Connected Vehicle Pilot Deployment Program Phase 2

Data Privacy Plan, Version 2 – Wyoming

www.its.dot.gov/index.htm
Draft — April 14, 2017
FHWA-JPO-17-469

U.S. Department of Transportation

Produced by DTFH6116H00027
U.S. Department of Transportation

Notice

Version History

#	Date	Author (s)	Comment
1	12/1/2016	Wyoming DOT	First draft of the Data Privacy Plan.
2	12/30/2016	Wyoming DOT	Updated draft based on USDOT comments.
3	04/14/2017	Wyoming DOT	Final version based on latest architectural design.

Technical Report Documentation Page

1. Report No. FHWA-JPO-17-469	**2. Government Accession No.**	**3. Recipient's Catalog No.**
4. Title and Subtitle Connected Vehicle Pilot Deployment Program Phase 2, Data Privacy Plan – Wyoming		**5. Report Date** 04/14/2016 **6. Performing Organization Code**
7. Author(s) Shane Zumpf (Trihydro), Tony English (Trihydro), Mohamed M. Ahmed (University of Wyoming),Deepak Gopalakrishna (ICF), Vince Garcia (Wyoming DOT)		**8. Performing Organization Report No.** Phase 2 – Task 2C 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		**10. Work Unit No. (TRAIS)** **11. Contract or Grant No.** DTFH6116H00027
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** Data Privacy Plan, 12/30/2016 **14. Sponsoring Agency Code**
15. Supplementary Notes Kate Hartman (AOR), Sarah Tarpgaard(AO)		

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 (concluded in September 2016) included 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 Data Privacy Plan. The Data Privacy Plan for the Wyoming CV Pilot describes the underlying needs of the Wyoming Pilot Deployment to protect the privacy of users, ensure secure communications, and outline a plan that addresses these needs.

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** 52	**22. Price** NA

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

Acknowledgements

We acknowledge the timely and high-quality support offered by USDOT, and the support contractor Noblis throughout Phase 2.

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 has completed the planning phase January 2016 to September 2016. The deployment process has started in the second phase (September 2016 to 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 Data Privacy Plan Introduction

The Data Privacy Plan (DPP) for the Wyoming CV Pilot describes the underlying needs of the Wyoming Pilot Deployment to protect the privacy of users, ensure secure communications, and outline a plan that addresses these needs. Furthermore, the DPP 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 DPP 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. The DPP was written with input from the Phase 1 Security Management Operating Concept (SMOC FHWA-JPO-16-288) document. The Phase 1 SMOC is consistent with the DPP.

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 the approach taken to manage data and maintain privacy where needed for the overall system. The second section will cover the controls (including technical, policy, standards, and physical) that will be used to protect data privacy. The third section will cover the compliance, including documented assurances that all team members and project participants will comply with the Privacy Management Plan. The final section will cover the resources the pilot will use in order to ensure compliance.

1.5 System Overview

At a very high level, the pilot scope includes the following implementation elements:

- **Deployment of about 75 roadside units (RSU)** that can receive and broadcast messages using DSRC along various sections on I-80.
- **Equip around 400 vehicles, a combination of fleet vehicles and commercial trucks, with on-board units (OBU).** Of the 400 vehicles, at least 150 would be heavy trucks. All vehicles are expected to be regular users of I-80. Several types of OBU are being procured as part of the pilot and differ based on their communication capabilities, ability to integrate with the in-vehicle network, and connectivity to ancillary devices and sensors. All OBUs will have the functionality to broadcast Basic Safety Messages (BSM) Part I and will include a human-machine interface (HMI) to share alerts and advisories to drivers of these vehicles.
- **Develop several V2V and V2I (and I2V) applications** that will enable communication with drivers for alerts and advisories regarding various road conditions. These applications include support for in-vehicle dissemination of advisories for collision avoidance, speed management, detours, parking, and presence of work zones and maintenance and emergency vehicles downstream of their current location.
- **Enable overall improvements in WYDOT's traffic management and traveler information practices** by using data collected from connected vehicles. Targeted improvements include better activation of variable speed limits (VSL) and improved road condition dissemination via 511, Dynamic Message Sings (DMS) and other WYDOT sources.

Systems and applications developed in the pilot will enable drivers of connected vehicles to have awareness of hazards and situations they cannot even see. The CV Pilot is considered a System of Systems, with two systems of interest: The *Vehicle System* and the *Wyoming CV System*, see Figure 1-1. The *Vehicle System* includes five Sub-Systems that represent the various vehicle and equipment

types to be used in the pilot. These Sub-Systems vary in their data collection and sharing capabilities. The *Wyoming CV System* includes the infrastructure used in the pilot and back-office systems in charge of the various processes that lead to the generation and distribution of advisories and alerts. Together, the Vehicle and *Wyoming CV System*s support a variety of V2V and V2I applications. Both systems interface with external systems, including WYDOT, USDOT and the National Weather Service (NWS).

The CV Pilot Project will, at its core, provide key information to the drivers through five on-board applications: i) Forward Collision Warning (FCW); ii) I2V Situational Awareness (SA); iii) Distress Notification (DN); iv) Work Zone Warning (WZW); and v) Spot Weather Impact Warning (SWIW). In addition, the CV Pilot project will support overall traffic management and traveler information services offered by WYDOT.

Through these applications and functions, WYDOT hopes to improve operations on the corridor especially during periods of adverse weather and when work zones are present. By means of 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, improved and new information outlets.

Details of the Wyoming CV pilot system are available in the Comprehensive Pilot Deployment Plan (FHWA-JPO-16-297), see Gopalakrishna et al. (2016).

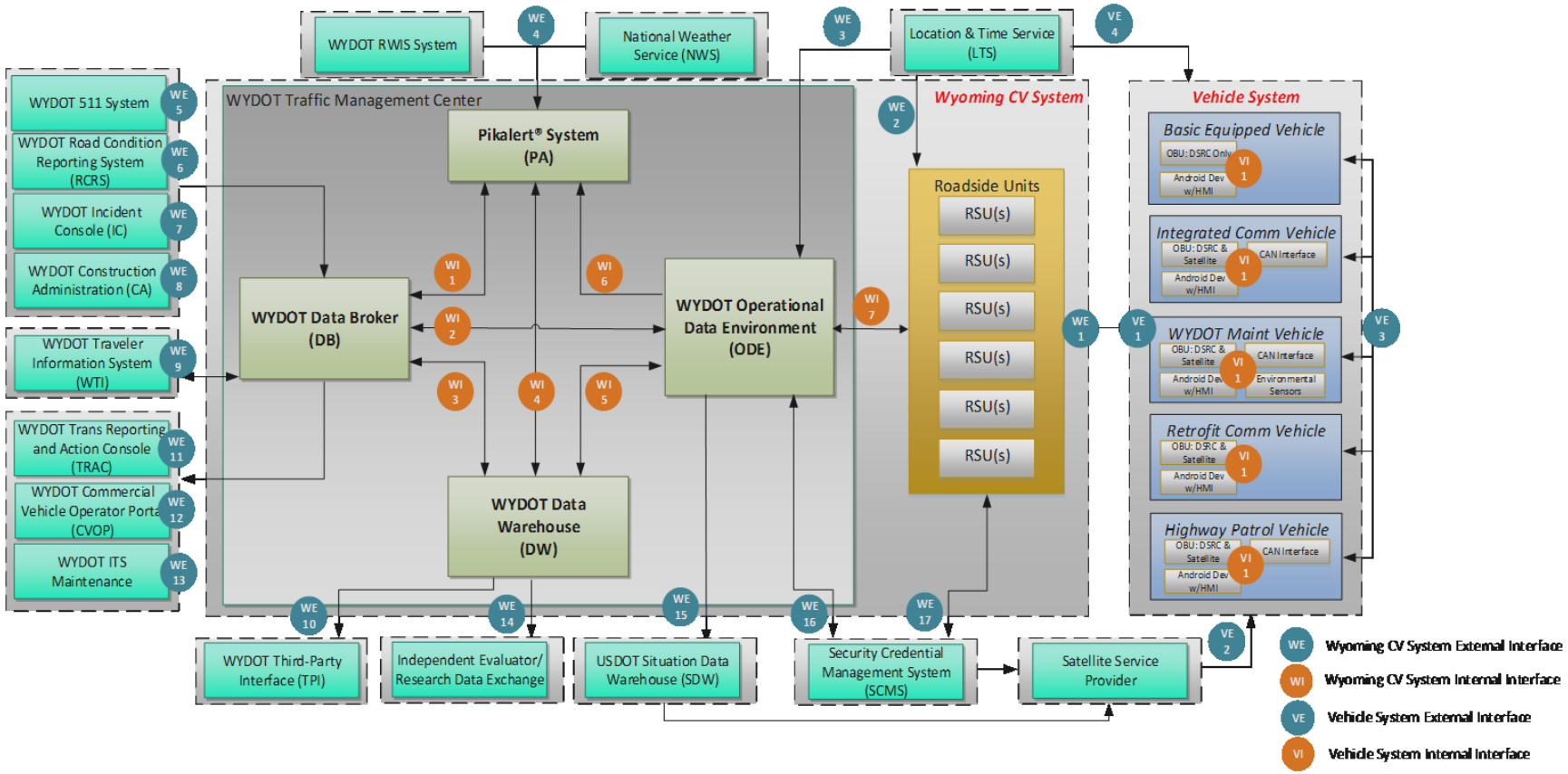

Figure 1-1. Physical View of WYDOT CV Pilot System Architecture. Source: WYDOT

1.5.1 External Interfaces

In addition to the Vehicle and Wyoming Systems, the following external interfaces support the CV Pilot Project by supplying and distributing information.

- **I2V DSRC Communications Interface** (Interface WE1) Wireless DSRC interface provides communication between Wyoming CV System and Vehicle System through exchange of messages conforming to SAE J2735 and SAE J2945/1.
- **Location and Time Service (LTS)** (Interfaces WE2 and WE 3) – Provides location and time information, which is later used to geotag and timestamp all information produced by the systems of interest.[1]
- **National Weather Service (NWS) and Road Weather Information System (RWIS)** (Interface WE4) – NWS provides regional weather data shared through National Oceanic and Atmospheric Administration's Meteorological Assimilation Data Ingest System. **RWIS** provides atmospheric and pavement condition information collected through Environmental Sensor Stations (ESS) deployed as part of the WYDOT RWIS network in the field.
- **WYDOT 511 Application** (Interface WE5) – Provides information to the public regarding I-80's road weather and traffic conditions (e.g., road closure). The application is currently being updated to also share crowdsourced truck parking information with the CV Pilot.
- **WYDOT Road Condition Report System (RCRS)** (Interface WE6) – An Android tablet-based application that resides in WYDOT snow plows which enables field personnel (e.g., snowplow operators) to report weather and roadway pavement conditions following WYDOT's 8 Code (roadway condition), 9 Code (atmospheric) and 10 Code (other road condition) system.
- **WYDOT Incident Control (IC)** (Interface WE7) – Provides timestamped and geotagged incident information on incidents along I-80 obtained from the WHP and other sources (e.g., maintenance).
- **WYDOT Construction Administration (CA)** (Interface WE8) – Provides timestamped and geotagged information of WYDOT's scheduled and unscheduled work-zone activities along I80.
- **Wyoming Traveler Information (WTI)** (Interface WE9) – Supports traveler information services to the public and to fleet management centers via various means (website, 511, 511 App, text, email, and alerts).
- **WYDOT Third Party Interface (TPI)** (Interface WE10) – A standardized interface based on the TMDD standard that can be used to support delivery of traveler information to external centers and information service providers.
- **WYDOT Transportation Reports and Action Console (TRAC)** (Interface WE11) – An operator console used in the TMC to monitor and manage planned, ongoing, and forecast events and actions on facilities monitored by the TMC. The TRAC provides a tabular list of currently ongoing events that require operator attention. These events may be entered

[1] The location is obtained from a GPS using WGS-84 coordinates system, and time is provided using UTC from GPS time.

manually and can be reported based on other systems like RCRS, radio communications with field personnel and citizen reports.

- **WYDOT Commercial Vehicle Operator Portal (CVOP)** (Interface WE12) – A subscription-based website created by WYDOT for providing advanced notification of forecasted conditions to commercial travelers and fleet managers. Currently there are over 800 companies subscribed to the CVOP. As part of the CV Pilot System, the CVOP will be enhanced to include current weather information for segments on I-80.
- **WYDOT ITS Maintenance** (Interface WE13) – Provides a mechanism to report service outages and resumption of services of WYDOT's ITS equipment.
- **Independent Evaluator (IE) (Interface WE14) –** Provides WYDOT CV Pilot data to the IE for use in independent analysis and impact evaluation across multiple CV pilots.
- **USDOT Situational Data Warehouse (SDW)** (Interface WE15) – A service operated by USDOT that stores near real-time data and shares them with the remote users and developers for further distribution. As shown, this interface also supports communication of messages through **Satellite Service Provider (SSP)** satellites, allowing the system to transmit traveler-related information.
- **USDOT Security Certification Management System (SCMS)** (Interfaces WE16 and WE17) – Generates security certificates to manage messages securely from connected devices. As shown, this interface also supports communication of messages through **SSP** satellites, allowing the system to share SCMS-related information.

1.5.2 Wyoming CV System

The *Wyoming CV System* includes the infrastructure used in the pilot and the back-office systems in charge of the various processes that lead to the generation and distribution of advisories and alerts for CV Pilot vehicles. The *Wyoming CV System* will be located at the WYDOT TMC. Additionally, this system provides external interfaces to share the advisories and alerts with the public and commercial vehicle operators.

The *Wyoming CV System* is composed of five Sub-Systems:

- Roadside Units (RSU)
- Operational Data Environment (ODE)
- Pikalert®[2] System (PA)
- Data Broker (DB)
- Data Warehouse (DW)

1.5.2.1 *Roadside Units*

This Sub-System describes the physical units for deployment as part of the system along I-80. RSUs include DSRC connectivity, application support, data storage, and other support services to enable CV applications, such as necessary certificates. WYDOT RSUs can be either fixed or portable equipment depending on the use. In general, RSUs serve as a two-way communication portal between

[2] Pikalert is a trademark of the University Corporation for Atmospheric Research (UCAR).

connected vehicles that provide information through DSRC and the Operational Data Environment. About 75 RSUs are planned to be deployed in the pilot.

1.5.2.2 *Operational Data Environment*

The USDOT Operational Data Environment Sub-System receives information collected with connected devices, checks its quality, and then shares it with other Sub-Systems in charge of analyzing and distributing the information. The ODE also exports data to the Situational Data Warehouse for USDOT-related activities. The ODE will be hosted at WYDOT TMC and uses the same codebase as the USDOT ODE. High-level requirements for the ODE are contained within the Task 4 ODE ConOps from the Southeast Michigan Test Bed Advanced Data Capture Field Testing. These include requirements for Validation, Integration, Sanitization, and Aggregation, which are combined in this document with the description of ODE processed data.

1.5.2.3 *Pikalert System*

The Pikalert System supports the integration and fusion of CV and non-CV weather data to develop alerts and advisories regarding adverse weather conditions along I-80. CV data are received from the ODE, while non-CV data derive from weather sources and the WYDOT Data Broker. To generate the alerts and advisories, the Pikalert System assigns CV and non-CV data to 1-mile segments on I-80 every 5 minutes. The CV data is quality checked, then passed to the Road Weather Hazard module (RWH). The RWH uses these data to produce the alerts and advisories for adverse weather and for a 72-hour forecast of road weather conditions and hazards. The generated information is then shared with the DB for further distribution. Pikalert can also access historical data stored at the DW.

1.5.2.4 *WYDOT Data Broker*

WYDOT DB receives information from the ODE, Pikalert and some external systems, analyzes them, and shares them with the corresponding system or service including other sources. The DB supports the information brokerage of road weather alerts and advisories to WYDOT's TPI, TRAC, WTI, RCRS, and CVOP. Additionally, this system takes in incident information from the Incident Console, work zone data from the Construction Administrator and parking availability information from the 511 Application. The DB also sends the information back to the ODE to support the dissemination of TIM to the RSUs and can also access historical data stored at the DW if needed.

1.5.2.5 *WYDOT Data Warehouse*

The WYDOT Data Warehouse stores various TMC- and CV-related data. The Data Warehouse includes timestamped and geotagged logs of CV and non-CV data—information collected, generated and shared within the *Wyoming CV System*—that will be used for performance measurement.

1.5.3 Vehicle System

The *Vehicle System* represents the deployment of on-board equipment, sensors, and a human-machine interface that will support CV applications. All vehicles that are part of the *Vehicle System* will have the following core capabilities:

- Ability to share and receive information via DSRC communication from other connected devices (vehicles and RSUs).
- Ability to broadcast Basic Safety Message Part I.
- Ability to receive Traveler Information Messages (TIM).

- A human-machine interface that allows alerts and advisories to be communicated with the driver.

Additionally, several vehicles that are part of the *Vehicle System* have further capability. Based on this, the *Vehicle System* is divided into five Sub-Systems, which define the various vehicle types for this pilot based on their data collection and communication capabilities. Each Sub-System and its rationale are described below.

1.5.3.1 *WYDOT Maintenance Vehicles*

This Sub-System represents the maintenance fleets operated by WYDOT. These include highway patrol and snow plow vehicles assigned to the I-80 corridor. These vehicles represent a set of vehicles over which WYDOT has full control as part of their operations. As such, the vehicles will be equipped with the full package of sensors and equipment necessary for the CV Pilot. Around 60 maintenance vehicles (snow plows) are expected to be part of this subsystem, which will have the ability to:

- Receive TIMs via DSRC and Satellite (or other remote communication methods).
- Integrate with the vehicle network via a CAN bus connection.
- Broadcast BSM Parts I and II.
- Collect weather sensor data.

1.5.3.2 *WYDOT Highway Patrol Vehicles*

This Sub-System represents the highway patrol fleet assigned to the I-80 corridor. While also operated by WYDOT, these vehicles represent a set over which WYDOT has less flexibility given the nature of their operations. Around 40 highway patrol vehicles are expected to be part of this subsystem, which will have the ability to:

- Receive TIMs via DSRC and Satellite (or other remote communication methods).
- Integrate with the vehicle network via a CAN bus connection.
- Broadcast BSM Parts I and II.

1.5.3.3 *Integrated Commercial Vehicles*

This connected trucks Sub-System represents a subset of commercial trucks owned and operated by fleet partners involved in the pilot that can be integrated with the vehicle network. In contrast to the WYDOT Maintenance Vehicles, and similar to Highway Patrol Vehicles, no external weather sensor data will be collected from these systems (i.e., only data from the vehicle). To summarize, this Sub-System will include the abilities to:

- Receive TIMs via DSRC and Satellite (or other remote communication methods).
- Integrate with the vehicle network via a CAN bus connection.
- Broadcast BSM Parts I and II.

In essence, these vehicles represent the capability to use vehicle data collected from trucks in the pilot. WYDOT anticipates that about 200 trucks will have this functionality.

1.5.3.4 *Retrofit Commercial Vehicle*

This Sub-System is for trucks and other fleet vehicles that do not include integration with Controller Area Network (CAN bus) data integration. This Sub-System is intended to simulate a commercial-off-

the-shelf (COTS) system that enables a vehicle to communicate data through DSRC to other connected devices and receive TIMs through DSRC or satellite. About 20–30 vehicles are expected in this category.

1.5.3.5 *Basic Equipped Vehicle*

This Sub-System includes vehicles equipped with just the core functionality for the *Vehicle System*, listed in the beginning of Section 1.5.3. About 100–150 vehicles are expected in this category. These vehicles enable WYDOT to equip vehicles inexpensively with the basic capability necessary to be part of the CV Pilot. All safety applications are supported by this Sub-System.

1.5.4 System Interaction and Data Flow

Many interactions occur within the CV Pilot and between its different entities. These interactions are enabled by interfaces that communicate (link) the Wyoming CV System, Vehicle Subsystems and External interfaces, listed in Table 1-1. It is important to note that some interfaces already exist and therefore are not considered as part of the development scope of this project. For instance, while the Wyoming CV System will support updates to the 511 App on road closure, traffic, weather and public information on the corridor that may be generated, an interface is currently in operation for such updating purposes and the CV Pilot plans to use it.

Table 1-1. List of interactions within the CV Pilot System.

Interface	Origin	Destination	Data / Information Shared	Type*
Wyoming CV System Interfaces				
WE1/ VE1	RSU	Vehicle System	TIM, Software Updates	External
WE1/ VE1	Vehicle System	RSU	SCMS-related (Misbehavior reports), CV-related (BSM, Event Log, Environmental Sensor (ES)), TIM, including DN	External
WE2	LTS	RSU	Location and time	External
WE3	LTS	ODE	Location and time	External
WE4	RWI	Pikalert	Atmospheric and pavement condition	External
WE4	NWS	Pikalert	Regional weather data	External
WE5	511 App	DB	Parking information	External
WE6	RCRS	DB	8 Code (roadway condition), 9 Code (atmospheric), 10 Code (crash and incident information)	External
WE7	IC	DB	Incident information	External
WE8	CA	DB	Scheduled and unscheduled WZ activities	External
WE9	WTI	DB	Posted speed, vehicle restrictions, messages, and closure information	External
WE9	DB	WTI	Current and forecasted segment-specific advisories/alerts	External
WE10	DW	TPI	Traffic condition	External
WE11	DB	TRAC	DN, Segment alerts	External
WE12	DB	CVOP	Current and forecasted segment-specific advisories/alerts	External
WE13	DB	ITS Maint.	System operational status	External
WE14	DW	IE/RDE	TBD	TBD
WE15	ODE	SDW	TIM	External
WE16	ODE	SCMS	Request for certificates, Misbehavior reports	External
WE16	SCMS	ODE	Certificates, Certificates Revocation List (CRL)	External
WE17	SCMS	RSU	Certificates, CRL	External
WE17	RSU	SCMS	Request for certificates, Misbehavior reports	External
WI1	Pikalert	Data Broker	Alerts and advisories within TIMs	Internal
WI1	DB	Pikalert	8 Code (roadway condition), 9 Code (atmospheric), 10 Code (crash and incident information)	Internal

Interface	Origin	Destination	Data / Information Shared	Type*
Wyoming CV System Interfaces				
WI2	ODE	DB	DN	Internal
WI2	DB	ODE	TIM, Alerts and advisories within TIMs	Internal
WI3	DW	DB	Road condition report, TIM, DN, Alerts and advisories within TIMs	Internal
WI3	DB	DW	TIM, DN, Alerts and advisories within TIMs	Internal
WI4	DW	Pikalert	Road section with mile marker information	Internal
WI4	Pikalert	DW	Alerts and advisories within TIMs	Internal
WI5	DW	ODE	Road section with mile marker information	Internal
WI5	ODE	DW	All collected and processed data	Internal
WI6	ODE	Pikalert	CV weather data (BSM Part II, CAN Bus), ES	Internal
WI7	ODE	RSU	TIM, Software Updates	Internal
WI7	RSU	ODE	SCMS-related (Misbehavior reports), CV-related (BSM, Event Log, ES), TIM, including DN	Internal
VE2	Satellite	Vehicle System (except Basic Veh.)	SCMS-related (Certificates, CRL), ODE-related, TIM	External
VE4	LTS	Vehicle System	Location and time	External
VE3	Vehicle System	Vehicle System	BSM, TIM, including DN	External
VI1	CAN Bus	OBU	Vehicle status	Internal
VI1	OBU	HMI	Processed TIM, including DN, CAN Bus, Notifications from on-board applications	Internal
VI1	ES	HMI	ES, including one or more of the following: Precipitation Type, Solar Radiation, Wiper Frequency, Orientation, GPS Coordinates, Ground Temperature, Ground Profile, Ambient Temperature, Barometric Pressure, Humidity	Internal

1.6 Security Overview

Figure 1-2 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 RSU's and traditional ITS equipment, data will be protected with Internet Protocol Security (IPSEC) Virtual Private Networks (VPN) or private networks.

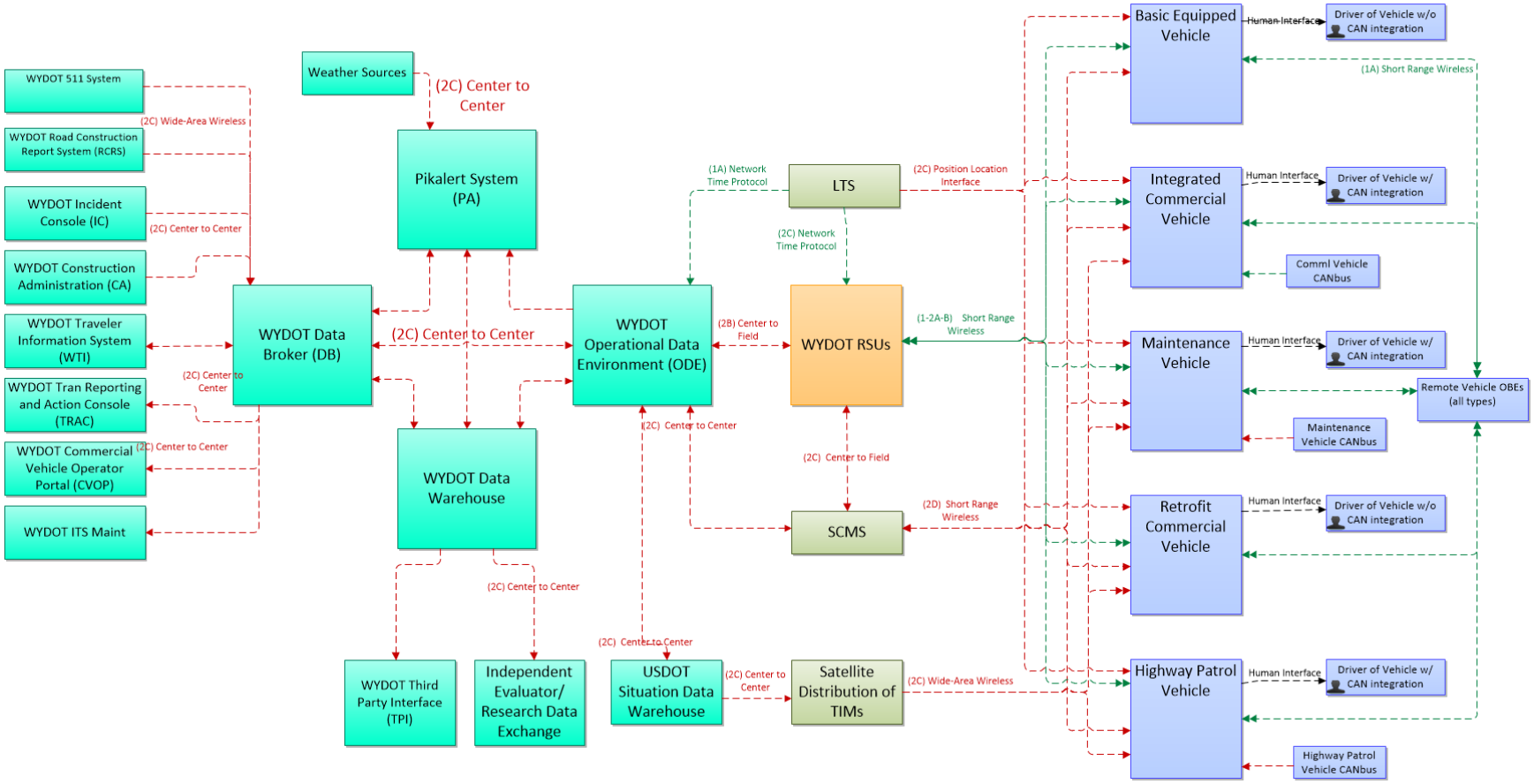

Figure 1-2. **Layer 0 Physical Diagram for the CV Pilot (Source: WYDOT)**

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.
10	SAE. (2014). J3067: *Candidate Improvements to Dedicated Short Range Communications (DSRC) Message Set Dictionary [SAE J2735] Using Systems Engineering Methods.* SAE International.
11	FIPS. (2004). PUB 199: *Standards for Security Categorization of Federal Information and Information Systems.* NIST.
12	FIPS. (2006). PUB 200: *Minimum Security Requirements for Federal Information and Information Systems.* NIST.
13	NIST (2013). 800-53: *Security and Privacy Controls for Federal Information Systems and Organizations.* NIST.
14	NIST (2012). SP 800-30: Guide for Conducting Risk Assessments. NIST.

15	Deepak Gopalakrishna, et al. (2015a). *CV Pilot Deployment Program Phase 1, Concept of Operations (ConOps), ICF/Wyoming*. U.S Department of Transportation.
16	Deepak Gopalakrishna, et al. (2015b). *CV Pilot Deployment Program Phase 1, Security Management Operating Concept (SMOC), ICF/Wyoming*. U.S Department of Transportation.
17	Booz Allen Hamilton (2015). Southeast Michigan Test Bed Advanced Data Capture Field Testing. Task 4: Operational Data Environment - Concept of Operations.
18	Deepak Gopalakrishna, et al. (2016). CV Pilot Deployment Program Phase 1, Comprehensive Deployment Plan, ICF/Wyoming. U.S Department of Transportation.
19	Deepak Gopalakrishna, et al. (2016). Performance Measurement and Evaluation Support Plan, FHWA-JPO-16-290.
20	Deepak Gopalakrishna, et al. (2016). Human Use Summary (FHWA-JPO-16-293)

3 Approach

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. The 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 Wyoming CV pilots approach to system threat assessment, analysis of application flows and device classifications is based on the process defined by the Federal Information Processing Standards (FIPS) publications 199 and 200. FIPS PUBS 199 categorizes information flows and systems based on confidentiality, integrity and availability defined 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 units. 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 or 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. 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 (RSU/OBU 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 Wyoming pilot will use the proof-of-concept SCMS provided the PKI via elliptical curve cryptography. It is a critical element of the solution for meeting the security requirements for this pilot.

3.1.6 SCMS

The National Highway Traffic Safety Administration (NHTSA) is drafting a proposed rule that will addressing 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., OBU 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 RSUs. Application certificates are required in order for the RSU 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). RSU and OBU 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 RSUs over the backhaul link or OBUs over the air. Blacklisted devices are revoked from receiving pseudonym certificates from the SCMS. Misbehavior detection will be done for RSU and OBU devices, however only OBUs will use the CRL. Misbehaving RSUs 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, OBU, RSU) 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 published version is IEEE 1609.2-2016. This standard describes secure message formats and processing for use by WAVE devices, including methods to secure WAVE management messages and methods to secure application messages. It also describes administrative functions necessary to support the core security functions.

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

- Signed messages, which are used by all broadcast communications (e.g., BSM, 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 (2016).
    - Web Security Agent (WSA) security profile is covered in IEEE 1609.3-2016.
- Mechanisms for peer-to-peer certificate distribution.

3.1.9 Privacy Concerns

Privacy, including the protection of Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII), 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:

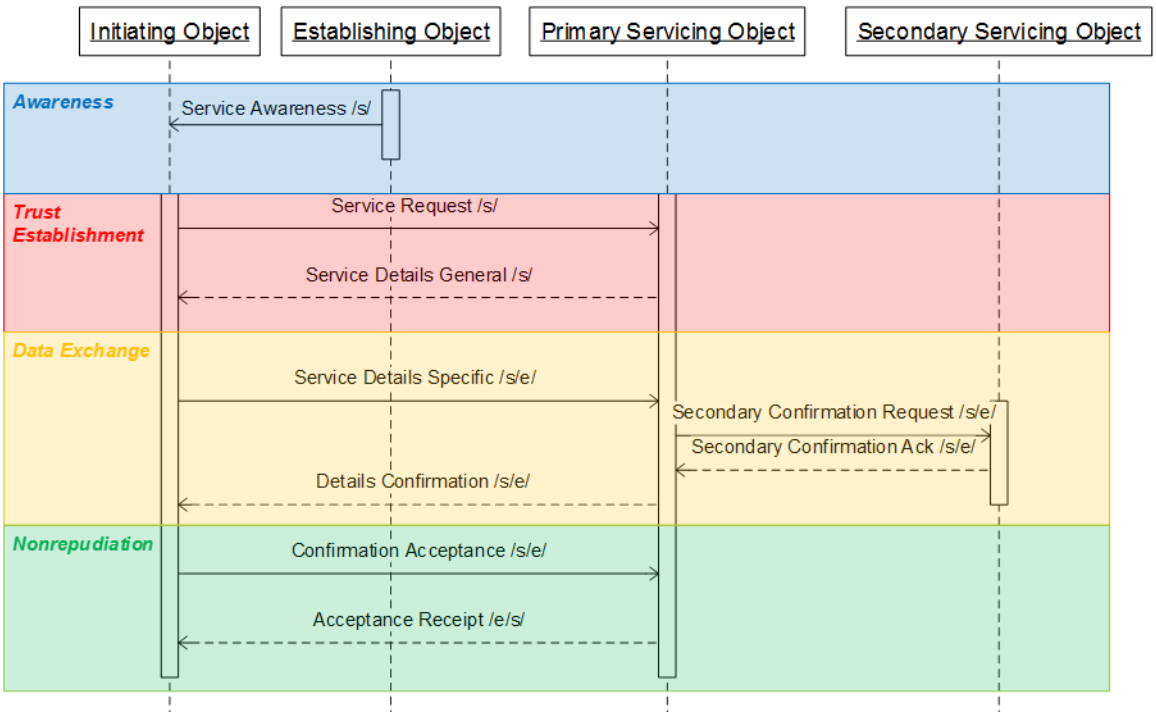

Figure 3-1. Phases of a Peer-to-Peer Data Exchange Message Sequence. Source: USDOT.

3.1.10 Data Sharing and Provision

A major goal of the USDOT funded Connected Vehicle program is to develop data that can be broadly utilized by researchers and application developers including other CV pilot projects to further advance the application and deployment of CV technologies. According to the Broad Agency Announcement (BAA) for the CV; "*Data sharing. Connected vehicle, mobile device, and infrastructure sensor data captured during the operational phase of the effort is expected to be broadly shared with the*

community to inform other deployers and prospective deployers of connected vehicle applications. However, data sharing is subject to the protection of intellectual property rights and personal privacy. Appropriately prepared system control, performance and evaluation data are expected to be shared with the USDOT and posted in timely fashion on resources such as the Research Data Exchange."

The data generated from CV Pilots will be available to three entities; 1) the USDOT Research Data Exchange (RDE), 2) the Saxton Traffic Operations Laboratory, and 3) the Independent Evaluators (IE).

PII will be stripped from data provided to the USDOT RDE and the Independent Evaluators. As discussed earlier, the CV System generated data will be locally collected (both from the field and the applications) until they are transferred and stored at the Wyoming CV system. The local data storage will be encrypted to protect the data until it is uploaded to the Wyoming CV System, and the locally stored data will be deleted after uploading is complete. This will support the Independent Evaluators and Performance Measurements for the pilot, while also protecting the privacy of the participants. Survey data will be anonymized before it is provided to the IE. More detail is provided in the Performance Measurement and Evaluation Support Plan, FHWA-JPO-16-290. Any data generated by the CV Pilots that cannot be shared to the public because of privacy considerations will be available to be stored within the Saxton Lab. Access to such data will be limited on a case-by-case basis with proper credentials. Data provided to the Saxton Lab may contain some PII. The data stored in the Saxton Lab are not available to the public.

3.2 Pilot Specific Application Security Analysis

This section reviews the five in vehicle applications being used by the pilot for CIA. In each of these categories a raking of low, medium or high will be assigned. The reader is referred to the CV-Pilot ConOps document (FHWA-JPO-16-287) for a more detailed explanation of each application, see Golapakrishna et al. (2015a). 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.

3.2.1 Forward Collision Warning (FCW)

Forward Collision Warning is a V2V communication-based safety feature that issues a warning to the driver of the connected host vehicle in case of an impending front-end collision with a connected vehicle ahead in traffic in the same lane and direction of travel on both straight and curved geometry roadways. FCW will help drivers avoid or mitigate front-to-rear vehicle collisions in the forward path of travel. This application is critically important for safety along I-80 in conditions when snow plows are moving slower than following traffic and/or when visibility may be limited due to adverse weather. The application does not attempt to control the host vehicle to avoid an impending collision. This application will follow the description from standard SAE J2945/1 March 2016 Section 4.2.4.

- **Confidentiality: LOW.** This application uses the broadcast BSM message data and is intentionally broadcast to all nearby connected vehicles. In some cases, BSM data may contain PII data for certain vehicles in the pilot program, this is done with the consent of pilot participants and PII data will be removed prior to posting on the RDE. Additionally, the data going to the driver via the HMI is not proprietary.

- **Integrity: MEDIUM.** Commercial trucks and operators will rely on BSM data for forward collision warning safety warnings which needs to be accurate and trustworthy. As the BSM information is signed to prevent tampering with and is compliant with J2945/1 for accuracy to mitigate these risk the integrity rating of medium is justified. The signed certificates are validated utilizing the SCMS and certificate revocation list (CRL) bad actors are also inherently ignored for use with FCW.
- **Availability: MEDIUM.** As BSMs will be sent at 10 Hz a moderate availability will be adequate to notify driver of forward collision risks.

3.2.2 Infrastructure-to-Vehicle (I2V) Situational Awareness

This application enables relevant downstream road condition information including weather alerts, speed restrictions, vehicle restrictions, road conditions, incidents, parking, and road closures to be broadcast from a roadside unit and received by the connected host vehicle. Such information is useful to connected host vehicles that are not fully equipped with weather sensors or to connected host vehicles in paths toward or entering areas with hazardous conditions. The Wyoming pilot will extend this application to use full coverage of the I-80 corridor with satellite communications to send road condition information directly to selected connected vehicles. This step is important for mitigating the short range and sparse placement of RSUs along the corridor. This application will follow the description from J3067 August 2014 Section 2.9.3.6.

- **Confidentiality: LOW.** The environmental data collected, road data, atmospheric data, and parking information data are publicly available and of low confidentiality.
- **Integrity: MEDIUM.** The data from this application is used to inform the driver about road closures, driving risks and to set variable speed limits. The integrity of this data is critical, to promote this level of protection the data is encrypted and signed to prevent tampering with and to provide for non-reputation by leveraging the SCMS and CRL.
- **Availability: MEDIUM.** Infrastructure to vehicle situational awareness data provided to drivers is only available via wireless mediums using DSRC and satellite making the maximum available be medium. This information is critical for driver safety and is therefore disseminated over dual medium to maximize availability on the I80 corridor.

3.2.3 Distress Notification (DN)

This application enables connected vehicles to communicate a distress status defined as:

- When the vehicle's sensors an air bag deployment over the CAN Bus
- The vehicle's operator manually initiates a distress status with a selection from the Human Machine Interface (HMI)

The vehicle then generates and broadcasts a distress message (e.g., Mayday) to the nearest RSU. When an RSU is not within communication range, the message is received by connected vehicles that are in the vicinity and forwarded to an RSU that forwards it to the Wyoming CV System. The Distress Message will include the location, time of message, distress message explanation (e.g., air bag deployed, vehicle disabled, operator initiated), and vehicle type. Additionally, the distress notification received by nearby connected vehicles is broadcast to notify oncoming vehicles that a distressed vehicle is ahead. Although this application is loosely based on the Mayday application description from

J3067 Section 2.5.3.3, it is built on a higher priority TIM communication using J2735 March 2016, Section 5.16, Part 3, Integrated Transport Information System (ITIS) advisory elements.

- **Confidentiality: LOW.** Distress Notification information flows need to be quickly disseminated to nearby connected vehicles to reduce the number of vehicles involved in cascading crashes. The data is not proprietary.
- **Integrity: HIGH.** These information flows indicate a distressed situation has occurred and where it is located. In order for other connected vehicles as well as 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.
- **Availability: MEDIUM.** Ideally, the availability for this application would have high availability to both surrounding vehicles and to the TMC in order to notify oncoming vehicles of distressed vehicles ahead and to be able to notify emergency responders to distress situations as quickly as possible. However, this is not currently possible since this application will only be able to use DSRC and have a limited number of road side units to communicate with the TMC. Additionally, the density of connected vehicles will reduce the effectiveness of this application as it will only be able to disseminate the distress notification to connected vehicles.

3.2.4 Work Zone Warnings (WZW)

This application provides information about the conditions that exist in a work zone toward which the vehicle is approaching. This capability provides approaching vehicles with information about work zone activities that could present unsafe conditions for the vehicle, such as obstructions in the vehicle's travel lane, lane closures, lane shifts, speed reductions or vehicles entering/exiting the work zone. This application will follow the TIM work zone warning described in J2735 part 3 in Section 6.142.

- **Confidentiality: LOW.** The data for work zones will be broadcast traveler information messages over DSRC and satellite available to everyone.
- **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.
- **Availability: MEDIUM.** 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 medium for availability seems warranted.

3.2.5 Spot Weather Impact Warning (SWIW)

Similar to situational awareness, this application enables relevant road condition information, such as fog or icy roads, to be broadcast from a roadside unit and received by the connected host vehicle. This application, however, is distinct from situational awareness in that it provides more localized information (i.e., at the segment level instead of area wide or region wide). This application will follow the TIM advisory content from part 3 defined in J2735 Section 6.142 for ITIS data elements 6.54 for

weather conditions and 6.55 for winds defined in J2540_2. This application includes information on parking availability, when needed, as part of the advisory.

- **Confidentiality: LOW.** The localized road data, and atmospheric data are publicly available and of low confidentiality. SWIW data displayed to the driver through the HMI is low confidentiality. Environmental data collected from the WYDOT Fleet has a vehicle identifier and data from the CAN which are medium confidentiality. Integrated Trucks have data from the CAN which is medium confidentiality. Retrofit and Basic vehicles do not collect environmental or CAN data.
- **Integrity: MEDIUM.** The data from this application is used to inform the driver about icy conditions, blow over risks, and other localized information. The integrity of this data is critical, to promote this level of protection the data is encrypted and signed to prevent tampering with and to provide for non-reputation by leveraging the SCMS and CRL. Data sent from the WYDOT fleet has vehicle identification information and requires high integrity.
- **Availability: MEDIUM.** SWIW data provided to drivers is only available via wireless mediums using DSRC and satellite making the maximum available be medium. This information is critical for driver safety and is therefore disseminated over dual medium to maximize availability on the I80 corridor.

4 Controls

4.1 Overview and goals

This section describes the technical, policy, standards and physical controls that will be used to ensure data privacy within the CV system.

4.2 Technical Controls

4.2.1 Access

Access to the CV WYDOT network infrastructure and applications are restricted by identity role-based authorization and authentication. Authorized administrators and users of WYDOT access applications using minimum access privileges needed in order to perform a given task.

All user accounts accessing WYDOT CV applications will require users to login using a password with a minimum length and complexity, and optionally may perform two-factor authentication at login using SMS to a registered mobile device for the specified user.

Passwords shall be changed every 90 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.

Within an active session user content is restricted to the minimum amount of data needed to perform an action. Likewise, the independent evaluator chosen to work on this WYDOT CV project will also be restricted to the minimum amount of data needed to adequately evaluate the performance of the pilot project. User roles restrict the type of data and actions that a user is able to perform within the system. WYDOT user access roles are described below:

With the WYDOT Pilot there are distinct classes of users that have unique privacy requirements based on employment contracts and public privacy expectations. Table 4-1 identifies these groups of users and provide short description of privacy expectations.

Table 4-1. 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

User Group	Owner	Short Description
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
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. 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
10. Wyoming Telecommunica-tions and IT Programs	State of Wyoming	Systems and users responsible for statewide communication linkages will have a low expectation of privacy
11. Independent Evaluators	Various	Independent Evaluators on the job 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 privacy with respect sharing information about them to the traveling public. The unicast communications will need to be

User Group	Owner	Short Description
		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 between the company and the truck driver over private satellite or cellular communication with dispatch center will have a very low expectation of privacy.
		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.

4.2.2 Logging and Monitoring

Accesses or attempted access to data within the system will be logged and recorded to a secure database location or file within the system, and made available for routine automated or manual review.

Servers within the system will record all API requests to REST services and will include information about the resources requested, accessed, and the source of the request to local log files. Log files will be replicated within the system and backed up on a routine basis.

4.2.3 Encryption

Data stored within the Data Warehouse will be encrypted using Oracle database Transparent Data Encryption. Transparent Data Encryption ensures data-at-rest encryption in the database layer.

Data in transit will be encrypted and transmitted over the network using Transport Level Security (TLS) protocol.

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.

4.2.4 Database

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. All 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.

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

4.3 Policy Controls

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.

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.

Additionally, the pilot program plans to put into place corridors and policies for when pilot data will be collected.

The following three sections are copied from the Security Management Operating Concept (SMOC FHWA-JPO-16-288) for clarity. Additional details are available within the SMOC.

4.3.1 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 will be taken by the Wyoming pilot program 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. All data sanitization is planned to occur within the Operational Data Environment (ODE) application currently in development under guidance of the USDOT with input from the Wyoming pilot team.

4.3.1.1 *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.

4.3.1.2 *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.

4.3.1.3 *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 OBU would truncate the start/end and low speed data; the more advanced algorithms would be done at the TMC center.

4.4 Standards Controls

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.

Security requirements for each device classification should specify hardware security control requirements. These requirements may differ among the PID, OBU, and RSU 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. Devices used within this pilot were evaluated using the FIPS 140-2 requirement, the full evaluation can be found in the Phase 1 SMOC document (FHWA-JPO-16-288), see Gopalakrishna et al. (2015b).

4.5 Physical Controls

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 in the Security Management Operating Concept (FHWA-JPO-16-288). 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.

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.

5 Compliance

This section describes the documented assurances that all team members and project participants will comply with the Data Privacy Plan as well as verification procedures on applications and data itself that validate privacy controls are effective.

5.1 Participant

Compliance with the data privacy plan is implemented by allocating responsibility for data protection to specific organizations in the pilot and implementing accountability measures for participants who have access to private, protected data.

For the pilot the prime responsibility for defining data protection requirements is the Wyoming Department of Transportation. These defined requirements are approved by the University of Wyoming Institutional Review Board (IRB). They ensure the requirements adequately protect and inform the participants with respect to the data collection and protection requirements applicable federal, international, state, and local laws, regulations, and policies that provide protection for human subjects participating in research.

Any project participants that have access to PII, including researchers, software developers, system testers, and project managers are required to complete and pass a training course regarding the protection of human subjects of research. This training includes review of: 1) The Belmont Report: Ethical Principles and Guidelines for the Protection of Human Subjects of; 2) the U.S. Department of Health and Human Services (HHS) regulations for the protection of human subjects at 45 CFR part 46; 3) the Federal Wide Assurance (FWA) for International Institutions and applicable Terms of the FWA for the University of Wyoming; and 4) the relevant University of Wyoming policies and procedures for the protection of human subjects. Each participant after passing the training course also signs an individual investigator agreement confirming their understanding of the required privacy protections. These agreements are maintained by the University of Wyoming.

All drivers that will be participating in the pilot, with CV equipment installed in their vehicles, are employees of the companies participating in the pilot. Participants (drivers) from WYDOT and Trihydro will be required to read and sign a consent form to collect PII data. Drivers will be told what data would be collected and how it would be used. However, consent forms will not be collected from Trucking Companies participating in the pilot, this requirement will be through the fleet managers. There will be a Memorandum of Understanding (MOU) agreement between WYDOT and the fleet owners. As such these driver participants are already subject to existing expectation of privacy clauses in their respective employee agreements. Greater detail is available in the Human Use Summary (FHWA-JPO-16-293).

Information identifying each driver participant in the pilot will be maintained in a Participant Tracking Database. This database will be encrypted to protect the PII in this repository. Access to this database will be restricted to a set of WYDOT employees subject to WYDOT and the State of Wyoming private

data access policies listed in the controls section of this document. In case of a data breach, either PII or SPII, the pilot officials will report the incident to law enforcement, and launch an internal investigation. In addition, the potential impacted users will be notified by mail. In case of data breach involving SPII, the affected users will be offered a one year of free credit monitoring and identity protection services.

5.2 Hardware

Hardware will be physically inspected prior to installation and regularly inspected to ensure no tampering is present. RSU and OBU physical devices are protected from tampering with an Hardware Security Device (HSM) defined with FIPS 140-2 level 3 for RSUs and level 2 for OBUs. Certificates that are no longer trusted will 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 RSUs over the backhaul link or OBUs over the air. Blacklisted devices are revoked from receiving pseudonym certificates from the SCMS. Misbehavior detection will be done for RSU and OBU devices, however only OBUs will use the CRL. Misbehaving RSUs 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.

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 will be addressed before CV data is collected or stored and periodic audits are to be scheduled.

6 Resources

This section will describe the minimum sufficient resources required to ensure compliance from the prospective of hardware and security.

6.1 Hardware

The following hardware resources will be needed in order to ensure compliance with the controls described in section 4.

OBUs and RSUs with appropriate FIPS ratings will be required for installation into the corresponding vehicle types. The appropriate FIPS ratings are described in detail in the SMOC (FHWA-JPO-16-288).

The firewall supporting the TMC is managed, monitored and updated by the WYDOT TMC Operators.

6.2 Security

The WYDOT 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.

7 Notes and Glossary

Table 7-1 defines selected project specific terms and Table 7-2 provides a list of the acronyms used throughout this Data Privacy Plan document.

Table 7-1. 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 (OBU/RSU)
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 7-2. 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
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

Acronym/Abbreviation	Definition
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
HMI	Human Machine Interface
HSM	Hardware Security Module
I	Integrity
I-80	Interstate 80
IDS	Intrusion Detection Sensor
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
OBU	On-board Unit
OS	Operating System
PCR	Platform Configuration Registry
PID	Personal Information Device
PII	Personally Identifiable Information
PKI	Public Key Infrastructure

Acronym/Abbreviation	Definition
POC	Point of contact
RDE	Research Data Exchange
REST	Representational State Transfer
RP	Revealed preference
RSU	Roadside Unit
RWE	Road Weather Equipment
RWIS	Road Weather Information Systems
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

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

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

FHWA-JPO-17-469

U.S. Department of Transportation