MCSAC Task 11-04: Electronic On-Board Recorders (EOBR) Communications Protocols, Security, Interfaces, and Display of Hours-of-Service Data During Driver/Vehicle Inspections and Safety Investigations

Discussion Notes from July 11-12, 2011 Subcommittee Meeting

Task 11-04*: Clarification is needed on the functionality of communication standards noted in Appendix A to Part 395 for the transmittal of data files from EOBRs. FMCSA requests that the MCSAC Subcommittee make recommendations on technical questions to improve the functionality of the information reporting requirements described in the April 5, 2010 EOBR Compliance Final Rule. Some potential issues, ideas and concepts for the Subcommittee to consider, that EOBR manufacturers could use to achieve compliance with the Agency's communications standards for the transmittal of data files from EOBRs to enforcement officials include:*

I. EOBR Location Database Precision

A. The EOBR database should contain locations for review which should be meaningful to the driver and can be easily interpreted by roadside enforcement systems. The data source for locations should be standardized, published by the FMCSA for references purposes and consistent across EOBR systems.

B. Recommendations:

1. Location position should be derived from GPS or other location determination method with similar accuracy.
2. Location should be noted with each duty status change and on an hourly basis when the vehicle is moving in accordance with FMCSA 395.16.
3. EOBR should display location to driver on driver display or print-out format in text description format. Location should be derived from a database that contains all cities, towns and villages with a population of 5,000 or greater based on combined GNIS database with census data added.
    a. Census data overlaid onto GNIS database.
    b. Should further clarify location description to driver on display (distance, direction to nearest 5,000 pop. city).
4. EOBR should pass Lat/Long coordinate location to roadside enforcement via export methods defined.

C. Subcommittee comments:

1. GNIS database version/year should be noted, and timeframe for update/refresh of GNIS database version. Regulation should require periodic GNIS database update, either via wireless connection or locally.

II. EOBR Marking

A. The EOBR should consistently display evidence of conformity to FMCSA 395.16.

B. Recommendations:

1. EOBR shall use screen or print-out display to indicate conformity to 395.16.
2. No faceplate/hardware marking should be required as this can be difficult to view by drivers or inspectors, depending on installation of EOBR.
3. Verbiage shall read **—** "USDOT-EOBR".

4. EOBR shall include this on upper right corner of the roadside enforcement manual inspection review hours screen.

C. *Subcommittee comments:*
   1. *Should specify manual review process screen.*
   2. *Note: If CPU or EOBR screen failed and driver has used paper logs, there is no way to tell if driver has a compliant EOBR if "USDOT-EOBR" marking is on display, as opposed to faceplate.*

III. Data Format for Export to Roadside Enforcement

A. The EOBR shall consistently export data to roadside enforcement in the flat file format identified within FMCSA 395.16. Each record has approximately 600 characters including as many as 400 blanks.

B. Recommendation: The use of Comma Separated Values (CSV) is both lightweight and human readable. It serves as a sound text based standard for data interchange and should be allowed for use in formatting log download files if peer to peer methods for data transfer are accommodated. The use of XML should be used for Commercial Mobile Radio Service (CMRS)-based approaches.
   1. The standard for CSV has been defined by the Internet Engineering Task Force (IETF) as: — "RFC 4180 – Common Format and MIME Type for Comma-Separated Values (CSV) Files."
   2. Flat file should be in one of the above specified formats.

C. Naming Convention Recommendation: Naming conventions have to consider the variety of OS platforms that may be employed in this solution and file systems with which they are compatible. The common denominator for file systems is FAT32. Assuming a FAT32 file system, the most common naming convention is Windows with the following limitations:
   1. File and folder names may be up to 255 characters.
   2. Full pathname is limited to 260 characters.
   3. Backslash — "\" is used a directory separator.
   4. File and directory names may not contain any of the following characters: "/*?<>|:
   5. Periods are allowed in file and directory names except as the final character.
   6. File and directory names preserve case but are not case-sensitive.

   Directory and file name for a generated eRODs file should include enough information to be unique but should also be meaningful to a human reader.

   The file location should be a nested two directory hierarchy. The first level is the carrier's FMCSA DOT Number. The second directory is the driver's carrier assigned Id. The name of the file is the UTC date time to the second of when the file was generated. It will be assumed that any file generated will include all relevant information for the driver's HOS at the time the file was created.

   For example, if driver John Smith working for a carrier with the DOT number 12345678 and having been assigned an ID of JS2393 by the carrier has an eROD file

generated for an official on September 1, 2012 at 3:14:02 PM (UTC) the resulting directory location and encrypted eRODs file name will be:

\123456789\JS2393\20120901151402.log

The corresponding manifest file directory and location will be:

\123456789\JS2393\20120901151402.manifest

Using this scheme log information is easily separated by carrier, driver, and time as needed by any consolidated storage repository.

D. Other Considerations:
   1. CSV is also the standard of choice for data downloads in — "SAE J2728: Heavy Vehicle Event Data Recorder (HVEDR) Standard."

IV. Sensor Failure Thresholds and Recovery

A. More definition is needed regarding limited sensor failures, recording of data without a particular sensor feed, and criteria and process for return to normal operation when sensor failure condition is cleared. Additionally, sensor failure events should be further analyzed to identify issues related false positives, potential tampering indicators, and verification of EOBR integral synchronization with the vehicle.

B. Recommendation: Further break down definition of EOBR — "ceases to function" into separate categories and correlate actions with each.

Failure Condition	Recommended Action
If CPU fails	System will not be able to trigger audible or visual alert. Required indicator for driver is blank screen.
If EOBR screen fails	System will not be able to trigger audible or visual alert. Required indicator for driver is blank screen.
If EOBR software fails (non-critical)	EOBR must alert driver via audible and visual alert and must attempt to recover from failure automatically. Secondary alert must be provided to driver once recovered.
If GPS sensor feed is lost	Only trigger alert to driver and note as a sensor failure within flat file *if* GPS is not working during a required record interval (duty status change, hourly when moving).
If ECM sensor feed is lost	Only trigger alert to driver and note as sensor failure within flat file *if* ECM readings cannot be detected for 5 or more minutes, or if the EOBR cannot calculate gaps in distance travelled during the 5 sensor failure based upon cumulative ECM readings.

C. Subcommittee comments:

1. *If EOBR software failure is non-drive time critical, no audible alert is necessary. No immediate safety concern.*
2. *Develop matrix of critical errors that warrant audible alert versus non-critical errors that warrant only visual alert.*
    a. *If EOBR system detects vehicle motion without anyone logged in, audible alert may be necessary. Driver should have to acknowledge the alert before it is turned off.*
    b. *EOBR Final Rule uses the word "and" to indicate both audible and visual alert is required.*
    c. *Develop matrix of current OEM practice regarding use of visual and audible alerts, when both are used, or one over the other.*
3. *For CPU or EOBR screen failure, with "USDOT-EOBR" on display screen (as opposed to faceplate), there would be no way to tell that an EOBR device was 395.16 compliant.*
    a. *There should be a definition for the timeframe a carrier must replace a nonfunctioning EOBR (Issue VII).*
4. *Note: Definition of alert is not precisely defined. Could also imply an indicator.*
5. *For CPU failure: Should accommodate situation where a mobile EOBR display remains operable but the synchronized EOBR component is inoperable. Note CPU failure on the mobile application. So long as a display continues to function, provide visual alert. Otherwise, blank screen is the required indicator.*

V. Testing Resources

A. Issue: There is a need for FMCSA to provide testing resources for EOBR providers to verify log data transfer capabilities and the presentation of driver log information as seen by enforcement for a wide range of test scenarios. The use of web services to transfer log files for viewing by law enforcement—during roadside inspections—will require an infrastructure, maintained by the FMCSA. Additionally, each provider must enroll and actively participate to be able to transmit logs to law enforcement.

B. Recommendation: The FMCSA would need to provide a point of contact for all EOBR providers, and a means of enrolling in these web services for the purpose of transferring log files. Once enrolled, there must be procedures in place to allow for the testing of the web services exchange between the FMCSA's system and the EOBR provider's system.
    1. In a testing environment, the EOBR provider should be able to send a log file to a queuing area for the FMCSA to import into their system. The FMCSA should be able to import the log file into a test environment, as well, to ensure quality of data being received from the EOBR provider.
    2. The FMCSA would not need to provide a document outlining the file requirements. The requirements set forth in 395.16, for file export, could be utilized. As part of the technical requirements for a "live" implementation of the web services exchange, after enrollment and testing, FMCSA must provide information outlining "where" the data file should be sent.

C. Conclusion: The FMCSA would essentially have to certify that each EOBR provider that wanted to be able to transfer log files for viewing by law enforcement, met the technical requirements summarized above. A major benefit of this process includes the FMCSA's ability to know exactly what providers are out there and ensure each of them, that are compliant with 395.16, will be able to provide information necessary, via web services, for roadside inspections.

D. Subcommittee comments:
    1. Qualcomm: Generally agree with recommendation but would add the following:
        a. The statement that: "The use of web services to transfer log files for viewing by law enforcement—during roadside inspections—will require an infrastructure, maintained by the FMCSA." is a suggested approach. It may be preferred by FMCSA and/or state enforcement agencies to provide such infrastructure on a regional or state basis. If the latter, then testing resources should be provided with each installation.
        b. The testing resources should be isolated from access to any live operational systems and databases.
        c. The testing resources should include algorithms developed for enforcement systems functions for presentation and interpretation of the data. This will enable EOBR providers to verify that log data that is sent from an EOBR system will be seen exactly the same as the log data is received on an enforcement system. It will also serve to identify exceptions with the algorithms on either end.
    2. Continental: Agree. In addition testing resources will be needed for all types of data transfer agreed on (e.g. direct via USB) EOBR interfaces. Those testing resources are not a substitute for a precise certification criteria and independent certification process.
    3. *Note: This approach noted here is only applicable to telematics application services approach, but there should be testing resources for peer to peer transfer as well.*
    4. *Is there an existing FMCSA protocol for accepting data from states? What are the budget implications for the Agency if not?*
        a. *FMCSA has certification process to get entities that want to connect to system authority to do so. Work with technical/administrative points of contacts to ensure that when data is sent, proper edit checks are taken.*
        b. *Part of data transfer testing is working with state and state vendors to ensure data uploaded is accurate.*
        c. *Data transfer testing is indicated by official letter from FMCSA.*
        d. *Timeframe from requesting data transfer testing to receiving: something on the order of months? Hundreds of EOBR services providers would create backlog in initial certifications.*
        e. *Budget implications: Would FMCSA be able to get a data transfer testing program off the ground by June 2012? Depends on how many vendors need initial data transfer testing.*

5. *Note: Data transfer testing discussed here is testing processes and resources, so not necessarily validation, but validation of data transfer platform. Different from EOBR System Certification discussed in Issue X below.*

VI. Event Coding/Error Reporting

A. Issue: There is an inconsistency of the recording of the error codes as defined in the FMCSA 395.16 Appendix A fields as defined in the below TABLE 3. There is no definition of content in the 2 digit Event Error Code nor is there sufficient field size (2) to enter the Diagnostic Event Code since the CODE is 6 characters.

Diagnostic Event Code. For diagnostic events (events where the A ..... 2 (See Table 3).

"Event Status Code" is noted as "DG"), records the type of diagnostic performed (e.g., power-on, self test, power-off, etc.).

Event Error Code ..... Error code associated with an event ..... A ..... 2 (See Table 3).

B. Recommendation: Recommendation is to assign a two digit letter code to the Code Class and Code within the Code Class. As Example: General Diagnostic would be "A" and the PWR_ON Code would be "A", Data Storage Diagnostic would be "B" and INTFUL would be "A" within that group. With identical cross reference table being incorporated into the FMCSA roadside programs. Below is the specification entry in the file to be downloaded.

It is also recommended that a review of eRODS intent for the use of this be accomplished with a focused task group to be sure that all the indicated diagnostics are:

(1) Identified as achievable and usable
(2) Identified as to criteria that is appropriate for use and content for EVENT ERROR CODE

TABLE 3—EOBR DIAGNOSTIC EVENT CODES

Code class	Code	Brief description	Full description
General System Diagnostic	PWR_ON	Power on	EOBR initial power-on.
General System Diagnostic	PWROFF	Power off	EOBR power-off.
General System Diagnostic	TESTOK	test okay	EOBR self test successful.
General System Diagnostic	SERVIC	Service	EOBR Malfunction (return unit to factory for servicing).
General System Diagnostic	MEMERR	memory error	System memory error.
General System Diagnostic	LOWVLT	Low voltage	Low system supply voltage.
General System Diagnostic	BATLOW	battery low	Internal system battery backup low.
General System Diagnostic	CLKERR	clock error	EOBR system clock error (clock not set or defective).
General System Diagnostic	BYPASS	Bypass	EOBR system bypassed (RODS data not collected).
Data Storage Diagnostic	INTFUL	internal memory full	Internal storage memory full (requires download or transfer to external storage).
Data Storage Diagnostic	DATACC	Data accepted	System accepted driver data entry.
Data Storage Diagnostic	EXTFUL	external memory full	External memory full (smartcard or other external data storage device full).
Data Storage Diagnostic	EXTERR	external data access error.	Access external storage device failed.
Data Storage Diagnostic	DLOADY	download yes	EOBR data download successful.
Data Storage Diagnostic	DLOADN	download no	Data download rejected (unauthorized request/wrong Password).
Driver Identification Issue	NODRID	no driver ID	No driver information in system and vehicle is in motion.
Driver Identification Issue	PINERR	PIN error	Driver PIN/identification number invalid.
Driver Identification Issue	DRIDRD	Driver ID read	Driver information successfully read from external storage device (transferred to EOBR).
Peripheral Device Issue	DPYERR	display error	EOBR display malfunction.
Peripheral Device Issue	KEYERR	keyboard error	EOBR keyboard/input device malfunction.
External Sensor Issue	NOLTLN	no latitude longitude	No latitude and longitude from positioning sensor.
External Sensor Issue	NOTSYC	no time synchronization	Unable to synchronize with external time reference input.
External Sensor Issue	COMERR	communications error	Unable to communicate with external data link (to home office or wireless service provider).
External Sensor Issue	NO_ECM	no ECM data	No sensory information received from vehicle's Engine Control Module (ECM).
External Sensor Issue	ECM_ID	ECM ID number mismatch.	ECM identification/serial number mismatch (with preprogrammed information).

1. For the EVENT ERROR CODE there is no definition anywhere in the regulation that indicates the content of the field. With the description in Table 3 it is not apparent that this code should be an indicated of PASS /FAIL.
2. LOWVLT as an example would be that if voltage went to a very lower level for power required for a device it would shut down processes immediately to protect itself and may not be able to record the failure. If battery buss bars were pulled in the maintenance shop, which for some maintenance practices is a safety procedure, there would be no opportunity to record an error.
3. PWR-ON, PWROFF could be normal events everyday for the device and the field can be Y/N, and Pass Fail (P/F) may not make practical implementation.
4. DATACC is this to be triggered for every entry by the driver of Duty Status change and annotation to RODS as example.
5. BYPASS – no indication of what the EVENT ERROR CODE could be for this and what is the difference between BYPASS and NODRID. This seems to be the same indicator.
6. Diagnostic identified for GPS unavailable during duty status or hourly motion segment. GPS is a receiver requiring line of site and although great strides have been made in GPS receivers for acquisition there are times that signal will temporarily may be unavailable.

7. The statement below contained within the lead paragraph of FMCSA 395.16 Appendix A has to say "Event Update Status Code".
8. In the last case, the corrected record must be recorded and noted as "current" in the "Event Status Code" data field, with the original record maintained in its unedited form and noted as "historical" in the "Event Status Code" data field. The second reference should be — EVENT STATUS UPDATE CODE. The EOBR Data Elements Dictionary is described in Table 2. The event codes are listed in Table 3. Event Update Status Code. A status of an event, either Current (the most up-to-date update or edit) or Historical (the original record if the record has subsequently been updated or edited). A ..... 1 C = Current, H = Historical
9. Additionally there is not a clear way to define and Annotated Record. There can be current and historical for all EVENT Status codes. Recommendation is to add "AN" as an Annotated Record to the EVENT STATUS CODE would be it clear and concise as the definition

C. Subcommittee comments:

1. *Would roadside enforcement be able to see these errors? Electronic inspection would reveal these errors. But not with manual inspection.*
2. *Annotated records are when the driver adds notes/remarks to the EOBR data.*
3. *This recommendation is consistent with prior recommendation made at May 2011 public meeting.*

VII. Recommended Actions for Diagnostic Events

A. Issue: EOBR and sensor failures result in the driver being alerted to prepare paper logs. As some sensor failures occur due to intermittent problems, e.g., loss of GPS signal, it would be expected that drivers are alerted of normal system operation and to end use of paper logs. However, the requirements for resolution and recovery from sensor failure events are not defined in 395.16.

B. Recommendation: A more definitive analysis of sensor failure events is needed, including:

1. Thresholds for identifying a failure of each sensor or system component (to minimize false positives and to identify potential tampering events).
2. Approach to automatic determination of normal operational status of the sensor or system component.
3. Requirements for driver‘s use of paper logs and entry of manual EOBR records.

C. Background/Recommendations:

1. GPS as stated earlier is a receiver that requires line of site to provide latitude and longitude to the EOBR for several transactions. GPS may not be available for short durations of time and allowance for entry of location as an override when GPS not available may be a correct method in duty Status Changes.
2. ECM is some vehicles on the J1939 ECM may be busy at the time of the required change, error should not be record and a time duration specified such as five minutes to allow acquisition of information.
3. EOBR processor unavailable may be as simple as the BLANK screen indicates to keep paper logs. Many systems in the field perform diagnostics

beyond what is defined in TABLE 3 to indicate to the driver to keep paper logs.

D. Subcommittee comments:
   1. Qualcomm: Generally agree with recommendation but would add the following:
      a. For some sensor failures such as GPS or ECM, it is feasible to alert the driver of the loss of automated data capture and for the EOBR to continue recording current duty status information – with the EOBR record containing accurate time and other measures that are available. The sensor failure would be identified in such records. These events could be highlighted with the driver review for record accuracy before log submittal. When the sensor failure is corrected (sometimes naturally within minutes), EOBR recording would be back to normal. It is suggested that such an approach is preferred to a driver handwriting all information on a paper log.
      b. Requirements of 395.16 do not specify requirements for resolution of sensor failures and criteria for returning an EOBR to normal service after a sensor failure. Some failure events such as loss of ECM signal, loss of power, and loss of GPS have the potential to occur naturally as well as due to tampering. It is recommended that in all cases that EOBR recovery to normal operations be allowed as soon as device self-diagnostics and/or host system remote diagnostics indicate normal operation. Additionally, all sensor failures should be reported to the motor carrier and/or EOBR services provider within 24 hours through automated EOBR system reporting or through driver communications. A requirement should also be stated that carriers, drivers, and EOBR service providers make a good faith effort to resolve sensor and EOBR failures on a timely basis.
   2. *Timeframe for repair of nonfunctioning EOBR.*
      a. *How do you put the unit back into service after a sensor failure? This is not explicitly addressed in the rule.*
      b. *Carrier should be allowed to make EOBR repair at next carrier facility, and not required to repair on the road. If carrier is required to have EOBR, requirement to repair failed EOBR before next dispatch from home terminal, or no later than fourteen days, whichever comes first, would be reasonable.*
      c. *Note: 49 CFR 385.811 currently requires repair in 14 days.*
   3. *If sensor failure is a result of temporary GPS signal loss, does driver need to use paper logs at that point? If change of duty status occurs during temporary loss of signal, is the EOBR nonfunctioning, i.e., must the driver us paper logs?*
   4. *Sensor failure issues are more significant for other non-recordable ECM data.*
   5. *Lack of definition would result in drivers going back to paper logs for temporary, line-of-sight failures.*
   6. *Thresholds for sensor failures are covered in Issue IV.*

7. *If EOBR system is down, and a driver is using paper, a roadside inspector does not necessarily have any way to determine how long the system has been down.*
8. *Suggestion: If ECM is temporarily not available, refer to GPS for mileage? Big departure from current rule. But would prevent having to go back to paper logs.*
    a. *There would need to be a threshold for how long the EOBR system can obtain mileage information from GPS (as the backup). Follow up by comparing GPS to ECM to validate mileage.*
9. *Temporary loss of signal is relatively frequent, but GPS/ECM signal failure is much less common.*
10. *Suggestion: If miles on ECM are consistently off, this could be accounted for in certification process.*
11. *If there's no location available at duty change period, look back to most recent location data (if it is "reasonably" recent).*
    a. *May want to use ignition off time as a trigger for reliability of when GPS signal was last valid.*
12. *If data is only partially recorded, that should be noted on the display. Should have indicator on display indicating problems with EOBR, so that the driver would see that and could annotate logs with missing information.*
13.

VIII. GPS DATA Format Correction

A. Issue: In the Appendix A there is no sign identified for the Latitude and Longitude. If there is an assumption that eRODS will put the field in for the +/- to be there prior to location lookup then the file structure can stand as is. There is no exposure as to what mapping tool or uses of this field in eRODS, therefore a need is there to work correctly with any mapping tool that would require a signed field for hemisphere location on a mapping product.
B. Recommendation: Add a designator to allow the GPS signal to indicate +/- for Lat/Long.

IX. EOBR 395.16 395.15 Interoperability with Migration

A. Issue: In the 395.16 regulation there is a Grandfather Clause that allows 395.15 devices installed prior to June of 2012 to remain in service for the useful life of the vehicle. Carriers that have voluntarily implemented EOBR systems for use will take financial advantage of this allowance to minimize capital investment until such time as the vehicle is replaced.
    1. Due to diverse operations in the Carrier environment there will be both 395.15 and 395.16 compliant devices in use in the same fleet for a lengthy period of time.
    2. Additionally it must be understood that drivers will move between vehicles with these devices and under current specifications in 395.16 can potentially defeat the purpose of the automatic recording of HOS information.
    3. Specifically there is no consideration to have electronic records from a 395.15 device in the 395.16 eRODS file definition.

4. The 395.15 device would have all the RODS/HOS information available but, not the diagnostic events and the hourly GPS while in motion that is required in 395.16.
5. Additionally may not have annotated records from a driver, nor Personal Conveyance tracking events since these are not requirements in 395.15.

Consideration must be given to Law Enforcement training and awareness of the situation and processes defined for audits as well as eRODS design allowance.

Drivers could be required to maintain copies of paper logs from the alternate device when a movement is required:

- This would defeat the purpose of the device
- Be a larger burden to roadside inspections
- Strongly suggest this would create a gap in the correct information in the EOBR for the 8 day cycle required
- This practice would foster internal Carrier DOT audits exceptions

B. Recommendation: At minimum create a record type in the Event Status Code in Appendix A that would allow at minimum posting of the information required for RODS/HOS information as defined in the 395.15 compliant requirements.

The information would have to be synchronized through the back office support system of the carrier and consolidated to create the 8 days required and sent over a telematics method or a controlled transfer method potentially by portable media. (media method may present risk)

Since there is the potential of other inputs such as paper logs entered into the system by an administrator when systems may be inoperable, it is also recommended that the Event Status Code be created to indicate the source of other log entry input such as this.

There may be other events that track driver duty while on Carrier premise such as a time clock system to show total work hours. Rules could be defined as to the process for sequencing information to be sure that insertion into the RODS is correct.

C. Subcommittee comments:
    1. Qualcomm: Generally agree with recommendation but would add the following:
        a. Allow for EOBR display of driver log data to include all available data sources with an indicator for the duty status event if the source is not the EOBR currently in use.
            i. *Other types of activities that should also be in record.*
        b. Any transfer of data to an EOBR for log data from other sources must be subject to secure data transfer and an effective authentication process that is controlled by the EOBR host system to authenticate the EOBR device and the driver.

    c. Specific guidance should be provided for presentation requirements and options for driver log information when it is not practical to provide information from all available sources, i.e., EOBR records have gaps that can be covered by 395.15 records or back office annotations, but such data is not currently available on the EOBR and would not typically be provided in paper form.

2. Continental: Partially agree. Agree that an Event Status Code should be created to account for manual inputs that could be allowed under precisely defined conditions.
    a. In addition a minimum set of requirements with which all devices (old and new) need to comply needs to be defined. Those devices that cannot fulfill all minimum requirements should be phased out. Carriers will still have the possibility to use those non-compliant systems for productivity purposes but would need to install in addition fully compliant EOBRs.
3. *Data file should also indicate whether log was created with a 395.15 device or a 395.16 device, so that enforcement could see that the record was created by EOBR 395.15 or 395.16 device.*
    a. *Concern is that years from now, a carrier/driver would be using a grandfathered 395.15 device with no standardized data interface, and a roadside inspector cannot receive their log data.*
4. *Potential regulatory obstacles to log data indicating 395.15 or 395.16 device?*
5. *Not a requirement for 395.15 devices, but an option.*
6. *Define the fields that come from a 395.15 device compared to Appendix A, and specifically define in the log data file whether the log was created by a 395.15 or 395.16 device.*
7. *When manual input is included, there should be a designation in the record to indicate that the data is from a manual log.*
    a. *May be cumbersome for some carriers to integrate manual log data into electronic record.*
    b. *Manual data should be integrated into electronic record within a certain number of days.*
8. *Sequence numbers no longer have any meaning when you bring in data from different sources.*
9. *Since there may be incomplete information (where HOS information is in electronic and manual form), it may not be possible to provide warnings prior to violations for the driver because the record does not include all hours.*
    a. *Potential situation to address: drivers who split their weeks between short haul operations and long haul operations. Currently drivers are not required to keep logs in this situation (travel within 100 air mile radius).*
10. *Purpose of recommendation is to make data view easier for roadside inspectors.*
11. *Three years from now, hours of service management system should include all data from all sources. For now, we should try and do that for EOBRs.*

12. *Two layers: (1) Recommendation to accommodate 395.15 data and outside data into 395.16 as part of the rule, and (2) Should there be a mandate to bring all data into one system?*
13. *If we have 395.15 data, how do we get that information to roadside inspectors? Critical to answer.*
14. *Time worked to maintain vehicle: With EOBRs, how is this taken into account? Manually change duty status (on duty, not driving), or on internet (online time card). Could be an annotation.*

X. EOBR System Certification

A. Issue: With the movements both legislative and from NPRM currently issued by FMCSA to have an EOBR mandate a certification process for compliant EOBR systems needs to be created. It is important to the current issued regulation with recommendation of a Telematics approach to transfer of eRODS information to enforcement at a potentially control FMCSA Cloud, Web Services or Portal that a certification process be put into place to at minimum certify authentication and credentials for the transferring of the required RODS information as defined in Appendix A of the current regulation.

B. Recommendation: From results of recommended testing processes we develop a certification process that would define:
   1. Authentication of file being transferred for enforcement
   2. File identification to have specifics for enforcement accurately reviewing the correct driver
   3. Encryption methodology
   4. Information content integrity and accuracy
   5. Overview that EOBR system components create a tamper proof device and compliant data captures
   6. Definition of enforcement verification that the CMV transfer process is understood and observed
   7. Understanding on EOBR provider architecture to support FMCSA transfer of information

C. Qualcomm comments: It is recommended that a detailed EOBR certification criteria and formal certification process be developed on a timely basis as these are essential prerequisites to an EOBR mandate. Development and specification of this certification approach will be a significant, time consuming effort and should involve all key stakeholders. It will be necessary to have this certification process in place at least 18 months in advance of the mandate to allow EOBR providers and the certification resources adequate time to execute the process for certification applicants.
   1. The EOBR system certification approach must be comprehensive, with coverage of the following:
      a. Certification criteria in regulation: EOBR systems must be "sufficiently tested to meet the requirements of § 395.16 and Appendix A to this part under the conditions in which they would be used."
      b. Suggestion: Add to current certification requirement end-to-end system security measures, providing verification of security features

for normal operations and identified security threat conditions. This includes effective authentication and security of wireless data transfers as described in the above recommendation.

c. EOBR device synchronization with the vehicle and tamper detection functions and features. Should be tested and reviewed as part of certification process.
d. EOBR system administration for access controls, driver identification management, and records management. Such back office functions need to be verified through certification process.
e. EOBR compliance management processes and controls for back office information reporting, log data management functions, and exceptions management including data corrections and device failures management.
f. EOBR system management processes and controls related to EOBR provisioning, EOBR device support including hardware repairs and software updates, back office application software updates, data backups and recovery, system and network downtime recovery, and updates to the technical infrastructure. If not part of certification, error in these areas could compromise integrity of EOBR system.
g. Other criteria yet to be developed.

2. Given the complex nature of EOBR systems, certification with a lab approach is considered to be inadequate. While process specifics must yet be defined, it is suggested that the certification approach will include the following:
    a. Comprehensive check list of items to be verified (defined certification criteria).
    b. 3rd party review of EOBR conformity to certification criteria with EOBR provider demonstration of EOBR system features to meet requirements.
    c. Follow-up 3rd party audits on a scheduled basis and as needed to review substantial changes in the EOBR system.
    d. Cuthbertson, XATA – I feel that a full certification at this stage beyond the Telematics protection certification would not be attainable. Certification verification could be added to the Testing Criteria as part of that process.
    e. I think a full certification process against 395.16 would not be attainable now but, necessary for a mandate of 395.16. Much of the changes we are requesting would greatly modify a certification process.
3. Would take at least 18 months to put certification process in place.
4. Self-certification is sufficient for current regulation, but if FMCSA moves to EOBR mandate, 3rd party certification and audits are recommended.

D. Continental comments: Partially agree.
    1. The data transfer process is only one part of the EOBR system. Whatever the data transfer process chosen, a security level needs to be defined to encompass the whole EOBR system (installation in vehicle, data collection, transfer between EOBRs, transfer to enforcement, storage at carriers). Then an

independent certification process should be established to test EOBRs against this clear security level.

2. We propose that FMCSA contracts an independent consultancy to prepare detailed certification criteria with input from all stakeholders. The certification criteria should include a clear security level using established IT security framework such as Common Criteria. This will allow a 3rd party certification process which is necessary for carriers as well as enforcement to clearly identify compliant EOBR systems and trust the data provided by those systems.
    a. Security level certification should apply to all levels of data transfer.

E. *Subcommittee comments:*
    1. *Certification must happen within a certain time period.*
    2. *Various levels of confidence in accuracy of driver's record of duty status: manual, 395.15 device, 395.16 device.*
    3. *Certification process will be necessary in the event of an EOBR mandate because market for supply of EOBR services will widen, and many carriers will reluctantly use EOBRs – must ensure that these carriers can use them effectively. E.g., engine connectivity, GPS capability – certification will ensure due diligence that these systems are capable of functioning effectively over time.*
    4. *Still need to have something in place to ensure security and encryption of data uploaded to FMCSA systems (for transfer to roadside inspectors) in time for June 2012 compliance.*
        a. *How far above self-certification do we need to go for June 2012 compliance with EOBR final rule?*
        b. *Need to define short term certification versus long-term certification process.*
    5. *Certification is important because carriers purchase what they think is DOT-compliant EOBR equipment have no way of verifying, and are relying on it to comply with HOS requirements.*
    6. *Suggestion: Ultimately, FMCSA should provide conforming product list for carriers to rely on.*
    7. *Should improve appropriate controls on driver IDs, how back offices do edits, how companies upgrade software. Need to test if companies have a viable approach to transmitting data.*
    8. *Two phases: (1) Establishing certification process; (2) Certifying all vendors.*
    9. *If there's not a certification process, how accurately can roadside inspectors treat the information?*
    10. *Hardware versus software issues: Can FMCSA move forward with 395.16 hardware changes, and address certification issues later?*
        a. *Could be both. Need to bring in knowledge of EOBR suppliers.*
        b. *As part of certification, you need to show that hardware is capable of functioning properly, proper storage.*
        c. *Would not expect to introduce new hardware requirements as a result of certification.*

d. Control processes need to be looked at in certification. Newer consumer-ready devices coming to market – how do you control that environment and ensure that those vendors have the controls in place?
e. Hardware is up front (one time), software is ongoing.
f. System must be tested end to end but system can be broken up to test pieces at a time.
g. Shouldn't be roadblocks to building compliant hardware once USB issue is resolved.

11. Certification should not dictate hardware. Must protect options that are available to carriers. Carriers make sizable investment in these existing technologies – options should remain available. Should not require a redundant second system to transmit data.
a. There are large carriers that do software programming themselves – need to keep that in mind. Carriers may also be required to go through the certification process.
12. Certification is important: Many different devices being used. There are many different EOBR suppliers that are not necessarily capable of providing reliable equipment. When an ECM has problems communicating information, vehicle systems may not operate.
13. Waiting to implement certification process is not advisable because the current rule is already moving towards increased adoption of EOBR technology. Need to start some process moving towards certification.

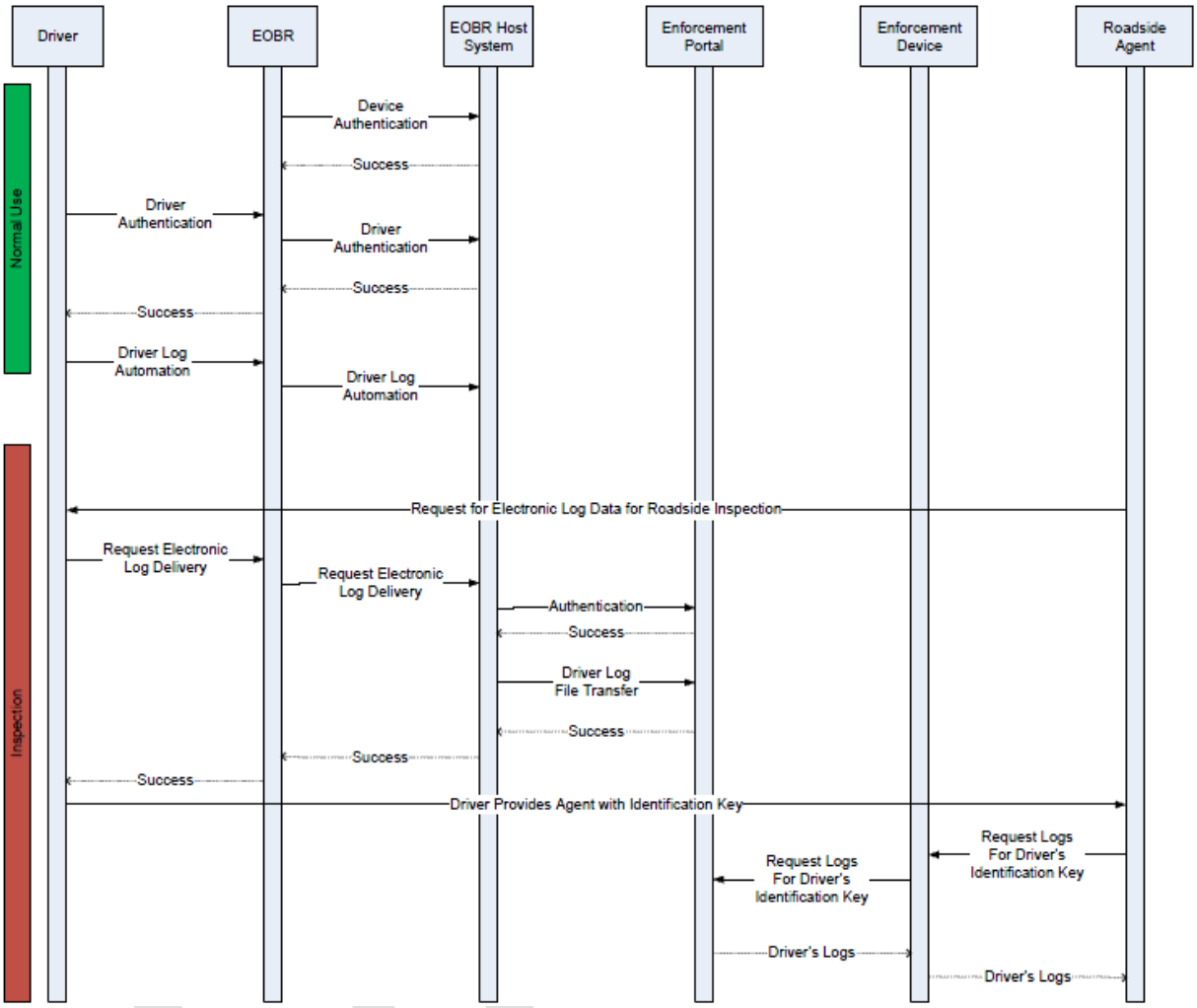
XI. Telematics Application Services Approach for Electronic Driver Log Downloads

A. Issue:
1. How an EOBR is able to wirelessly identify external networks and devices and securely connect to them to transmit HOS information.
2. Establishing a secure and reliable communications protocol that will allow data transmission in a timely manner.
3. Clarification of methodologies and the required interfaces and applications to securely and reliably transmit HOS data via telematics applications services.

B. Recommendation – Conceptual Framework for Telematics Application Services Approach: Key concepts as discussed in May 31, 2011 public meeting on EOBR technical issues:
1. Telematics service provider (or carrier host system) manages information security of driver logs as recorded on the vehicle EOBR device and at the EOBR host system, and with data communications of driver logs between vehicle device and host system.
2. Electronic driver log download for roadside inspection is initiated by the driver.
3. Log file transfer is a push of data from vehicle EOBR system to EOBR host system and then from host system to enforcement network center or portal via internet communications structure.
4. Roadside enforcement retrieves (pulls) data from a portal and other network resource as data download becomes available. Optionally, the enforcement

device address may be provided to the log download initiation process for an end-to-end push of the download.

C. Recommended Design:



D. Requirements for Process Steps:

1. Device Authentication – Performance requirement that the host system authenticates all EOBR device connections to the host system.
2. Driver authentication – Clarification of the performance requirement per 395.16 (j) Driver Identification. The performance requirement should include EOBR host system authentication of the driver ID and password or other biometric identifier.
3. Driver Log Automation – Per the performance requirements of 395.16 and 395 Appendix A.
4. Request for Electronic Log Data for Roadside Inspection – Request is a face to face interaction between enforcement agent and driver.
5. Driver Log File Generation – An EOBR function for driver initiation of electronic log download. This function triggers synchronization of the EOBR

log data with the EOBR host system. The function automatically generates a file identifier for the driver to convey to the enforcement agent. Alternative design approaches may be considered for distributed enforcement portals, or for enforcement systems to pull data from EOBR host system. Formatting of the log download will be accomplished by the host system to include:

a. Flat file record generation per field definitions as specified in 395.16 Appendix A.
b. The file will be formatted using the XML standard.

6. EOBR Host System Authentication – The EOBR host system will initiate a connection with the enforcement portal following trigger of the driver's electronic download. The authentication will utilize a
7. Log File Transmitted and Acknowledged – After a connection and authentication is completed between the EOBR Host System and the Enforcement Portal, the file will be transmitted via web services approach to utilize the Simple Object Access Protocol (SOAP). After successful transmission of the file, the enforcement portal will send an acknowledgement message via web services.
8. Agent Retrieves / Receives Driver Log File – The agent is expected to have connectivity with the enforcement portal and will be alerted when the file is available. An alternative design approach allows direct routing of the file download directly to the enforcement device at roadside. It is assumed that information security is management in the enforcement systems and no additional requirements are needed.
9. Inspection Completed – As closure, the inspection is completed with no violation, or with initiation of another process to deal with the violation.

E. Additional Notes:
   1. Overall cycle time from log download initiation to receipt by the enforcement device is expected to be approximately a few minutes assuming no exceptions in the process.
   2. FMCSA will provide and manage the enforcement portal services.
   3. FMCSA will provide, support, and manage authentication credentials with EOBR telematics service providers and carriers as operators of their own EOBR host system.
   4. FMCSA may revoke authentication credentials for any service provider that does not provide log download files per specified requirements or does not perform on a timely and reliable basis.

F. Requirements for Log Download Exceptions:
   1. Device Authentication Exceptions:
      a. Out of coverage and authentication not completed.
         i. EOBR continues to function to record driver logs but records are identified as subject to device authentication.
         ii. Log downloads cannot be initiated by a device not connected and authenticated by the EOBR host system.
      b. Device authentication failed.
         i. Driver alerted of sensor failure and the need to record paper RODS.

ii. Continued automated recording subject to resolution of sensor failure and recovery issue. Recommend that EOBR continues to function to record driver logs but records are identified as subject to device authentication. If authentication is restored, then records accepted. If authentication not restored, manual logs must be processed.
iii. Log downloads cannot be initiated by a device not authenticated by the EOBR host system.

2. Driver Authentication Exceptions:
   a. Out of coverage and authentication not completed.
      i. EOBR continues to function to record driver logs but records are identified as subject to driver authentication.
      ii. Log downloads cannot be initiated until EOBR connected and driver authenticated by the EOBR host system.
   b. Driver authentication failed.
      i. Driver alerted of access denied for EOBR use and the need to record paper RODS.
      ii. Continued automated recording of all vehicle movement and any sensor failure events.
      iii. Log downloads cannot be initiated by a driver not authenticated by the EOBR host system.
3. Driver Log Automation Exceptions
   a. Sensor or EOBR system failures resulting in drivers recording paper RODS.
4. Request for Electronic Log Data for Roadside Inspection Exceptions
   a. Driver provides incorrect file identifier to enforcement agent resulting in file not found by agent.
      i. Recommend that EOBR provide a re-display of file name used.
   b. If enforcement routing address used – Driver enters incorrect address resulting in failure of file transfer. Resolution options:
      i. Driver and enforcement agent may decide to reenter address and restart file transfer process.
      ii. Host system identifies data transfer failure and sends message to driver to restart file transfer process.
5. Driver Log File Generation Exceptions
   a. Gaps in log data.
      i. Driver had prior duty status events where paper RODS used.
      ii. Driver had prior duty status events in other vehicle with 395.15 compliant AOBRD where data has not been applied to EOBR currently in use.
      iii. Recommend that at a minimum driver is alerted of all gaps in electronic log as recorded on EOBR currently being used. Subject to resolution of issue on log data integration, recommend also that driver and back office make best effort attempt to provide integrated electronic records for complete driver log.

b. Annotated records on EOBR host system not applied to EOBR currently in use.
    i. Back office annotations to correct driver errors (e.g., driver failed to enter off-duty when taking a break).
    ii. Back office annotation to apply corrections to driver violation of company policy (e.g., driver entered off-duty for break when not authorized to be off-duty).
    iii. Back office entry of driver other work that was otherwise recorded as off-duty (e.g., driver work in warehouse or work with other employer).
    iv. Recommend that driver is alerted of all back office annotations to log records. Subject to resolution of issue on log data integration, recommend also that driver and back office make best effort attempt to provide integrated electronic records for complete driver log. Alternatively, recommend that EOBR provide a display of all back office annotated records.
c. EOBR host system not available.
    i. Driver may be detained for some period waiting for log download.

6. Mutual Authentications Exceptions
    a. Authentication fails.
        i. Recommend that FMCSA portal services provide 24X7X365 support to resolve authentication failures on a timely basis. Support services also to provide timely resolution for persistent connection failures and recovery of system availability if portal system fails.
        ii. Recommend that EOBR host system service providers be required to disclose their hours of support to their customers and FMCSA portal services support center.
    b. FMCSA enforcement portal not available.
        i. Recommend that FMCSA establish and achieve a service level agreement that will support the needs of the enforcement community for access to driver log downloads for roadside inspection.
7. Log File Transmitted and Acknowledged Exceptions
    a. Connection fails during file transmission.
        i. Recommend that service provide automatically detect connection failure and trigger restart of connect, authentication, and file transmission process.
    b. Acknowledgement not received.
        i. Recommend that service provide automatically if acknowledgement not received in defined time period and trigger restart of connect, authentication, and file transmission process.

ii. Recommend that FMCSA portal services and EOBR host system services provider each provide 24X7X365 support to resolve file transmission failures on a timely basis.

8. Agent Retrieves / Receives Driver Log File Exceptions
    a. Agent cannot connect and/or authenticate with FMCSA portal.
    b. Enforcement device cannot process downloaded file.
    c. Enforcement device provides different interpretation of driver log data than EOBR (e.g., violation determination on one system but not the other).
    d. Agent does not have device or operating device to receive downloads.
    e. Recommendation: FMCSA and/or state enforcement agencies should establish a remote support services function to leverage review of electronic log data via voice support to roadside inspections. The roadside agent remains responsible for violation determination and enforcement, but is assisted as the support service provides input based on review of the driver‘s electronic log data pertaining to:
        i. Verification of authenticity of log displays and/or printouts available at roadside based on log summary data of system identifying information (i.e., check on potential counterfeit log printouts or log display system in driver possession).
        ii. Confirmation or disproval of determination of violation for complex log data scenario.
        iii. Identification of log data abnormalities and information gaps to be substantiated further through manual inspection based on detailed data analysis of GPS positions (with map interface), event status data, and record annotation details.
9. Inspection Completed Exceptions
    a. Inspection not recorded in SMS.

G. Subcommittee comments:
1. Qualcomm: Generally agree with recommendation but note that some design specifications are yet to be developed. Among the technical details to be specified are:
    a. EOBR host system and enforcement portal mutual authentication.
    b. XML schema.
    c. Connection exception processes.
2. XATA: Principally agree but, feel that design with input directly from enforcement to comprehend further design consideration should be included.
3. Continental: We do not agree that Telematics Application Services should be the only allowed method to transfer data to the enforcement. Continental would recommend that direct communication approach and Telematics approach should both be defined as available options.
4. DriverTech: Data needs for just HOS data is much less significant than a fleet management system.
5. *Telematics Application Services Approach will involve a user fee of some sort for carriers.*

6. *Concern for small carriers not getting the most efficient data plan pricing.*
7. *May be a workable solution for EOBR compliance for large carriers who already have fleet management systems in place.*
8. *This one option for the wireless data transfer of log data as specified in 395.16.*

XII. USB Data Transfer

A. Approach for USB Peer to Peer Roadside Data Transfer (Against):

1. Issue: The use of USB for data transfer between an EOBR system and roadside enforcement system is problematic due to the following:
    a. The requirements in 395.16 do not specify authentication requirements for when USB is used. Authentication features are not available with the USB 2.0 standard, nor are there off-the-shelf USB devices for data storage or wired transfer that would provide effective capabilities for device-to-device authentication. Without effective authentication, the use of USB with EOBR log downloads is easily vulnerable to data manipulation and other security risks.
    b. USB features for AutoRun cause its usage to be prone to malware vulnerability. EOBR devices, law enforcement computers and mass storage devices are equally at risk for being infected with malware.
    c. Many enforcement computer systems have USB connections disabled or are prohibited from using USB for file transfers due to malware and security concerns. As result, USB for log data transfers would only be supported by enforcement on a haphazard basis although all EOBRs are required to support this.
    d. There are physical considerations for the use of USB. The location of the USB port varies among systems and is sometimes on a processor unit that is separate from the display unit. Access to such units may require an extender cable which is not conducive to physical verification of the source device.
2. Recommendation: Eliminate USB as a requirement in 395.16.
3. Other considerations:
    a. A team of security experts at Qualcomm, Inc. as part of the Qualcomm Product Security Initiative (QPSI) conducted an assessment of the risks in using USB for driver log data transfers with 395.16 compliant EOBRs. The report, “Risk Analysis of USB Communications for EOBRs” is attached. The report strongly recommends against enabling a wired or portable media USB data connection as a channel for transmitting electronic driving records for EOBR devices. The primary factors, described in the report, include:
        i. Lack of secure authentication.
        ii. Unauthorized Read/Write/Code Execution.
        iii. Malware vulnerability.
        iv. Physical limitations of USB connections.
    b. There may be some that suggest that potential options exist to implementing a model where authentication credentials may be

applied in data transfers using USB media or cables for EOBR log downloads. However, among the requirements to be considered for such a program are the following:

c. A Credential Issuing Authority must be established. If controlled by one or more government entities, then legislation may be needed to establish, fund and give authorities for the new government functions. If performed by private enterprise, then performance requirements and an oversight function are needed.
d. Added technical requirements for EOBRs, including:
    i. Design specification and specialized manufacture of secure USB or other physical media device.
    ii. Design specification and specialized manufacture of EOBR devices with embedded public key credential.
e. On-going operational support services, including:
    i. Administration of authentication credentials.
    ii. Distribution of credentials to EOBR manufacturers, CMV drivers, motor carriers, and enforcement.
f. Given the above considerations, this type of program is well beyond the scope of implementing USB for log data transfers with 395.16.

4. Subcommittee comments:
    a. Continental: We disagree with the analysis leading to the conclusion that a reliable and tamper resistant log transfer using the USB interface on EOBRs cannot be done.
    b. *Europe has not experienced problems with malware transmission or file tampering. Countries have penalties for file tampering.*
    c. *USB wired approach is not practical because laptops in patrol cars and/or EOBRs are usually secured and cord lengths are limited to 15 feet.*

B. Approach for USB Peer to Peer Roadside Data Transfer (For)
1. Technically 2 main data transfer methods can be envisioned:
    a. Direct communication of the RODS file from the EOBR to the enforcement at the roadside via USB (either with a peer to peer 2 way communication or a portable data carrier),
    b. Indirect communication via wireless communication and Telematics Application Services.
2. For both concepts similar security mechanisms can be implemented in order to obtain a security level that might/should be required (for the time being 395.16 does not specify any security level). Those security mechanisms should allow to:
    a. Authenticate the source of the RODS file (which EOBR from which supplier).
    b. Detect a file manipulation.
    c. Prevent the transmission of malware to enforcement systems.
3. The same security level should be required for the log data transfer as for the overall system. Therefore in a first step a targeted security level for the overall

system should be defined, then appropriate security mechanisms can be defined for log data transfers at roadside check.

4. Independently of the data transfer approach, direct communication via USB or Telematics Application Services, in order to reach a high security level for the overall EOBR system a key management system with Public and Private Key infrastructure will be needed. A key management system will allow a truly reliable authentication of the file source (a) and detection of a file manipulation (b).
5. Direct communication of the RODS file from the EOBR to the enforcement can be performed using the USB type A connector. Several approaches are possible:
    a. A- USB storage device: Use of a dedicated USB memory stick provided by enforcement.
    b. B- WPAN USB dongle

A short range wireless USB dongle that will establish a local secure connection between the EOBR and the enforcement's computer. The most common Wireless Personal Area Network (WPAN) are Bluetooth and ZigBee.

The communication channel consists of a Bluetooth (or ZigBee) network that contains two peers: a Bluetooth Coordinator installed at the Enforcement Officer's Device (EOD) side and a Bluetooth end device installed at the EOBR side.

The EOBR provides a USB-Port (type A receptacle connector)

The enforcement officer's device (EOD) provides a USB-Port (type A receptacle connector) or an integrated Bluetooth connection.

A USB-dongle acting as a Bluetooth Coordinator (BC), connected at the EOD, USB-dongle acting as a Bluetooth End Devices (BED), connected at the EOBR.

For performing a data transfer during a roadside inspection the enforcement officer will provide an already paired Bluetooth End Device to the driver who will plug it into the EOBR USB port.

The Bluetooth network will be created automatically with the enforcement's computer and the data transfer done using the HTTPS protocol. The HTTPS is a ubiquitous protocol used for encryption and authentication of communications between Web servers and browsers on the World Wide Web. The protocol relies on a Public Key Infrastructure (PKI) to provide mutual authentication, hence the confidentiality of the transferred data is assured. Integrity and authenticity is also guaranteed by the protocol.

    c. C- USB networking cable (also called USB-USB bridge cable) to establish a connection to a laptop or handheld device

6. Security mechanisms to prevent the transmission of viruses.
    a. USB storage device

The EOBR is clean from viruses and also immune to viruses. However, viruses and worms can spread through USB Drives.

To prevent this threat, the following approaches can be taken:

- Implement strict guidelines to use USB keep personal and business USB drives separate – Enforcement should not use personal USB drives on business computers, and not plug USB drives containing enforcement information into personal computers. Unknown USB drive shouldn‘t be plugged into enforcement computers.
- EOBR shall remove the Autorun.inf file, if such file exists. This method only breaks the chain of virus propagation, in case that the USB drive used for the road side inspection was infected.
- Disable USB Autorun function on the computers owned by enforcement.
- Use and maintain security software, and keep all software up to date - Use a firewall, anti-virus software, and anti-spyware software to make computers less vulnerable to attacks, and make sure to keep the virus definitions current.

b. WPAN – USB dongle

The EOBR is clean from viruses and also immune to viruses.

If desired the USB ports of the enforcement‘s computers could be restricted to accept only the Bluetooth (or other WPAN) dongle and communication with authenticated EOBRs, therefore eliminating the threat of virus transmission from other USB devices. The enforcement‘s computers could also have an integrated Bluetooth.

c. USB networking cable

The EOBR is clean from viruses and also immune to viruses.

If desired the USB ports of the enforcement‘s computers could be restricted to accept only the USB networking cable and communication with authenticated EOBRs, therefore eliminating the threat of virus transmission from other USB devices.

C. *Subcommittee comments:*

1. DriverTech: Disagree with this USB approach. Security structure concerns.
2. Qualcomm: Disagree with this USB approach. Security structure concerns. Malware vulnerability concerns.
3. XATA: Feels that there are more specific definitions and implementation description in this area that needs to be described before any acceptance of the methods could be reviewed for acceptance or further comment. There are Operating System considerations and significant architecture that may be required to support the systems suggested that could add notable cost to the

EOBR. Equipment described can be more sensitive to environmental compromise.

4. JJ Keller: Many law enforcement are prohibited from using USB ports on computers, so is USB approach feasible.
5. PeopleNet: Security structure concerns. Lack of enforcement compatibility concerns.
6. *Additional peer to peer transfer suggested option: encrypted reader/transport device.*
7. *Concern about excluding data transfer options at this point.*
8. *EOBR manufacturers need to know which secure data transfer options they must make available in order to provide customers with compliant EOBR systems.*
9. *EOBR manufacturers (not Continental) need to see a more detailed security model for peer to peer USB transfer to satisfy security and malware concerns.*
10. *If we are able to address security concerns for USB, will state agencies change their policy (re: compatibility with USB)?*

XIII. Approach for 802.11

A. Issue: The use of 802.11 for data transfer between an EOBR system and roadside enforcement system is problematic due to the following:
   1. The requirements in 395.16 do not specify device authentication requirements when 802.11 is used. Again, EOBR providers have no control over counterfeit devices so it is assumed that authentication is controlled by the enforcement systems. However, valid EOBR systems are not required to present any credential, so this appears to be a significant security vulnerability.
   2. 802.11 features cause its usage to be prone to information security vulnerabilities. Broadcast of the SSID may invite unwanted guests to the network, but features for ease of connectivity are essential for usability by drivers.
   3. Most state enforcement agencies have not identified plans for implementing 802.11 for support of log downloads. As result, 802.11 for log data transfers would only be only be supported by enforcement on a haphazard basis.
   4. Implementation of a security model for mutual authentication with EOBR connections to local area networks on a national scale is very challenging and would require significant time and investment for a log download method that appears to have little interest by EOBR providers and the enforcement community.

B. Recommendation: Eliminate 802.11 as a wireless data transfer option in 395.16.

C. *Subcommittee comments:*
   1. *Why could the market not decide whether it is a viable data transfer technology? Important to provide various, flexible data transfer solutions.*
   2. *Another concern is how effectively can it work with law enforcement considering the security restrictions they are under.*
   3. *We should not allow a data transfer method without a security model.*

XIV. Manual Inspections

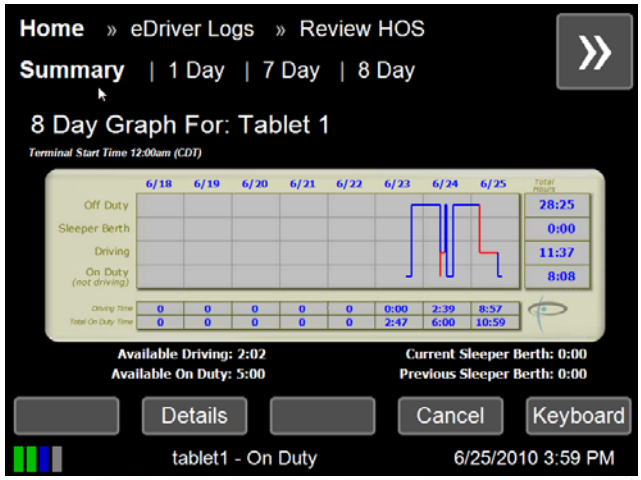
A. Issue: Automated inspections by roadside enforcement shall be the preferred method for reviewing EOBR data. However, in some cases, roadside enforcement may not have the means to conduct an electronic inspection. A manual inspection method shall be enabled for those cases. Inspection methods shall be consistent across EOBRs to simplify the interaction between drivers and roadside enforcement. This will help with training and implementation of EOBR enforcement. The approach must also address effective authentication of the driver log information source.

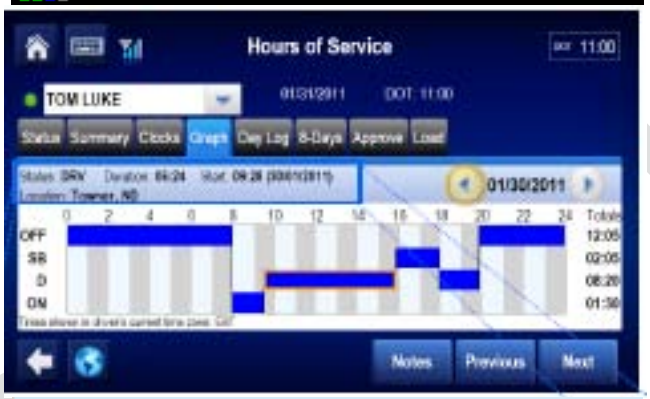
B. Recommendation: Create a standard ―EOBR Manual Inspection Review‖ layout which includes the following data elements as noted in FMCSA 395.16:

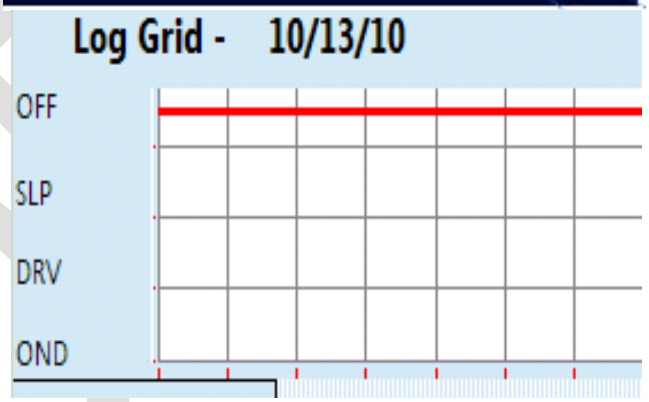
1. Driver name and EOBR login ID on all EOBR records associated with that driver including those in which the driver serves as co-driver
2. Driver‘s total hours of driving during each driving period (7 days prior) and the current duty day
3. Total hours on duty for the current duty day
4. Total miles or kilometers of driving during each driving period and the current duty day
5. Total hours on duty and driving time for the prior 7 AND 8 consecutive day period, including the current duty day
6. The sequence of duty status for each day and the time of day and location description for each change of duty status, for each driver being inspected
7. EOBR Serial Number or other identification and identification numbers of the vehicles operated that day
8. Remarks including fueling, waypoints, loading and unloading times, unusual situations, or other violations
9. Driver override of an automated duty status change to driving if using the vehicle for personal conveyance or yard movement

Define standard formats for three distinct types of EOBR output (one would be sufficient):

1. Graphical display – should display a graphical grid representation of all data elements on a single screen or a summary screen with easy to access drill down screens to see applicable detail. Examples are shown below:







2. Text display – should display all data elements required in a consistent flow and manner within EOBR screen/screens – One summary and detail available for each day. Sample format noted below:

Driver name: USDOT- EOBR EOBR login ID: EOBR Serial Number: Vehicles Operated:
Driving Hours Total (current day):
Hours On Duty (current duty day):
Miles Driving (current day):
Hours On Duty (prior 7):
Hours Driving (prior 7):
Hours On Duty (prior 8):
Hours Driving (prior 8):
Remarks:
Duty Status Detail: DRILL DOWN – ONE SCREEN WITH SCROLLING TO SHOW: Sequence of duty status for each day and the time of day and location description for each change of duty status, for each driver using the EOBR; include within the duty status changes any overrides, annotations and/or remarks

3. Print out – should print a graphical grid representation or text description of data elements noted above.
    - Displays can be fix-mounted, untethered or tethered but removable from cab. This will allow for flexibility to ensure reliability and allow for optimal mounting configurations for driver's convenience and safety.

C. Subcommittee comments:

1. Qualcomm: Agree with recommendation and additionally note the following: Any printouts for the past 7 seven days may have been produced from other EOBRs or AOBRDs (if driver operated other vehicles) and from EOBR support system (for log records from 395.15 devices or paper rods entered into the system). It is recommended that no special printing requirements be imposed to verify authenticity of such printouts as proof of actually being produced from EOBRs, AOBRDs, or EOBR host system printers. Rather, printouts should be reviewed with the same scrutiny as applied to paper RODS.
2. XATA: Similar comment on printouts from other participant comments that qualification of printout source should be identified to verify they were generated from a host system that supplies the support for internal DOT office and or back office support system as identified in the regulation.
3. Continental: Displays might vary in size, readability and handling that will result in the impossibility for enforcement to conduct a manual inspection. It is recommended that a standard unique format be required in printed form, similar to the one currently used in paper RODS. Printers are a proven reliable, cost effective solution used by several suppliers in similar applications in many countries.
4. PeopleNet, DriverTech and JJ Keller support the recommendation above which allows for printed format and/or display formats.

5. *Law enforcement does not want to be responsible for removing a device from a vehicle. At the same time, law enforcement should not have to climb into a vehicle to inspect the display.*
6. *Law enforcement would rather see a grid, than a text statement of hours because it is easier to view patterns, which is what officers are trained for to look for homeland security and drug concerns.*
    a. *Print out is ideal so that they could look back to regulations if necessary.*
7. *Must balance motor carrier cost consideration against need for backup manual inspection mechanism.*
    a. *For many small business carriers, viewing display or printing will not be the backup view, but will be the primary form of inspection.*
8. *Some law enforcement officers do not have computers, but there are millions of trucks that would have to install printers.*
9. *There is disagreement regarding whether printers in vehicles are cost effective.*
10. *If the movement is to electronic data transfer, should think about requiring printing to fill a temporary gap. However, currently there are very few law enforcement inspectors that have connectivity for wireless data transfer.*
11. *Data could be sent to a centralized facility via fax for review. But central inspection review would not necessarily be able to tell a HOS violation as well as a roadside inspector.*
12. *Law enforcement study and EOBR manufacturer studies have been done to assess current technology availability.*
13. *Options (flesh out details in matrix including costs and benefits):*
    a. *"Or" approach: screen display with a graph, screen display plus a printout, or text display.*
        i. *Pros: flexibility for carrier, EOBR manufacturer.*
        ii. *Cons: text display (w/o printout) is more difficult to read, may have to climb into vehicle.*
    b. *Require printer for all CMVs with EOBR systems.*
        i. *Pros: continuity for law enforcement.*
        ii. *Cons: additional layers of cost (initial printer cost, ongoing paper, maintenance), security issue (is the printout valid? Does law enforcement have to watch being printed out?).*
            i. *Could devices that are already out there be retrofitted with a printer? Not immediately clear.*
            ii. *Mobile display devices – potential complexity involved in connecting to printer.*
    c. *Just require single graphical display:*
        i. *Pros: Simpler than requiring printer.*
        ii. *Cons: Law enforcement would have to climb into cab.*
    d. *Provide printers to law enforcement.*
14. *Integral synchronization to ECM must be indicated on physical display.*

XV. Personal Conveyance and Yard Moves

A. Issue: Clarification is needed for the definition of yard moves and how such events are to be recorded as 395.16 has the following inconsistent requirements in this area:
   1. Personal conveyance and yard move events must be displayed . . . 395.15 (n) EOBR display requirements. (10) Driver‘s override of an automated duty status change to driving if using the vehicle for personal conveyance or for yard movement.
   2. Personal conveyance may be entered as an annotation prior to driving . . . 395.16 (d) Duty status defaults. (1) An EOBR must automatically record driving time. If the CMV is being used as a personal conveyance, the driver must affirmatively enter an annotation before the CMV begins to move.
   3. Yard moves may not be entered as an annotation to driving . . . 395.16 (h) Review of information by driver. (3) The driver may annotate only nondriving- status periods and the use of a CMV as a personal conveyance as described in paragraph (d)(1) of this section.

B. Recommendation: It is recommended that yard moves should be explicitly defined in 395.2 Definitions, and requirements for recording yard moves should be specified in 395.8 Drivers Record of Duty Status as well as in 395.16.
   1. It is also recommended that the yard move recording requirements should be consistent for paper RODS and EOBRs to avoid any disincentives for and/or confusion with EOBR use. Drivers using EOBRs should not be subject to different HOS recording rules for personal conveyance and yard moves. The consistency issue remains with the EOBR mandate as drivers will still continue to use paper RODS when performing work away from the vehicle and when EOBRs fail or are not available in the truck being used.
   2. In the absence of this definition, EOBRs should:
      a. Allow for personal conveyance as an override/annotation to driving.
      b. Allow for a reasonable EOBR movement tolerance to allow for yard moves.

C. Subcommittee comments:
   1. DriverTech: We agree completely with the sub-committee recommendation on Issue 15 with comment on 1 and 2 above.
      a. Allowance for personal conveyance may be accomplished with the addition of a line 5 on the daily log.
      b. It is our experience today that a small amount of distance is needed for very short yard moves and would benefit all parties to allow for this.
   2. Qualcomm: Agree with recommendation and additionally note the following:
      a. If HOS rules allow drivers and carriers to gain advantage in application of those rules by using paper RODS rather than EOBRs, than the following behaviors could be expected:
         i. EOBR voluntary adoption may be deterred. Over the past 18 months, we have seen a rapid increase in EOBR system adoption based in part on the launch of CSA and this momentum could be substantially reduced.
         ii. Drivers working in the yard away from their vehicle may not log on to the EOBR device and record such work as on-duty

not driving and any off-duty breaks on paper RODS. They may not log on until they actually leave the yard. They may also immediately log off from the EOBR when arriving on private property as they pursue work activities away from the vehicle and subsequently go off-duty – again recording such time on paper RODS. These drivers are subject to additional processes to ensure that paper RODS for on duty time get properly recorded as annotations to EOBR recorded off-duty time. Any movement of the vehicle while the driver is not logged on will be recorded as unassigned driving time suggesting that maintenance or yard personnel were operating the vehicle.

iii. Drivers may experience a higher failure rate with sensors or EOBR devices that require them to use paper RODS.

iv. Carriers may assign EOBR IDs to maintenance and yard personnel with a policy that such IDs are not to be disclosed to drivers.

b. The Committee should seek input of safety managers from carriers with proven safety records to gain an understanding of what parameters could be effectively applied in EOBR measures of vehicle movement relative to HOS event recording.

3. XATA: We feel that further conditions for movement should be identified and that identification of a conveyance should be displayed to be in conjunction with the fact that the Event Status Code is identified as "PC" but, no specifications for display exist only file transfer.
4. *Yard moves today – fleets can set a threshold on their EOBRs. Under strict interpretation of 395.16, that goes away. Once wheels start moving, it is recorded as driving.*
5. *Should not be treated as annotation, but actual changes in duty status.*
6. *Personal conveyance should be recorded, but Appendix A does not indicate how to display that.*
7. *Current systems do have indicator for personal conveyance – counted as off duty hours but with remarks/notation for personal conveyance. Yard moves? There should be a tolerance for flexibility.*
8. *Consider situation where in very large facility, there is a significant amount of yard movements (perhaps multiple miles).*
9. *Current rule does not address how to count yard moves.*
10. *If regulation micro-manages yard moves, carriers may be reluctant to voluntarily adopt EOBR systems.*
11. *There are inconsistencies across fleets re: treatment of yard moves.*
12. *Minor move of comfort at a facility could disrupt a drivers rest period – need flexibility to not be counted as off duty for those situations.*
13. *If there's a practical way to recommend EOBRs should treat these incidental moves, voluntary adoption would not be discouraged.*
14. *However, also must consider how to ensure drivers do not take advantage of such flexibility for incidental moves, e.g., allow only a 1 or 2 mile incidental move that would not change duty status.*

15. *Personal conveyances should be addressed with different resolution than yard moves.*
    a. *Need definitions of personal conveyance and yard move (currently carriers treat these issues differently):*
    b. *Personal conveyance: Suggested that if driver is on 10 hour rest period, 1 hour personal conveyance allowance; if driver is on 34 hour rest period, 2 hour personal conveyance allowance.*
    c. *Yard move:*
16. *A lot of layovers occur while driver is under load (laden).*
17. *How could the Agency draw the line between personal conveyance while under load, and extending on-duty driving hours?*
18. *Practically, there should be a mileage radius and timeframe limit.*
19. *Law enforcement has concerns about being able to tell whether someone is actually on personal conveyance (going home), or is just going to pick up another load.*
20. *Current 395.16 requires personal conveyance to be indicated, but it would be up to the inspector whether that noted time period was actually used for personal conveyance. EOBR providers can work with rules to indicate precisely personal conveyance and yard moves, but they need precise definitions of personal conveyance and yard moves.*
21. *Subcommittee subgroup should work between now and August 1-2 to develop recommended definitions for the subcommittee to discuss.*
22. *Recommendation: Appendix A should have "PC" as an Event Status Code, instead of personal conveyance just being indicated by an annotation.*
    a. *From carrier standpoint, this would be cleaner, instead of finding annotations and having to determine what it means.*
23.

XVI. Timeline to EOBR Compliance Date

A. Issue: Implementation of 395.16 or other form of EOBR technical/performance specifications is an urgent matter but must be done with proper diligence and must allow time for vendors to properly design, test and certify systems.

B. Background: EOBR software updates typically take 18 months to implement due to the sophistication of the systems and the required accuracy of the information for the users. In general, EOBR systems require the following from the point of rule clarification:
    1. 4-6 months for development
    2. 4-6 months for software quality assurance testing
    3. 4-6 months for external certification/validation and deployment across back office systems and to trucks (wireless updates or manually downloading to each unit)
    4. 2 months for training for drivers in the change as well as enforcement
    5. TOTAL = 14-20 months

C. Recommendation: Allow at least 12 months after requirements are finalized to enable EOBR providers to have adequate time to properly develop, test, certify, and deploy the new system capabilities. The revised compliance date should also allow adequate

time for the enforcement system to be fully tested with national deployment and training to be fully operational by the compliance date.

D. Subcommittee comments:
    1. Qualcomm: The expected implementation of an enforcement portal system by FMCSA and/or other enforcement agencies to support log downloads via telematics application services will add a schedule dependency for testing. Following availability of this/these portal(s), it is recommended that at least 6 to 8 months be allowed for EOBR provider testing, self-certification, and deployment of 395.16 EOBR systems providing log downloads to these portals.