Connected Vehicle Pilot Deployment Program Phase 2

Comprehensive Maintenance and Operations Plan – Wyoming

www.its.dot.gov/index.htm

Draft Report — July 6, 2018

Publication Number: FHWA-JPO-17-473

U.S. Department of Transportation

Produced by DTFH6116H00027

U.S. Department of Transportation

Intelligent Transportation Systems (ITS) Joint Program Office

Notice

Technical Report Documentation Page

1. Report No. FHWA-JPO-17-473	2. Government Accession No.	3. Recipient's Catalog No.
4. Title and Subtitle Connected Vehicle Pilot Deployment Program Phase 2, Comprehensive Maintenance and Operations Plan – Wyoming		5. Report Date July 6, 2018 6. Performing Organization Code
7. Author(s) Vince Garcia (WYDOT), Ali Ragan (WYDOT), Brian Peel (WYDOT), Deepak Gopalakrishna (ICF), Nayel Ureña Serulle (ICF), Tony English (Trihydro), Shane Zumpf (Trihydro)		8. Performing Organization Report No. Task 2I - Comprehensive Maintenance and Operations Plan
9. Performing Organization Name and Address Wyoming DOT, 5300 Bishop Boulevard, Cheyenne, WY 82009 ICF International, 1725 Eye St NW, Washington DC, 20006 Trihydro Corporation, 1252 Commerce Drive, Laramie, WY 82070		10. Work Unit No. (TRAIS) 11. Contract or Grant No. DTFH6116RA00027
12. Sponsoring Agency Name and Address ITS-Joint Program Office 1200 New Jersey Avenue, S.E., Washington, DC 20590		13. Type of Report and Period Covered Draft Report 01/2018 – 04/2018 14. Sponsoring Agency Code HOIT-1
15. Supplementary Notes Work performed for: Kate Hartman (COR), Sarah Tarpgaard (CO)		

16. Abstract

The Wyoming Department of Transportation's (WYDOT) Connected Vehicle (CV) Pilot Deployment Program is intended to develop a suite of applications that utilize vehicle-to-infrastructure (V2I) and vehicle- to-vehicle (V2V) communication technology to reduce the impact of adverse weather on truck travel in the I-80 corridor. These applications support a flexible range of services from advisories, roadside alerts, parking notifications and dynamic travel guidance. Information from these applications are made available directly to the equipped fleets or through data connections to fleet management centers (who will then communicate it to their trucks using their own systems). The pilot is being conducted in three Phases. Phase I includes the planning for the CV pilot including the concept of operations development. Phase II is the design, development, and testing phase. Phase III includes a real-world demonstration of the applications developed as part of this pilot.

This Comprehensive Maintenance and Operations Plan (CMOP) provides details of the operations and maintenance of all in-vehicle, roadside, mobile device, center, and other equipment and supporting capabilities required in the deployed system. As such, this document identifies the types and provides a number of equipment required to be maintained and summarizes key operational methods and procedures that ensure safe and efficient operations in Phase 3 of this pilot. Additionally, the CMOP includes a description of the required elements of a maintenance-focused demonstration to be included as part of the ORP

17. Key Words Connected Vehicle Technology, I-80 Corridor, Road Weather, Truck Safety, Maintenance, Operations	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) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 54	22. Price

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 Introduction

1.1 Project Scope

Wyoming Department of Transportation (WYDOT) is one of the first wave of Connected Vehicle (CV) Pilot sites selected to showcase the value of and spur the adoption of Connected Vehicle Technology in the United States. Connected Vehicle Technology is a broad term to describe the applications and the systems that take advantage of dedicated short-range communications (DSRC) between vehicle to vehicle (V2V), vehicle to infrastructure (V2I) and infrastructure to vehicle (I2V) 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 worked in a planning phase through September 2016. The deployment process will happen in the second phase (ending in August 2018) followed by an 18-month demonstration period in the third phase (starting in September 2018). 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) 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 four 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), that support a variety of V2V and V2I applications. Both systems interface with external systems, including WYDOT, USDOT and the National Weather Service (NWS).

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.

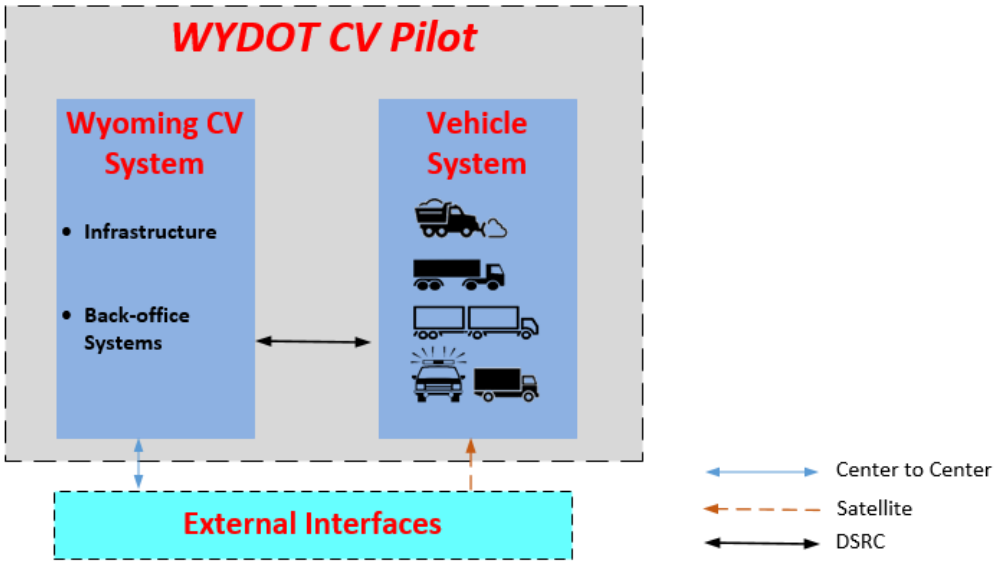


Figure 1-1 Wyoming CV Pilot System of Systems. Source: WYDOT

1.2 Purpose of this Comprehensive Maintenance and Operations Plan

The purpose of this Comprehensive Maintenance and Operations Plan (CMOP) is to provide details of the operations and maintenance of all in-vehicle, roadside, mobile device, center, and other equipment and supporting capabilities required in the deployed system. As such, this document identifies the types and provides a number of equipment required to be maintained and summarizes key operational methods and procedures that ensure safe and efficient operations in Phase 3 of this pilot. Additionally, the CMOP includes a description of the required elements of a maintenance-focused demonstration to be included as part of the ORP (Stephens et al, 2018).

1.3 Document Organization

The CMOP includes the following sections:

- **Section 2** lists all sources of information contained in this report.
- **Section 3** provides a high-level description of the system.
- **Section 4** describes the operation and maintenance procedures for in-vehicle devices.
- **Section 5** describes the operation and maintenance procedures for field devices.
- **Section 6**. describes the operation and maintenance procedures for TMC – CV Systems.
- **Section 7** provides a list of monitoring tools that will be used throughout the operation and maintenance of the CV Pilot systems.
- **Section 8** lists who will be involved with maintaining the systems and/or equipment.
- **Section 9** lists who will be involved with operating the systems and/or equipment.
- **Section 10** describes the configuration management procedures that will be followed and the interactions that will occur for maintaining the configuration information for the hardware and software actually installed.
- **Section 11** lists all software and products/services that will be used during the operation and maintenance of the system
- **Section 12** details the individuals who can sign off and say the system is safe and efficient for operations and maintenance covering the entire system and can proceed to the next stage.
- **Appendices A through D** provides supporting documentation of maintenance and operational procedures.

2 References

Table 2-1 lists the documents referenced in the CMOP.

Table 2-1. References

#	Document
1	Deepak Gopalakrishna, et al. (2018). Connected Vehicle Pilot Deployment Program Phase 2, System Requirement Specification (SyRS) – Wyoming CV Pilot, FHWA-JPO-16-291. U.S. Department of Transportation
2	English, T., et al., (2018a) Connected Vehicle Pilot Deployment Program Phase 2, System Design Document (SDD) – Wyoming CV Pilot, FHWA-JPO-17-468. U.S. Department of Transportation
3	Deepak Gopalakrishna, et al. (2016a). Connected Vehicle Pilot Deployment Program Phase 1, Security Management Operational Concept, Version 2 – ICF/Wyoming, FHWA-JPO-16-288. U.S. Department of Transportation
4	Deepak Gopalakrishna, et al. (2016b). Connected Vehicle Pilot Deployment Program Phase 1, Safety Management Plan, Version 2 – ICF/Wyoming, FHWA-JPO-16-289. U.S. Department of Transportation
5	Denny Stephens, et al. (2018). Connected Vehicle Pilot Deployment Program Phase 2, Operational Readiness Plan – WYDOT CV Pilot, FHWA-JPO-17-472. U.S. Department of Transportation
6	SAE. (2016a). J2945/1: Dedicated Short Range Communication (DSRC) Minimum Performance Requirements. SAE International.
7	English, T., et al., (2018b) Connected Vehicle Pilot Deployment Program Phase 2, Comprehensive Installation Plan (CIP) – Wyoming CV Pilot, FHWA-JPO-17-471. U.S. Department of Transportation
8	English, T., et al., (2017) Connected Vehicle Pilot Deployment Program Phase 2, Comprehensive Acquisition Plan (CAP) – Wyoming CV Pilot, FHWA-JPO-17-470. U.S. Department of Transportation
9	Deepak Gopalakrishna, et al. (2015). *CV Pilot Deployment Program Phase 1, Concept of Operations (ConOps), ICF/Wyoming (FHWA-JPO-16-287)*. US Department of Transportation
10	Booz Allen Hamilton (2015). Southeast Michigan Test Bed Advanced Data Capture Field Testing. Task 4: Operational Data Environment - Concept of Operations

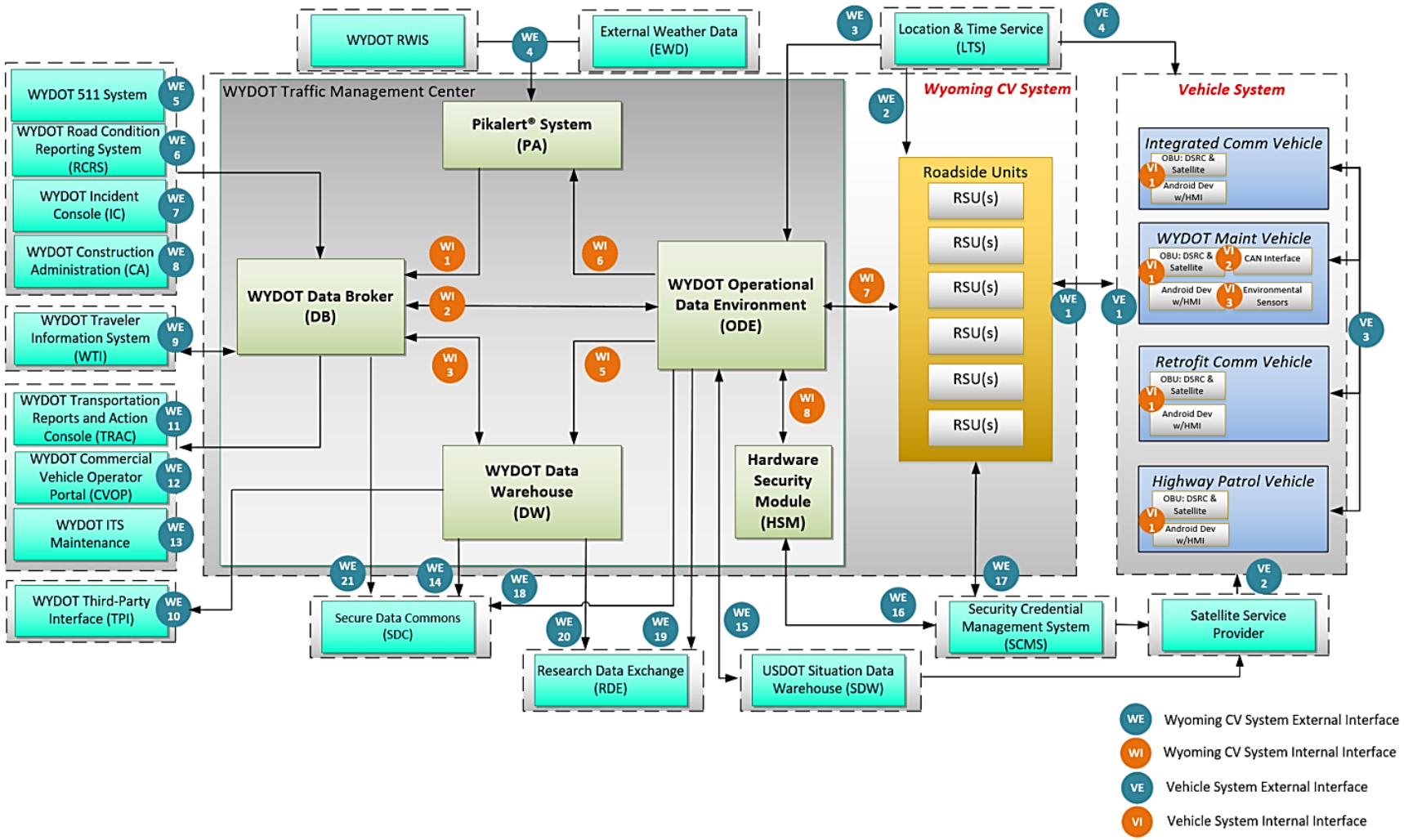
3 System Overview

3.1 System Context

This project will develop systems that make relevant information directly available to, and shared among, equipped fleets. Information is also shared through linkages with fleet management centers (who can then communicate it to their trucks using their own communication systems) and other external agencies and partners. Supporting the applications and the CV environment of roadside, vehicle and back-office infrastructure are core services that allow safe, secure, reliable operations of the system. The main project objectives of the pilot to be accomplished and demonstrated are as follows:

- Deploy and operate a set of vehicles that are equipped with on-board units (OBU) with DSRC and satellite connectivity. These vehicles will be a combination of snow plows, fleet vehicles, emergency vehicles and private trucks that will broadcast a basic safety message, collect vehicle, weather and road condition data, and provide it remotely to the WYDOT Transportation Management Center. These vehicles will also receive in-vehicle alerts through the infrastructure (RSU-OBU) and wirelessly (satellite-OBU) from various applications developed as part of the pilot through a human-machine interface (HMI).
- Deploy roadside units (RSUs) with DSRC connectivity that are able to transmit advisories and alerts to equipped vehicles along I-80.
- Leverage the data provided from the equipped vehicles to develop and demonstrate a suite of V2V and V2I applications. As part of the pilot, several applications will be developed to support wide-area travel advisories, variable speed limit postings, forecast road condition information, spot-specific warnings, work zones, distress notifications, and parking notifications.

Figure 3-1 shows the physical architecture with interfaces numbered for reference. A detailed explanation of the Wyoming CV Pilot project can be found in *Connected Vehicle Pilot Deployment Program Phase I, Concept of Operations (ConOps) (*Gopalakrishna, et al., 2015).



NOTE: The Wyoming CV System Interface WI4 (PA→DW) was not implemented in the final system design.

Figure 3-1. Physical View of WYDOT CV Pilot System Architecture with Numbered Interfaces. Source: WYDOT

3.2 Vehicle System

The *Vehicle System* represents the deployment of on-board equipment, sensors, and an HMI 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 from other connected devices.
- Ability to broadcast BSM.
- An HMI 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 four Sub-Systems, which define the various vehicle types for this pilot based on their data collection, communication capabilities and fleet/vehicle type. Each Sub-System and its rationale are described below.

3.2.1 WYDOT Maintenance Vehicles

This Sub-System represents the maintenance fleets operated by WYDOT. This includes, but is not limited to, 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, some of the vehicles will be equipped with the full package of environmental sensors and equipment necessary to support the CV Pilot applications.

Around 95 vehicles are expected to be part of this sub-system, but not all with the same capabilities. Al vehicles will have the ability to:

- Receive TIMs via DSRC and Satellite.
- Broadcast BSM Parts I and II.

Whereas 50 of them are expected to be able to:

- Collect weather sensor data.

All vehicles within this subsystem will have the capability to integrate its network via a Controller Area Network (CAN bus) connection. Although it should be noted that the actual number of vehicles to have this connection is expected to be a limited and will be determined at a later stage of deployment.

3.2.2 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 35 highway patrol vehicles are expected to be part of this sub-system, which will have the ability to:

- Receive TIMs via DSRC.
- Broadcast BSM Parts I and II.

3.2.3 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 some of 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) and there is not CAN Bus integration. To summarize, this Sub-system will include the abilities to:

- Receive TIMs via DSRC and Satellite (or other remote communication methods).
- 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 250 trucks will have these functionalities.

3.2.4 Retrofit Commercial Vehicle

This Sub-system is intended to simulate a commercial-off-the-shelf system—which is different from the one installed on the integrated commercial vehicles—that enables a vehicle to communicate data through DSRC to other connected devices and receive TIMs through DSRC or satellite. About 25 vehicles are expected in this category and their abilities include:

- Receive TIMs via DSRC and Satellite (or other remote communication methods).
- Broadcast BSM Parts I and II.

3.3 Wyoming 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 Transportation Management Center (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)
- Hardware Security Module (HSM)
- Pikalert System
- Data Broker (DB)
- Data Warehouse (DW)

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

3.3.2 Operational Data Environment

The WYDOT ODE Sub-System receives information collected from connected devices, checks its quality, and then shares it with other Sub-Systems in charge of analyzing and distributing the information. The ODE also sends information to RSUs and exports data to the Secure Data Commons (SDC), the SDW and the RDE 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* (Booz Allen Hamilton, 2015). These include requirements for Validation, Integration, Sanitization, and Aggregation, which are combined in this document with the description of ODE processed data.

3.3.3 Hardware Security Module

The Wyoming CV Pilot uses the IIS/GHS[1] rented, black box hardware security module (HSM) in the Cheyenne TMC. It has a Representational State Transfer (RESTful)[2] endpoint that receives an unsigned TIM and outputs a signed TIM. The HSM also has a link to the ISS/GHS Certificate Management System (CMS) to get updated certifications. It should be noted that its internal workings are a black box that is proprietary code, and therefore WYDOT will not have access to it. WYDOT will physically have two 1U rack[3] units that each have dual power supplies and are fail over in capability. The units also have a gig Ethernet connection with IPv4 and IPv6.

3.3.4 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 weather data environment (WDE). To generate the alerts and advisories, the Pikalert System assigns CV and non-CV data to 1-mile segments on I80 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.

3.3.5 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 Third-Party

[1] IIS/GHS is the company hosting the pilot's certificate management system (i.e., INTEGRITY Software Services/Green Hills Software).

[2] https://en.wikipedia.org/wiki/Representational_state_transfer

[3] Rack height unit 1.75" (https://en.wikipedia.org/wiki/Rack_unit)

Interface (TPI), TRAC, WTI, Road Condition Reporting System (RCRS), and CVOP. Additionally, this system takes in incident information from the Incident Console (IC), 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.

3.3.6 WYDOT Data Warehouse

The WYDOT DW stores various TMC- and CV-related data. The DW 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.

3.4 Wyoming CV System External Interfaces

The Wyoming CV System includes the following external interfaces for exchanging data and information with external WYDOT and USDOT systems.

- **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.[4]
- **External Weather Data (EWD) and RWIS** (Interface WE4) – EWD provides regional weather data shared through sources outside of WYDOT's system, such as National Oceanic and Atmospheric Administration's Meteorological Assimilation Data Ingest System and USDOT. **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 was updated to also share crowdsourced truck parking information with the CV Pilot.
- **WYDOT 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 (incident condition) system.
- **WYDOT IC** (Interface WE7) – Provides timestamped and geotagged incident information on incidents along I-80 obtained from the WHP and other sources (e.g., maintenance).

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

- **WYDOT Construction Administration (CA)** (Interface WE8) – Provides timestamped and geotagged information of WYDOT's scheduled and unscheduled work-zone activities along I80.
- **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 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 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 manually and can be reported based on other systems like RCRS, radio communications with field personnel and citizen reports.
- **WYDOT 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 all road segments.
- **WYDOT ITS Maintenance** (Interface WE13) – Provides a mechanism to report service outages and resumption of services of WYDOT's ITS equipment.
- **Secure Data Commons (SDC) / Research Data Exchange (RDE)** (Interfaces WE14, WE18, WE19, WE20, and WE21) **–** Provides WYDOT CV Pilot data to the independent evaluators and the RDE for use in independent analysis and impact evaluation across multiple CV pilots.
- **USDOT 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 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 SCMS-related information.

3.5 Pilot On-Board Applications

The WYDOT CV Pilot will develop five on-board applications that will provide key information to the drivers of equipped vehicles:

- Forward Collision Warning (FCW)
- Infrastructure-to-Vehicle (I2V) Situational Awareness
- Distress Notification (DN)

- Work Zone Warning (WZW)
- Spot Weather Impact Warning (SWIW)

In addition to on-board applications, information generated by the *Wyoming CV System* is planned to support ongoing WYDOT traffic management and traveler information services.

- Setting and removing VSLs along the I-80 corridor.
- Supporting 511 and other traveler information.
- Supporting road weather advisories and freight-specific travel guidance through WYDOT's CVOP.
- Supporting crowd-sourced freight parking information which is critical during road closures.

3.6 System Modes and States

This section describes the following modes of operation for the proposed system.

3.6.1.1 Normal Operations

During normal operations, the full suite of CV applications, described in Section 3.5, are available. Objects in the CV environment are being monitored by the WYDOT TMC and are functioning normally.

3.6.1.2 Degraded Mode

In a degraded mode, some of the vehicle or infrastructure objects in the CV environment are not functioning as intended. Depending on the nature of the degradation, different functions and processes are available. For example, *Vehicle System* malfunctions would limit the availability of on-board applications. Operations are limited to wide area advisories via 511 and the use of traditional ITS (DMS and HAR) for roadside communications through existing WYDOT interfaces. On the other hand, failure of specific RSUs in the proposed system can be managed by maintaining wide area communications (such as satellite).

3.6.1.3 Back-up Mode

In a back-up mode, some of the *Wyoming CV System* Sub-Systems like the ODE, Pikalert, DB are not functioning as intended. Due to the risk associated with malfunctioning center system, all CV-related use-cases would be suspended and the proposed system would revert back to pre-CV state of operations.

3.7 System Updates

System updates will be required from time to time, as they are released by the vendors, and will be carefully managed to help maintain system integrity. This process is described in detail in the System Design Document (Tony English, et al. 2018). WYDOT staff involved in the software update process will be well-versed in the processes described in the System Design Document. The

WYDOT team will have an Update Test Document (UTD), which will be a reduced version of the ORTP, containing detailed steps on how to test updates to the OBU, RSU, HMI App, Weather Cloud and Tablets. The UTD will include tests on FCW, DN and a small subset of TIMs (for both RSUs and Satellite).

The following are high level description of the update process of the different equipment and applications.

The process to update OBUs includes five steps.

1. WYDOT receives a new firmware version from its vendors.
2. WYDOT first bench-test the new firmware and, if it passes, the firmware is then tested on test OBUs.
3. Once tested and approved, WYDOT uploads the new firmware version to the TMC update server and updates a subset of OBUs and does testing.
4. After testing is completed and signed off on by the TMC staff, the new firmware is marked as the latest version to be broadcast and pushed to the RSUs for dispersal.
5. The firmware is then broadcast out to all OBUs along I-80.
6. OBUs download the firmware update and prompt the user on the HMI to install the new firmware upon the next system startup.

Updates to the RSUs will be as follow:

1. WYDOT receives a new firmware version from its vendors.
2. WYDOT first bench-test the new firmware and, if it passes, the firmware is then tested on test RSUs.
3. Once tested and approved, WYDOT uploads the new firmware version to a subset of RSUs and does testing.
4. After testing is completed and signed off on, the new firmware is marked as the latest version to be broadcast and pushed to the ODE for dispersal to all RSUs along I-80.

For the HMI, the vendor application will be tested on every update (with a test OBU) and when there is an update to the OBU. Once approved, the vendor will upload the update to the Google Play Store and it will be downloaded automatically once the HMI connects to the internet. It should be noted that the tablets could have updates of their own (e.g., updates from Samsung). Once notified of an update to the tablets, WYDOT will test for compatibility with HMI applications.

The same document above will detail processes for HMI and Weather Cloud updates.

As for the Weather Cloud sensors, this will be an ad hoc process. Vendors will provide the update to WYDOT and they will update the software during their regular vehicle maintenance schedule. More integrated approaches are being assessed for future implementation.

3.8 Mutual Operating Agreements (MOAs)

A copy of the existing Mutual Operating Agreement is included as Appendix A.

"Priority 1-defined as an outage that affects the safety of the traveling public and that has no work-around acceptable to the WYDOT user. In general, automated gates and closures, RSUs, and flashing beacons used for regulatory purposes such as road closures or chain laws, and variable speed limit signs are considered Priority l. Road weather information sensors and speed sensors within VSL sections or defined high wind corridors are considered Priority 1, with some exceptions. In some instances, other devices may also be considered Priority 1. Notification will occur if TMC is unable to remedy the situation remotely. Initial response will begin within one hour. Dispatch to the site, if necessary, should occur within two hours unless unsafe conditions exist."

3.9 Security and Privacy

System security is described in detail in the Security Management Operational Concept (Gopalakrishna, et al., 2016a).

3.10 Safety

Safety considerations are described in detail in the Safety Management Plan (Gopalakrishna, et al., 2016b).

4 In-Vehicle Devices

As described in Section 3, the *Vehicle System* is composed of vehicles equipped with a set of in-vehicle devices (i.e., OBU, antennas, wiring, HMI and weather sensors) with different levels of capabilities, which conform the four different vehicle subsystems. Despite of the vehicle subsystem, the maintenance and operation needs are common to all equipment. As such, this CMOP provides guidance on how to identify and address the following scenarios:

- Malfunction of a single in-vehicle component and/or software.
- Simultaneous malfunction of multiple in-vehicle components and/or software.
- Maintenance to one in-vehicle component.
- Maintenance schedule harmonization of multiple in-vehicle components.

It should be noted that while the O&M needs are independent of the vehicles where they are installed on, the process to address them is. This is due to the fact that each equipment can be installed in either a vehicle that WYDOT controls or have direct access to, such as WYDOT and Trihydro fleets, or a vehicle outside of WYDOT's control, such as those installed in partnered commercial vehicles. The CMOP provides guidance on the O&M procedures for the equipment installed on both WYDOT and fleet partner vehicles.

4.1 WYDOT Units

4.1.1 Operation Procedures

4.1.1.1 Operational Modes

4.1.1.1.1 Normal Operations

Operations are considered to be normal if all in-vehicle devices are working correctly, if an isolated OBU or HMI is malfunctioning, or if a non-critical system malfunctions (i.e., environmental sensor).

In the event of a failure, efforts will be made to bring non-critical systems back online as soon as practical during normal business hours. Support personnel will coordinate with the TMC if any further disruption of service is expected and when repairs are completed, they will let the TMC know.

On a periodic basis, WYDOT-owned fleet vehicles will be evaluated by Telecommunications personnel to ensure that OBUs, HMIs and environmental sensors are working correctly. If a problem is identified, corrective action will be taken, and if a fix cannot be implemented before the equipment is needed, the operators of the vehicle will be notified and the equipment will be scheduled for repair.

All software updates and repairs will be documented and recorded in the Google Sheet entitled "CV System Update."

4.1.1.1.2 Emergency Operations

Emergency operations will be declared if a security breach is detected to any in-vehicle device, a failure is experienced with a critical system or a series of OBUs malfunction.

In the event Emergency Operations are declared, the responsible person noted in Section 9 and GIS/ITS Program Manager will be notified as soon as possible and all efforts must be made to correct the problem expeditiously. Emergency call-back time and overtime will be authorized for anyone required to work on the outage. Repairs to critical systems will be documented and recorded in the Google Sheet entitled “CV System Log.”

If an in-vehicle device is suspected or identified to be under attack by a malicious software or by an unauthorized source, the event must be reported by the staff or user that first notice this event. ETS will be notified as well, although they are not expected to engage on it.

4.1.1.2 Diagnostic and Error Handling Procedures

In the event of an error to an in-vehicle device, any available error codes or screen captures will be documented along with the date and time they were noticed. This information will be stored in the Google Sheet entitled “CV System Log.” The responsible person noted in Section 9 must be notified, as appropriate, and work should commence to understand and mitigate the error as directed by the responsible person.

4.1.1.3 Restart/Recovery Procedures

In order to ensure the in-vehicle devices can be recovered in the event of a disaster, WYDOT will maintain proper backup and recovery procedures. Current versions of software for HMI, OBU and Weather Cloud sensors will be made available to each Telecommunications technician such that recovery can take place quickly.

4.1.1.4 Monitoring

The GIS/ITS Program will take the lead in monitoring in-vehicle devices and systems but other groups will also be involved. A layered approach will be used to secure and monitor OBUs, HMI and Weather Cloud Sensors.

Any abnormal network activities, data breaches or inappropriate attempts to access systems must be reported as soon as possible to the ETS security team, the GIS/ITS Program Manager, WYDOT’s leadership and to the responsible person identified in Section 9.

4.1.2 Maintenance Procedures

4.1.2.1 Regular Maintenance

WYDOT fleet vehicles are inspected daily with repair requests serviced by fleet mechanics and a rigging shop. The elevated mounts and external equipment to the vehicles for the CV pilot have been added to inspection routine. WYDOT’s Telecommunications program will be notified of any problem and the issue logged in WYDOT’s Vehicle Inspection Report system. If a pattern emerges, information will be logged in the CV System log.

In-vehicle systems will be tested during the evaluation phase and as soon as practical upon recognizing a problem. The OBUs, HMIs and environmental sensors will be periodically maintained and evaluated by Telecommunications techs every six months with records retained in the Google Spreadsheet entitled CV Maintenance Logs.

Inspection of the OBUs will focus on:

1. Antenna installation on roof of vehicle (Antenna is lying flat on roof or mount) and is not loose.
2. Wires are not fraying or broken.
3. OBU antenna connections are secure and not loose.
4. Wi-Fi antenna on OBU are secure and not loose.
5. Power source is connected securely and powers on the OBU unit when the vehicle is turned on.
6. OBU GPS readings are successfully coming in from the Lear HMI App.
7. Connection of OBU via a laptop to verify offloading of logfiles and receipt of TIMs via an RSU.

HMIs inspection will focus on:

1. Wires are not fraying or broken.
2. HMI is connected to a power source and successfully connects to the OBU after powered on when the vehicle has been running for more than 2 minutes.
3. Visual and Audio alerts are provided successfully.

Weather Cloud Sensors inspection will focus on:

1. Wires are not fraying or broken.
2. Sensor installation and connections are secure and not loose.
3. Information is being transmitted successfully to the OBU.

4.1.2.2 Software Updates

Software updates for OBUs and weather sensors will be tested by the GIS/ITS team before being delivered to Telecommunications for installation on OBUs. Software updates will also be recorded in the Google Spreadsheet entitled CV Maintenance Logs. HMI updates will be tested and provide by the vendors. When possible, software updates will be performed over-the-air (OTA) and through automated updates, as described in Section 3.7.

4.1.2.3 Modifications and Replacements

When modifications or hardware replacements are necessary to any in-vehicle device for issues that are not solved with OTA software or automated updates, the GIS/ITS staff will notify WYDOT Telecommunications staff to schedule any update on snow plows, patrol cars and other WYDOT fleet vehicles. The dates and software update versions, as well as any modifications and replacements, will be noted for all vehicles in an electronic Google Sheet entitled “CV System Update.” The TMC will monitor WYDOT in-vehicle devices on a continuous basis using the applicable tools noted in Section 7.

4.1.3 Roles and Responsibilities

Details of the personnel in charge of maintenance and operation of WYDOT's in-vehicle devices can be found in Sections 8 and 9, respectively.

4.1.4 Typical Scenarios

Table 4-1 showcases the maintenance and operational procedures for some typical scenarios that may occur during the demonstration period. Over the course of the demonstration period, any additional scenario will be logged.

Table 4-1. Typical Maintenance and Operation Scenarios for WYDOT's Units

Scenario	Procedure
Reported malfunction of an single in-vehicle component and/or software.	Vehicle inspections are performed before and after a driver's shift. Additionally, any problems identified during the shift will be reported to the TMC. Any issues will be notified to WYDOT Telecommunication, which will implement maintenance procedures described in Section 4.1.2.
System-level software bug identified for in-vehicle devices	Any system-level software issue will be handled by the GIS/ITS program. The GIS/ITS staff will coordinate with the different technical leads and vendors to develop the best approach to solve the problem. Updates will be sent OTA when possible.
System-level hardware issue identified for in-vehicle devices	Any system-level hardware issue will be handled by the GIS/ITS program. The GIS/ITS staff will coordinate with the different technical leads and vendors to develop the best approach to solve the problem.

4.2 Fleet Partner Units

4.2.1 Operation Procedures

WYDOT will not monitor fleet partner in-vehicle devices (i.e., HMI and OBU), as this would break privacy agreements with the partnering fleets.

4.2.2 Maintenance Procedures

4.2.2.1 Troubleshooting

WYDOT will provide fleet partners with basic troubleshooting guidance on all devices. This will be included in the installation kit and all training sessions provided to each fleet partner.

4.2.2.2 Software and System Updates

Software and system updates to the OBU and HMI will be performed as described in Section 3.7. It should be noted that fleet partner vehicles will not be equipped with environmental sensors.

4.2.2.3 Maintenance Request

Fleet partners will monitor their devices and report any issues to the WYDOT point of contact (POC) provided in Section 9. The Installation Kit will be available to the fleet partners throughout the demonstration period, which can be used for testing and troubleshooting.

WYDOT will provide technical support through telephone and email. WYDOT will coordinate the replacement of any in-vehicle device.

Any equipment replacement will be logged on the electronic Google Sheet "CV System Update."

4.2.3 Roles and Responsibilities

Each fleet partner will have a designated POC that will maintain a two-way communication with WYDOT's POC during the demonstration phase.

4.2.4 Typical Scenarios

Table 4-2 showcases the maintenance and operational procedures for some typical scenarios that may occur during the demonstration period for fleet partner vehicles. Over the course of the demonstration period, any additional scenario will be logged.

Table 4-2. Typical Maintenance and Operation Scenarios for Fleet Partner Units

Scenario	Procedure
Reported malfunction of an single in-vehicle component and/or software.	Partner reports through POC. WYDOT coordinates any support through email or telephone. WYDOT coordinates any repair and/or replacement.
System-level software bug identified for in-vehicle devices	Software updates will be sent OTA when possible.
System-level hardware issue identified for in-vehicle devices	WYDOT will communicate with partner through POC. WYDOT coordinates any support through email or telephone. WYDOT coordinates any repairs and/or replacement.

5 Field Devices

The CV Pilot System contains different field devices, namely RSUs and a set of network infrastructure, each with specific needs. The CMOP provides guidance on how to identify and address the following scenarios:

- Malfunction of a single RSU.
- Simultaneous malfunction of multiple RSUs.
- Maintenance to one RSU.
- Maintenance schedule harmonization of multiple RSUs.
- Malfunction of a single network infrastructure.
- Simultaneous malfunction of multiple network infrastructures.
- Maintenance to one network infrastructure.
- Maintenance schedule harmonization of multiple network infrastructure.

5.1 Operation Procedures

Software updates and restarts of RSUs under the purview of the GIS/ITS support team will be scheduled with the TMC to ensure minimal disruption of systems. No modifications or planned disruptions of the systems will be allowed during busy TMC periods, typically days with severe weather or expected heavy traffic. When necessary updates/restarts are completed, the TMC must be notified that all systems are returned to normal and the TMC must ensure systems are running correctly. The dates of all RSUs updates as well as any restarts of the devices will be recorded in an electronic Google Sheet entitled “CV System Log.” Any unusual restarts will be logged in the spreadsheet and if problems are noted, they will be addressed in a timely manner.

Updates or restarts to network infrastructure will largely be conducted by personnel from the Enterprise Technology Services (ETS) division of the State of Wyoming. Effort has been made by WYDOT to ensure ETS personnel have been involved in the planning of the CV Pilot project and that they understand the significance of reliable network operations. ETS personnel will notify and work with the TMC to minimize disruption during peak periods before any planned upgrades or restarts are executed.

The TMC will monitor field devices on a continuous basis using the applicable tools noted in Section 7.

5.1.1 Operational Modes

5.1.1.1 Normal Operations

Operations are considered to be normal if all systems are working correctly or if an isolated field device is malfunctioning. Note that RSUs are considered a critical component of this pilot.

In the event of a failure, efforts will be made to bring non-critical systems back online as soon as practical during normal business hours. Support personnel will coordinate with the TMC if any further disruption of service is expected and when repairs are completed, they will let the TMC know.

Problems with RSUs will be recorded in the GroupLink ticket system and addressed in accordance with the Mutual Operating Agreement. All software updates and repairs will be documented and recorded in the Google Sheet entitled “CV System Update.”

5.1.1.2 Emergency Operations

Emergency operations will be declared if a security breach is detected to any RSU or a series of RSUs malfunction. In the event Emergency Operations are declared, the responsible person noted in Section 9 and GIS/ITS Program Manager will be notified as soon as possible and all efforts must be made to correct the problem expeditiously. Emergency call-back time and overtime will be authorized for anyone required to work on the outage. RSUs and supporting field devices/communications will be addressed in accordance with the stablished Mutual Operating Agreement. Repairs to the critical field devices will be documented and recorded in the “CV System Log.” Repairs to RSUs will be documented in the Grouplink trouble ticket system as well.

If a roadside device is suspected or identified to be under attack by a malicious software or by an unauthorized source, the event must be reported by the staff or user that first notice this event. ETS will be notified as well, although they are not expected to engage on it.

5.1.2 Diagnostic and Error Handling Procedures

In the event of an error to a field device, any available error codes or screen captures will be documented along with the date and time they were noticed. This information will be stored in the “CV System Log.” The responsible person noted in Section 9 must be notified, as appropriate, and work should commence to understand and mitigate the error as directed by the responsible person.

5.1.3 Monitoring

The GIS/ITS Program will take the lead in monitoring devices, but other groups will also be involved. A layered approach will be used to secure and monitor roadside communications, network connectivity, and RSUs.

Any abnormal network activities, data breaches or inappropriate attempts to access systems must be reported as soon as possible to the ETS security team, the GIS/ITS Program Manager, WYDOT’s leadership and to the responsible person identified in Section 9.

5.2 Maintenance procedures

5.2.1 Regular Maintenance

Roadside units will be tested during the evaluation phase and as soon as possible upon recognizing a problem. The RSUs will be maintained and evaluated at least every 6 months with records retained in the Google Spreadsheet entitled CV Maintenance Logs. Logs will also be kept in cabinets at the roadside for quick access to previous issues. Radio communication, power, backup batteries, mounting brackets and bolt tension of RSUs will be inspected during semi-annual maintenance visits.

Roadside units will be inspected to ensure they are properly secured to their support structure and the following will be checked:

1. Power to the device can be verified based on the RSU LED light turned on.
2. Technician can log into the RSU via SSH from a secured connection.
3. Drive-bys of the RSU will then be performed to verify that TIMs and BSMs are broadcasting correctly from the RSU and received log files/BSMs from an OBU are correctly forwarded to the ODE system.

5.2.2 Software Updates

Software updates for RSUs will be tested by the GIS/ITS team before being delivered to ITS technicians for installation on RSUs. Software updates will also be recorded in the Google Spreadsheet entitled CV Maintenance Log. When possible, RSU updates will be performed OTA.

5.2.3 Modifications and Replacements

When OTA updates are not possible, WYDOT GIS/ITS will be tasked with conducting a site visit and identifying the issue, which may be related to the RSU or its power infrastructure. WYDOT GIS/ITS is also task with the replacement of any malfunctioning device or infrastructure.

WYDOT Telecommunications is tasked with replacing any malfunctioning communication infrastructure at their earliest possible convenience.

5.2.4 Roles and Responsibilities

Details of the personnel in charge of maintenance of field decides can be found in Section 8.

5.3 Typical Scenarios

Table 5-1 showcases the maintenance and operational procedures for some typical scenarios for field devices that may occur during the demonstration period. Over the course of the demonstration period, any additional scenario will be logged.

Table 5-1. Typical Maintenance and Operation Scenarios for Field Devices.

Scenario	Procedure
Individual RSU is: • Non-responsive, • Reporting an error, or • Performing at a degraded level.	TMC will monitor all RSUs through the System Monitoring Device Management (SMDM) tool. Any issues will first be addressed remotely. If the issue cannot be solved remotely, the TMC will dispatch the necessary personnel based on the stablished MOA. Any repair or replacement will follow the process described in Section 5.2.
System-level software bug identified for RSUs	TMC will monitored all RSUs through the System Monitoring Device Management (SMDM) tool. Any issues will first be addressed remotely. TMC will coordinate with the GIS/ITS to deploy any necessary OTA update. If the issue cannot be solved remotely, GIS/ITS will be tasked with coordinating any system-level software update.
System-level hardware issue identified for RSUs	TMC will monitored all RSUs through the System Monitoring Device Management (SMDM) tool. If the issue cannot be solved remotely, GIS/ITS will be tasked with coordinating any system-level repair and/or replacement of devices.

6 Transportation Management Center – CV Systems

The CV Pilot System contains different CV Systems (i.e., back-office) hosted by the TMC that ensure the ingest, validation, processing, analysis and distribution of information. In detail, the CV system encompass subsystems of the *Wyoming CV System* and *External Interfaces*—see Sections 3.3 and 3.4. The CMOP provides guidance on how to identify and address scenarios that impact their operations, such as:

- Malfunction of a single CV System.
- Simultaneous malfunction of multiple CV Systems.
- Maintenance to one CV System.
- Maintenance schedule harmonization of multiple CV Systems.

6.1 Operational Procedures

Software updates and restarts of the CV Systems under the purview of the GIS/ITS support team will be scheduled with the Transportation Management Center to ensure minimal disruption of systems. No modifications or planned disruptions of the systems will be allowed during busy TMC periods, typically days with severe weather or expected heavy traffic. When necessary updates/restarts are completed, the TMC must be notified that all systems are returned to normal and the TMC must ensure systems are running correctly. The dates of all CV System updates as well as any restarts of the devices will be recorded in an electronic Google Sheet entitled “CV System Log.” Any unusual restarts will be logged in the spreadsheet and if problems are noted, they will be addressed in a timely manner.

The TMC will monitor CV Systems on a continuous basis using the applicable tools noted in Section 7.

6.1.1 Operational Modes

6.1.1.1 Normal Operations

Operations are considered to be normal if all systems are working correctly or if a non-critical system malfunctions. Non-critical CV systems include:

- Pikalert
- Service Monitor Device Management
- Mobile app for Truck Parking
- Commercial Vehicle Operator Portal

In the event of a failure, efforts will be made to bring non-critical systems back online as soon as practical during normal business hours. Support personnel will coordinate with the TMC if any further disruption of service is expected and when repairs are completed, they will let the TMC know.

All software updates and repairs will be documented and recorded in the Google Sheet entitled "CV System Update."

6.1.1.2 Emergency Operations

Emergency operations will be declared if a security breach is detected to any system and/or a failure is experienced with a critical system. Critical systems include:

- CV Data warehouse
- WTI Data Broker
- Operational Data Environment (ODE)
- Third party data feed
- Transportation Reports and Action Console (TRAC)
- Travel Information Message Builder

In the event Emergency Operations are declared, the responsible person noted in Section 8 and GIS/ITS Program Manager will be notified as soon as possible and all efforts must be made to correct the problem expeditiously. Emergency call-back time and overtime will be authorized for anyone required to work on the outage. Issues with the CV Systems will be addressed by the person identified in Section 8. Repairs to critical systems will be documented and recorded in the Google Sheet entitled "CV System Log."

If a CV System is suspected or identified to be under attack by a malicious software or by an unauthorized source, the event must be reported in accordance with ETS Policy 9400-P190: Reporting Security Events and Vulnerabilities, attached as *Appendix B*, and ETS Policy 9400-P191: Security Incident Management, attached as *Appendix C*.

6.1.2 Diagnostic and Error Handling Procedures

In the event of an error to a central CV system, any available error codes or screen captures will be documented along with the date and time they were noticed. This information will be stored in the Google Sheet entitled, CV System Log. The responsible person noted in Section 9 must be notified, as appropriate, and work should commence to understand and mitigate the error as directed by the responsible person.

6.1.3 Restart/Recovery Procedures

In order to ensure the CV Systems can be recovered in the event of a disaster, WYDOT will maintain proper backup and recovery procedures. The Pikalert, database, data warehouse, Data Broker, TMDD data feed, Operational Data Environment and more will be backed up to tape using the *full daily back-up* method. Tapes will be shuttled off-site to the WYDOT vault and backup procedures will be tested on the first Monday of every month with a complete restore to virtual machines. Any changes or improvements to this process will be recorded on a separate document.

6.1.4 Monitoring

The GIS/ITS Program will take the lead in monitoring the central systems but other groups will also be involved.

Any abnormal network activities, data breaches or inappropriate attempts to access systems must be reported as soon as possible to the ETS security team, the GIS/ITS Program Manager, WYDOT's leadership and to the responsible person identified in Section 9.

6.2 Maintenance Procedures

6.2.1 Regular Maintenance

CV Systems will be maintained continuously with software patches and upgrades applied monthly to address hardware issues, security updates and system enhancements. Zero-day vulnerabilities will be patched rapidly to ensure the integrity of the systems. Operating systems, databases, and CV-specific software will be considered for zero-day and routine updates. Hardware replacements will be performed by the GIS/ITS team after consultation with the pilot's Technical Lead.

In the case of HSM, WYDOT is currently pursuing a contract with Greenhills Software to provide maintenance and management, and to provide training to WYDOT staff on high-level maintenance.

6.2.2 Software Updates

Software updates, database changes and enhancements to CV Systems will be tested by the GIS/ITS team before being applied to production systems. All modifications will also be recorded in the Google Spreadsheet entitled "CV System Updates."

6.2.3 Roles and Responsibilities

Details of the personnel in charge of CV Systems maintenance can be found in Section 8.

7 Monitoring Tools

The TMC will monitor field devices, in-vehicle devices and core CV systems on a continuous basis using a subset of tools noted in Table 7-1. Periodic software updates will be considered normal operations with updates coordinated with the TMC and documented in the Google Sheet entitled "CV System Log."

Table 7-1. Monitoring Tools and Responsibilities.

Focus	Tool	Responsibility	Notes
Virus/Malware protection	Crowdstrike	ETS Security Team	In accordance with Policy 3200-P161: Malicious Code Prevention
Hardware	HSM	GIS/ITS	HSM on RSUs, OBUs and in the TMC
Network reliability	Solarwinds	GIS/ITS, ETS and Telecommunications	Firewall, router, switch, power, radio and connectivity monitoring
Network access control	Firewalls	GIS/ITS, ETS	Access is limited and logs retained
RSUs	SMDM	GIS/ITS	Service Monitor Device Management (SMDM) - capable of checking health of roadside units and upgrading roadside systems.
	Web Dashboard	GIS/ITS	Web-based dashboard for viewing RSU status.
OBU and HMI on WYDOT vehicles	Putty	GIS/ITS and Telecommunications	Periodic health check of in-vehicle systems
Weather Cloud Sensor	No tool available at this time	GIS/ITS	This will be done ad hoc, through the revision of the logs.
Backups	Veritas BackupExec	GIS/ITS	Backup of database and other critical systems
Database	Access Controls, Logs and Encryption	GIS/ITS	Tables including personally identifiable information are encrypted. Access is limited and activity is logged.
Disk and Memory	Watchdog	GIS/ITS	Monitoring of database tables, disk space and memory of critical systems
HVAC	Environmental sensors	Buildings and Grounds	Moisture and heat sensing in server area
Power	UPS and Generator	Buildings and Grounds	Generator tested weekly with fuel replaced periodically. UPS tested and inspected annually.
Server Room	Access Control	Buildings and Grounds	Camera and door logs of access to server area

8 Maintenance Roles and Responsibilities

Maintenance of the different WYDOT's CV Pilot components will be performed by various individuals and groups around the Department, as listed below.

- Telecommunications personnel will be responsible for periodically ensuring OBUs, HMIs and WC are functioning properly and they will be responsible for the wireless network infrastructure necessary to connect land-based systems to road-side units.
- Enterprise Technology Services personnel will be responsible for the land-based network systems to include communication links and routers necessary to connect field equipment to WYDOT's TMC.
- WYDOT's GIS/ITS personnel will be responsible for RSUs and software updates to the central CV systems, on-board units and the central database.
- WYDOT's Buildings and Grounds personnel will be responsible for generated power, UPS and HVAC systems for the TMC personnel and for the CV computer systems.

The specific personnel envisioned for each activity is listed in Table 8-1.

Table 8-1. Maintenance Roles and Responsibilities

Name	Organization	Role
Troy Babbitt	WYDOT Telecommunication Program	In-vehicle Hardware Manager WYDOT fleet. Roadside communication to RSUs.
Tommy Scott	WYDOT GIS/ITS Program	RSU Hardware Manager
Various	Fleet companies	In-vehicle Hardware Manager private fleet
Brian Peel	WYDOT GIS/ITS	In-vehicle Software Manager WYDOT fleet. CV Software and Database systems support. POC for HSM Maintenance and Operations.
Tom Schreur	WYDOT GIS/ITS	CV Computer systems support
Ray Vigil	WYDOT Buildings and Grounds	Generated power, UPS and HVAC for CV computer systems and TMC operations
Shaik, Nazeer	Lear	Provide technical support on Lear Hardware and Software. The POC contact information is provided below: Nazeer Shaik Ph: 510-861-8614 Nshaik@lear.com
George Greenwood	Weather Cloud	Provide technical support on Weather Cloud Hardware and Software.

		The POC contact information is provided below: George Greenwood Sr. Mngr. Partner Relations, Client Engagement Fathym (www.fathym.com) 5485 Conestoga Ct., Suite 210 Boulder CO 80301 Phone: (303) 817-2993 Email: george.greenwood@fathym.com
Kane, Jeffrey	Sirius XM	Provide technical support on Sirius XM Hardware and Software. The POC contact information is provided below: Jeffrey Kane Director - Product Development 27200 Haggerty Rd. Suite B-3 Farmington Hills Mi 48331 Phone: (248) 699-0470 Cell: (248) 470-1120 Email: jeffrey.kane@siriusxm.com

9 Operations Roles and Responsibilities

After the performance and evaluation period of the pilot project, WYDOT intends to continue to offer a functioning CV system. RSUs will remain on the roadside and all in-vehicle equipment will remain operational in WYDOT vehicles. Fleet partners are encouraged to continue system operation, but will be responsible for establishing their own operations plans.

WYDOT TMC will play the key role in operating the *Wyoming CV System* and monitoring for abnormalities. The CV development team has made considerable effort to ensure TMC Operators are not burdened by new systems. While the TMC Operators will be presented with new information from environmental sensors and the Pikalert system that will improve road and travel condition reporting accuracy and variable speed limit postings, the vast majority of CV operational tasks have been integrated into existing systems such that no additional actions are required of the TMC staff. This includes the posting of Traveler Information Messages (TIMs) which are automatically done using existing processes.

There are several operational support roles filled by WYDOT's Telecommunication Program and WYDOT's GIS/ITS staff. The Telecommunication staff will play two major roles in the Wyoming CV Pilot project. First, they will install in-vehicle systems (OBUs, HMIs, WC) and conduct periodic tests to ensure the equipment is working properly. Second, they will monitor the roadside network to ensure it is working properly, and if a problem is identified, they will respond with priority as described in WYDOT's stablished Mutual Operating Agreement.

The GIS/ITS staff will support the CV computer infrastructure (CV central systems, which include back office systems and the support of hardware and disaster recovery systems), they will make or lead software adjustments as needed, they will provide firmware updates to RSUs and they will ensure the RSUs are working properly. In the event of a problem to a roadside system, the GIS/ITS field staff will respond with priority as described in WYDOT's Mutual Operating Agreement.

Table 9-1 lists the responsible parties for operating and maintaining the CV systems during the evaluation period and beyond.

Table 9-1. Operation Roles and Responsibilities

System/ Component	Name	Organization	Role
In-vehicle devices – WYDOT Units	Troy Babbitt	WYDOT Telecommunication Program	In-vehicle system Hardware Manager WYDOT fleet
	Brian Peel	WYDOT GIS/ITS	OBU Software Manager WYDOT fleet
	Various	Fleet companies	OBU Hardware Manager private fleet

In-vehicle devices – Fleet Partner	Vince Garcia (with support from all WYDOT GIS/ITS staff)	WYDOT GIS/ITS	WYDOT's POC to Fleet Companies
RSU	Tommy Scott	WYDOT GIS/ITS Program	RSU Hardware Manager
	Troy Babbitt	WYDOT Telecom	Roadside communication to RSUs
Back-Office	Brian Peel	WYDOT GIS/ITS	CV Software and Database systems support
	ETS	Enterprise Technology Services	Network infrastructure
	Tom Schreur	WYDOT GIS/ITS	CV Computer systems support
	Ray Vigil	WYDOT Buildings and Grounds	Generated power, UPS and HVAC for CV computer systems and TMC operations
	Kevin Cox	WYDOT GIS/ITS	Operation of CV systems from TMC

10 Configuration and Inventory Management

The CV Central System consists of two servers and a storage area network housed in the ITS server room in Cheyenne, Wyoming. The CV systems reside on Dell 730 series servers labeled as CR-731 and CR-732 and connect to a database system that resides on two Sun servers labeled as ODB01 and ODB02. The CV system is a number of virtual servers running on the Microsoft Hyper-V platform. The facility is supported by battery backup and a generator that is tested on a weekly basis. The facility is monitored with a camera and the door can only be accessed by a small and defined list of people who have card key access. The details of the configuration are provided in Appendix D.

The systems that reside on the CR-731 server are:

- CVODEDP01 - Connected Vehicle Operational Data Exchange Development - 10.145.9.204
- CVPIKPP01 - Connected Vehicle Pikalert Production - 10.145.200.54

The systems that reside on the CR-732 server are:

- CVODEPP01 - Connected Vehicle Operational Data Exchange Production - 10.145.9.205
- CVPIKDP01 - Connected Vehicle Pikalert Development - 10.145.200.53
- CVPTDP01 – Participant Tracker (development) - 10.145.9.206
- CVPTPP01 – Participant Tracker (production) - 10.145.9.207
- TMDD-DEV-WYDOT - Connected Vehicle TMDD Feed Development - 10.145.200.49
- TMDD-PROD-WYDOT - Connected Vehicle TMDD Feed Production - 10.145.9.5

11 Software Licensing

WYDOT will ensure the following products are properly licensed throughout the project.

Table 11-1. Software Licensing

Item	Details
Software	Oracle RDBMS
Version	12c
Responsible Party	Brian Peel
Software	Microsoft Hyper-V
Version	2016
Responsible Party	Tom Schreur

12 Approvals

This plan is effective as of the most recent date from the signatures provided below. All signatures indicate acceptance of the CMOP.

R. Vince Garcia (Site Lead)	Date
Brian Peel (GIS/ITS Technical Supervisor)	Date
Tom Schreur (GIS/ITS)	Date
Troy Babbitt (Telecommunications Program Manager)	Date
Ray Vigil (Buildings and Grounds Supervisor)	Date

Appendix A. Sample MOA

WYDOT ITS Devices-Mutual Operating Agreement
Original: March 13, 2007

1. Introduction

This Mutual Operating agreement (MOA) outlines fundamental principles regarding Intelligent Transportation System (ITS) devices as described in the following. This agreement will provide broad outlines for responsibilities, priorities and measures for use among key Wyoming Department of Transportation (WYDOT) and Enterprise Technology Services programs involved with maintenance of ITS devices.

2. Scope

This agreement addresses the following devices. See Section 3 for service priority levels. Devices may be in more than one category or move between categories - depending on function, inter-dependency with another system, operational needs, or other circumstances.

A. Regulatory Devices Directing the Public (such as Black and White Signs)
- Road Closure Gates
- Variable Speed Limit (VSL) Signs
- Flashing Beacon Signs
- Permanent Dynamic Message Signs (most cases)
- Portable Dynamic Message Signs (some cases)

B. Informational Devices Advising the Public (such as Black and Yellow Signs)
- Permanent Dynamic Message Signs (some cases)
- Portable Dynamic Message Signs (most cases)
- Permanent Highway Advisory Radio (HAR)
- Portable Highway Advisory Radio (HAR)
- Warning Systems
- Internet Access for Conditions and Web-cams
- Information Beacon Signs (Tune to 1610, and so forth)
- Connected Vehicle Roadside Units (RSUs)
- Connected Vehicle On-board Units (OBUs)

C. Support Devices Providing Information to the Traffic Management Center (TMC)
- Road and Weather Information Systems (RWIS)
- Traffic Speed Sensors
- Fixed and Pan/Tilt/Zoom (PTZ) Web Cameras

D. Other Devices
- Weigh-In-Motion Traffic Sensors
- Wi-Fi Radios and Antennas

E. Out-of-scope Devices and Systems
- Traffic Signals
- Traffic Counters
- Curve Warning Devices
- Local Closed Circuit TV (CCTV) Video systems that are not remotely accessed

- Rest Area Kiosk WiFi

3. Service Priority Levels and Maintenance Response Times

The following service level priority definitions and maintenance response times will be used under this agreement.

A. **Priority 1**-defined as an outage that affects the safety of the traveling public and that has no work-around acceptable to the WYDOT user. In general, automated gates and closures, RSUs, and flashing beacons used for regulatory purposes such as road closures or chain laws, and variable speed limit signs are considered Priority l. Road weather information sensors and speed sensors within VSL sections or defined high wind corridors are considered Priority 1, with some exceptions. In some instances, other devices may also be considered Priority 1. Notification will occur if TMC is unable to remedy the situation remotely. Initial response will begin *within one hour.* Dispatch to the site, if necessary, should occur *within two hours unless unsafe conditions exist.*

B. **Priority 2**-defined as an outage with the potential to affect the safety of the traveling public, but one for which a workaround acceptable to the WYDOT user exists. Permanent dynamic message signs, OBUs, portable dynamic message signs, Roadside and fuel site Wi-Fi radios and antennas will be considered Priority 2. Notification will occur *during normal waking hours including weekends* (defined for purposes of this agreement as 7 a.m. to 10 p.m.). Work will begin *no later than the next business day.* All devices that utilizing commercial communication services, that the provider can't guarantee Priority 1 service.

C. **Priority 3**-defined as an outage not affecting the safety of the traveling public. Notification will occur *the next business day during normal working hours.* Work will be scheduled to occur *within one week.*

D. **Priority 4**-includes Preventive Maintenance and all other work related to Telecom Devices. Work will occur as scheduled by IT, ITS, ETS, or WYDOT Telecom.

E. **Priority Guidelines:**
   1. In considering service level priorities, use the example of when work takes precedence over a dental appointment. Work categorized at the Priority 1 or Priority 2 level takes precedence over a hypothetical dental appointment; work categorized at the Priority 3 or Priority 4 level does not.
   2. When issue response priority is determined, consideration should be given to whether a work-around exists. Issues with workarounds that can be implemented in the appropriate maintenance response time should be assigned lower priority (i.e. the next business day for Priority 2 issues).
   3. In general, response priority will be given to those systems rated as high volume routes (Interstates, principal arterials, and urban routes) on the current Snow Control Priorities Map.
   4. Other events and local conditions will also be considered and judgment calls will be allowed when priorities are assigned. Outage response may be escalated or deferred by Telecom, ITS, or the TMC lead as appropriate and documented on Grouplink ticket by the owner of the Grouplink Ticket.

4. Primary Service Responsibility and Roles

Programmatic authority and responsibility for maintaining the devices described in this agreement rests with the GIS-ITS Program. Following are responsibilities under this agreement:

WYDOT IT/ETS-WYDOT base network, IP backhaul routers at telecommunications radio sites, any shared network monitoring application, general PC support and network-connected Wi-Fi at WYDOT buildings, fuel sites, and upkeep/maintenance of SolarWinds.

GIS-ITS-Deployment; software maintenance; specialty computer hardware; programmatic decisions including budget, 24 hours/7 days a week device monitoring, cellular modems; roadside location infrastructure (excluding power where there is no GIS-ITS device), CompassTrac, RSUs, Road Condition Reporting App, reporting app tablet computers and WiFi security management that supports the tablet.

Telecommunications-commercial communications services (excluding cellular modems); HAR systems and related infrastructure; WYDOT wireless communication systems and programming configurations, to include roadside WiFi radios and antennas; and in-vehicle electronics integration; in support of ITS devices and systems.

5. Grouplink, Documentation & Mutual Aid

Grouplink tickets will be opened by the TMC when possible. TMC will notify appropriate ITS or Telecom Tech of outage. If the outage involves ETS managed routers, the TMC will contact ETS at 777-3995. If Telecom or ITS notices an outage first, they will contact the TMC to verify the outage, and request the TMC to open a Grouplink ticket. All Grouplink tickets shall be routed and assigned to the appropriate TMC, ITS, or Telecom Programs and personnel. Each ticket must include details of the "positive" handoff to the next responsible Program person (i.e. a phone call to a Program On-Call technician). When comments, actions, or resolutions are added to a ticket, include all affected Program personnel on the Cc line, including the affected district's ITS and Telecom technicians (such as phone techs for DSL problems). Assigned technicians will close the Grouplink ticket when completed, upon verifying with TMC that all affected devices are operational.

"Mutual Aid" is a Cross-Program arrangement created to help minimize outage times by decreasing response time to an outage. As needed, if an assigned tech is out of position or requires extend travel time, they may contact the closest tech to ask for assistance with basic troubleshooting of the outage. This assistance is to follow the Subject to Call guidelines.

6. Agreement

The following agree to the terms of this document. Terms will be re-evaluated periodically.

R. Vince Garcia, P.E., GIS-ITS Manager

_____ Date _____

Dan Tolman, Information Technology Manager

_____ Date _____

Troy Babbitt, Telecommunications Manager

_____ Date _____

<Name>, ETS Manager

_____ Date _____

Appendix B. 9400-P190: Reporting Security Events and Vulnerabilities

I. PURPOSE

This policy establishes requirements for reporting and responding to information security events and vulnerabilities.

Note: This policy deals with cyber (information technology) security and does not address the physical security of facilities or assets. Response to a breach of physical security shall be governed by other policies/procedures as appropriate. If unauthorized physical access to a technology resource leads to unauthorized logical access to state information, multiple reporting policies, including this policy, are applicable.

II. SCOPE

This policy applies to all executive branch agencies, boards, and commissions (collectively referred to as “agencies”) of the State of Wyoming.

III. POLICY

As a condition of access to state information resources, all members of the workforce shall report events, suspected incidents, or system vulnerabilities to a supervisor and/or appropriate agency IT staff in a timely manner. Supervisors shall ensure that IT is informed.

Note: This requirement shall NOT be construed in any manner to encourage, authorize, or condone an intentional search for system weaknesses and/or malfunctions. Intentional acts of exploring state information resources to discover weaknesses or malfunctions in security controls by personnel who are not authorized to do so shall be deemed to be malicious and unauthorized hacking.

An event shall be declared a security incident by an agency-identified security and/or technical professional when there is sufficient evidence to indicate that it is adverse to the interests of the agency’s information stewardship and/or meet pre-established criteria for security incident declaration.

Agencies shall respond to all reported events that have the potential to become security incidents.

Agencies shall have a working plan for reporting on, responding to, recovering from, and preventing recurrence of information security incidents. The plan shall be kept up to date and continually improved upon with lessons learned. Procedures to execute the plan shall be repeatable and thorough, yet flexible enough to handle an ever-changing threat environment.

Detailed procedures and contingencies for the implementation of incident response shall be labeled confidential and distributed on a need-to-know basis.

Executives responsible for the impacted agency shall participate in the incident response process.

Personnel tasked with incident response shall be proficient in their specific responsibilities (see Pending Policy 9400-P191: Security Incident Management).

System administrators of state information resources are empowered and expected to terminate communications with internal or external entities operating in a manner injurious to the security and operations of the agency or the state's wide area network (WAN). Administrators shall take measures to stop the threat then perform the required notifications. The appropriate notifications shall be made when time permits on the events and actions taken during the emergency.

CIO Approved Date: 03/18/2009

Appendix C. 09400-P191 Information Security Incident Management and Reporting Policy

I. Purpose

This policy establishes requirements to ensure the scope and impact of IT security incidents are properly evaluated, coordinated, and reported. This centralized approach is used to determine if, when and how to communicate notification of an incident.

II. Scope

This policy applies to all agencies as defined in W.S. 9-2-2904(a)(i).

III. Policy

A. Agency responsibilities:

   a. All users of the State of Wyoming's computer networks are responsible for ensuring that all known or suspected information, information technology security incidents or threats are reported to their supervisor.

   b. Supervisors shall ensure that appropriate IT staff is informed.

   c. Agencies may also have internal reporting policy which must be followed.

   d. Where incident reporting is required for the purpose of meeting compliance guidelines, agencies are responsible for reporting their own cybersecurity incidents to the appropriate compliance authority.

B. Enterprise support responsibilities:

   a. There shall be an enterprise level procedure to ensure that suspected cybersecurity incidents and threats can be reported, validated, classified and tracked.

   b. There shall be an enterprise level procedure to ensure appropriate and timely response to any discovered cybersecurity incidents or threats.

Appendix D. CV Central System Configuration

The following are the different components of the CV Central System.

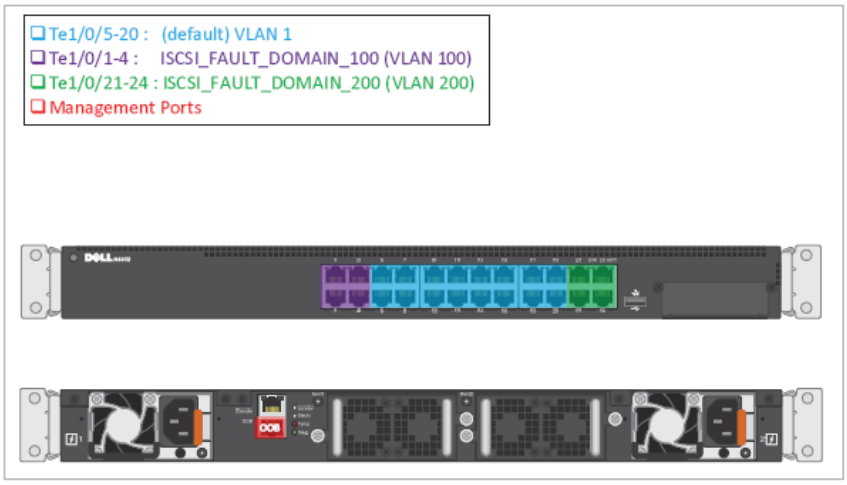


Figure D- 1. Connected Vehicle – Dell N4032 Switch (24 ports, 10GBase-T). Source: Dell

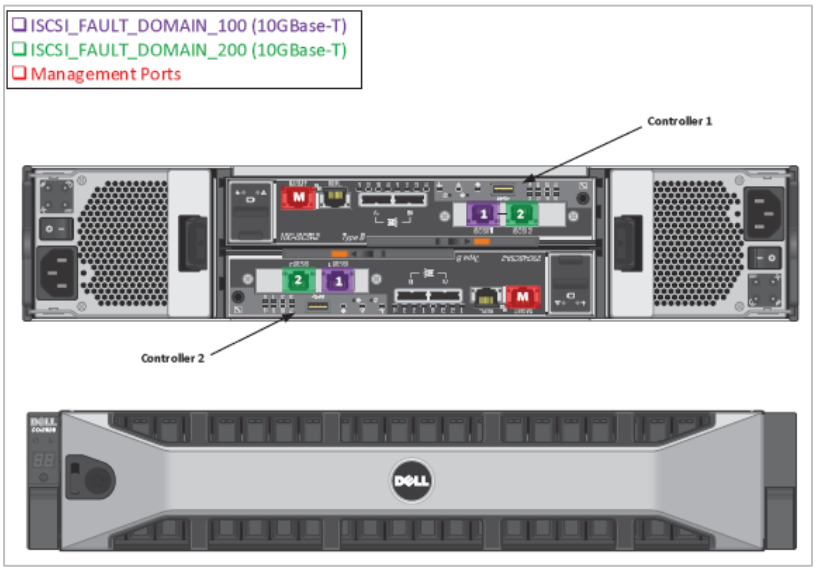


Figure D- 2. Connected Vehicle – Dell SCv2020 Storage Array. Source: Dell

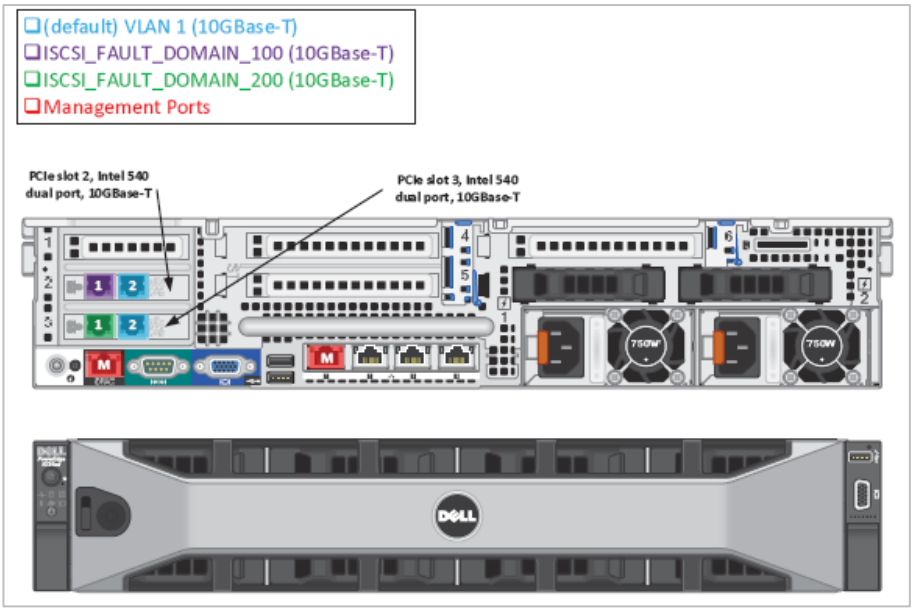


Figure D- 3. Connected Vehicle – Dell R730 Server. Source: Dell

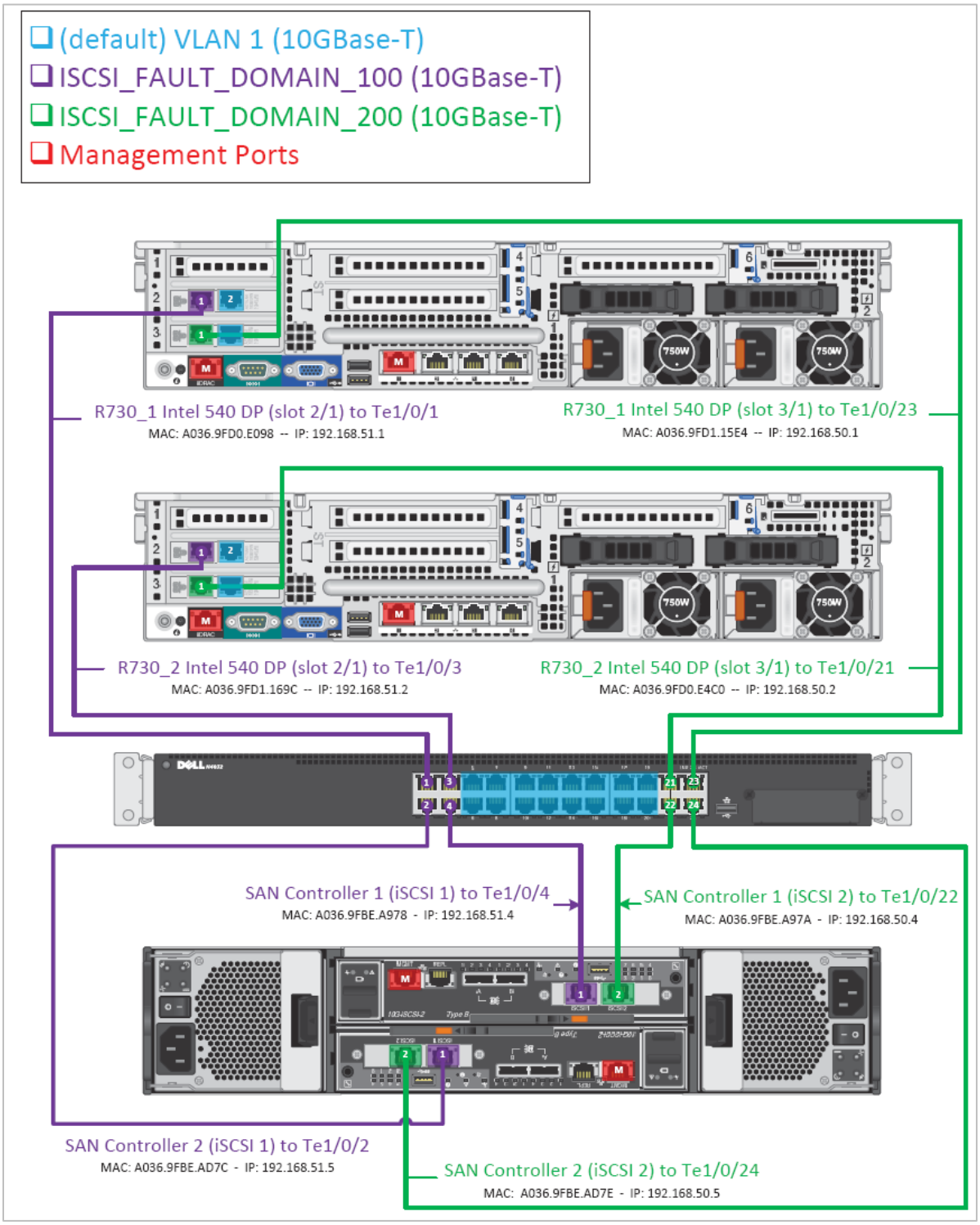


Figure D- 4. Connected Vehicle - 10GBase-T Storage Area Network. Source: Dell

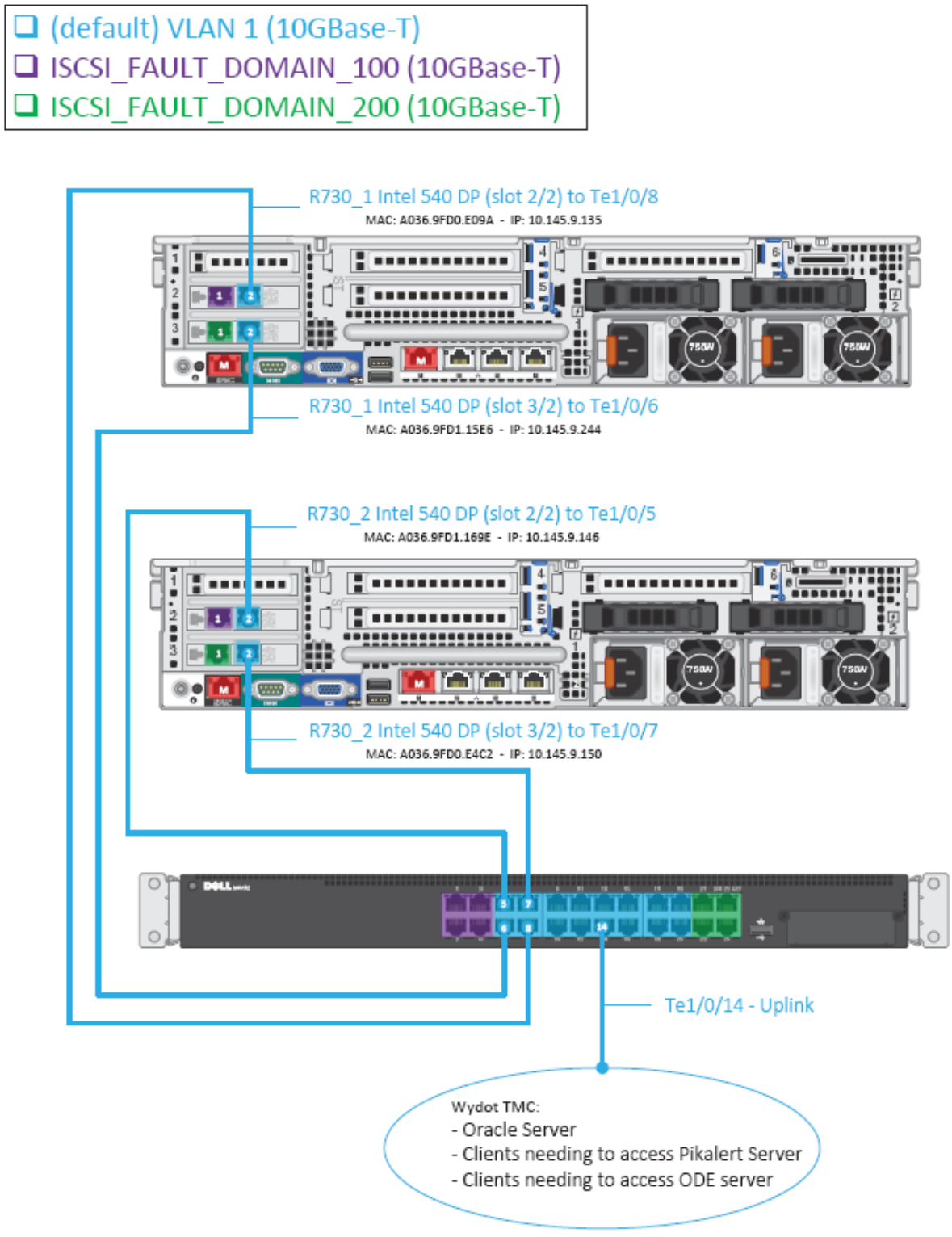


Figure D- 5. Connected Vehicle - Server Data Network. Source: Dell

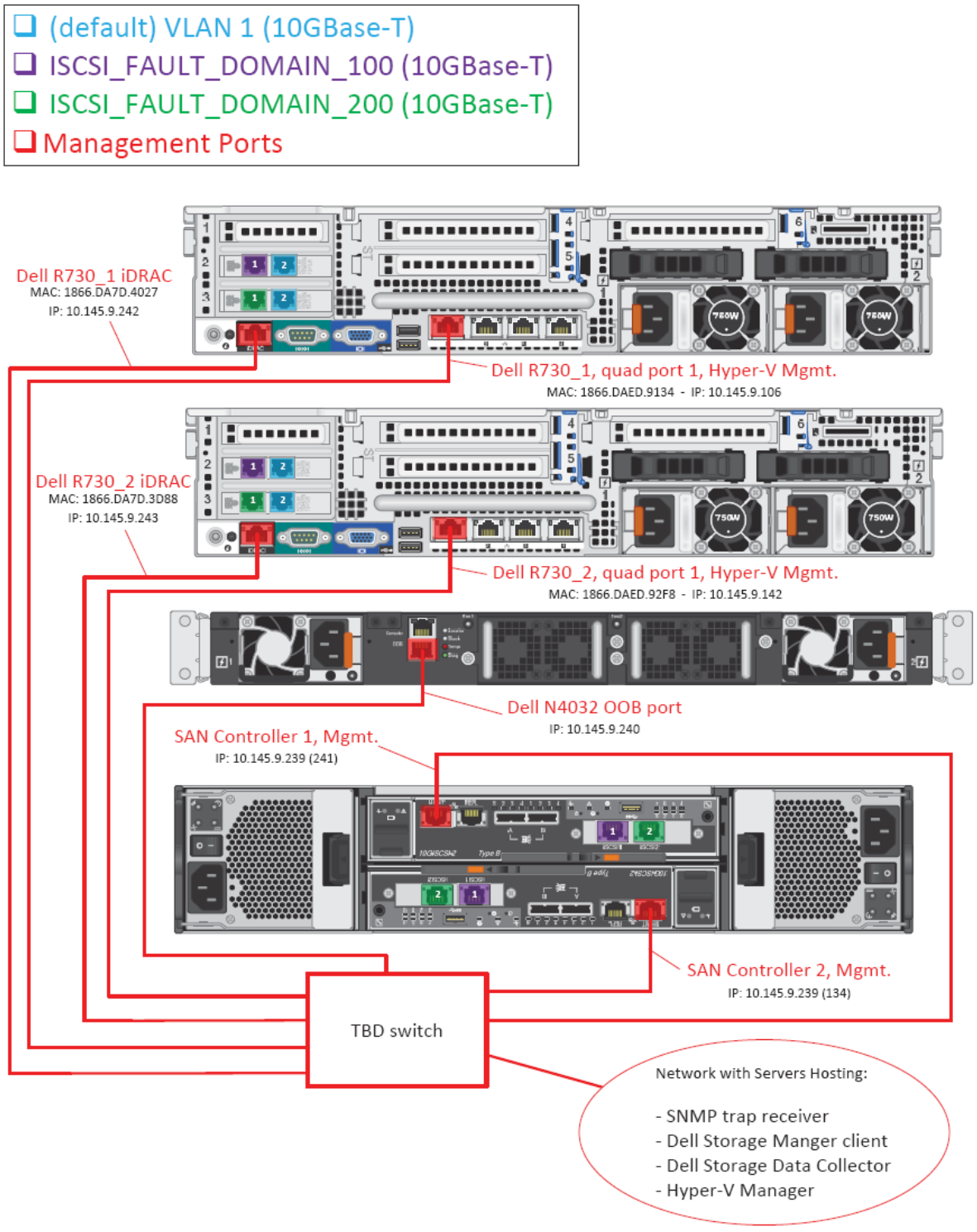


Figure D- 6. Connected Vehicle Management Network. Source: Dell

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-17-473

U.S. Department of Transportation