Recommended Guidance for Remote OBD I/M Programs

September 2010

Transitioning I/M Workgroup

Mobile Source Technical Review Subcommittee

Clean Air Act Advisory Committee

Table of Contents

Appendices

I. Introduction

This document is intended to provide guidance to states that are considering implementing a Remote Onboard Diagnostic (OBD) Inspection/Maintenance (I/M) program either as an addition to an existing periodic inspection system or as a stand-alone program. It presents one approach that constitutes a recommended method for obtaining continuous testing credit using wireless technology. There may be other ways to obtain continuous testing credit that are not identified in this document. Likewise, there may be uses of wireless OBD testing other than that presented in this guidance. The term "Remote OBD I/M" as used in this document refers to wireless, continuous OBD testing. This represents a new approach to I/M that has not been fully deployed in a program to date, although several pilot studies and initial roll outs are underway. Thus, this guidance is intended to raise issues and make recommendations to facilitate the use of wireless technologies in I/M settings. This guidance sets out a framework for states to use in Requests for Proposals and overall program development when using Remote OBD in an I/M program. It will be important for I/M programs and other stakeholders to consider other important issues, such as data collection methods, motorist privacy issues, technology utilization, and third party business models prior to implementing any such program. The work reflected here is the effort of the Remote OBD Workgroup and the Transitioning I/M Workgroup, which are part of the Mobile Source Technical Review Subcommittee. The Workgroup approved this recommended guidance in a meeting on September 27, 2010 in Breckenridge, Colorado. More information and the charter for the workgroup can be found in Appendix 1. The purpose of the workgroup as expressed in this report is to recommend to EPA a national technical standard for Remote OBD I/M.

A Remote OBD system is comprised of three basic elements:

1. A Remote OBD Link, which is a device on-board the vehicle that continuously captures data from the OBD system and transmits it wirelessly.
2. A method of receiving the data from the Remote OBD Link, which may be an existing wireless network or one specifically created for the purpose.
3. A Data Management System (DMS) that processes the Remote OBD data and performs I/M specific functions including determining pass/fail conditions and reporting to the administrative agencies and motorists.

The Workgroup has attempted to address many of the technical and policy questions related to implementing Remote OBD. One goal was to make it easier for states to add a Remote OBD program to Requests for Proposals. Another goal was to standardize to the extent reasonable the approach to Remote OBD such that systems and technologies may be compatible across state lines.

II. General Design Requirements

Remote OBD offers the opportunity for owners of OBD-equipped vehicles to avoid having to get a periodic, physical inspection of their motor vehicle, and yet still comply with the requirements for an OBD inspection. Due to the *continuous* nature of Remote OBD, as opposed to the annual or biennial tests now done in periodic I/M programs, Remote OBD can find problems with motor vehicles more quickly, leading to faster repairs and, thus, more emission benefits. In addition, continuous monitoring allows the program to specify more stringent readiness criteria than a

periodic program. This means determining the malfunction indicator light (MIL) is off and all monitors are ready prior to concluding that a vehicle is repaired, and in the case of persistent failure to set readiness, it allows for corrective action.

In broad terms, a Remote OBD program will involve either installing a device on a 1996 or newer OBD equipped vehicle or using existing on-vehicle telemetrics to monitor the OBD system on a *continuous* basis. When a problem occurs with the vehicle's emission control system and the MIL is "commanded on," the motorist will be notified that vehicle repair work is required. In such cases, the program will take steps to follow-up on such vehicles to ensure that the MIL goes "off" within the grace period allowed for repairs. This approach frees the motorist from having to show up for a periodic inspection of the vehicle, and might be substantially less expensive than the traditional periodic inspection program.

One of the basic questions regarding Remote OBD is what constitutes *continuous* monitoring. The following working definition is recommended and used as the basis for this guidance:

> A Remote OBD system should be designed such that 80% of the vehicles enrolled in the program and operated routinely in the area communicate with the network at least once every 14 days, with the other 20% "seen," i.e., they communicate with the network, at least once per month. It is expected that vehicles will drop out of the program as they are transferred out of the area or scrapped, and that such withdrawals should be excluded from this calculation. If after 2 months a vehicle is not seen by the Remote OBD system, the motorist should be contacted to determine the cause. Action should be taken as appropriate to either remove non-respondents, transferred vehicles, and scrapped vehicles from the DMS or to fix any problem that might prevent the required transmission of data from the vehicle to the network. A vehicle that is routinely "seen" according to this standard would be considered in compliance with the information reporting standards and eligible for re-registration.

Another basic question relates to the conditions under which a motorist participates in Remote OBD. The Workgroup believes that states may, at least initially, take a voluntary approach to implementing Remote OBD, allowing motorists to opt into the program and out of periodic inspection. The Workgroup recommends that motorists that wish to opt in to Remote OBD enter into an agreement with the I/M jurisdiction. In such an agreement, the motorist will:

- Agree to abide by the terms and conditions of the Remote OBD program.
- Agree not to tamper with or destroy the Remote OBD device.
- Commit to timely servicing, of the vehicle after being notified by the I/M program that repairs are needed.
    - If a motorist fails to comply with the repair requirements, then the program will need to take enforcement action to ensure that compliance is achieved. This may be accomplished by removing the vehicle from the Remote OBD program and immediately scheduling it for a periodic inspection. Alternatively, license or registration suspension can be used to bring motorists into compliance.
- Commit to be "seen" in the I/M area and, if necessary, intentionally drive by a monitor periodically so that the OBD system can transmit required data.

    - Some very small fraction of vehicles that are used rarely or only for limited trips may not come into range of a monitor frequently enough to meet the 80/20 criteria above and those motorists may need to intentionally operate the vehicle in range of a receiver in order to comply. Proximity to a motorist's personal wireless home network, laptop, or cell phone might be sufficient to provide for frequent data collection in such circumstances, dependant on program design.
    - The agreement should also address situations such as "snow-birds", vehicle owners in the military and students who spend long periods of time outside of the I/M area and thus may not be "seen" often enough to meet the continuous inspection criteria. Such vehicles should be allowed to participate in the program with the understanding that they will be operating in the I/M area and thus "seen" during some parts of the year. Special conditions for vehicle reporting and criteria for authorizing vehicle re-registration may be necessary to address the unique circumstances involved, as is currently done in periodic programs.
- Notify the program if the vehicle is sold or if the owner moves from the I/M area.

As part of the enrollment process for the Remote OBD program, the Workgroup recommends that a "fingerprint" of the vehicle be taken and stored at the time of installation of the Remote OBD link or program enrollment. This will involve creating a master record (capturing monitor supported status, PID count, OBD VIN and similar vehicle characteristics) to prevent the link from being usable in another vehicle. As part of the Quality Assurance process, the fingerprint should be routinely compared with the inspection record to look for discrepancies that might indicate vehicle switching, tampering or defeat devices.

To expedite the notification and repair process and minimize program costs, it is recommended that the motorist provide an electronic method, e.g., email address or text message, to be used to contact the motorist when the MIL comes on or if the vehicle is not adequately seen by the monitoring system.

At a minimum, specific "key events" must be captured and transmitted to the data management system (DMS) that will identify the date/time the remote OBD link initially detects a MIL on and the post-repair occurrence of supported readiness monitors restored to "ready" without triggering a subsequent MIL on (indicating that the vehicle is operating properly). Transmitted records must be stored on the DMS for analysis and historical reporting. When effective vehicle repairs have been made, subsequent transmissions will allow the DMS to determine that the original diagnostic trouble codes that triggered the MIL on event have not recurred. By defining specific key events that are important to determining the condition of emission related components relevant to an I/M program, the program can limit the amount of data that needs to be transmitted to the DMS to keep the record volume manageable. The system should be able to determine that the OBD link is present, attached to the correct vehicle, and functioning properly. The system also needs to ensure that reported events are time-stamped accurately.

This minimum specification does not preclude a manufacturer of a Remote OBD system from transmitting any additional information deemed important to its design and functionality. An OBD Link should not make pass/fail decisions and should not alter data values. The intent is to ensure that the analysis of the data for I/M program purposes is performed by the DMS.

By maintaining a historical record of events and resolved events, logged by date and time, the DMS will be able to analyze and report on the data en masse or by individual vehicles. Such analysis can include support for quality assurance and auditing, information for motorists, reporting vehicle status to authorities for enforcement action, and statistical analysis to measure program effectiveness. Data mining on the DMS can provide state government agencies with information to help estimate air quality benefits of Remote OBD as compared to traditional periodic vehicle inspection and maintenance programs.

Any Remote OBD device should meet the minimum requirements specified in this guidance for I/M purposes. However, other events can be defined and recorded to provide additional functionality for states or vehicle owners. Additional functionality targeted at specific market segments can be provided by individual manufacturers of Remote OBD systems as long as the minimum specifications are met and the integrity of essential data is not compromised.

The Remote OBD program should clearly articulate a privacy policy. The policy should specify which OBD parameters must be observed and how the data will be handled by the jurisdiction or its designee. No party should sell, trade, or otherwise transfer *personally identifiable information* to outside parties without the express consent of the vehicle owner. Location information should not be stored in the inspection record. In order to assess the effectiveness of a node in a wireless network, the frequency of contact information can be made available without associating it with personally identifiable information. Likewise, data from the program can be used to assess overall program effectiveness, OBD system performance and similar matters of interest to both state and Federal agencies charged with overseeing the I/M program without including personally identifiable information.

The network design should also prevent unauthorized access to the vehicle or base station communication, especially in the event of transferring the contract and equipment to a new vendor. Finally, the system should employ measures to prevent or detect data corruption. Required key events must be reliably communicated to the host without interception or compromise.

The remainder of this report delves into further detail on many of the issues covered in this section.

III. Repair / Retest Considerations

A Remote OBD system must be able to identify when the MIL is commanded on and also when Diagnostic Trouble Code (DTC) conditions have been resolved. Once a continuous inspection failure (see glossary for definitions) has occurred, the motorist should be notified that repairs are required. The Remote OBD management system should be structured to continue monitoring vehicles that have been flagged as needing repair to determine if and when the MIL is off with all supported monitors ready.

The Remote OBD system must also be able to identify when a vehicle has one or more monitors that are persistently not ready. If a particular monitor on a particular vehicle fails to become ready over the course of time, this may indicate that a problem exists with the OBD system. This

situation should prompt notification and repair as if the MIL were commanded on. In periodic I/M programs, EPA and the states instituted the practice of allowing vehicles with one or two monitors not ready to be tested anyway so as not to unduly inconvenience motorists. With the Remote OBD approach, this practice is no longer needed. Allowing vehicles to pass with monitors not ready reduces the emission reduction benefit of the program. However, it may be the case that some vehicles have known persistent readiness monitor problems and will need to be excluded from the requirement for full readiness if the vehicles are accepted into the program.

IV. Record Structure and Format

Each set of OBD test data associated with an event must be transmitted as a distinguishable unit and subsequently must be compiled with related data generated by the data management system into a complete test record capable of fulfilling the jurisdiction's emissions testing program needs. Consequently, each such record must:

- contain the set of OBD data that comprises a complete test record, and
- be transmitted in a form that conforms to accepted formatting conventions so it is interpretable upon receipt by the data management system.

Table 1 summarizes the vehicle-generated data fields that should be collected and Appendix Three provides an XML schema for encoding this information. These are powertrain control module-generated test record elements that, when combined with additional vehicle and programmatic data, enable a jurisdiction to comply with federal requirements and effectively audit test results.[1] Recommended data field formats are similar to those in SAE Standard J1979[2] for some parameters, but consolidate monitor support and monitor readiness flags into a single one-character field.

The OBD bulb check result – a test record element normally produced during a traditional OBD test – is absent from the Remote OBD test record. From a SIP compliance perspective, this absence causes no loss in I/M Program benefit because Remote OBD will notify the motorist that the MIL is commanded on despite failure of the bulb, and trigger repairs as if the motorist were responding to the illuminated MIL. This process might lead to bulb repairs as well since the motorist that receives a notification that they need repair will wonder why the MIL is not visibly illuminating.

Like conventional OBD testing, Remote OBD presents an opportunity to capture numerous ECU-generated data fields for inclusion in each test record. Many of these fields can provide a jurisdiction with useful programmatic information. For instance, time since DTCs were cleared can help identify fraud in conjunction with persistent readiness issues for a particular vehicle. Additionally, such data can be helpful in diagnosing vehicle conditions resulting in a test failure. When designing a DMS, however, jurisdictions should consider not just the utility of all these additional data, but also their data storage implications, repair community impacts, and any other significant programmatic consequences.

---

1 As indicated in the section on Acceptance Criteria, these elements are a combination of Mode 01, Mode 03, and Mode 09 data.

2 Surface Vehicle Recommended Practice: Diagnostic Trouble Code Definitions, SAE J2012, revised Dec 2007

Table 1: Minimum Data Elements Constituting a Remote OBD Test Record

#	Field Description	Variable Name	Length	Type	Layout	Comments
1	Device Serial Number	LINK_ID	12	A		Begin with MFG ID
2	Electronic Vehicle Identification Number	VIN	17	A		
3	Date of Data Collection	DATE	8	A	YYYYMMDD	Universal coordinated time
4	Time of Data Collection	TIME	6	A	HHMMSS	Universal coordinated time
5	Communications Protocol	COMM_PROT	3	A	AAA	See Attached Defintions
6	MIL Commanded On	MIL	1	A	Y, N	Yes, No
7	OBD Monitor Status - Catalyst	CAT_STATUS	1	A	U, R, N	See Attached Defintions
8	OBD Monitor Status - Evap	EVAP_STATUS	1	A	U, R, N	See Attached Defintions
9	OBD Monitor Status - Secondary Air	AIR_STATUS	1	A	U, R, N	See Attached Defintions
10	OBD Monitor Status - Oxygen Sensor	O2_STATUS	1	A	U, R, N	See Attached Defintions
11	OBD Monitor Status - Oxygen Sensor Heater	HEATEDO2_STATUS	1	A	U, R, N	See Attached Defintions
12	OBD Monitor Status - EGR	EGR_STATUS	1	A	U, R, N	See Attached Defintions
13	OBD Monitor Status - Comprehensive Components	COMP_STATUS	1	A	U, R, N	See Attached Defintions
14	OBD Monitor Status - Fuel System	FUEL_STATUS	1	A	U, R, N	See Attached Defintions
15	OBD Monitor Status - Misfire	MISFIRE_STATUS	1	A	U, R, N	See Attached Defintions
16	OBD Monitor Status - Air Conditioning	AC_STATUS	1	A	U, R, N	See Attached Defintions
17	OBD Monitor Status - Catalyst Heater	CATHTR_STATUS	1	A	U, R, N	See Attached Defintions
18	Engine RPM	RPM	4	N	NNNN	At time other data is saved
19	PID Count	PID_COUNT	3	N	NNN	As per ETI flow diagram
20	PCM ID	PCM	2	A		Binary, engine control unit
21	Calibration ID	CAL_ID	16	A		From ECU
22	Calibration Verification Number	CVN	8	A		Binary
23	Diagnostic Trouble Code 1	DTC_1	5	A	PNNNN	
24	Diagnostic Trouble Code 2	DTC_2	5	A	PNNNN	
25	Diagnostic Trouble Code 3	DTC_3	5	A	PNNNN	
26	Diagnostic Trouble Code 4	DTC_4	5	A	PNNNN	
27	Diagnostic Trouble Code 5	DTC_5	5	A	PNNNN	
28	Diagnostic Trouble Code 6	DTC_6	5	A	PNNNN	
29	Diagnostic Trouble Code 7	DTC_7	5	A	PNNNN	
30	Diagnostic Trouble Code 8	DTC_8	5	A	PNNNN	
31	Diagnostic Trouble Code Count	DTC_COUNT	3	N	NNN	
32	Pending Diagnostic Trouble Code 1	PEND_DTC_1	5	A	PNNNN	
33	Pending Diagnostic Trouble Code 2	PEND_DTC_2	5	A	PNNNN	
34	Pending Diagnostic Trouble Code 3	PEND_DTC_3	5	A	PNNNN	
35	Pending Diagnostic Trouble Code 4	PEND_DTC_4	5	A	PNNNN	
36	Pending Diagnostic Trouble Code Count	PEND_DTC_COUNT	3	N	NNN	
37	Permanent Diagnostic Trouble Code 1	PERM_DTC_1	5	A	PNNNN	
38	Permanent Diagnostic Trouble Code 2	PERM_DTC_2	5	A	PNNNN	
39	Permanent Diagnostic Trouble Code 3	PERM_DTC_3	5	A	PNNNN	
40	Permanent Diagnostic Trouble Code 4	PERM_DTC_4	5	A	PNNNN	
41	Distance travelled while MIL is activated	MILEAGE_SINCE_MIL	5	N	NNNNN	Kilometers
42	Number of warm-ups since DTC cleared	WARMUPS_SINCE_CC	3	N	NNN	
43	Distance since diagnostic trouble codes cleared	MILEAGE_SINCE_CC	5	N	NNNNN	Kilometers
44	Minutes run by the engine while MIL activated	MIN_SINCE_MIL	5	N	NNNNN	Minutes
45	Time since diagnostic trouble codes cleared	MIN_SINCE_CC	5	N	NNNNN	Minutes
46	Device Status	DEVICE_STATUS	12	A		
47	Device Firmware Number	DEVICE_FIRMWARE	12	A		

V. Security and Tamper Protection

Remote OBD Information Path

OBD system information is generated within a vehicle's on-board computer(s). The vehicle communicates required OBD information to the Remote OBD Link through communication protocols standardized by California, federal OBD regulations and the Society of Automotive Engineers (SAE). The OBD link then typically relays this information wirelessly to a vendor's server. The server then uploads the data to the jurisdiction's database. In some cases, information may pass directly from the Remote OBD Link to the jurisdiction's database.

Vehicle ⟶ Remote OBD Link ⟶ Vendor Server ⟶ Jurisdiction's Database

Adequate information security requires steps to deter inappropriate data manipulation throughout the information path.

Ensuring Accuracy Between the Vehicle and the Remote OBD Link

Tamper resistance measures need to be taken to deter inappropriate manipulation of the data before it is received by the Remote OBD Link. Both basic and more advanced data security measures are identified below. The capture of additional fields beyond the minimum data elements will be required in many cases.

1. Code Clearing:

Code clearing is a term that refers to the practice or occurrence of extinguishing the MIL and erasing stored information concerning detected malfunctions just prior to an inspection. This can occur by connecting a commonly available diagnostic tool to the vehicle's data port, or in many cases, by disconnecting the battery for a period of time. Stored readiness indicators are reset to not-ready when on-board fault information is cleared.

Owners of vehicles that frequently or continually do not meet set readiness requirements should be notified of the problem with instructions on how it should be addressed (See Compliance Monitoring and Auditing section). Frequent code clearing may indicate an attempt to hide an active fault. This practice can be detected through analysis of the readiness indicators over time. Readiness state changes from ready to not-ready is indicative that code clearing is occurring or that the vehicle has a malfunction affecting the proper operation of its OBD system.

Another tool for fraud detection is present in 2008 and newer, and many 2005 to 2007 models. The OBD system can report distance traveled, time and number of warm-up cycles since code clearing. Jurisdictions can establish criteria for the purposes of detecting when OBD information is cleared routinely, or with unusually high frequency.

2. Clean Scanning:

Clean scanning refers to the practice of generating a fraudulent OBD test result, often using information from one OBD equipped vehicle to represent the OBD system status of another. In the context of a Remote OBD program, this practice is most likely to be carried out by removing the Remote OBD Link from the vehicle with a fault, and installing it on a "clean" vehicle (i.e., a vehicle with no detected faults).

One of the design requirements of this document is that the DMS must be able to detect when the link is not in the intended vehicle. Information available from vehicle on-board computers can be used to confirm that the required OBD information actually originated from the vehicle that is intended to be inspected. The information (beyond fault code and readiness information) typically varies to some degree by manufacturer and vehicle model. Inspection programs can examine this information to see if it is consistent with the vehicle model being tested. To facilitate this, the "fingerprint" of the vehicle should be used with each transmittal as a reference to ensure the device is transmitting data from the correct vehicle. The types of information that are available for vehicle identification include:

- The communication protocol(s) specific to a given vehicle. This includes SAE J1850, ISO 9141-2, ISO 14230-4 (Key Word Protocol 2000), and ISO 15765-4 (CAN Protocol). Some of these protocols permit the use of options that effectively create distinct sub-protocols. If Remote OBD links are designed to support only one protocol, this safeguard would be implemented for all intents and purposes.
- The readiness profile of the vehicle. This provides information on which of the 11 readiness monitors are "supported" by the vehicle. The profile is most often affected by whether or not the vehicle is equipped with secondary air or exhaust gas recirculation.
- Module ID's and addresses. Vehicle computer networks typically connect multiple computer modules together, including the engine control module, the transmission control module, and often times other modules. The manufacturer assigns an ID or address for each of these modules. There is no required convention for how these module ID's are assigned, so they typically vary between manufacturers and even between models within a manufacturer's product line. Many I/M programs currently collect the address for the Powertrain Control Module (PCM).
- Parameter Identification Count (PID count). This value can be calculated by the inspection equipment from information reported by the on-board computer and indicates how many parameters are available for downloading through the vehicle's data stream. The value varies for different vehicle makes and models. As a result of valid updates to a vehicle (such as an ECU re-flash), the enrolled fingerprint may need to be updated.

The data parameters identified above can be compared to known values for each vehicle being inspected in order to detect data transmissions that are likely not legitimate. These known values can be established in the vehicle fingerprinting at the time of enrollment

into the Remote OBD program. Newer vehicles include additional sources of information, which can go as far as positively confirming whether or not the downloaded data is from the vehicle purportedly being inspected, independent of other vehicle fingerprint data.

- Calibration ID (Cal ID), a number assigned by the manufacturer to identify the software calibration of the vehicle. This ID is usually unique to a particular vehicle model.
- Calibration Verification Number (CVN). This value is computed based on contents of the on-board computer's software. It is typically unique to a specific CAL ID for a particular vehicle model, or even at the sub-model level.
- Vehicle Identification Number (VIN). Newer model year vehicles (2005 and later) store the VIN electronically in the on-board computer. This value uniquely identifies the test vehicle.

3. Detect Reprogramming in the on-board computer

Unauthorized reprogramming may be detectable by comparing stored CVN values with known correct entries for a given calibration ID number. Jurisdictions need to be aware of the fact that aftermarket companies offer vehicle calibration changes that are not considered to constitute emission-related tampering. These changes will alter the CVN and possibly the Cal ID, but should not solely be the basis for rejecting a vehicle subject to Remote OBD inspection. The jurisdictions' DMS will need to contain a list of OEM Cal ID and CVN data along with acceptable aftermarket values in order to effectively use CVN data for the purposes of this paragraph.

4. Detect Defeat Devices

Alterations to the data reported by the OBD link can occur through reprogramming or replacement of the link. The devices should not be updateable in the field without adequate safeguards. Replacement of the link with a device that emulates proper communication but with fixed compliant data can render the Remote OBD program ineffective for the vehicle in question. As stated previously, the system must be designed to determine if the link is in the correct vehicle.

Defeat device detection can be achieved in some instances through sophisticated use of information available to the on-board computer. For example, devices that simulate the post-catalytic converter oxygen sensor signal might be detected through analysis of oxygen sensor values available through the OBD data link. Transmission of sufficient data to carry out such tasks may require the duration of the communication session between the vehicle and the receiver to exceed practical limits for some data network designs. Periodic random collection of additional real time engine parameters (e.g., coolant temperature, engine speed, calculated load, etc.) can provide for effective detection of such devices.

5. Tamperproof Devices

The device installed in a vehicle should have a unique internal identifier that accompanies each test record transmitted to the DMS. Vendors of such devices should be expected to demonstrate the they are sufficiently protected from physical alteration or unauthorized re-programming.

Ensure Database Security

Access to the vendor's server(s) needs to be protected through limited access and password protection. Access to jurisdiction's database server also needs to be protected through limited access and password protection.

VI. Data Capture

A significant difference between the continuous testing effects of a Remote OBD monitoring strategy and periodic OBD inspection is the virtually unlimited volume of test data available per vehicle. This section will address two different aspects of the continuous inspection process, 1) the frequency at which the Remote OBD link captures data from the vehicle's OBD system and 2) the criteria by which data records are considered "key events," which should be stored in the DMS.

On-Board Capture Rates

The on-board capture rate strategy can be driven by either the precision needed for certain transient events or the network design criteria. The stringency of this requirement, however, may be dictated more by program integrity issues (such as those discussed in the previous section on Security and Tamper Protection) rather than the more basic interest in producing a daily inspection record.

The preferred means of assuring that significant events are not lost is for the wireless link to perform a J1979 interrogation at least once per trip (engine RPM over 500 for more than 10 seconds) or once per operating hour

Key Events

Specific key events should initiate the process of transmitting a test record to the DMS. The minimum key events include:

1. Change of MIL status
2. Change of status of any monitor
3. Change of fingerprint data
4. Remote OBD link disconnected
5. Other anomalous conditions

To minimize data handling and storage, not all records need to be stored if there is no key event.

VII. Compliance Monitoring and Auditing

The goals associated with the use of compliance monitoring and auditing for a Remote OBD implementation include:

- Ensuring owners take appropriate action when certain events occur
- Preventing fraud
- Verifying adequate network coverage
- Verifying program effectiveness
- Quantifying benefits of the program
- Taking corrective action for shortcomings and inappropriate activities

Ensuring Owners Take Appropriate Action and Preventing Fraud

A key benefit to continuous monitoring of vehicle emission performance is the potential for a dramatic reduction in the average time that elapses between the occurrence of an emission-related malfunction and its diagnosis and repair. Jurisdictions must ensure that vehicle owners act promptly in response to an illuminated MIL in order for potential emission benefits to be realized. Other conditions may exist that also require prompt action on the part of the vehicle owner to ensure that emission-related malfunctions are not overlooked.

Table 2 identifies the events that warrant attention in the form of communication between the jurisdiction or its contractor and the vehicle owner. The purpose of the communication is to provide vehicle owners with instructions and reminders to resolve circumstances of concern. If a vehicle owner is unresponsive to the notices sent, a decision to drop the vehicle from the Remote OBD program may become necessary. The table also includes the timing of the communications in relation to the occurrence of the event of concern.

Additional action may be necessary for vehicles that are frequently found to need attention. Such circumstances could indicate that the vehicle owner is periodically modifying the vehicle or clearing on-board information specifically for the purposes of addressing one or more of the issues of concern identified in the table.

Verifying Adequate Network Coverage

Adequate frequency of remote OBD data collection from vehicles depends on adequate network coverage over streets and highways within the jurisdiction. Network coverage is a key component to the design of a Remote OBD implementation and must be considered carefully by jurisdictions. However, verifying that network coverage once implementation has begun is also critical. Unreliable or spotty network coverage will tend to increase the percentage of vehicles within the jurisdiction for which the collection of data lacks adequate frequency. Jurisdictions should have methods in place to evaluate network coverage on a periodic basis.

Table 2: Conditions Requiring Motorist Notification or Other Jurisdictional Action

Condition	Requirements for Correction	Initial Notification		Second Notification		Final Notification	
		Action	Timing	Action	Timing	Action	Timing
Presence of anomalous data	Physical inspection of vehicle	Owner notified of need for inspection or vehicle will be dropped if not inspected in 14 days.	Immediate	Owner notified of need for inspection or vehicle will be dropped if not inspected in 7 days.	7 days from initial notification	Owner notified they are dropped from the program and report for inspection	14 days from initial notification
MIL On	MIL Off Monitor readiness achieved (all supported monitors reporting ready)	Notice sent to motorist stating that diagnosis and repair of fault is needed	Whenever MIL is commanded on	Notice sent to motorist indicating continued need for action or if fingerprint changed, need for inspection	30 days from initial notification or immediately on fingerprint change	Notice sent to motorist indicating vehicle is dropped from program and to report for inspection within 15 days	15 days from second notification
Lack of Vehicle Reporting	Valid record needs to be received from vehicle	Notice sent to motorist. Include instructions on how to get reporting to occur and how to contact program administrator if vehicle is not in use or out of the area.	After 14 consecutive days without received record	Notice sent to motorist indicating continued lack of reporting data without valid explanation	30 days from initial	Notice sent to motorist indicating that registration will not be renewed until vehicle is physically inspected.	60 days from second notification
Failure to achieve readiness	Monitor readiness achieved (all supported monitors reporting ready)	Notice sent to motorist. Information on how to increase chances of monitor operation included	Adequate readiness not seen over last 10 days	Notice sent to motorist suggesting that vehicle should be examined by technician	20 days from initial	Notice sent to motorist indicating that vehicle will be dropped from program if no readiness in 21 days	30 days from second notification

Verifying Program Effectiveness
A critical issue for I/M program effectiveness is whether corrective action taken to bring vehicles into compliance provides for lasting emission benefits. Issues that affect benefits have historically included:

- Motorist response to MIL illumination
- Repair effectiveness
- Actions taken to get unrepaired vehicles to inappropriately pass inspection

Analysis of collected OBD data can be used to detect some types of inspection fraud as indicated in the Security and Tamper Protection Section. Repair effectiveness can also be examined through continued monitoring of OBD information for redetection of malfunctions that have previously been repaired to extinguish the MIL.

Quantifying Benefits of the Program
Data collected during the remote I/M program can be used towards calculating the emission benefits of the Remote OBD inspection program. Important data items include:

- Vehicle failure rates categorized by component or fault code
- Average vehicle usage statistics
- Data or estimates concerning the impact of individual components and failure modes on vehicle emission levels.

Taking Corrective Action for Shortcomings and Inappropriate Activities.
I/M program administrators should use compliance monitoring data to periodically identify and address program design and enforcement issues that impact overall program effectiveness. Actions can include:

- More stringent enforcement actions such as license or vehicle registration suspension if a motorist fails to comply;
- Shortening length of time owners have to respond to notices;
- Modifying notices and actions intended to prompt vehicle owners to take necessary action;
- Strategies to ensure that vehicle service providers are properly trained and equipped to effect long-lasting emission-related repair work.

VIII. Communication Protocols

This section discusses the Remote OBD communication process and protocols necessary to transmit the appropriate data from the OBD system to the link, from the link to the transceiver, and finally to the jurisdiction's database. The process is characterized by the following:
The communication between the vehicle computer or ECU and an SAE J1979 compliant device. This communication is defined by J1979 and is adhered to by every vehicle manufacturer. Therefore, this protocol requires no further definition.

Communication between the Remote OBD link and the Transceiver

This can be cellular based, WI-FI, FM Simplex, AM Simplex or just about any kind of radio wave based system. There are examples of all of these methods that have been used, or are being used currently. It is recommended that whatever communication protocols are used, the program should allow for current telemetrics on OEM vehicles and proprietary systems developed for Remote OBD.

Communication between Base Stations and the DMS

This is the portion that can and should be standardized. Multiple contractors and OEM proprietary systems can all participate in a program that standardizes this portion of the communications. The contractor, subcontractor or vendor, must package the data from each vehicle in a highly structured database format using secure TCP/IP internet connections.

The basic flow of communication information is illustrated in Figure 1.

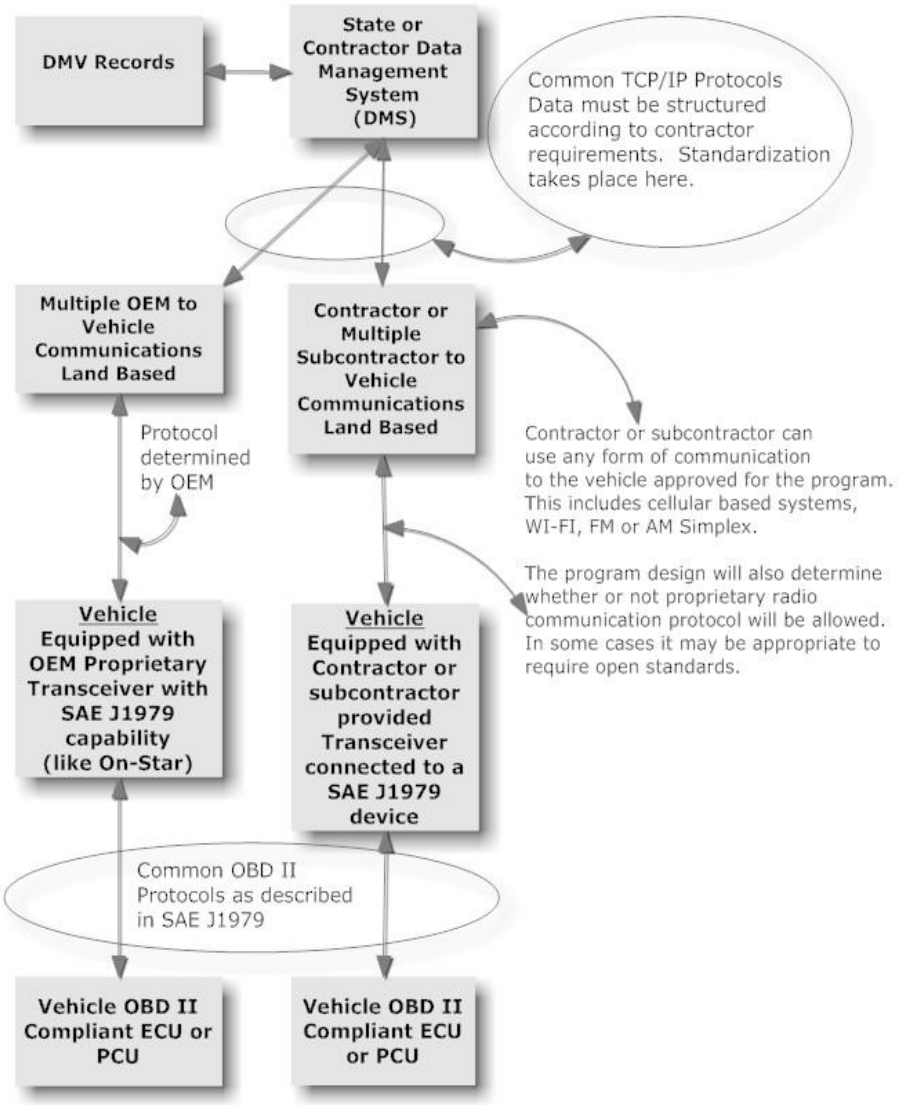
As long as every on-board device can communicate properly with every vehicle and as long as every land based data acquisition system can communicate with the DMS, the rest of the system can be configured in various ways using multiple contractors, subcontractors or vendors and each can use whatever communication system, protocol and transmission method they would like as long as what comes out of their system is reported to the DMS in the exact same way as everyone else's system. This allows for the maximum amount of flexibility and inter-operability.

OEM telemetric systems are not left out. The OEM data center captures the required data from registered vehicles, packages that data in the required DMS format for each state implementation and sends it at required intervals. OEMs will not have to reconfigure their vehicles for each jurisdiction. They will only have to create different data output template for each jurisdiction, fill in the record for each vehicle and send that record to the jurisdiction.

It is highly unlikely that jurisdictions will agree completely on what data to collect, but it may be possible to agree on a database super-set that would cover all or most data possibilities. From this super-set, jurisdictions can choose the data elements they are interested in and at least insure that the data they choose will be formatted the same as in other jurisdictions.

Another possible solution is to define a subset containing required data elements that every jurisdiction must capture using specific fields in specific formats. This will allow data to be easily transferred from one contractor or vendor in one jurisdiction to another jurisdiction with little trouble. In this case, rules will have to be set up that dictate a standardized data record that all jurisdictions must adhere to for inter jurisdictional reporting. A required subset can also be helpful to national entities trying to perform statistical analysis across multiple jurisdictions.

Figure 1: Remote I/M Protocol Flow Chart



IX. Acceptance Criteria

Guidelines for acceptance of Remote OBD vehicle inspection systems are an essential part of the acquisition of Remote OBD services. Performing acceptance testing of the Remote OBD system is critical to a successful program because there has to be absolute confidence in the data produced because it will be used for pass/fail and fraud detection decisions. Only acceptance testing in a laboratory environment and then beta testing in the installation location can

completely test the system. This section provides test scenarios that can be used to evaluate Remote OBD test equipment.

Remote OBD test systems may include different components based on the system design proposed. Basic components of the system which need to be evaluated and are included in these acceptance testing procedures include the following:

1. Remote OBD link
2. Hot spot/receiver
3. The DMS where the Remote OBD data is received, stored and processed

While these systems could be acceptance tested individually, the overall goal is to prove accurate end-to-end capture and transmission of vehicle OBD data. Therefore, end-to-end testing (where all components are tested together) is preferred. Remote OBD system acceptance testing is similar to the testing required for traditional, analyzer-based OBD test systems with the exception that the connection between the scan tool and the DMS is wireless and may be non-continuous. The Remote OBD link functions are similar to traditional systems with the exception of the frequency with which the testing occurs and the potential time game before the data is uploaded to the DMS. Because of the wireless connection, special acceptance testing about what data is stored, what data is transmitted, and how special testing cases are dealt with is needed. Other significant differences compared to traditional systems include the connector status (damaged, tampered, etc.) and the key-on-engine-off (KOEO) and key-on-engine-running (KOER) results which are not part of the pass/fail decision making process.

As noted, various system designs have been proposed for Remote OBD which may include different components. The components listed below may be tested in a system and are the basis for the acceptance testing scenarios provided.

1. Remote OBD Link
    a. Communication ability testing via SAE J1699-2
    b. Data transmission frequency
    c. Data transmission security
    d. Device tampering security testing
    e. Equipment durability – Longevity when exposed to expected environmental conditions in a vehicle (temperature, humidity, vibration, etc.), interference with connector, ability to remain connected
2. Hot Spots/Receivers
    a. Does geographic distribution meet area coverage criteria?
    b. Does geographic distribution result in the required frequency of vehicle observation?
    c. Data security

3. Data Management System
    a. Proper record structure and format
    b. Data processing for pass/fail using local program logic including proper exception handling (readiness excluded vehicles, etc.)
    c. Motorist notification logic testing
    d. Automated fraud detection
    e. Data integration with historical datasets and new non-Remote OBD data sets

Acceptance testing procedures for each of the above are described in the following sections. However, the Remote OBD link and the DMS will be subject to the same acceptance criteria. No acceptance testing is complete without beta testing the hardware on a variety of vehicles and full evaluation of "live" data.

Remote OBD Link

Scenarios have been designed to exercise the standard business rules for an OBD testing program and allow for review for correct data at the DMS. These scenarios should be conducted while using an OBD vehicle simulator. The scenarios include vehicles with readiness exemptions (if any) which will need to be handled at the DMS and are designed to exercise all communication protocols. The scenarios include variations in Mode 01, Mode 03 and Mode 09 data which will be confirmed by reviewing data at the DMS.

The scenarios are designed to evaluate a device which is designed to transmit a full set of data when there is a key event. However, if the program transmits all data at each communication, the scenarios are outlined in sufficient detail to allow them to also to be used for that purpose.

Because of the many varied forms Remote OBD may take, acceptance testing protocols and pass/fail criteria cannot be generically defined, but will need to be developed specifically around the hardware and program design type being used. The logic used in the testing scenarios attached is based on an adaptation of the ETI Technical Guidance "PC-LDT OBD IM Flowchart" developed by Bernard Carr of Bosch and Michael McCarthy of the California Air Resources Board.

For purposes of this OBD testing, four test outcomes are possible, Pass, Fail, Not Ready and Abort.

1) The vehicle passes if the MIL is not commanded on, the vehicle meets readiness criteria and there is no reason to suspect fraud (e.g., no change in fingerprint).
2) The vehicle fails if the MIL is commanded on regardless of readiness status or communication cannot be established.
3) The vehicle is not ready if the MIL is not commanded on and the vehicle does not meet readiness criteria.
4) The test result is an abort (but data is transmitted) when the vehicle is not OBD compliant or the data from the last time the device was used has changed which could indicate fraud. The following are examples:

a) The E-VIN has changed
b) The PCM ID has changed
c) The PID count has changed
d) The CAL ID has changed
e) The CVN has changed

The test scenarios included in Appendix Two provide for testing of most common OBD I/M test logic, and provide data for testing of logic which may be included at the DMS to detect fraud. The scenarios are each represented by a column of data, with a description of what is being tested at the top, settings for an OBD simulator below these, and overall results at the bottom of the column as well as a result indicating if the full test record should be transmitted when connection is made to a receiver. This is based on the logic that if the vehicle passes all checks, then only a "Healthy" indication needs to be transmitted. All of the OBD communication protocols which can be tested with common simulators are included in the scenarios to confirm communication of the device with all possible protocols. Note that actual VINs and year, make and model combinations have been included and every effort has been made to ensure the vehicles have the indicated parameters. However, since the tests should be conducted with a simulator, actual vehicle parameters should not be required (such as an older Ford using SAE J1850 variable pulse width "VPW" communications protocol).

In the scenarios, note that cells highlighted in yellow indicate a change in a parameter which will be part of determining the outcome of the scenario, therefore care should be taken to ensure these parameters are properly setup. The definition of terms used in the scenarios is as follows:

A. Communication Protocols
   (1) V = SAE J1850 VPW (VPW)
   (2) P = SAE J1850 PWM (PWM)
   (3) I = ISO 9141-2 (ISO)
   (4) Kf = ISO 14230-4 (KeyWord fast initialization)
   (5) Ks = ISO 14230-4 (KeyWord slow initialization)
   (6) C11 = ISO 15756-4 (CAN - 11 bit)
   (7) C29 = ISO 15756-4 (CAN - 29 bit)
B. Readiness Status
   (1) P = Pass - Ready
   (2) NR = Not Ready
C. Monitor Readiness Result
   (1) U = Monitor is unsupported
   (2) R = Monitor is complete (ready)
   (3) N = Monitor is not complete (not ready)
D. Overall Result
   (1) P = Pass

(2) F = Fail
(3) NR = Not Ready
(4) A = Abort – Invalid results

As noted, logic for testing if the device can capture potential fraud should be tested as part of acceptance testing. In item 4 above indicating five reasons a test should indicate a result of "abort" are cases where the device may have been removed from the vehicle and installed in another vehicle or something about the vehicle has changed indicating potential fraud (such as a change in CVN indicating possible reprogramming).

Manufacturers of interrogation/transceiver devices should be required to submit information with their equipment indicating their schema for data transmission security. This should be evaluated during acceptance testing to evaluate if it meets the program requirements.

Equipment manufacturers should be required to submit information about environmental testing performed on the devices (temperature, humidity, vibration, etc.) to ensure equipment durability and longevity. Depending on the program specifics, a wide range of environmental testing may be required. For example, Remote OBD devices used in cold areas of the country will need to be able to tolerate very low temperatures and those used in the south will need to be able to tolerate high temperatures and high humidity levels. All devices made for use in automotive applications should be required to withstand high levels of vibration without adverse impacts. Manufacturers should also demonstrate their plans to ensure the device stays in place while the vehicle is in operation and that the device does not interfere with the vehicle operators' use of the vehicle controls. The device should also be tested using the certification type test tool used by US EPA to ensure it still allows for connection to the OBD port and that the vehicle can still perform all OBD functions.

As noted, it may be that the device is designed so that it only transmits a full data packet under specific circumstances. The test scenarios indicate when data should be transmitted. The device will also need to be tested so that more than one set of "results" are obtained by the device before it has a chance to transmit them, to determine if the correct information is transmitted.

Base Stations

Base stations must have sufficient geographic coverage to provide the defined frequency of observing the Remote OBD equipped vehicles in the fleet (the 80/20 rule). If the receivers are cellular-based or satellite-based, then geographic coverage is much less of an issue. Modeling of the fleet activity relative to the locations of the receivers should be submitted by the equipment manufacturers to prove geographic coverage. This should then be verified after program startup during a "beta testing" period where the frequency of observation is evaluated to ensure it meets program requirements.

Manufacturers of receivers should be required to submit information with their equipment indicating their schema for data transmission security and to prevent a security breach of the receiver where falsified data could be submitted. Data security should be evaluated during

acceptance testing to evaluate if the manufacturers security methods meet the program requirements.

Data Management System
Standard functions of the vehicle information database which should be confirmed in all programs include using the detailed test scripts to evaluate if the proper data are populated in the DMS, and if the proper pass/fail/potential fraud decisions are being made. The scenarios can be used to test these decisions and overall results for the scenarios appear near the bottom of the scenario sheets. A function of the DMS which may also be tested could be vehicles which fail a test and the system for notification of customers that their vehicle is in need of repairs. In addition, the "clearing" of a vehicle failure indication after achieving passing status should be tested against local program design rules.

An aspect of DMS operation that will be important for Remote OBD programs is the ability to detect potential fraud in the data stream as noted above. Scenarios have been included which should allow for the DMS to evaluate the data for potential fraud such as changing parameters.

A last function of the DMS which needs to be considered is the integration of Remote OBD data with data from non-Remote OBD testing. It is expected that in some cases, Remote OBD and traditional, periodic OBD testing could be occurring concurrently. If so, the DMS must be able to accommodate both types of data, because the analysis for fraud is significantly different (in Remote OBD sequential records should be similar, while in traditional testing sequential records should not be similar) and the data fields required will be different (Remote OBD data will not have KOEO and KOER data).

X. Administrative Reporting

In order to assess the effectiveness of a Remote OBD program as a stand-alone program or as a part of a traditional I/M program, certain information beyond that collected in a traditional I/M program, is needed. The state will need to track and maintain records on:

1. Participants registered in the Remote OBD program, and those that have dropped out.
2. Data on the vehicle sightings, to be used to evaluate if network coverage is adequate.
3. Data on fault detection, MIL illumination, and MIL resets given the expected higher frequency of these occurrences in a Remote OBD program.

These data are similar to that collected for traditional I/M participants but need to be reported and tracked separately.

Some examples of reporting considerations are:

1. **Test Frequency Demonstration:** For a program that claims benefits for continuous testing, data should be retained that at the very least are sufficient to demonstrate that the vehicle and its wireless link are intact and available to report a fault condition according to the interval described in the general design requirements..

2. **Repair Compliance:** Continuous monitoring may afford an automated means of determining the approximate length of time between fault identification and effective repair. Automated entry of repair data through an integrated web portal may augment this reporting activity and provide a wealth of information on technician proficiency and repair effectiveness.
3. **Repair Durability:** For determinations of repair durability, test records that indicate the timeframe after which the relevant monitor(s) have been enabled, as well as the interval before a similar DTC recurs may be of significant interest.
4. **Final Inspection Disposition:** A unique capability of continuous monitoring is the ability to observe factors that may indicate test avoidance or other vehicle incapacity on a much more current basis than an annual or biennial test cycle would permit. For example, a vehicle that generally reports on a high frequency basis, then after an initial failure does not report for more than 90 days, is a trigger for further administrative action.
5. **Fleet Activity:** Various methods for assessment of approximate fleet characterization of relative model year activity, changes in travel patterns, etc., may be gathered from a continuous monitoring network without discrete vehicle geo-mapping.

XI. Glossary of Terms

1. Continuous Inspection Failure – The determination that a MIL has been commanded on at any time. The failure is considered resolved after 3 or more days of the MIL being continuously off with all supported monitors ready.

2. DMS – Data Management System. A repository of data collected by the Remote OBD Link and transmitted over a network. The DMS is a relational database that supports quality assurance, data sorting and filtering, reporting and connectivity to other databases including state agencies, I/M program DMSs and the Internet.

3. DTC – A Diagnostic Trouble Code is a code that is set by a vehicle's on-board computer when an emission-related component or system has been determined by the OBD system to be malfunctioning. DTCs are and reported through the data link connector (DLC).

4. DLC – Data Link Connector is a standard female socket that allows for connection to a vehicle on-board diagnostic system.

5. Remote OBD Link – Is a device that connects to the DLC and captures information from the vehicle OBD system for wireless transmission to the DMS.

6. Base Stations – These are the devices with which the Remote OBD link communicates and transmits data records. They are also referred to as hotspots and transceivers. These may be

satellites in the case of cellular systems or radio-frequency antennas connected to computers that receive communications. Other technologies are possible.

7. Relational Database – An electronic database comprising multiple files of related information, usually stored in tables of rows (records) and columns (fields) that allows a link to be established between separate files that have a matching field, such as a column of invoice numbers, so that the two files can be queried simultaneously by the user.

8. Dedicated Short-Range Communication (DSRC) – Dedicated short-range communications (DSRC) are one-way or two-way short- to medium-range wireless communication channels specifically designed for automotive use and a corresponding set of protocols and standards. It offers communication between the vehicle and roadside equipment. It is a sub-set of the RFID-technology. This technology for ITS applications is working in the 5.9 GHz band (U.S.) or 5.8 GHz band (Japan, Europe).

9. Clean Scanning – A form of I/M test fraud by which an inspector tests a vehicle known to be passing I/M standards in place of a vehicle that will fail and applies the passing result to the failing vehicle. Clean scanning can also be performed using an OBD simulator in place of a known passing vehicle.

Appendix One – Remote OBD Workgroup Charter

Objective: Recommend a national technical standard for Remote OBD I/M.

Background
Motor vehicle manufacturers have been required to install onboard diagnostic systems on motor vehicles since 1996. These systems are now widely used to pass/fail motor vehicles in I/M programs. This technology offers the opportunity to inspect vehicles in new ways. One way that can reduce costs and increase benefits is to conduct remote, continuous monitoring of the system and require repairs when a failure occurs, rather than the periodic (annual or biennial) approach traditionally used in such programs. This approach is known as Remote OBD.

There are several states that either already have or are in the planning stages of a Remote OBD I/M program. There are several companies and vehicle manufacturers that have some type of vehicle telemetrics device that could be used in a Remote OBD IM program. At this time, there are no uniform standards for Remote OBD I/M. This makes implementing a program more complex and costly, and may preclude some vendors and vehicle manufacturers from participating. Establishing a national standard will help facilitate greater participation, simplify implementation, inform program design, and reduce the costs of implementing and operating Remote OBD I/M.

There are three basic continuous monitoring methods that could be used for Remote OBD that will be addressed in this protocol. They include: 1) cellular/satellite network, 2) dedicated short-range communication (DSRC), and 3) wireless networking technology (Wi-Fi). This sub-group will work to develop a national protocol for using this technology to capture, store, and report the status of OBD systems in a secure, consistent and reliable manner such that I/M program administrators and motorists can take full advantage of these technological advances.

Membership
Participation in this subgroup is open to all interested parties. The voting members of the subgroup are:

Alan Lyons, CA, Co-Chair	Joel Unverzagt, ESP
Vincent Mow, Mactec, Co-Chair	John Cabaniss, AIAM
Amanetta Wood, EPA Region 4	John Wallauch, CA
Andrew Ferguson, Paxtel	Kevin McCarthy, Davis
Bill Dell, Systech International	Larry Sherwood, CA
Chris Ransom, Network Car	Michael St Denis, Revecorp
Chris Stock, Consultant	Nancy Seidman, MA
Christopher S. Brown, GM	Paul Davis, MA
David Amlin, CA	Kathleen Field, MD
David Patterson, Mitsubishi	Richard Joy, Gordon-Darby
Eric Berkobin, Hughes Telematics	Richard Olin, VA
Gene Tierney, US EPA OTAQ	Rob Schell, NJ
Guy Hoffman, TX	Stephen Hirschfeld, WI
Jim Kemper, CO	Sandeep Kishan, ERG

Appendix One – Remote OBD Workgroup Charter

Initial Outline of National Protocol

I. Definitions of Terms
II. Network Design Criteria
III. Repair / Retest Considerations
IV. Communication protocols
V. Security & tamper detection
VI. Record structure & format
VII. Reporting methods & frequency
VIII. Compliance monitoring
IX. Auditing criteria

Method of Operation and Time Frame

The workgroup will conduct periodic meetings to discuss and decide the elements of the protocol. The work is anticipated to take approximately 6-12 months to complete. In person attendance is not required at meetings as telephone conferencing will be available to those who are unable to attend in person.

Appendix Two – Acceptance Testing Scenarios

Remote OBDII Acceptance Testing Scenarios		REMOTE OBDII TEST SCENARIOS									REMOTE OBDII TEST SCENARIOS								
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Test Parameters	**Options**	Pass All, Check PID Count Correct, should be bits in positions 5, 20, 25, 40, 45, 60, 65	Ready - MIL On	Not Ready (pre-2001)	Not Ready (2001+)	1996 Subaru, Should Be Excluded From Readiness Criteria	No Communication Test	Not Ready - MIL On, Evap DTC Present	Not Ready - MIL On, Catalyst DTC Present	Hybrid, No RPM, Not Ready	Vehicle is not OBDII compliant and cannot be tested	Do not allow test, plugged into EASE simulator	DTC's Present, MIL NOT On	E-VIN has changed	PID Count has changed	PCM ID has changed	Communication protocol has changed	CAL ID has changed	CVN has changed
OBDII SIM settings		1	2	3	4	1		5	6	7	8	9	10	10	11	12	13	14	15
Comm protocol	I / C / K / V / P (f=FAST, s=SLOW, 11=11 bit, 29=29 bit)	V	I	I	P	V		Kf	Ks	C11	V	P	C29	C29	C29	C29	V	V	V
Powertrain Control Module Identification Address (PCM ID)		01	02	03	04	10		05	06	07	09	FD	08	08	08	10	10	10	10
PID Count		4	12	13	14	15		17	18	19	20	21	15	15	16	16	16	16	16
Calibration ID (Cal ID)		10000002	10000003	10000004	10000005	10000005		10000007	10000008	10000009	10000010	10000011	12345678	12345678	12345678	12345678	12345678	11111111	11111111
Calibration Verification Number (CVN)		20000001	20000002	20000003	20000004	20000005		20000007	20000008	20000009	20000010	20000011	99999999	99999999	99999999	99999999	99999999	99999999	22222222
PID $1C		01	03	07	09	01		0B	0D	01	02	01	01	01	01	01	01	01	01
MIL commanded on	Y/N	N	Y	N	N	N		Y	Y	N	N	N	N	N	N	N	N	N	N
Misfire	U/R/N	R	R	R	R	R		R	R	R	R	R	R	R	R	R	R	R	R
Fuel system	U/R/N	R	R	R	R	R		R	R	R	R	R	R	R	R	R	R	R	R
Comp. Component	U/R/N	R	R	R	R	R		R	R	R	R	R	R	R	R	R	R	R	R
Catalyst	U/R/N	R	N	N	N	N		N	R	R	R	R	R	R	R	R	R	R	R
Heated Catalyst	U/R/N	R	R	R	R	R		R	R	N	R	R	R	R	R	R	R	R	R
Evap system	U/R/N	R	R	N	N	N		N	R	R	R	R	R	R	R	R	R	R	R
Secondary Air System	U/R/N	U	R	N	U	N		N	R	R	R	R	R	R	R	R	R	R	R
Air conditioning system	U/R/N	R	R	R	R	U		R	R	R	R	R	R	R	R	R	R	R	R
Oxygen sensor	U/R/N	R	R	R	R	R		R	R	R	R	R	R	R	R	R	R	R	R
O2 sensor heater	U/R/N	R	U	R	R	R		U	R	R	R	R	R	R	R	R	R	R	R
EGR system	U/R/N	R	R	U	R	R		R	U	N	R	R	R	R	R	R	R	R	R
DTC1			P0101					P0442	P0432				P0201	P0201	P0201	P0201	P0201	P0201	P0201
DTC2			P0102										P0202	P0202	P0202	P0202	P0202	P0202	P0202
DTC3			P0103										P0203	P0203	P0203	P0203	P0203	P0203	P0203
DTC4			P0104										P0204	P0204	P0204	P0204	P0204	P0204	P0204
DTC5			P0105										P0205	P0205	P0205	P0205	P0205	P0205	P0205
DTC6			P0106										P0206	P0206	P0206	P0206	P0206	P0206	P0206
DTC7			P0107										P0207	P0207	P0207	P0207	P0207	P0207	P0207
DTC8			P0108										P0208	P0208	P0208	P0208	P0208	P0208	P0208
DTC9			P0109										P0209	P0209	P0209	P0209	P0209	P0209	P0209
DTC10			P0110										P0210	P0210	P0210	P0210	P0210	P0210	P0210
Electronic VIN													1FAFP34NX6W255974	1FAHP36NX6W119138	1FAHP36NX6W119138	1FAHP36NX6W119138	1FAHP36NX6W119138	1FAHP36NX6W119138	1FAHP36NX6W119138
TEST Configuration																			
Vehicle VIN		5LMFU28A7YLJ43683	JM1BJ2253104765 59	SAJJA42C7YNA08325	4S2DM58W514320621	JF1GC4552TH510783	1HGCD5632VA077293	W06VR52R0WR032392	WVWVD63B92E192292	JTDKB22U767061800	1FACP52U1PA160663	2G1WH55K529334729	1FAFP34NX6W255974	1FAFP34NX6W255974	1FAHP36NX6W119138	1FAHP36NX6W119138	1FAHP36NX6W119138	1FAHP36NX6W119138	1FAHP36NX6W119138
Vehicle Model Year	(XXXX)	2000	2001	2000	2001	1996	1997	1998	2002	2006	1993	2002	2006	2006	2006	2006	2006	2006	2006
Vehicle Make		Lincoln	Mazada	Jaguar	Isuzu	Subaru	Honda	Cadiliac	VW	Toyota	Ford	Chevrolet	Ford	Ford	Ford	Ford	Ford	Ford	Ford
Vehicle Model		Navirator	Protege	XK8	Rodeo	Impreza	Accord	Catera	Passat	Prius	Taurus	Impala	Focus	Focus	Focus	Focus	Focus	Focus	Focus
RESULTS																			
PID Count has changed	Y/N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N
PCM ID has changed or could be a simulator	Y/N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	Y	N	N	N
Communication protocol has changed	Y/N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N
CAL ID has changed	Y/N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N
CVN has changed	Y/N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	N	Y
E-VIN has changed	Y/N	N	N	N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N
Non-OBDII compliant PCM	Y/N	N	N	N	N	N	N	N	N	N	Y	N	N	N	N	N	N	N	N
MIL COMMAND ON	P/F	P	F	P	P	P	P	F	F	P	P	P	P	P	P	P	P	P	P
OBD COMMUNICATION	P/F	P	P	P	P	P	F	P	P	P	P	P	P	P	P	P	P	P	P
READINESS STATUS	P/NR	P	P	NR	NR	NR	P	NR	P	NR	P	P	P	P	P	P	P	P	P
Full data packet transmission required?	Y/N	N	Y	Y	Y	Y	Y	Y	Y	Y	Y	Y	N	Y	Y	Y	Y	Y	Y
Overall Result	**P/F/NR/A**	**P**	**F**	**NR**	**NR**	**NR**	**F**	**F**	**F**	**NR**	**A**	**A**	**P**	**A**	**A**	**A**	**A**	**A**	**A**

Comm Protocols	**V**	SAE J1850 VPW (VPW)
	P	SAE J1850 PWM (PWM)
	I	ISO 9141-2 (ISO)
	K	ISO 14230-4 (KeyWord fast and slow initialization)
	C	ISO 15756-4 (CAN - 11 bit and 29 bit)
Overall Result	**P**	Pass
	F	Fail
	NR	Not Ready
	A	Abort - Status cannot be determined
Readiness Status	**P**	Pass - Ready
	NR	Not Ready
Monitor Readiness Result	**U**	Monitor is unsupported
	R	Monitor is complete (ready)
	N	Monitor is not complete (not ready)

Appendix Three – XML Schema for Data Records

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema id="RemoteObd" targetNamespace="urn:RemoteObd-epa-gov" xmlns="urn:RemoteObd-epa-gov" elementFormDefault="qualified"
xmlns:xs="http://www.w3.org/2001/XMLSchema">
  <xs:element name="RemoteObd">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="PayloadDateTime" type="xs:dateTime" />
        <xs:element name="LINK_ID" type="xs:string" />
        <xs:element name="RECEIVER_ID" type="xs:string" />
        <xs:element name="Signature" type="xs:string" minOccurs="0" />
        <xs:element name="RemoteObdTest">
          <xs:complexType>
            <xs:all>
              <xs:element name="TestDateTime" type="xs:dateTime" />
              <xs:element name="LINK_ID" type="xs:string" />
              <xs:element name="VIN">
                <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:maxLength value="20" />
                  </xs:restriction>
                </xs:simpleType>
              </xs:element>
              <xs:element name="MIL">
                <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="Y" />
                    <xs:enumeration value="N" />
                  </xs:restriction>
                </xs:simpleType>
              </xs:element>
              <xs:element name="COMM_PROTOCOL">
                <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:maxLength value="3" />
                  </xs:restriction>
                </xs:simpleType>
              </xs:element>
              <!-- Monitors -->
              <xs:element name="Misfire" type="MonitorResult" />
              <xs:element name="Fuel" type="MonitorResult" />
              <xs:element name="Comprehensive" type="MonitorResult" />
              <xs:element name="Catalyst" type="MonitorResult" />
              <xs:element name="HeatedCatalyst" type="MonitorResult" />
              <xs:element name="EvapSystem" type="MonitorResult" />
              <xs:element name="SecondaryAir" type="MonitorResult" />
              <xs:element name="ACSystem" type="MonitorResult" />
              <xs:element name="O2Sensor" type="MonitorResult" />
              <xs:element name="HeatedO2Sensor" type="MonitorResult" />
              <xs:element name="EGR" type="MonitorResult" />
              <xs:element name="NotReadyCount" type="xs:integer" />
              <xs:element name="DtcCount" type="xs:integer" minOccurs="0" />
              <xs:element name="DTC1" type="DtcCode" minOccurs="0" />
              <xs:element name="DTC2" type="DtcCode" minOccurs="0" />
              <xs:element name="DTC3" type="DtcCode" minOccurs="0" />
              <xs:element name="DTC4" type="DtcCode" minOccurs="0" />
              <xs:element name="DTC5" type="DtcCode" minOccurs="0" />
              <xs:element name="DTC6" type="DtcCode" minOccurs="0" />
              <xs:element name="DTC7" type="DtcCode" minOccurs="0" />
              <xs:element name="DTC8" type="DtcCode" minOccurs="0" />
              <xs:element name="PendingDtcCount" type="xs:integer" minOccurs="0" />
              <xs:element name="PendingDTC1" type="DtcCode" maxOccurs="0" minOccurs="0" />
              <xs:element name="PendingDTC2" type="DtcCode" maxOccurs="0" minOccurs="0" />
              <xs:element name="PendingDTC3" type="DtcCode" maxOccurs="0" minOccurs="0" />
              <xs:element name="PendingDTC4" type="DtcCode" maxOccurs="0" minOccurs="0" />
              <xs:element name="PermanentDtcCount" type="xs:integer" minOccurs="0" />
              <xs:element name="PermanentDTC1" type="DtcCode" maxOccurs="0" minOccurs="0" />
              <xs:element name="PermanentDTC2" type="DtcCode" maxOccurs="0" minOccurs="0" />
              <xs:element name="PermanentDTC3" type="DtcCode" maxOccurs="0" minOccurs="0" />
              <xs:element name="PermanentDTC4" type="DtcCode" maxOccurs="0" minOccurs="0" />
              <xs:element name="RPM">
                <xs:simpleType>
                  <xs:restriction base="xs:decimal">
```

Appendix Three – XML Schema for Data Records

```
        <xs:totalDigits value="5" />
        <xs:fractionDigits value="2" />
      </xs:restriction>
    </xs:simpleType>
  </xs:element>
  <xs:element name="PCMID">
    <xs:simpleType>
      <xs:restriction base="xs:string">
        <xs:pattern value="[a-zA-Z0-9]{2}" />
      </xs:restriction>
    </xs:simpleType>
  </xs:element>
  <xs:element name="PidCount">
    <xs:simpleType>
      <xs:restriction base="xs:integer">
        <xs:minInclusive value="0" />
        <xs:maxInclusive value="32" />
      </xs:restriction>
    </xs:simpleType>
  </xs:element>
  <xs:element name="CAL_ID" type="xs:string" />
  <xs:element name="MileageSinceMil">
    <xs:simpleType>
      <xs:restriction base="xs:decimal">
        <xs:totalDigits value="5" />
      </xs:restriction>
    </xs:simpleType>
  </xs:element>
  <xs:element name="WarmupsSinceCodesCleared">
    <xs:simpleType>
      <xs:restriction base="xs:decimal">
        <xs:totalDigits value="3" />
      </xs:restriction>
    </xs:simpleType>
  </xs:element>
  <xs:element name="MileageSinceCodesCleared">
    <xs:simpleType>
      <xs:restriction base="xs:decimal">
        <xs:totalDigits value="5" />
      </xs:restriction>
    </xs:simpleType>
  </xs:element>
  <xs:element name="MinutesSinceMil">
    <xs:simpleType>
      <xs:restriction base="xs:decimal">
        <xs:totalDigits value="5" />
      </xs:restriction>
    </xs:simpleType>
  </xs:element>
  <xs:element name="MinutesSinceCodesCleared">
    <xs:simpleType>
      <xs:restriction base="xs:decimal">
        <xs:totalDigits value="5" />
      </xs:restriction>
    </xs:simpleType>
  </xs:element>
  <xs:element name="SoftwareVersion" type="xs:string" />
  <xs:element name="RecordId" type="xs:string" />
  <xs:element name="DeviceStatuse">
    <xs:simpleType>
      <xs:restriction base="xs:string">
        <xs:maxLength value="12" />
      </xs:restriction>
    </xs:simpleType>
  </xs:element>
  <xs:element name="DeviceFirmware">
    <xs:complexType>
      <xs:sequence>
        <xs:any />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:all>
```

Appendix Three – XML Schema for Data Records

```
        </xs:complexType>
       </xs:element>
       <xs:element name="QaData" minOccurs="0">
        <xs:complexType>
         <xs:sequence>
          <xs:element name="Parameter" type="ParameterData" />
         </xs:sequence>
        </xs:complexType>
       </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
  <xs:simpleType name="MonitorResult">
    <xs:restriction base="xs:string">
      <xs:enumeration value="U" />
      <xs:enumeration value="R" />
      <xs:enumeration value="N" />
    </xs:restriction>
  </xs:simpleType>
  <xs:simpleType name="DtcCode">
    <xs:restriction base="xs:string">
      <xs:pattern value="[PCBU][0-3][0-9A-F]{3}" />
    </xs:restriction>
  </xs:simpleType>
  <xs:complexType name="ParameterData">
    <xs:simpleContent>
      <xs:extension base="xs:string">
        <xs:attribute name="Mode" type="xs:integer" />
        <xs:attribute name="Pid" type="xs:integer" />
      </xs:extension>
    </xs:simpleContent>
  </xs:complexType>
</xs:schema>

<?xml version="1.0" encoding="utf-8"?>
<!--This file is auto-generated by the XML Schema Designer. It holds layout information for components on the designer surface.-->
<XSDDesignerLayout Style="LeftRight" layoutVersion="2" viewPortLeft="0" viewPortTop="-8778" zoom="100">
    <RemoteObd_XmlElement left="1350" top="8890" width="8652" height="5530" selected="0" zOrder="19" index="0" expanded="1">
      <RemoteObdTest_XmlElement left="10636" top="-6307" width="8202" height="19817" selected="0" zOrder="20" index="4" expanded="1">
        <VIN_XmlElement left="19472" top="-18757" width="5292" height="900" selected="0" zOrder="53" index="2" expanded="1">
          <_x0028_VIN_x0029__XmlSimpleType left="25398" top="-19881" width="5292" height="3149" selected="0" zOrder="55" index="0" expanded="1" />
        </VIN_XmlElement>
        <MIL_XmlElement left="19472" top="-15100" width="5292" height="900" selected="0" zOrder="57" index="3" expanded="1">
          <_x0028_MIL_x0029__XmlSimpleType left="25398" top="-16224" width="5292" height="3149" selected="0" zOrder="59" index="0" expanded="1" />
        </MIL_XmlElement>
        <COMM_PROTOCOL_XmlElement left="19472" top="-11443" width="5292" height="900" selected="0" zOrder="61" index="4" expanded="1">
          <_x0028_COMM_PROTOCOL_x0029__XmlSimpleType left="25398" top="-12567" width="5292" height="3149" selected="0" zOrder="63" index="0"
expanded="1" />
        </COMM_PROTOCOL_XmlElement>
        <RPM_XmlElement left="19472" top="-7786" width="5292" height="767" selected="0" zOrder="65" index="36" expanded="1">
          <_x0028_RPM_x0029__XmlSimpleType left="25398" top="-8910" width="5292" height="3149" selected="0" zOrder="67" index="0" expanded="1" />
        </RPM_XmlElement>
        <PCMID_XmlElement left="19472" top="-4129" width="5292" height="767" selected="0" zOrder="22" index="37" expanded="1">
          <_x0028_PCMID_x0029__XmlSimpleType left="25398" top="-5253" width="5292" height="3149" selected="0" zOrder="24" index="0" expanded="1" />
        </PCMID_XmlElement>
        <PidCount_XmlElement left="19472" top="-405" width="5292" height="767" selected="0" zOrder="26" index="38" expanded="1">
          <_x0028_PidCount_x0029__XmlSimpleType left="25398" top="-1596" width="5292" height="3149" selected="0" zOrder="28" index="0" expanded="1" />
        </PidCount_XmlElement>
        <MileageSinceMil_XmlElement left="19472" top="3252" width="5292" height="767" selected="0" zOrder="30" index="39" expanded="1">
          <_x0028_MileageSinceMil_x0029__XmlSimpleType left="25398" top="2061" width="5292" height="3149" selected="0" zOrder="32" index="0"
expanded="1" />
        </MileageSinceMil_XmlElement>
        <WarmupsSinceCodesCleared_XmlElement left="19472" top="6909" width="5292" height="767" selected="0" zOrder="34" index="40" expanded="1">
          <_x0028_WarmupsSinceCodesCleared_x0029__XmlSimpleType left="25398" top="5718" width="5292" height="3149" selected="0" zOrder="36"
index="0" expanded="1" />
        </WarmupsSinceCodesCleared_XmlElement>
        <MileageSinceCodesCleared_XmlElement left="19472" top="10566" width="5292" height="767" selected="0" zOrder="38" index="41" expanded="1">
          <_x0028_MileageSinceCodesCleared_x0029__XmlSimpleType left="25398" top="9375" width="5292" height="3149" selected="0" zOrder="40" index="0"
expanded="1" />
        </MileageSinceCodesCleared_XmlElement>
        <MinutesSinceMil_XmlElement left="19472" top="14223" width="5292" height="767" selected="0" zOrder="42" index="42" expanded="1">
          <_x0028_MinutesSinceMil_x0029__XmlSimpleType left="25398" top="13032" width="5292" height="3149" selected="0" zOrder="44" index="0"
expanded="1" />
```

Appendix Three – XML Schema for Data Records

```
        </MinutesSinceMil_XmlElement>
        <MinutesSinceCodesCleared_XmlElement left="19472" top="17880" width="5292" height="767" selected="0" zOrder="46" index="43" expanded="1">
          <_x0028_MinutesSinceCodesCleared_x0029__XmlSimpleType left="25398" top="16689" width="5292" height="3149" selected="0" zOrder="48"
index="0" expanded="1" />
        </MinutesSinceCodesCleared_XmlElement>
        <DeviceStatuse_XmlElement left="19472" top="21537" width="5292" height="767" selected="0" zOrder="73" index="46" expanded="1">
          <_x0028_DeviceStatuse_x0029__XmlSimpleType left="25398" top="20346" width="5292" height="3149" selected="0" zOrder="75" index="0"
expanded="1" />
        </DeviceStatuse_XmlElement>
        <DeviceFirmware_XmlElement left="19472" top="22812" width="5292" height="3149" selected="0" zOrder="80" index="47" expanded="1" />
      </RemoteObdTest_XmlElement>
      <QaData_XmlElement left="10636" top="26469" width="5292" height="3148" selected="0" zOrder="69" index="5" expanded="1">
        <Parameter_XmlElement left="16562" top="26469" width="5291" height="3148" selected="0" zOrder="71" index="0" expanded="1" />
      </QaData_XmlElement>
    </RemoteObd_XmlElement>
    <MonitorResult_XmlSimpleType left="1317" top="20199" width="5292" height="3149" selected="0" zOrder="50" index="1" expanded="1" />
    <DtcCode_XmlSimpleType left="7594" top="24421" width="7144" height="3148" selected="0" zOrder="51" index="2" expanded="1" />
    <ParameterData_XmlComplexType left="16432" top="24248" width="5292" height="3149" selected="0" zOrder="52" index="3" expanded="1" />
</XSDDesignerLayout>
```