 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 3-1 to calculate risk) on the system along with countermeasures. Table 9-2 has a detailed analysis of threats for the CV pilot. The pilot security team has reviewed previous attacks to advanced vehicle systems as well as recent cyber-attacks against large scale financial and retail locations to develop confidence with the threats and likelihood as well as countermeasures presented.

Table 3-1. 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.

3.1.4 Vulnerabilities Assessment for System and Software

The two type of vulnerabilities are system and software related to the CV pilot. A system vulnerability is a flaw or weakness in security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy. A software vulnerability is a mistake that can be directly used by a hacker to gain access to a system network. Common Vulnerabilities and Exposures (CVE) considers a mistake a vulnerability if it allows an attacker to use it to violate a reasonable security policy for that system.

Understanding and mitigating vulnerabilities is a key strategy for reducing cybersecurity risk. Some ways to mitigate vulnerabilities are:

- Identify vulnerable components (RSE/OBE equipment, data, applications, communications)
- Identify threat vectors (malware, hacks, rogue applications)
- System exposure (gaps between existing defense capabilities and potential threat vectors)

Based on the vulnerability severity, based on impacts to the system or software, risks are accepted or mitigated.

3.1.5 Public Key Infrastructure

The SCMS utilizes a Public Key Infrastructure (PKI) approach to support trusted and secure communications. Public key systems use asymmetric key systems. There are two separate but mathematically related keys. The private key is kept secret by its owner, while the public key may be distributed to anyone (hence the name public key). Knowledge of the public key does not enable anyone to derive the private key. Use of a public key system simplifies issues of key management and distribution, since public keys require no security. However, an infrastructure device will be required to generate and manage its private and public keys.

Users can encrypt data intended for a particular recipient by encrypting it using the recipient's public key. The data can only be unencrypted by someone who possesses the corresponding private key, i.e., the intended recipient. Messages can also be digitally signed by computing a digest of the message (a mathematically computed hash) and using the sender's private key as input to the digital signature algorithm (RSA, Elliptic Curve Digital Signature Algorithm (ECDSA), etc.). Recipients will use the message digest (computed independently from message body), the sender's public key and the digital signature attached to the message as inputs to the signature verification function. The signature verification function will compare two separate mathematical values to verify the authenticity of the signature. If the mathematical values match, then the message must have been sent by the claimed sender, as only they have their private key, and the message was not altered during transmission (since if it had been changed, the hashes would not match).

The proof-of-concept SCMS provides the PKI via elliptical curve cryptography for use by the CV Pilots. It is an important element of the solution for meeting the security requirements for each this pilot.

3.1.6 The SCMS

National Highway Traffic Safety Administration (NHTSA) is drafting a proposed rule that will address equipping light vehicles with V2V technology capable of transmitting BSM which include vehicle data such as position, speed, and heading. In order for potential such systems to be trusted, it is important to be able to verify that these messages are authentic. At the same time, privacy is very important, and the security system is being developed in such a way that prevents individual vehicles or drivers from being identified by the messages they transmit. The SCMS is a critical element of this approach. The SCMS design calls for the use of a PKI where a central authority issues credentials in the form of short-lived pseudonym certificates to certified devices (e.g., OBE on vehicles) that possess a valid enrollment certificate. These short-lived certificates are used to sign BSMs prior to transmission. The device changes these pseudonym certificates on a regular basis over the course of each trip in order to protect the end user privacy. The purpose of attaching certificates and signing each BSM is to allow the receiver to determine if the transmitter is authorized and to ensure the integrity of the signed message. This is accomplished by verifying the digital signature on the message and verifying the transmitter's short-lived certificate by following the chain of trust, verifying the transmitter has adequate credentials to send the message contents, as well as verifying that the credentials have not expired. The receiving device must also verify that the credentials of the transmitter have not been placed on a global revocation list that is managed and distributed by the SCMS.

The process for obtaining an enrollment certificate was developed in such a way that no single organization has sufficient information to re-identify a device. It will take the cooperation of two entities, e.g., in response to a court order, to re-identify a device.

The SCMS is also capable of providing V2I enrollment and application certificates to RSEs. Application certificates are required in order for the RSE to digitally sign any messages that it transmits, such as Traveler Information Message (TIM), Signal Phase and Timing (SPAT), and MAP messages. This ensures that any device receiving these messages can verify that they were transmitted by an authorized device in the CV environment. These V2I certificates are distinct from the certificates issues to vehicles (V2V certificates) because privacy is not a requirement for roadside units (RSU) as they are typically owned by a public agency or toll authority.

CAMP, LLC, as part of a cooperative agreement with USDOT, is developing the proof-of-concept SCMS, which will be operated by CAMP. Once development is completed this system will be set up and operated on behalf of the USDOT to support the CV Pilots and other research, field testing, and early deployment users. It is this SCMS that this CV pilot will interface with and use.

3.1.7 Misbehavior Detection and Certificate Revocation

Misbehavior detection is the process of detecting malfunctioning or compromised devices. This can be done by reviewing field device messages and by reviewing physical devices. Field devices

detection will be based on each applications definition of message parameters that fall outside of limits or logic (for example vehicle speeds over 200 miles per hour (MPH)). RSE and OBE physical devices can be inspected for tamper evidence as well as compromised certificates be used by unauthorized devices.

Based on misbehavior detection analysis, certificates that are no longer trusted can be added to Certificate Revocation List (CRL) or the device can be placed on the SCMS internal blacklist. The CRL is periodically updated and re-distributed to RSEs over the backhaul link or OBEs over the air. Blacklisted devices are revoked from receiving pseudonym certificates from the SCMS. Misbehavior detection will be done for RSE and OBE devices, however only OBEs will use the CRL. Misbehaving RSEs will be powered down and replaced or repaired as necessary.

Misbehavior detection and certificate revocation will not initially be supported by the SCMS and the specifications for misbehavior reporting don't currently exist. The Wyoming CV pilot will internally track misbehavior and manually remove devices as necessary. As the specifications become defined and made available within the SCMS, this capability will be formally added as part of an update to the system.

3.1.8 IEEE 1609.2

All WAVE devices (i.e., PID, OBE, RSE) shall comply with IEEE 1609.2: Standard for WAVE – Security Services for Applications and Management Messages. The TMC should also comply with IEEE 1609.2 and contain the necessary libraries, along with the necessary SCMS point of contact (POC) interface requirements. The current working version is IEEE 1609.2v3 D12. Full publication is expected in 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, TIM).
- Encrypted messages, which are used for Internet Protocol version 6 (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.
    - Web Security Agent (WSA) security profile is covered in IEEE 1609.3v3 D6.
- Mechanisms for peer-to-peer certificate distribution.

3.1.9 Privacy Concerns

Privacy, including the protection of PII, is closely linked to security. The applications and communications for the pilot are formulated to protect the privacy of the users to the highest degree possible. This is challenging in a multi-application setting, because the user may have higher privacy requirements than a specific application does and there is an additional threat to the privacy of the user when factoring in correlations between applications. Some applications by their nature will have

to reveal sensitive or user-specific information: for example, BSMs reveal vehicle location. This makes it all the more important to ensure that applications do not reveal this information unless it is absolutely necessary, as revealing the information within application A will allow it to be correlated with information from application B.

To address these concerns for broadcast and transactional unicast communications the following considerations will be made:

- Service Discovery
- Authorization
    - The definition of “authorized to use the service” will be application specific.
- Privacy
    - Not require either party to reveal sensitive information unencrypted.
    - Not contain the User’s location information unless this is necessary as part of service.
    - Not use identifiers that can be straightforwardly linked to the User’s real-world identity (vehicle identification numbers (VIN), license number, etc.).
    - Use temporary and one-time identifiers. Separate instances of the exchange shall not use identifiers (USER MAC address, User Equipment Identified (International Mobile Equipment Identify) (UE-ID (IMEI)), IP address, certificate, temporary ID, session ID, etc.) that have been used in a previous instance of the exchange.
- Integrity
- Replay / message order
- Non-repudiation / Audit
- Performance
- Removal of Misbehaving Objects

The following flow chart in Figure 3-1 demonstrates this for a transactional unicast communication:

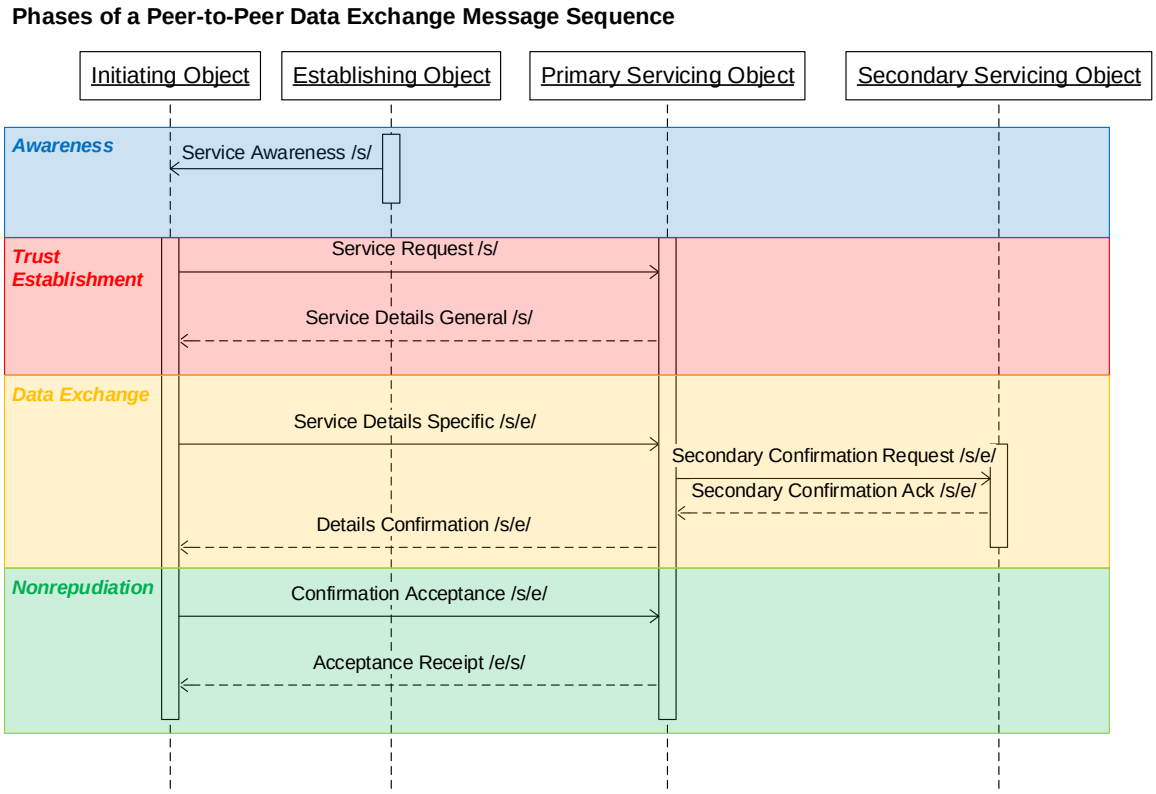

Figure 3-1. Phases of a Peer-to-Peer Data Exchange Message Sequence (Source: USDOT).

3.2 Pilot Specific Application Security Analysis

This section reviews the seven applications being used by the pilot for CIA. In each of these categories a raking of low, medium or high will be assigned. This raking will be defined by reviewing the individual flows (Table 9-1) for CIA within the application and selecting the highest level for each category. The reader is referred to the CV-Pilot ConOps document (Golapakrishna et al., 2015) for a more detailed explanation of each application. All data flows over DSRC will be signed with SCMS certificates and non-broadcast messages transmitted over DSRC will be encrypted as well as signed. Table 9-1 has the detailed flow analysis for each application.

3.2.1 Road Weather Advisories for Trucks

This application provides the capability of collecting road weather data from WYDOT Fleets and Connected Trucks and using that data to develop short term warnings or advisories that can be provided to individual commercial vehicles or to commercial vehicle dispatchers. The raw data will be processed in a controlling center (WYDOT TMC) to generate road segment-based data outputs. The

processing will also include a road weather commercial vehicle alerts algorithm to generate short time horizon alerts that will be pushed to fleet management systems and available to commercial vehicle dispatchers. In addition, the information collected can be combined with observations and forecasts from other sources to provide medium (next 2-12 hours) or long term (more than 12 hours) advisories through a variety of interfaces including web based and CV-based interfaces. While these advisories are generated for trucks, road weather advisories can also be shared with the general traveling public through existing traveler information portals.

- **Confidentiality: MEDIUM.** Some of the information shared through this application is sensitive and should be protected.
    - For WYDOT fleet vehicles only, additional information regarding the identity of the vehicle and linked location will be collected for performance measures and classified as a confidentiality of medium—therefore protected, not publicly released and will only be retained for the pilot period. This data will be encrypted before being transmitted over the air or maintained with the OBE, and it will be stored and protected at the TMC. For commercial vehicles this PII data will not be collected with a confidentiality of low.
    - Weather-related information collected through OBEs and the vehicle's own sensors are of low confidentiality. This data does not contain sensitive information and will be aggregated, validated and publically posted.
    - Road weather advisory information communicated between the TMC and WYDOT snow plows contain actionable information for snow plows that could affect decisions the snow plow drivers make. This information contains proprietary data specifically for snow plows and is medium confidentiality.
- **Integrity: HIGH.** Drivers in the area must be able to trust any road weather advisories received. If incorrect or incomplete information is received or no road advisories are provided, then drivers may proceed to drive in unsafe conditions or conditions that they are not comfortable with. This action could lead to a severe or catastrophic adverse effect on organizational operations and drivers.
- **Availability: MEDIUM.** Alternatives to road weather advisories still exists where drivers can obtain weather information, such as a third-party source. Additionally, the driver can opt to proceed traveling with the assumption that the road ahead is accessible and/or without complications. However, without the road weather advisory, a driver may continue on a route and may get stuck in slow moving traffic or on roads with unsafe driving conditions. Therefore, any information must be received within a specific timeframe in order to be of use.

3.2.2 Automatic Alerts for Emergency Responders

This application provides the capability for connected trucks to transmit an emergency message when the vehicle has been involved in a crash or other distress situation. In addition to driver initiation, an automatic crash notification feature transmits key data on the crash recorded by sensors mounted in the vehicle (e.g. deployment of airbags) without the need for involvement of the driver.

Connected trucks would attempt to provide notification via cellular communication in the corridor. In areas with inadequate cellular coverage, the emergency message is broadcast to passing CVs, who

can relay the message to other CVs as well as roadside "hotspots." Once received by WYDOT TMC (either through emergency vehicles or through the roadside equipment), the appropriate response to the vehicle situation can be carried out by emergency response services. This application allows a vehicle to forward mayday requests even in areas where no V2I infrastructure exists.

- **Confidentiality: MEDIUM.** Some of the information flows are sensitive and should be protected these are described below.
    - Information regarding the identity of the vehicle and linked location is confidential and should be protected. This data will be only used for drivers that opt-in for automated alerts or manually sent, giving this data a confidentiality of medium.
    - General incident-related information including Global Positioning System (GPS) location and airbag deployment status collected through OBEs and the vehicle's own sensors are of low confidentiality as they need to be shared with respective response agency or other CVs and don't contain PII.
    - Incident information communications between the WYDOT TMC and local Emergency Medical Services (EMS) center regarding vehicle location information and routing information should be treated as medium confidentiality in order to protect personal information from people involved in the crash.
- **Integrity: HIGH.** These alerts indicate a crash or distress situation has occurred and where it is located. In order for emergency responders to respond in a timely manner, the information needs to be accurate and complete. If the information does not meet the required level of integrity, response time may be affected and this could lead to an escalation of severity of the incident, such as loss of life or limb of a person.
- **Availability: MEDIUM.** Ideally, the availability for this application would be high in order to be able to respond to crashes or distress situations as quickly as possible. However, this is not currently possible since the presence of this application can only benefit users by reporting crashes in a timelier manner.

3.2.3 CV-enabled Weather-Responsive VSL

This application uses road weather information from connected trucks and WYDOT Fleet vehicles as well as current and historical data from multiple sources to determine the appropriate current safe speed and other traffic management strategies. The application provides real-time information on appropriate speeds for current conditions and warns drivers of coming road conditions.

- **Confidentiality: MEDIUM.** Information to and from the variable speed limit applications may be sensitive and should be protected.
    - Control commands information going to VSL RSE from the TMC may contain some proprietary information based on the equipment used but is considered of low confidentiality.
    - Snow plow and Highway Patrol suggested Speed Limit information going to the WYDOT TMC contains proprietary and sensitive information and is considered of medium confidentiality for the purposes of this pilot.

  - VSL information being broadcast to vehicles along the roadway would be considered low in confidentiality since speed limit information is purposefully being distributed to any and all drivers.
- **Integrity: HIGH.** Drivers in a variable speed limit zone rely on speed limits to determine safe driving conditions. If the information provided to the driver were inaccurate it may cause the driver to travel at unsafe speeds in zones with lowered drivability conditions. This unsafe behavior could cause a crash which would have severe or catastrophic adverse effect on organizational operations and drivers, such as loss of life or limb to a person. Additionally, if an unauthorized vehicle is able to send requests to change the speed limit they could potentially slow down traffic dramatically, causing delays through the variable speed limit zone.
- **Availability: MEDIUM.** The alternative to variable speed limit signs is traditional signage and no ability to alter speed limits based on current weather and road conditions. The difference between traditional signage and variable speed limits is significant. However, the use of traditional signage may be catastrophic only under certain scenarios, such as when sudden changes in road conditions may cause deadly crashes. Because missing a message may result in loss of life or limb, a high availability rating is recommended in order for the system to work correctly. Since a high availability is not possible due to the nature of the communication medium and the fact that having the system in place will only have a positive impact when communications work correctly, a medium availability seems appropriate here.

3.2.4 Spot Weather Impact Warning

This application will alert drivers to unsafe conditions or road closures at specific points on the downstream roadway as a result of weather-related impacts (e.g., high winds, flood conditions, ice, and fog). The application is designed to use standalone weather systems to warn drivers about inclement weather conditions that may impact travel conditions. Real-time weather information is collected via RWIS or via vehicle-based probe data from commercial, specialty, or public vehicles. The information is processed to determine the nature of the alert or warning to be delivered and then communicated to CVs. If the warning includes a road closure, diversion information can be provided. For non-equipped vehicles the alerts or warnings will be provided via roadway signage or through third-party applications.

- **Confidentiality: MEDIUM.** The communications from the WYDOT snow plows and Highway Patrol could contain some sensitive or proprietary information. The communications from the commercial vehicle connected trucks does not contain sensitive or proprietary information.
  - Information regarding the identity of the vehicle and linked location is confidential and should be protected. This will be collected for performance evaluation for the duration of the pilot only for WYDOT vehicles (this vehicle identity information will not be collected for commercial connected vehicles). This data should be considered medium confidentiality.
  - Information flowing between the snow plows, Highway Patrol, commercial CVs, and the WYDOT RSE regarding road information can contain information such as spot weather codes and road conditions and should be considered as low confidentiality.

    - Information from the WYPDOT RSE regarding spot weather information being broadcast to all vehicles is purposefully broadcast to everyone and should be considered as low confidentiality.
- **Integrity: HIGH.** Drivers in the area must be able to rely on spot weather impact warnings received. If incorrect information is received or no spot weather impact warnings are seen, then drivers may proceed to drive in unsafe conditions or conditions that they are not comfortable with. This action could lead to severe or catastrophic adverse effect on organizational operations and drivers, such as loss of life or limb of a person.
- **Availability: MEDIUM.** If no spot weather impact warning is present, the driver may not be aware of upcoming road conditions that may impact their travel. This information needs to be mostly available to the system for this application to work correctly.

3.2.5 Work Zone Warnings

This application provides information about the conditions that exist in a work zone to vehicles that are approaching the work zone. This application provides approaching vehicles with information about work zone activities that may result in unsafe conditions to the vehicle, such as obstructions in the vehicle's travel lane, lane closures, lane shifts, speed reductions, or vehicles entering/exiting the work zone.

- **Confidentiality: MEDIUM.** Most of the data for work zones will be broadcast data available to everyone. However, some data flows from the TMC to the WYDOT RSE may contain sensitive or proprietary information.
    - Information flowing from the WYDOT TMC to the WYDOT RSE contains some limited proprietary information on the operation of the RSE and contains sensitive information that needs to be encrypted. This needs to be protect with confidentiality of medium.
    - Information broadcast from WYDOT RSE to vehicle OBE's are low confidentiality due to the fact that this information is purposefully being broadcast to all vehicles.
- **Integrity: HIGH.** Work zone warnings provide drivers with upcoming work zone information. If this information is inaccurate, the impact may result in traffic slowing in an area where no work is being performed or drivers not paying attention to traditional signage. In the case of the latter, drivers may cause a crash in a work zone, potentially leading to severe or catastrophic adverse effect on organizational operations and drivers, such as the loss of life or limb to a person.
- **Availability: LOW.** If the work zone warnings are unavailable, traditional signage and construction zone warnings with flashing lights to indicate an upcoming work zone are still available, so the system availability is not required for driver safety. Since this is the case a low for availability seems warranted.

3.2.6 Situational Awareness

The application determines if the general road conditions (not at specific points) measured by other vehicles represent a potential safety hazard for the vehicle containing the application. To enable this application, other vehicles broadcast relevant road condition information, such as fog, icy roads,

slowing speeds, or brake lights. This application supports the capability for CVs to share situational awareness information even in areas where no roadside communications infrastructure exists. This application can be useful to vehicles that are not fully equipped with sensors, or vehicles entering an area with hazardous conditions.

- **Confidentiality: LOW.** The data for this application is intentionally transmitted to everyone by broadcast via DSRC for other CVs and RSEs to receive.
- **Integrity: HIGH.** The data for this application contains general information about vehicle speed, direction, and environmental data in order to provide information to the driver such as collision warning information. This information could help the driver avoid crashes with other vehicles and allow vehicles to harmonize speeds to slow delays in traffic. If this data were to be compromised, then either no warning may be sent or false warnings may be sent to the driver that may cause the driver to no longer trust the system. Since this is the case, a high integrity seems like the best option.
- **Availability: MEDIUM.** Data to avoid collision warning must be available to the driver as soon as possible in order to avoid the collision. Collision avoidance alerts require the application. Only a wired connection can have an availability of high. Wireless DSRC can't achieve high availability because the interference and jamming from other devices can easily make the signal unavailable. A high availability would be selected if it were an option for DSRC. Since the high available is not an option, medium availability is the best option.

3.2.7 Freight-Specific Dynamic Travel Planning

This application provides both pre-trip and en-route travel planning, routing, and commercial vehicle related traveler information. Both real-time and static information can be provided directly to fleet managers, to mobile devices used by commercial vehicle operators, or directly to in-vehicle systems as commercial vehicles approach roadway exits with key facilities such as parking. The application also supports advisories to specific categories of advisories (restrictions on lightweight or high-profile vehicles for example).

- **Confidentiality: MEDIUM.** The data for this application may contain sensitive or proprietary information transmitted to and from the commercial vehicle operator portal. This data is not being sent via DSRC; it is being made available via a portal web site. This data could be leveraged by freight centers to send to fleets via existing protected services.
- **Integrity: MEDIUM.** Commercial trucks and operators who are traveling in an area covered by the freight-specific dynamic travel planning application will rely on the application to provide accurate truck parking and travel information. If this information is not accurate it may lead to travel delays and/or truck parking problems in areas with limited availability during road closures.
- **Availability: MEDIUM.** Commercial truck drivers who have been traveling regularly along the I-80 corridor through Wyoming have become accustomed to parking to wait out road closures. If some messages go missing, there may be an impact to local communities but no loss of life or serious economic impacts.

4 Software and OS Security for Pilot Deployment Devices

4.1 Overview and goals

This section describes hardware, software, and OS security for systems that run DSRC applications that use cryptographic private keys and certificates in the format specified by IEEE Std 1609.2-2016 and that are issued by the SCMS.

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 HSM is further explained in section 4.4.

The goals of these requirements are:

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

This document does not address processes for certifying that systems meet the requirements; its purpose is simply to state the requirements.

4.2 Architectures

The requirements below cover three architectures.

- **Integrated architecture** (Figure 4-1): The host processor and the HSM are the same processor.

- **Connected architecture** (Figure 4-2): 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.
- **Networked architecture** (Figure 4-3): The host processor and the HSM are different and are connected over a network or bus that has other processors connected to it.

The document provides requirements for the host processor and the HSM separately in sections 4.3 and 4.4 respectively, and then provides architecture-specific requirements in section 4.5.

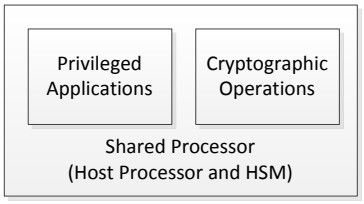

Figure 4-1. Integrated architecture

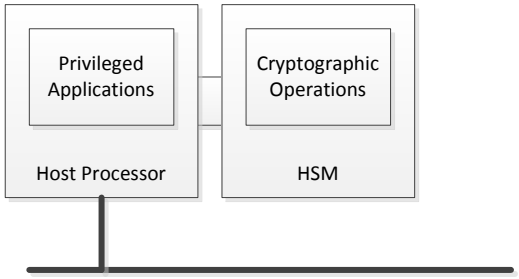

Figure 4-2. Connected architecture Integrated architecture

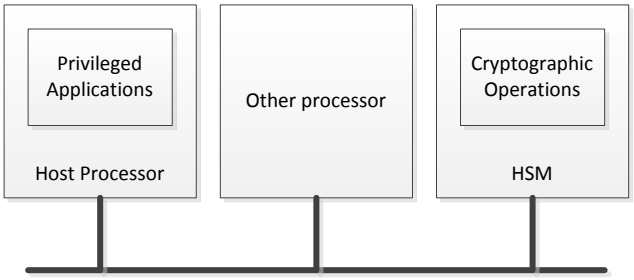

Figure 4-3. Networked architecture

4.3 Host processor

4.3.1 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)[1] mechanism of the Trusted Computing Group (TCG)'s Trusted Platform Module (TPM).[2]

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.

4.3.2 Operating system

The host processor OS shall meet the following requirements (derived from FIPS 140-2):

- The OS shall support roles that are used as specified below. Each privileged application shall map to a role.
- The discretionary access control mechanisms of the OS shall be configured to:
    - Specify the set of roles that can execute stored software and firmware.
    - 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.

[1] Shielded locations to protect the contents of a log of events that affect the security state of a platform at least through the boot process.
[2] An architecture for cryptographic modules and techniques for hardware based root of trust at the edge of the network (OBE/RSE).

- 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 write private key material to the HSM.
- The OS may allow roles to operate without explicit authentication, or may require authentication if that software or firmware is signed.
- The OS shall not allow processes that modify executing processes without explicit authentication
- The OS shall not allow processes that read private cryptographic key material from the HSM (NOTE: The HSM should also not provide this functionality).

4.3.3 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 1) ensures that the software is signed by an authority with appropriate permissions before 2) proceeding with the installation or rejecting the installation if the signature or any of the validity checks on the software or its signing certificate fail.
- If this approach is taken, 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.
- If this approach is taken, the device shall require that the user is authenticated using two-factor authentication and that at least one of the two factors is protected by cryptographic hardware on the device.

NOTE: The host processor may optionally not require a user to provide two-factor authentication to perform a factory reset (i.e., to wipe all software, all sensitive data, and all secret cryptographic material). The ability to perform a factory reset without two factor authentication is necessary to allow the device to be reused in the event of a failure of the two factor authentication subsystem. The host processor may allow a user to perform a factory reset without any authentication if the mechanism for a reset guarantees that the user is physically present.

4.4 HSM

The HSM shall meet the requirements for an OS 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 (MAC) or digital signature algorithm) shall be applied to all cryptographic software and firmware components within the HSM.
    - The 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 OS that meets the functional requirements specified in the Protection Profiles listed in FIPS 140-2 Annex B and is capable of evaluation at the Common Criteria Evaluation Assurance Level 2 (CC EAL2), or an equivalent trusted OS.
- To protect plaintext data, cryptographic software and firmware, cryptographic keys, and authentication data, the discretionary access control mechanisms of the OS 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 OS 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-OS processes (i.e., operator-initiated), cryptographic or not.
- The OS shall prevent operators and executing processes from reading cryptographic software stored within the cryptographic boundary.

4.5 Users rights requirements for RSE and OBE

For the ICF/Wyoming pilot the OS on the device (RSE or OBE) will manage process separation, the HSM need only maintain two roles:

- User (who can execute software and firmware, write and delete cryptographic keys, and install signed software and firmware)
    - These users will be part of the Information Technology (IT) team at WYDOT
- Security Officer (who can install unsigned software and firmware)
    - This role will be restricted to the pilot architect and lead developer

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 Hardware Security

Hardware used for RSE and OBE will be selected based on the analysis conducted in Section 3 for the applications and data they will host.

5.1.1 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. FIPS 140-2 covers the questions asked by the USDOT during the "Preparing a Security Operational Concept for CV Deployments" webinar presented on 9 December 2015, including protections to prevent device tampering such as tamper evident protections and tamper resistant protections. This section will give an overview of FIPS 140-2 and recommended FIPS 140-2 levels for each type of device.

5.1.2 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.

5.1.3 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.

5.1.4 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 OS evaluated at CC EAL2 (or higher). Level 2 also adds the requirement of role-based authentication to perform a specific set of services appropriate to the role.

5.1.5 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 OS evaluated at CC EAL 3 (or higher). Level 3 also requires identify-based authentication in addition to the role-based authentication of Level 2. Level 3 also requires that Critical Security Parameter (CSP) entry and output are executed using physically separated ports, or enter and exit in encrypted form.

5.1.6 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 OS evaluated at CC EAL 4 (or higher).

Table 5-1. 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
Operational Environment	Single operator. Executable code. Approved integrity technique.	Referenced PPs evaluated at EAL2 with specified discretionary access control mechanisms and auditing.	Referenced PPs plus trusted path evaluated at EAL3 plus security policy modeling.	Referenced PPs plus trusted path evaluated at EAL4.
Cryptographic Key Management	Key management mechanisms: random number and key generation, key establishment, key distribution, key entry/output, key storage, and key zeroization.			
	Secret and private keys established using manual methods may be entered or output in plaintext form.		Secret and private keys established using manual methods shall be entered or output encrypted or with split knowledge procedures.	
EMI/EMC	47 CFR FCC Part 15. Subpart B, Class A (Business use). Applicable FCC requirements (for radio).		47 CFR FCC Part 15. Subpart B, Class B (Home use).	
Self-Tests	Power-up tests: cryptographic algorithm tests, software/firmware integrity tests, critical functions tests. Conditional tests.			
Design Assurance	Configuration management (CM). Secure installation and generation. Design and policy correspondence. Guidance documents.	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.			

5.1.7 Device Classifications

Devices that are appropriate for use with CIA analysis of low, medium, medium (LMM) are used for smartphone applications with PIDs. Low confidentiality is appropriate for flows that are broadcast to a wide audience. Integrity of medium allows for false messages being accepted, resulting in false positives and false negatives which 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. PID devices work with applications appropriate for an LMM classification and FIPS 140-2 Level 1 standard is consistent with other information flow and device classification projects such as the Threat Definition for V2I Architecture Projects.

Devices that are appropriate for use with CIA analysis of medium, medium, medium (MMM) are being used for commercial vehicle OBEs. Moderate confidentially indicates that flows could, but not necessarily, contain: i) information that the owner has a reasonable desire not be disclosed, such as PII; ii) sensitive business information that would allow someone to gain some advantage; and/or iii) personal financial information that could lead to personal financial loss. Integrity of medium allows for false messages being accepted resulting in false positives and false negatives, which increase physical risk without directly causing physical harm. Commercial vehicle OBE devices work with applications appropriate for an MMM classification and FIPS 140-2 Level 2 standard is consistent with other information flow and device classification projects such as the Threat Definition for V2I Architecture Projects.

Devices that are appropriate for use with CIA analysis of medium, high, medium (MHM) are being used for RSEs, snow plows and Highway Patrol vehicles. These devices all process data that has an increased integrity component. This is largely due to these devices processing data that updates road conditions for the safety of the driving public. Moderate confidentially indicates that flows could, but not necessarily, contain information such as PII 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. RSEs, snow plows and Highway Patrol vehicles devices work with applications appropriate for an MHM classification and FIPS 140-2 Level 3 standard is consistent with other information flow and device classification projects such as the Threat Definition for V2I Architecture Projects.

5.1.8 Device Hardware Security Requirements

Different devices require different hardware security requirements depending on the cryptographic needs and threats, see Table 5-2. Requirements may also need to be evaluated and downgraded based on assessed risk—i.e., Confidentiality (C), Integrity (I), and Availability (A)—and development costs. The team believes that this also applies to the V2X devices in this CV Pilot. The recommended FIPS 140-2 level depends on the device functionality, cost considerations, and risk.

Table 5-2. Device hardware security requirements

Object Name	Security Class	Rationale
Personal Information Device	1: C Low, I Medium, A Medium	Level 1 C - Most flows are low, cell phones will need to implement controls with OS security rather than hardware security. I - Most applications require medium integrity in order to ensure communications are accurate A - All application communications require at a minimum, medium availability.
Roadside infrastructure (RSE-s and network connections)	3: C Medium, I High, A Medium	Level 3 C - Most flows are medium, due to some sensitive or proprietary information between the WYDOT TMC and RSE communications I - Most applications require high integrity in order to ensure communications are accurate A - All application communications require at a minimum, medium availability.
Highway Patrol and Snow Plows OBE	3: C Medium, I High, A Medium	Level 3 C - Most flows are medium, due to some sensitive or proprietary information between the highway patrol/snow plows and the WYDOT TMC communications I - Most applications require high integrity in order to ensure communications are accurate A - All application communications require at a minimum, medium availability.
Commercial Vehicle OBE	2: C Medium, I Medium, A Medium	Level 2 C - Most flows are low, but due to some personal information and privacy concerns medium seems reasonable. I – Flows that are being pushed from the vehicle's OBE only require medium integrity. A - Application communications such as situational awareness require at a minimum, medium availability.

6 Network, Database and Center Security

This section will describe the key concepts for the proposed system, focusing on the new security requirements that are needed to support the changes identified in sections three and four. Security requirements for the proposed system will be listed for the Data Center in charge of storing the Data Warehouse, Data Clearinghouse, and any other devices storing data related to the CV pilot. Requirements will also be listed for the database and network transmission of data related to the CV pilot.

6.1 Center Security

The center security system will comprise of physical restrictions to the main center. Physical restrictions include only authorized data center managers having access to the physical hardware. Additionally, any servers and hosts that support the CV Pilot program will be registered in a database that contains contact information and details about any PII contained within the database.

People who are allowed to access the data center must have verified background security checks completed with an approved local authority such as the Wyoming Department of Criminal Investigation. Contractors who need access to the center to perform support functions on an infrequent basis will not be required to have a background check but will not be allowed access to the center without being accompanied by an escort who is background verified.

Consultants who remotely access systems within the data center must comply with the WYDOT's Computer Environment Access and Non-Disclosure Agreement, a copy of which is included as Appendix A.

In some cases, systems may be hosted with cloud service providers. These providers must have an approved data center security policy that addresses physical access and non-disclosure.

6.2 Database Security

WYDOT will host an Oracle database responsible for the storage and distribution of all CV data. For the CV Pilot program an analysis of each data field will be performed. If it is determined that the field could contain sensitive, proprietary, or PII, the field will be marked and any data added or stored to the field will be required to be encrypted.

Symmetric-key locking using Advanced Encryption Standard (AES) or Triple Data Encryption Standard (3DES) at the column level or table space will be required of any database that stores PII.

All server systems within the data center, including the systems that support the Oracle database, will have OS and application patches applied on a regular basis, although critical patches are installed as soon as practical. They may be put off to accommodate critical TMC functions.

Critical systems are maintained in geographically separate cities for redundancy and to ensure systems can be recovered in the event of a disaster.

Backups shall be performed on a daily basis and stored in a fireproof locked vault/safe. AII information on backup media shall be encrypted, whether the backup media is part of WYDOT's rotation or a cloud hosted service. Media retention should be a minimum of 3 months.

Database backups are currently maintained for several weeks and include a combination of internal binary-level backups and exports.

Developers who access the database must have a reason to access the data and sign a Computer Environment Access and Non-Disclosure Agreement with WYDOT. Developers and consultants will be assigned unique database accounts with appropriately restricted access to information.

The Oracle database will implement audit logging for appropriate PII-related information.

6.3 Network Security

Network security for the CV pilot study will be achieved through a combination of using SSL, firewalls, site to site VPNs and the use of SCMS-issued certificates to sign and encrypt (IEEE 1609.2) data transmissions.

Firewalls that prevent network access to CV data must be maintained and patched on a monthly basis. Critical patches will be applied as soon as practical. Strict access control lists will be maintained and periodically reviewed for relevancy.

Resources that are made available to outside entities must be placed in a demilitarized zone (DMZ) with firewall separation maintained between the CV systems.

Network resources not housed in a secure datacenter will be reviewed to determine the risk level and measures will be taken to assure proper physical access requirements are met.

6.4 General Security

WYDOT and the State of Wyoming employ industry accepted best practices for ensuring a safe computing environment. All State of Wyoming employees are required to review periodic online training materials and demonstrate mastery of skills learned within the courses. These courses focus on such things as awareness to phishing scams, protection of sensitive data, proper use of computing resources and more.

The Geographic Information System (GIS)/ITS Program has a private network separated by firewalls from all other computing resources in state government. GIS/ITS Program personnel will apply patches to servers and desktop computers in alignment with vendor patches.

WYDOT had an active security audit underway during January and February of 2016 to evaluate threats across the IT, Telecom, GIS/ITS, and Traffic systems. Auditors have been given access to internal systems and roadside systems in an effort to find any potential weaknesses. Preliminary results are very favorable for the GIS/ITS systems that will support the CV project. Any problems noted by the security audit must be addressed before any CV data is collected or stored and periodic audits must be scheduled. Based on the result of this audit Intrusion Detection Sensor (IDS) technology will be considered for the network and selected hosts.

Passwords shall be changed every 30 days and must meet complexity requirements (upper and lower case letters with at least 1 special character and a minimum of 8 characters in length) and shall not be shared with others.

Antivirus is centrally administered and configured such that the end users and server systems cannot modify ability or functionality. All alerts are sent to a central administrator for fast response.

When people leave the program, access to systems is removed and shared system passwords are changed to protect the program and the individual who left the program.

7 Privacy Management

7.1 Privacy Overview

This section covers the individual privacy considerations for V2X communications and application data. The section focuses on the privacy by design aspects of the SCMS POC and specific application considerations where data could be seen as PII-related or some other privacy intrusion.

7.2 Standards

The privacy guidance standard provided in NIST Special Publication 800-53 Rev 4 with the Differential Mobility Analysis (DMA) bundle privacy reporting criteria is the set of quantifiable guidelines for data privacy used in this pilot. The framework laid out in this report defines the structured Privacy Management.

7.3 Privacy Requirements by User Class

With the ICF/Wyoming Pilot there are distinct classes of users that have unique privacy requirements based on employment contracts and public privacy expectations. Table 7-1 identifies these groups of users and provide short description of privacy expectations.

Table 7-1. Privacy Expectations of User Groups for the WYDOT CV Pilot.

User Group	Owner	Short Description
		Centers
1. TMC - Operators	WYDOT	WYDOT staff on the job have a low expectation of privacy
2. TMC - Traveler Information	WYDOT	WYDOT staff on the job have a low expectation of privacy
3. TMC - Weather Providers	WYDOT	WYDOT staff on the job have a low expectation of privacy
4. Highway Patrol - Dispatch	WYDOT	Highway Patrol staff on the job have a low expectation of privacy
5. Maintenance - Dispatch	WYDOT	WYDOT staff on the job have a low expectation of privacy

User Group	Owner	Short Description
6. ITS Maintenance	WYDOT	WYDOT staff on the job have a low expectation of privacy
7. Adjacent State DOT Centers	Colorado, Utah and Nebraska	Adjacent state DOT centers expect to be identified. The privacy of individual users is protected.
8. Fleet Management Centers - CVOP Only	Various	This information will be posted through a web site and users will expect to be identified by username internally to WYDOT. Logs of CVOP interactions will be maintained privately inside WYDOT.
9. Fleet Management Centers - Pilot Users	Various	These users will transmit data to fleet drivers and have a low expectation of privacy
10. Truck Parking Facility Operators	Various	Private truck parking facility managers along I-80 corridor will have low expectations of privacy
11. NWS Forecast Offices	NWS	Systems and personnel at the NWS Forecast Offices in the I-80 Corridor will have a low expectation of privacy
12. TMC – Performance Management	WYDOT	Systems and personnel required to support performance management, data archiving, and system evaluation needs during the pilot will have a low expectation of privacy
13. Wyoming Telecommunica-tions and IT Programs	State of Wyoming	Systems and users responsible for statewide communication linkage will have a low expectation of privacy
14. Special Event Venues	Various	Systems and personnel at arenas, universities and major employers will have a low expectation of privacy
		Field
1. Maintenance Supervisors	WYDOT	Maintenance supervisors in districts who are responsible for tactical operations will have a low expectation of privacy
2. Snow Plow Operators	WYDOT	Operators of snow plow vehicles who are on the frontlines of weather event response will have a low expectation of privacy. They will be identified with location, speed, heading, and probe data.
3. Highway Patrol - Field	WYDOT	Operators of highway patrol cars on I-80 who are on the frontlines for incident response will have a low expectation of privacy with respect to the WYDOT TMC. They will be identified with location, speed, heading, and probe data. They will expect

User Group	Owner	Short Description
		privacy with respect sharing information about them to the traveling public. The unicast communications will need to be signed and encrypted. Broadcast communications will be signed, but not encrypted.
4. Commercial Truck Drivers	Various	Commercial truck drivers who travel the I-80 corridor as part of their freight movement will have a high expectation of privacy for vehicle telemetric data over DSRC. The expectations of privacy over private satellite or cellular communication with dispatch center will have a very low expectation of privacy.
5. Personal Auto Travelers	Various	Personal auto travelers who travel the I-80 corridor as part of the trip will communicate via PID (cellular communications) which provide moderate protections of privacy. The pilot will protect privacy at similar levels with cellular applications.
		Wide area users
1. 511 Phone, App and Website Users and Media	Various	General users of WYDOT's travel information system services. This group includes users of various WYDOT pre-trip traveler information services including 511 phone, website and app. These users will have a low expectation of privacy protection.

7.4 Privacy Management

Users' privacy will be managed through the collection of only required data, aggregated where possible to further protect individual privacy. An example of this is to provide a count of CVs that pass an RSE to the Center rather than provide individual vehicle data to the Center to calculate the count. Once data is collected it will be encrypted both over the air for unicast data and on the wire to the Center (using IPSEC VPN technology) to protect privacy. To protect user data over DSRC radio communications the pilot will use the USDOT SCMS POC system to sign communication and provide certificates for encryption. More details about the SCMS PKI system are provided in section 3.1.5.

7.4.1 PII Data

PII, defined as any data emitted, collected, or stored that can be used alone, or in combination with other data, to distinguish or trace an individual's identity, will be only collected where necessary to demonstrate the effectiveness of CV during the pilot phase. This will be needed for some of the performance measurements required to demonstrate the safety improvements of the system. For this pilot, WYDOT's fleet vehicles will be used for performance measures and data will be collected to track individual vehicles' BSM data as well as weather data. There are other occasions where PII can be developed by the aggregation of data from multiple sources. For example, if an incident were to occur in view of a camera and RSE these two data feeds could be aggregated to produce PII. This is

true with general travel outside of the CV pilot and the pilot does not add privacy protections to remove these currently available systems. The data collected containing PII for performance measurement will be encrypted in transmission as well as in storage to protect privacy.

A key concept in privacy analysis is proper handling of PII. PII is any information that can be used to distinguish or trace an individual's identity. A piece of data may be considered PII even if it cannot be used by itself to track an individual. The challenge with PII is recording only what is necessary to achieve the experiment or deployment functions, but still having the required data. Also, what is considered PII, how should it be handled, and how should it be archived? First, how this data is derived should be covered.

Take for instance the case of recording vehicle information in an RP or SP (revealed or stated preference) survey of driving patterns. Recording make/model/color of a vehicle alone may not be enough to identify an individual, but when combined with GPS traces, could identify the home, work, or any other location that the user travels on a routine basis. For this reason, any information that can be used in conjunction with other data to identify or track an individual will be considered PII. The following sections describe types of PII and examples from the CV pilot.

7.4.1.1 *Non-PII*

This data cannot be traced back to an individual. This includes time zone, traffic count information, general trends on network conditions, date and time.

7.4.1.2 *PII*

PII is information that alone, or in combinationwith other data, can be used to distinguish or trace an individual's identity, such as their name, VIN, and telephone numbers.

7.4.1.3 *Locational-PII*

Information that alone, or in combination with other data, can be used to track an individual at a particular location. This includes GPS tracking information (Latitude/Longitude), roadway video data, video of faces, in-vehicle video.

7.4.1.4 *Sensitive Personally Identifiable Information (SPII)*

SPII is a subset of PII, which if lost, compromised or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual. Social Security Number (SSN), passport number, and driver's license number are always SPII. These require stricter handling guidelines because of the increased harm to an individual if the data are disclosed. The ICF/Wyoming pilot will not use SPII data.

7.4.2 Pilot Data Collected, Transmitted, and Accessed

Data for the CV pilot will be collected on equipped vehicles at the OBE; data will only be stored encrypted on the OBE for up to the last rolling 10 minutes. PID users in the pilot will not have DSRC

radios and will not be collecting data for the pilot. This data will be communicated to other vehicles and to the TMC as described below:

- WYDOT Fleet used for pilot activities and performance evaluation
  - Data Collected
    - Vehicle Telematics date from the Controller Area Network (CAN)/OBD II bus and other sensors
    - Atmospheric and road condition data from sensors
    - Location/Time data from GPS sensors
  - Data Communicated
    - V2V data will be communicated to vehicles in DSRC range
      - BSM part 1/2 data
      - Emergency Alert of accident
        - GPS location, time, BSM part 1/2 data
    - V2I data communicated with TMC
      - Limited to road weather, work zone, atmospheric data, VSLs, truck parking, and traffic flow
      - Vehicle telematics data (PII)
      - Vehicle Specific Identifier may be needed for performance evaluation (PII)
      - Emergency Alert of accident
        - GPS location, time, BSM part 1/2 data
- Commercial Fleet used for pilot activities
  - Data Collected
    - Vehicle Telematics date from the CAN/OBD II bus and other sensors
    - Atmospheric and road condition data from sensors
    - Location/Time data from GPS sensors
  - Data Communicated
    - V2V data will be communicated to vehicles in DSRC range
      - BSM part 1/2 data
      - Emergency Alert of accident
        - GPS location, time, BSM part 1/2 data
    - V2I data communicated with TMC
      - Limited to road weather, work zone, atmospheric data, VSLs, truck parking, and traffic flow
      - Emergency Alert of accident
        - GPS location, time, BSM part 1/2 data
    - V2I data communicated with private fleet management
      - Road weather, work zone, atmospheric data, VSLs, truck parking, and traffic flow from CVOP
- PID users with the pilot activities
  - Data Collected
    - none
  - Data Communicated

- V2V data will be communicated to vehicles in DSRC range
  - None (will not have DSRC capabilities)
- V2I data communicated with TMC
  - Limited to receiving road weather, work zone, atmospheric data, VSLs, truck parking, and traffic flow
  - Emergency Alert of accident can be sent via text or email
    - GPS location, time, note

The TMC will encrypt CV data that is personally identifiable and the servers/databases that house this data will be assessable only to TMC staff who have had a background check conducted and have a need to know. The data will also be used by the pilot development and performance management team. The data will be shared with USDOT after being sanitized of PII for evaluation.

7.4.3 Use of Data Collected

PII can be derived from a number of data sources. This section will describe a few data elements and what measures can be taken to ensure a privacy-secured dataset. The data collected from this pilot will be used to set safe speed limits, notify drivers of unsafe road conditions due to surface and atmospheric conditions, notify drivers of upcoming work zones, send information to emergency responders about a crash, and notify drivers of road closures with parking availability. For this CV pilot, data that is collected and provided to the Research Data Environment (RDE) will be anonymized by removing data points at the beginning, end, and stopping points for drives. The beginning/end will be truncated randomly three to ten minutes and speeds under 20 MPH will not be collected. With this pilot being for the I-80 corridor, these constraints will not adversely affect the performance data, safety application or traveler information systems. Non broadcast data will be both signed and encrypted during transit. Broadcast data will be only signed during transit. PII data will be encrypted for storage as well as transit.

7.4.3.1 *Survey Data*

Data collected directly through participant surveys are a major source of privacy concern. This will contain PII. This information is important to collect for the performance measures part of the ICF/Wyoming pilot and will contain information such as address, telephone number and name, which will not be released to the general public. Surveys will include other types of information, such as opinions about the deployment itself, general driving or travel experiences, or familiarity with the area, that can also be of a sensitive nature, such as opinions about the deployment itself, general driving or travel experiences, or familiarity with the area. These pieces of information will only be linked to the participant's PII through a privately held code that is not released to outside agencies. By doing this, outside agencies will not be able to link information such as age, gender, income, education level, etc. back to an individual. Since the link between the user and their information is kept safely away from the dataset, PII will not be released to individuals acquiring the data after a large scale data release.

7.4.3.2 *GPS Trajectories*

GPS location data can be acquired through a number of different means, the most prominent for the CV pilot deployment is through DSRC transmitted BSM intended for V2V or V2I communications. Another form is via cellular communication. Many applications now use smartphone applications (e.g., Waze, Google maps, Instamapper) that relay information through the 4G network. There are a few ways that this sensitive data can get into the wrong hands. The obvious way for this data to be obtained is through data release after the pilot program for general research on the RDE. Measures in the RDE will be in place to reduce the level of PII that is included in large time-series GPS files.

During this CV pilot, a two-month sample of driving behavior for a small number of vehicles over a wide area could contain sensitive location information that an individual would not want released into a large dataset: home, work, children's school, etc. By finding the most commonly visited locations, and tying BSM data such as vehicle size and system capabilities, a malicious user could tie normal travel patterns back to an individual on the road (for example, if the data file contains a windshield wiper setting in the BSM part 2, they can look up what car models send these messages and look for those vehicle types along the same route that the GPS traces show). All of the data made available for public release will be reviewed and cleaned for PII. This is why the data will be truncated as described in 7.4.3.

7.4.3.2.1 De-Identification

The preeminent method for transitioning between complete GPS travel data to secure GPS traces is to use a de-identification method. These methods generally remove any data that can lead to someone being able to determine through statistical methods important locations or predict future travel from the historic GPS data. It is also important to keep the information that would be useful (to the fullest extent possible) for future research. Any points within a certain distance threshold of a destination would also be removed, as the destination can be easily estimated from the trajectory of the approaching points. Not all important locations can be determined by vehicle stops; many times the driver turns around in a driveway, U-turns at an important road, or picks up another individual from their dwelling. Again, a number of procedures can be done to take care of these issues. By removing GPS traces depending on land use type (residential or school), it is easier to remove those points that may have privacy considerations. Also, removing GPS trajectories where a 180-degree turn was just performed oftentimes removes a pick-up or drop-off occurrence. Another concept (which removes points based on how many intersections a user has passed through (hence adding uncertainty)) can also help anonymize travel data. Still, this may not be enough de-identification for a large scale data release due to historic travel patterns creating noticeable trends in data that may not show in a one-day or one-week sample. To see large trends in historic GPS travel data, a density of points can be done in a GIS system. If there remains a high density of points at a certain location, it may be wise to remove any of those locations as well. Clearly, there are many approaches and procedures to de-identify GPS travel data which can be employed. While this is not an exhaustive list, it is a good starting point to understand the concerns and first steps in keeping the data private and secure. Given sufficient complexity, a GPS data sanitization algorithm will be developed for the ICF/Wyoming site, or the USDOT developed de-identification algorithm will be used. The data collected at the OBE would truncate the start/end and low speed data; the more advanced algorithms would be done at the TMC center.

7.4.4 BSM

The BSM is transmitted over DSRC. DSRC is a one- or two-way short- to medium-range (300-500 meters) wireless communication channel which was made available for use in Intelligent Transportation Systems in 1999, when the Federal Communications Commission (FCC) designated 75MHz of spectrum in the 5.9GHz band. Connected vehicles broadcast BSMs with the intent that any nearby system can receive and interpret them. User privacy is protected by not sending any PII within the BSM. In the ICF/Wyoming pilot, BSMs will only be collected along I-80 which will further protect user privacy by not having RSE in school, residential or commercial areas. Connected V2V and V2I applications that are built around the SAE J27352 BSM contain two parts:

7.4.4.1 *BSM part 1*

BSM part 1 includes vehicle size, position, speed, heading, acceleration, brake system status. This data is transmitted at a 10Hz frequency.

7.4.4.2 *BSM part 2*

BSM part 2 is added to the BSM part 1 dataset depending upon event occurrence (e.g., anti-lock braking system (ABS), windshield wipers activated).

7.4.5 DSRC

DSRC will be transmitted over-the-air for many of the CV applications. It is important to understand the privacy implications of sending data over the air, as it is now possible to set up RSE that is able to "sniff" for DSRC data. Since this data can be combined with other pieces to create PII, it should be protected similarly to data that is being released to the public. Data can be encrypted before being sent over the air; encryption should be considered when sending large amounts of historical data which can be analyzed to find patterns or sensitive information.

8 Key Challenges

The major challenges for security and privacy include:

- Balancing security needs, usability, and costs
- Security in a complex system of systems
- SCMS integration

This section will cover the key challenges directly related to this Pilot and how they are being addressed.

8.1 Balancing security needs, usability, and costs

No system is totally secure. Security requires making tradeoffs among multiple factors, including security, usability, and cost. Excess security can reduce system usability while raising costs. At the same time, inadequate security can result in breaches that result in financial losses, loss of privacy, identity theft, and lack of trust in the system. For this reason, a risk-based approach that examines the types of security needed as well as the likelihood and impact of security breaches is recommended as the starting point for determining security requirements.

Currently, production equipment that meets the certification requirements of this document is not available. With deployment in late 2016 and 2017, vendors may have equipment available. As the standards continue to evolve and the security software (like SCMS) are made production-ready, this challenge may be alleviated.

8.2 Complex System of Systems

This pilot involves multiple interconnected IT systems, some of which are outside of the control of the CV Pilot team. This makes security a greater challenge, since these systems and communications links may or may not adequately address the security needs of the pilot applications. This pilot team will work with USDOT to better understand the security in place before using the Data Warehouse, Data Clearinghouse, System Monitor and the SCMS. The pilot security team is also vetting the freight partners for security controls for data use. This will be further mitigated by not providing data to freight partners that contains PII.

8.3 SCMS Integration

The SCMS proof-of-concept system is an external system provided by the Federal government. This pilot will interface with the SCMS and use it as part of the security solution.

The SCMS proof-of-concept is currently being developed in parallel with the CV Pilot planning phase under a cooperative agreement between the USDOT and CAMP, LLC. This increases the challenges associated with incorporating it into each pilot and adds risk. However, the interface protocols for interfacing with the SCMS are currently being documented. This is the key document that the pilot will use to implement SCMS services.

9 CIA Analysis

Table 9-1 provides the CIA analysis for the proposed applications in the pilot. Table 9-2 provides the consolidated V2X Threat Assessment for the pilot.

Table 9-1. CIA Analysis

Type	Application	Sender	Receiver	Information type	Confidentiality	Integrity	Availability
V2I Mobility	VSLs for Weather-Responsive Transportation Management	WYDOT RSE	ITS Road Weather Equipment (RWE)	Traffic situation data	low	medium	medium
V2I Mobility	VSLs for Weather-Responsive Transportation Management	WYDOT RSE	ITS RWE	Environmental Situation Data	low	medium	medium
V2I Mobility	VSLs for Weather-Responsive Transportation Management	WYDOT RSE	Vehicle OBE	Speed Management Information	low	high	medium
V2I Mobility	VSLs for Weather-Responsive Transportation Management	WYDOT RSE	Vehicle OBE	Vehicle Signage Data	low	medium	medium
V2I Mobility	VSLs for Weather-Responsive Transportation Management	WYDOT RSE	Snow Plow & Highway Patrol OBE	Speed Management Information	low	high	low
V2I Mobility	VSLs for Weather-Responsive Transportation Management	WYDOT RSE	Snow Plow & Highway Patrol OBE	Vehicle Signage Data	low	low	low
V2I Mobility	VSLs for Weather-Responsive Transportation Management	WYDOT RSE	TMC	Speed Management application status	low	medium	medium
V2I Mobility	VSLs for Weather-Responsive Transportation Management	WYDOT RSE	TMC	Traffic situation Data	low	medium	medium
V2I Mobility	VSLs for Weather-Responsive Transportation Management	WYDOT RSE	TMC	environmental situation data	low	medium	medium
V2I Mobility	VSLs for Weather-Responsive Transportation Management	ITS RWE	WYDOT RSE	vehicle signage local data	low	high	medium
V2I Mobility	VSLs for Weather-Responsive Transportation Management	ITS RWE	TMC	environmental sensor data	low	high	medium
V2I Mobility	VSLs for Weather-Responsive Transportation Management	ITS RWE	TMC	traffic flow	low	high	medium
V2I Mobility	VSLs for Weather-Responsive Transportation Management	ITS RWE	TMC	variable speed limit status	low	high	medium

Type	Application	Sender	Receiver	Information type	Confidentiality	Integrity	Availability
V2I Mobility	VSLs for Weather-Responsive Transportation Management	ITS RWE	TMC	roadway information system status	low	medium	medium
V2I Mobility	VSLs for Weather-Responsive Transportation Management	TMC	ITS RWE	variable speed limit control	low	high	medium
V2I Mobility	VSLs for Weather-Responsive Transportation Management	TMC	ITS RWE	roadway information system data	low	medium	medium
V2I Mobility	VSLs for Weather-Responsive Transportation Management	TMC	ITS RWE	environmental sensors control	low	medium	medium
V2I Mobility	VSLs for Weather-Responsive Transportation Management	TMC	ITS RWE	traffic sensor control	low	medium	medium
V2I Mobility	VSLs for Weather-Responsive Transportation Management	TMC	WYDOT RSE	speed management application information	low	high	medium
V2I Mobility	VSLs for Weather-Responsive Transportation Management	Vehicle Databus	Vehicle OBE	host vehicle status	low	high	medium
V2I Mobility	VSLs for Weather-Responsive Transportation Management	Vehicle Databus	Vehicle OBE	driver input information	medium	medium	medium
V2I Mobility	VSLs for Weather-Responsive Transportation Management	Vehicle OBE	Vehicle Databus	driver update information	medium	medium	medium
V2I Mobility	VSLs for Weather-Responsive Transportation Management	Vehicle OBE	WYDOT RSE	vehicle environmental data	low	low	low
V2I Mobility	VSLs for Weather-Responsive Transportation Management	Vehicle OBE	WYDOT RSE	vehicle location and motion for surveillance	low	medium	low
V2I Mobility	VSLs for Weather-Responsive Transportation Management	Snow Plow OBE & Highway Patrol OBE	WYDOT RSE	vehicle environmental data	medium	high	medium
V2I Mobility	VSLs for Weather-Responsive Transportation Management	Snow Plow OBE & Highway Patrol OBE	WYDOT RSE	vehicle location and motion for surveillance	medium	high	medium
V2I Mobility	VSLs for Weather-Responsive Transportation Management	Snow Plow OBE & Highway Patrol OBE	TMC	VSL Change Recommendation	medium	high	medium
V2I Mobility	Road Weather Advisories	WYDOT TMC	Utah, Colorado, and Nebraska TMC	road weather advisories	low	medium	medium
V2I Mobility	Road Weather Advisories	WYDOT TMC	CVOP	road weather advisories	low	medium	medium
V2I Mobility	Road Weather Advisories	WYDOT TMC	CVOP	road network environmental situation data	low	medium	medium
V2I Mobility	Road Weather Advisories	WYDOT Weather Service	WYDOT TMC	Weather information	low	medium	medium

Type	Application	Sender	Receiver	Information type	Confidentiality	Integrity	Availability
V2I Mobility	Road Weather Advisories	WYDOT TMC	CVOP	road network conditions	low	medium	low
V2I Mobility	Road Weather Advisories	WYDOT TMC	Public	road weather advisories	low	high	medium
V2I Mobility	Road Weather Advisories	WYDOT TMC	PID	road network conditions	low	high	medium
V2I Mobility	Road Weather Advisories	WYDOT TMC	PID	road weather advisories	low	high	medium
V2I Mobility	Road Weather Advisories	WYDOT TMC	PID	road network environmental situation data	low	medium	low
V2I Mobility	Road Weather Advisories	WYDOT TMC	WYDOT RWE	environmental sensors control	medium	high	medium
V2I Mobility	Road Weather Advisories	WYDOT RSE	WYDOT TMC	environmental situation data	low	medium	medium
V2I Mobility	Road Weather Advisories	WYDOT RSE	Vehicle OBE	road closure information	low	medium	medium
V2I Mobility	Road Weather Advisories	WYDOT RSE	Vehicle OBE	road weather advisories	low	high	medium
V2I Mobility	Road Weather Advisories	WYDOT RSE	Snow Plow OBE	road weather advisories	low	high	medium
V2I Mobility	Road Weather Advisories	WYDOT RSE	Snow Plow OBE	road network environmental situation data	low	medium	medium
V2I Mobility	Road Weather Advisories	WYDOT RSE	Snow Plow OBE	road network conditions	low	medium	medium
V2I Mobility	Road Weather Advisories	WYDOT RSE	WYDOT TMC	Environmental Situation Data	low	high	medium
V2I Mobility	Road Weather Advisories	Vehicle OBE	WYDOT RSE	vehicle environmental data	medium	medium	medium
V2I Mobility	Road Weather Advisories	Snow Plow OBE	WYDOT RSE	vehicle environmental data	medium	high	medium
V2I Mobility	Road Weather Advisories	Snow Plow OBE	WYDOT TMC	vehicle environmental data	medium	high	medium
V2I Mobility	Road Weather Advisories	WYDOT RWE	WYDOT RSE	environmental sensor data	low	high	medium
V2I Mobility	Road Weather Advisories	WYDOT RWE	WYDOT TMC	environmental sensor data	low	high	medium
V2I Mobility	Automatic alerts for emergency responders	WYDOT TMC	Highway Patrol OBE	emergency dispatch requests	medium	high	medium
V2I Mobility	Automatic alerts for emergency responders	WYDOT TMC	WYDOT RSE	emergency acknowledge	medium	medium	low
V2I Mobility	Automatic alerts for emergency responders	WYDOT TMC	Vehicle OBE	emergency acknowledge	low	medium	low
V2I Mobility	Automatic alerts for emergency responders	WYDOT TMC	Local EMS Center	incident report	medium	high	medium
V2I Mobility	Automatic alerts for emergency responders	Local EMS Center	WYDOT TMC	incident report	medium	high	medium
V2I Mobility	Automatic alerts for emergency responders	Highway Patrol OBE	WYDOT TMC	emergency notification relay	low	high	medium
V2I Mobility	Automatic alerts for emergency responders	WYDOT RSE	WYDOT TMC	emergency notification relay	low	high	medium
V2I Mobility	Automatic alerts for emergency responders	WYDOT RSE	WYDOT TMC	emergency notification	medium	high	medium
V2I Mobility	Automatic alerts for emergency responders	WYDOT RSE	Vehicle OBE	emergency acknowledge	low	medium	medium

Type	Application	Sender	Receiver	Information type	Confidentiality	Integrity	Availability
V2I Mobility	Automatic alerts for emergency responders	Vehicle OBE	WYDOT RSE	emergency notification relay	low	high	medium
V2I Mobility	Automatic alerts for emergency responders	Vehicle OBE	WYDOT RSE	emergency notification	low	high	medium
V2I Mobility	Automatic alerts for emergency responders	Vehicle OBE	Highway Patrol OBE	emergency notification relay	low	high	medium
V2I Mobility	Automatic alerts for emergency responders	Vehicle OBE	Highway Patrol OBE	emergency notification	low	high	medium
V2I Mobility	Automatic alerts for emergency responders	Vehicle OBE	WYDOT TMC	emergency notification relay	low	high	medium
V2I Mobility	Automatic alerts for emergency responders	Vehicle OBE	WYDOT TMC	emergency notification	low	high	medium
V2I Mobility	Automatic alerts for emergency responders	Vehicle OBE	Vehicle Database	driver update information	medium	high	medium
V2I Mobility	Automatic alerts for emergency responders	Vehicle OBE	Remote Vehicle OBE	emergency notification	low	high	medium
V2I Mobility	Automatic alerts for emergency responders	Vehicle OBE	Remote Vehicle OBE	emergency notification relay	low	high	medium
V2I Mobility	Automatic alerts for emergency responders	Vehicle OBE	Remote Vehicle OBE	emergency acknowledge	low	medium	low
V2I Mobility	Automatic alerts for emergency responders	Vehicle Database	Vehicle OBE	driver input information	medium	medium	medium
V2I Mobility	Automatic alerts for emergency responders	Vehicle Database	Vehicle OBE	Host Vehicle Status	medium	high	medium
V2I Mobility	Automatic alerts for emergency responders	Remote Vehicle OBE	Vehicle OBE	emergency notification	low	high	medium
V2I Mobility	Automatic alerts for emergency responders	Remote Vehicle OBE	Vehicle OBE	emergency notification relay	low	high	medium
V2I Mobility	Automatic alerts for emergency responders	Remote Vehicle OBE	Vehicle OBE	emergency acknowledge	low	medium	medium
V2I Safety	Spot weather impact warning	WYDOT TMC	Snow Plow OBE	road weather advisories	low	high	medium
V2I Safety	Spot weather impact warning	WYDOT TMC	Vehicle OBE	road weather advisories	low	high	medium
V2I Safety	Spot weather impact warning	WYDOT TMC	WYDOT TMC	road network environmental situation data	medium	high	medium
V2I Safety	Spot weather impact warning	WYDOT TMC	WYDOT RSE	road weather advisories	low	high	medium
V2I Safety	Spot weather impact warning	WYDOT RSE	WYDOT TMC	environmental situation data	low	medium	medium
V2I Safety	Spot weather impact warning	WYDOT RSE	WYDOT TMC	road weather advisory status	low	medium	medium
V2I Safety	Spot weather impact warning	WYDOT RSE	Snow Plow OBE	road weather advisories	low	high	medium
V2I Safety	Spot weather impact warning	WYDOT RSE	Snow Plow OBE	Reduced Speed Notification	low	high	medium
V2I Safety	Spot weather impact warning	WYDOT RSE	Snow Plow OBE	lane closure information	low	high	medium
V2I Safety	Spot weather impact warning	WYDOT RSE	Snow Plow OBE	road closure information	low	high	medium
V2I Safety	Spot weather impact warning	WYDOT RSE	Vehicle OBE	Reduced Speed Notification	low	high	medium
V2I Safety	Spot weather impact warning	WYDOT RSE	Vehicle OBE	lane closure information	low	high	medium
V2I Safety	Spot weather impact warning	WYDOT RSE	Vehicle OBE	road closure information	low	high	medium
V2I Safety	Spot weather impact warning	WYDOT RSE	WYDOT TMC	environmental situation data	low	medium	medium
V2I Safety	Spot weather impact warning	WYDOT RSE	WYDOT TMC	reduced speed warning status	low	medium	medium

Type	Application	Sender	Receiver	Information type	Confidentiality	Integrity	Availability
V2I Safety	Spot weather impact warning	WYDOT TMC	WYDOT TMC	road network conditions	medium	high	medium
V2I Safety	Spot weather impact warning	WYDOT TMC	WYDOT RSE	reduced speed warning information	low	high	medium
V2I Safety	Spot weather impact warning	WYDOT TMC	WYDOT RWE	Environmental Sensors Control	low	high	medium
V2I Safety	Spot weather impact warning	WYDOT TMC	WYDOT RWE	variable speed limit control	medium	medium	medium
V2I Safety	Spot weather impact warning	WYDOT RWE	WYDOT RSE	environmental sensor data	low	medium	low
V2I Safety	Spot weather impact warning	WYDOT RWE	WYDOT TMC	environmental sensor data	low	medium	medium
V2I Safety	Spot weather impact warning	WYDOT RWE	WYDOT TMC	variable speed limit status	low	high	medium
V2I Safety	Spot weather impact warning	Vehicle OBE	WYDOT TMC	vehicle environmental data	medium	medium	medium
V2I Safety	Spot weather impact warning	Vehicle OBE	WYDOT RSE	vehicle environmental data	medium	medium	medium
V2I Safety	Spot weather impact warning	Vehicle OBE	Vehicle Databus	driver update information	medium	high	medium
V2I Safety	Spot weather impact warning	Snow Plow OBE	Vehicle Databus	driver update information	medium	high	medium
V2I Safety	Spot weather impact warning	Snow Plow OBE	WYDOT TMC	road condition information	low	high	medium
V2I Safety	Spot weather impact warning	Snow Plow OBE	WYDOT TMC	vehicle environmental data	low	high	medium
V2I Safety	Spot weather impact warning	Vehicle Databus	Snow Plow OBE	driver input information + host vehicle status	medium	medium	medium
V2I Safety	Spot weather impact warning	Vehicle Databus	Vehicle OBE	driver input information + host vehicle status	medium	medium	medium
V2I Safety	Work Zone Warnings	WYDOT TMC	WYDOT RWE	roadway information system data	low	high	medium
V2I Safety	Work Zone Warnings	WYDOT TMC	WYDOT RSE	vehicle signage application info	medium	high	medium
V2I Safety	Work Zone Warnings	WYDOT TMC	WYDOT TMC	work zone information	medium	high	medium
V2I Safety	Work Zone Warnings	WYDOT RSE	WYDOT TMC	vehicle signage application status	low	medium	low
V2I Safety	Work Zone Warnings	WYDOT RSE	WYDOT RWE	roadway information system data	low	medium	medium
V2I Safety	Work Zone Warnings	WYDOT RSE	Vehicle OBE	vehicle signage data	low	medium	medium
V2I Safety	Work Zone Warnings	WYDOT RWE	WYDOT TMC	roadway information system status	low	medium	low
V2I Safety	Work Zone Warnings	WYDOT RWE	WYDOT RSE	roadway information system status + vehicle signage local data	low	medium	medium

Type	Application	Sender	Receiver	Information type	Confidentiality	Integrity	Availability
V2I Safety	Work Zone Warnings	WYDOT TMC	Vehicle OBE	broadcast traveler information	low	medium	medium
V2V	Situational Awareness	Vehicle OBE	vehicle databus	driver update information + collision warning information	low	medium	medium
V2V	Situational Awareness	Vehicle OBE	Remote Vehicle OBE	vehicle control event + vehicle environmental data	low	high	medium
V2V	Situational Awareness	Remote Vehicle OBE	Vehicle OBE	vehicle control event + vehicle environmental data	low	high	medium
V2V	Situational Awareness	Vehicle Databus	Vehicle OBE	Host Vehicle Status	low	medium	medium
C2C	Freight-Specific dynamic travel planning	Parking Management System	WYDOT TMC	Parking information	low	medium	low
C2C	Freight-Specific dynamic travel planning	WYDOT TMC	WYDOT Public Communications	Parking information	low	medium	medium
C2C	Freight-Specific dynamic travel planning	WYDOT TMC	Parking Management System	Reservation information	low	medium	medium
C2C	Freight-Specific dynamic travel planning	WYDOT TMC	CVOP	freight-specific traveler information	low	medium	medium
C2C	Freight-Specific dynamic travel planning	CVOP	WYDOT TMC	commercial vehicle trip information + freight traveler information preferences	low	medium	medium
C2C	Freight-Specific dynamic travel planning	WYDOT Weather Service	WYDOT TMC	weather information	medium	medium	medium

Table 9-2. Consolidated V2X Threat Assessment.

Threat ID	Source(s)	Description	Relevant Object	Impact	Notes and Countermeasures
T.Extract.1	[1], [2], [4]	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, 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 to attack or maliciously interact with RSEs, PIDs, and the SCMS. Countermeasures would be to use HSM and log monitoring.
T.Extract.2	[2], [4]	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, SCMS	High if easily scalable, moderate otherwise	See T.Extract.1.
T.Extract.3	[1], [2], [4]	An attacker learns physically protected restricted information on the device, such as private keys, using a physical attack.	OBE, RSE, PID	High if easily scalable, moderate otherwise	See T.Extract.1.
T.Integrity.1	[1], [2], [4]	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 are designed to reduce the chance that replayed messages are accepted unless there is significant clock skew between devices. Use UTC time based on GPS signal and SCMS certificates to mitigate. Messages that are old will be ignored.

Threat ID	Source(s)	Description	Relevant Object	Impact	Notes and Countermeasures
T.Integrity.2	[1], [2], [4]	An attacker modifies the sensor inputs on a single device before the device uses them to generate and send a BSM or other system message.	OBE, RSE	Moderate	The effectiveness of Target of Evaluation's (TOE) primary functions, including sending/receiving BSMs with accurate information that can be trusted, is reduced. This is moderate rather than high impact because it is not scalable: the TOE under attack will still only produce the expected number of BSMs per second, and Sybil attacks are not possible. Mitigate by looking for only reasonable values for inputs, if they are significantly skewed, ignore.
T.Integrity.3	[1], [2], [4]	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, RSE, PID	Moderate	The effectiveness of TOE'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 TOEs under attack will still only produce the expected number of BSMs per second. Mitigate by looking for only reasonable values for inputs, if they are significantly skewed, ignore.
T.Integrity.4	[2], [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	OBE, RSE, PID	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

Threat ID	Source(s)	Description	Relevant Object	Impact	Notes and Countermeasures
		device/system (e.g., use private key to sign a message without completing one of the T.Extract attacks).			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. Require signed software to be installed as countermeasure.
T.MBD.1	[2]	An attacker who knows about the misbehavior detection algorithms (and associated parameters) manipulates the content of the BSM to evade detection.	OBE	High if scalable, moderate otherwise	The ability of the system to mitigate the damage caused by compromised TOEs is reduced. Require signed software to be installed as countermeasure.
T.MBD.2	[1], [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	Moderate	The ability of the system to mitigate the damage caused by compromised TOEs is reduced. This attack is unlikely to be scalable. By signing all messages with SCMS certificates, this problem is mitigated.
T.MBD.3	[2], [4]	An attacker who knows about the misbehavior detection algorithms (and associated parameters) manipulates misbehavior reports to implicate innocent devices/systems and evade detection.	OBE	High if scalable, moderate otherwise	The ability of the system to mitigate the damage caused by compromised TOEs is reduced. By signing all messages with SCMS certificates, this problem is mitigated.
T.Track.1	[1], [2], [4]	An attacker uses the change pattern(s) of certificates and other BSM-relevant information to track a vehicle.	OBE, PID	Moderate	Significant damage to TOE's privacy. Mitigate with HSM and SCMS proper implementation.
T.Track.2	[2], [4]	An attacker uses BSM data to track a vehicle/device.	OBE, PID	High	Similar effects as T.Track.1, but the attack can be launched at a larger scale with little extra resources. Mitigate with HSM and SCMS proper implementation.
T.TOE.1	[2]	An attacker installs malware on a device/system that prevents receiving, or making use of, or providing user	OBE, RSE, PID	High	TOE is not able to perform its primary functions, such as sending/receiving

Threat ID	Source(s)	Description	Relevant Object	Impact	Notes and Countermeasures
		interaction based on, BSMs or other system messages.			BSMs. Mitigate with HSM and requiring signed applications.
T.TOE.2	[1]	An attacker uses the device as an attack vector on the rest of the vehicle/system.	OBE, RSE, PID	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. Mitigate with HSM and requiring signed applications.
T.DOS.1	[5]	An attacker transmits noise and energy on the same frequency as the DSRC safety channel.	OBE, RSE, PID	Low	Local impact. Denial of service (DOS) 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. Can only physically locate the jamming device and turn it off. Mitigate by logging the location and report.
T. DOS.2	[5]	An attacker transmits messages to jam or distract. These messages may contain incorrect information but are validly signed or may appear valid but have a bad cert or signature.	OBE, RSE, PID	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
T.Sybil.1	[5]	Attacker sends multiple messages by concurrently using all certificates which are valid for a given time period to emulate multiple devices.	OBE, PID	Low	Local impact. Enforcement should be able to be carried out through misbehavior detection and secure, tamper resistant hardware. Linked to T. Extract.1,2,3

It should be noted that Table 9-2 was originally authored by THEA team.

10 Notes and Glossary

The following table defines selected project specific terms used throughout this ConOps document.

Table 10-1. Glossary of Terms

Term	Definition
Advanced Automatic Crash Notification Relay (AACN-Relay)	An application that provides the capability for a vehicle to automatically transmit an emergency message when the vehicle has been involved in a crash or other distress situation.
CVOP	Provides forecasted road condition information on common commercial vehicle routes.
Core Authorization	A CV support application that manages the authorization mechanisms to define roles, responsibilities and permissions for other CV applications.
Data Distribution	A support application that manages the distribution of data from data providers to data consumers and protects those data from unauthorized access.
Freight-Specific Dynamic Travel Planning	An application that provides both pre-trip and en route travel planning, routing, and commercial vehicle related traveler information, which includes information such as truck parking locations and current status.
GIS/ITS Program	GIS/ITS - WYDOT's primary division responsible for ITS.
Infrastructure management	A support application that maintains and monitors the performance and configuration of the infrastructure portion of CV.
Location and Time	A support application that shows the external systems and their interfaces to provide accurate location and time to CV devices and systems.
Object Registration and Discovery Service	Application that provides registration and lookup services necessary to allow objects to locate other objects operating within the CVE.
Platform Configuration Registry	Shielded locations to protect the contents of a log of events that affect the security state of a platform at least through the boot process.
Proof of Concept SCMS	The Security and Credential Management System being built by USDOT and Crash Avoidance Metrics Partnership (CAMP) to support the CV pilots

RCR System	An Android-based mobile app that is being used on 10-inch tablets mounted in snowplows and allows maintenance personnel to update WYDOT's public facing traveler information systems directly from the field.
Road Weather Information for Freight Carriers	An application that is a special case of the Road Weather Advisories and Warnings for Motorists application focuses on Freight Carrier users.
Situational Awareness	An application that determines if the road conditions measured by other vehicles represent a potential safety hazard for the vehicle containing the application.
SWIW	An application that will alert drivers to unsafe conditions or road closure at specific points on the downstream roadway as a result of weather-related impacts.
Telecom Program	WYDOT's Telecommunications Program is responsible for the statewide WyoLink radio system, most in-vehicle electronics integration, and various wireless networks including backhaul from roadside electronics devices and Wi-Fi hotspots.
TMC	Center that collects information and informs the public about changing travel conditions.
TCG's TPM	An architecture for cryptographic modules and techniques for hardware based root of trust at the edge of the network (OBE/RSE)
Warnings about Upcoming Work Zone (WUWZ)	An application that provides information about the conditions that exist in a work zone to vehicles that are approaching the work zone.
WyoLink Radio Network	Statewide digital trunked VHF P-25 compliant public safety land mobile radio communications system, used for voice traffic and secondarily for low-speed mobile data communications.

Table 10-2. Acronym List

Acronym/Abbreviation	Definition
A	Availability
AACN-Relay	Advanced Automatic Crash Notification Relay
ABS	Anti-lock Braking System
AES	Advanced Encryption Standard
BSM	Basic Safety Messages
C	Confidentiality

Acronym/Abbreviation	Definition
C2C	Center to Center
CAN	Controller Area Network
CC EAL	Common Criteria Evaluation Assurance Level
CIA	Confidentiality, integrity, and availability
CMVP	Cryptographic Module Validation Program
ConOps	Concept of Operations
CRL	Certificate Revocation List
CSP	Critical Security Parameter
CV	CV
CVE	Common Vulnerabilities and Exposures
CVOP	Commercial Vehicle Operator Portal
CVRIA	CV Reference Implementation Architecture
DMA	Differential Mobility Analysis
DMS	Dynamic Message Signs
DMZ	Demilitarized zone
DSRC	Dedicated Short Range Communications
ECDSA	Elliptic Curve Digital Signature Algorithm
EMC	Electromagnetic compatibility
EMI	Electromagnetic interference
EMS	Emergency Medical Services
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
GHz	Gigaghertz
GIS	Geographic Information System
GPS	Global Positioning System
HAR	Highway Advisory Radios
HSM	Hardware Security Module
I	Integrity
I-80	Interstate 80
IDS	Intrusion Detection Sensor

Acronym/Abbreviation	Definition
IPSEC	Internet Protocol Security
IPv6	Internet Protocol version 6
ISP	Information Service Provider
IT	Information Technology
ITS	Intelligent Transportation System
LMM	Low, medium, medium (CIA)
MAC	Message authentication code
MAP	Mapping for intersection
MHM	Medium, high, medium (CIA)
MHz	Megahertz
MMM	Medium, medium, medium (CIA)
MPH	Miles per hour
NHTSA	National Highway Traffic Safety Administration
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Laboratory Accreditation Program
NWS	National Weather Service
OBE	Onboard Equipment
OS	Operating System
PCR	Platform Configuration Registry
PID	Personal Information Device
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
POC	Point of contact
RDE	Research Data Environment
REST	Representational State Transfer
RP	Revealed preference
RSE	Roadside Equipment
RSU	Roadside Unit
RWE	Road Weather Equipment
RWIS	Road Weather Information Systems

Acronym/Abbreviation	Definition
SCMS	Security Credential Management System
SET-IT	Systems Engineering Tool for Intelligent Transportation
SP	Stated preference
SPAT	Signal Phase and Timing
SPII	Sensitive Personally Identifiable Information
SSL	Secured Socket Layer
SSN	Social Security Number
SWIW	Spot Weather Impact Warning
TCG	Trusted Computing Group
TIM	Traveler Information Message
TMC	Transportation Management Center
TPM	Trusted Platform Module
3DES	Triple Data Encryption Standard
UE-ID (IMEI)	User Equipment Identified (International Mobile Equipment Identify)
USDOT	United States Department of Transportation
USER MAC	Computer media access control
V2I	Vehicle to infrastructure
V2V	Vehicle to vehicle
V2X	Vehicle to everything
VIN	Vehicle Identification Numbers
VPN	Virtual Private Network
VSL	Variable Speed Limit
WAVE	Wireless Access in Vehicular Environments
WSA	Web Security Agent
WUWZ	Warnings about Upcoming Work Zone
WYDOT	Wyoming Department of Transportation

Appendix A

Computer Environment Access & Non-Disclosure Agreement (included as separate pdf in draft)

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-16-288

U.S. Department of Transportation