Qualcomm Comments RE: MCSAC_FMCSA 395.16 (subcommittee edits)

Page 1

- (a)(1) Comment: Not sure why truck manufacture date is used as this may be a disincentive to buy new trucks in order to keep using and reinstalling 395.15 systems.
  Recommendation: The criteria should be based on when the system is installed.
  Revise to – "As of the compliance date, any new installation of electronic systems for hours of services compliance recording and reporting must be 395.16 certified. Previously installed 395.15 certified systems may continue to be used and maintained on the CMV on which they are installed for as long as that vehicle is kept in service by the carrier."

  (b)(1) Comment: NIST SP 800-122 provides guidelines about protecting PII.
  Recommendation: Requirements of 395.16 that address PII protection should reference NIST SP 800-122 or other guidance. Delete reference to "password" as this is part of a security control and is not identifying information.

Page 2

- (d)(3) Comment: This is redundant with requirement (o)(3).
  Recommendation: Delete (d)(3) and expand requirement for self-test to define what must be recorded. – see page 7 comments.

Page 3

- (f)(2) Comment: Requirement to identify "nearest" city, town, or village implies an algorithm based on map straight line, truck routing distance, any route distance, nearest along planned route, or other method – i.e., this may not be consistent unless a standard algorithm is defined.
  Recommendation: revise to – "identify city, town, or village as the location or relative proximity of distance and direction to an identifiable location."

- (f)(3) Comment: Requirement does not specifically define location data to be recorded.
  Recommendation: Add – "location data to be recorded includes event latitude, event longitude, place name, and place distance miles and direction as specified in Appendix A Table 2."

- (f)(4) Comment: Again the requirement does not specifically define location data to be recorded.
  Recommendation: Add – "location data to be recorded includes event latitude, event longitude, place name, and place distance miles and direction as specified in Appendix A Table 2."

- (f)(4) Comment: Again the requirement is to identify "nearest" city, town, or village implies an algorithm which may not be consistent among systems.
  Recommendation: revise to – "identify city, town, or village as the location or relative proximity of distance and direction to an identifiable location."

Page 4

- (i)(5) Comment: This requirement is quite confusing when driver log data is from multiple sources – i.e., 395.16 EOBRs, 395.15 AOBRDs, EOBR host system portal entries by the driver for non-driving on-duty work, EOBR host system entries by carrier management for driver RODS (paper logs) and for edits of log corrections, and paper log images and paper records archives. It is also ambiguous what the driver must provide for inspection when records for that driver are recorded or documented by multiple sources.
  Additionally, requirements for electronic data transfer capabilities and processes should be addressed in a separate paragraph of the rule – suggest adding of a "paragraph (r)" – see notes for page 9.
  All references in this section to USB, 802.11, and CMRS should be removed.
  Recommendation: Separate the requirements for how information is stored, what is acceptable for roadside, and the allowed methods for data transfer. Revise (i)(5) to replace all current text with the following:
  "Drivers must have in their possession a record of duty status for the current day and immediate access to records of duty status for the prior 7 days.
  (i) Information for roadside inspection of current day and prior 7 days provided may include EOBR display or printouts, printed records from the EOBR support system or other driver logging system, paper logs, ~~fax~~ report of driver's current and prior work days via fax or email from the EOBR support system, electronic file transfer of the driver's current and prior work days from the EOBR support system, or any combination to provide a complete accounting of current day and prior 7 days.
  (ii) The EOBR support system may include records from sources other than the EOBR such as AOBRD records and entries of paper logs and log corrections into the support system. Such records must accurately reflect the data as recorded by the other source.~~meet the information recording requirements as defined in paragraphs (b) and (c).~~ Additionally, those records from non-EOBR sources ~~will –~~must be so identified by record type as defined in Appendix A.
  (iii) Drivers may initiate a fax or email of a report from the EOBR support system to the inspection site or to a remote inspection support site for current and prior days records of duty service to the extent that such information is available on the support system. The fax report must provide the information as identified in paragraph (n). If the driver is found to be in violation, the driver is required to re-produce paper records for entire prior work period if the fax report or other displays or printouts are not available at the inspection site.
  (iv) Drivers may initiate an electronic file transfer of current and prior 7 days records of duty status to the extent that such information is available on the support system. Such file

transfer will be accomplished by the methods described in paragraph (r) and technical requirements as specified in Appendix A Section 2. If the inspection site is not able to process an electronic file transfer, then the driver will provide information as defined above."

Page 5

- (i)(6) Comment: Reference is made to data transfer via portable storage media such as CD-ROM or USB. Would suggest that other forms of electronic data transfer be considered as support systems may apply a computing model with other data transfer capabilities.
  Recommendation: Revise to – "The system must produce a copy of files for electronic file transfer via the methods described in Appendix A Section 2 or via a portable storage media (e.g., CD–RW or USB external storage device) upon request of authorized safety assurance officials."

- (k)(1) and (k)(2) Comment: This is a direct overlap of the recommendations made for (i)(5) above.
  Recommendation: Delete (k).
  Instead of creating new paragraph (r), an option is to apply recommendations for paragraph (r) as replacement for paragraph (k) – see comments for page 9.

- (k)(3) Comment: This section deals with sensor failures but needs more specificity including definition of failures and corresponding actions and information recording requirements. The sensor failure matrix identified as a recommendation in Appendix A Table 3 should be referenced.
  Recommendation: Delete (k)(3)(iv) and ~~R~~revise (k)(i)(ii)(iii) to – "If there is a failure with an EOBR system, component, or vehicle sensor, there are actions required for the driver, carrier, and EOBR system.
  Specific failures and action requirements are specified in Appendix A Table 3.
  (i) For failures that result in the EOBR becoming inoperable, the driver is required to prepare paper logs for the current day and continuing to do so until the EOBR is returned to normal service. A driver may also need to prepare paper logs for prior days subject to records availability as specified in (i)(5).
  (ii) For failures that result in limited system or sensor input, the driver is required to enter additional data at each change of duty status. The additional data requirements per sensor failure are specified in Appendix A Table 3.
  (iii) Drivers are required to report any EOBR system, component or vehicle sensor failure to the carrier as early as practical and not longer than 2 days after the failure occurred.
  (iv) Carriers are required to repair the failure and return the EOBR to normal service as early as practical and not longer than 14 days after the failure occurred."

Page 6

- (n) Comment: The idea of standardized screens should not be addressed in the rule but rather through recommended practices of CVSA and TMC to reflect the needs of the key stakeholders.
  Recommendation: The TMC EOBR Task Force is planning to address a recommendation on suggested EOBR display formats for enforcement use and then have CVSA finalize requirements. The end standard is expected to be published by TMC and endorsed by CVSA and included in CVSA training programs.

- (n)(9) Comment: The "Remarks" data field is a useful place to describe record annotations.
  Recommendation: Expand requirement for remarks – "Remarks also to include description or reason for an annotation."

Page 7

- (o)(3) Comment: The requirement is only to record that a self-test was done with pass-fail indicator to be recorded. The self-test, if failures found, should trigger sensor failue actions.
  Recommendation: Expand self-test recording requirement to include – "If any EOBR component or sensor is determined to in a failed or below acceptable performance status, the self-test will trigger recording of such failures consistent with the requirements of Appendix A Table 3."

- (o)(5) Comment: Include caveat about information being available similar to requirement for (o)(4).
  Recommendation: Revise to include - . . . must "to the extent the information is available," provide . . .

Page 8

- (o)(11) Comment: The requirement suggests that the details of all annotations are provided on the EOBR display. This is problematic due to the amount detail possible as well as due to many annotations being made on the EOBR support system.
  Recommendation: Suggest the following revision – . . . "EOBR display or printout must provide the remarks that describe an annotation to the extent that such information is available. The EOBR support system must identify annotations made to all records, the date and time the annotations were made, the remarks that describe the reason for the annotation, and the identity of the person making them."

- (o)(13) Comment: The need for "security" is identified but there is not a specific standard reference. It is important that security is addressed covering all aspects of EOBR systems as well as covering the technical, operational, and management focus on security. It is also important that security requirements be based on widely accepted standards from

established standards organization(s). Details of EOBR device level security and tamper proofing should be left to the EOBR manufacturers as different computing platforms may have different requirements.
Recommendation: Suggest the following – "EOBR service providers and carriers in managing EOBR system use must apply security measures consistent with those as defined in FIPS Publication 200 – Minimum Security Requirements for Federal Information and Information systems, and security controls consistent with NIST SP 800-53 – Recommended Security Controls for Federal Information Systems. EOBR systems and EOBR devices must provide technical features to enable applicable minimum security requirements and security controls."

Page 9

- (r) ***NEW*** Comment: Suggestion to add a new paragraph to define requirements for electronic data transfer capabilities. **SPECIFIC REQUIREMENTS SUBJECT TO A MORE DETAILED DESIGN TO BE DEFINED BY A JOINT WORKING SESSION BETWEEN SELECTED EOBR PROVIDERS AND SELECTED FMCSA IT STAFF**.
- Recommendation: Preliminary suggested text – "EOBR support systems must be able to provide driver records of duty service for current day and prior 7 days via an electronic data transfer to the extent that such records are available on the support system. The approach to providing driver records via electronic data transfer are specified in Appendix A Section 2 and subject to the following requirements:
  (i) The EOBR support system service provider, or the carrier if acting as its own service provider, must obtain from FMCSA an electronic certificate for authentication for data transfers via web services using transport layer security mechanisms as described in Appendix A Section 2. FMCSA will manage a registry of authorized service providers for data transfer and will issue authentication certificates based on completed application, proof of manufacturer certification of EOBR conformity to 395.16 requirements, satisfactory test of electronic data transfer capabilities, and agreement to terms and conditions by the service provider. FMCSA retains the right to revoke the authentication certificate if the service provider fails to meet the terms and conditions or fails to comply with requirements for electronic data transfers.
  (ii) Security of the electronic file transfers must apply transport layer security (TLS) as defined in Internet Engineering Task Force (IETF) RFC 5246, and service providers will maintain security controls consistent with NIST SP 800-85 Web Services Security Guidelines.
  (iii) Electronic file transfers will utilize a flat file approach with data records coded in an XML schema as defined in Appendix A Section 2."