MCSAC Task 11-04 Technical Workgroup
October 24 – 25, 2011

I. Security (data protection, encryption, access control, confirmation of successful file transaction)

A. Use NIST SP 800-53 Revision 3, Recommended Security Controls for Federal Information Systems and Organizations, as a general guideline
   1. Agency could consider incorporating specific sections by reference
   2. References ISO 27001
   3. FIPS 140-2 for encryption

B. Access Control
   1. Device must be uniquely identified.
      a. Government-issued 2 digit alpha vendor identifier
      b. 6-12 digit device unique identifier managed by vendor
      c. Allowance to use existing serial number with 2-digit vendor identifier
   2. Users must be uniquely identified for EOBR access (drivers and carriers).
      a. Driver ID # in flat file should be associated with last 4 digits of driver's operator's license # (or portion) for verification by enforcement that the license he holds relates to the information he has received.
   3. The EOBR system shall implement, manage, and maintain an access control system that authorizes user access levels.
   4. All subsystems that transmit, receive, or store data on behalf of the EOBR system shall maintain data access controls.
   5. All EOBR system users (drivers and other motor carrier personnel) shall be registered and authorized by the access control system.
   6. The EOBR system shall control access to data based on access rules and the assignment of user roles.
   7. The EOBR shall restrict access to those parts of the system for which a user is not authorized.
   8. The EOBR shall detect and alert attempts to access parts of the EOBR system by unauthorized users.
   9. Authorized Motor Carrier/Service Provider users shall be granted access to EOBR information pertaining to their operations.
   10. Authorized Commercial Motor Vehicle Driver users shall be granted access to EOBR application and support systems information pertaining to their operations.
   11. The EOBR application and support systems shall allow access to EOBR data with or without the unique identification data elements intact, depending on the user access privileges.
   12. The EOBR application and support systems shall include time and date stamp and source for all data events. [Note: use similar language to the vacated regulation.]

C. Data Protection
   1. Encryption of PII data at rest and in transit (if PII is determined)

a. NIST SP 800-122, Guide to Protecting the Confidentiality of PII
b. Driver ID # in flat file should be associated with last 4 digits of driver's operator's license # (or portion) for verification by enforcement that the license he holds relates to the information he has received.

2. The EOBR shall implement measures to protect data privacy and maintain system security:
    a. Data at rest and in transit must be protected from unauthorized access, use, modification (including corruption), and destruction and denial of service attack.
    b. The EOBR shall protect EOBR data collected, stored, disseminated, or transmitted from inadvertent alteration, spoofing, tampering, and other deliberate corruption.
    c. All subsystems which transmit, receive or store EOBR data shall also handle the data in accordance with federal regulations including the Drivers Privacy Protection Act.
    d. The EOBR and application support systems shall implement methods for system disaster recovery and rebuild.
    e. The EOBR and application support systems shall provide auditing capability.
    f. The EOBR shall provide a self check to ensure accuracy of data.
    g. The EOBR shall use industry best practices for the formats of files transmitted to safety and law enforcement officials.
    h. The EOBR device must allow only one-way wired or wireless transfer of data to data terminals used by safety enforcement officials.
    i. The EOBR device and support system shall be tamper resistant to address moderate and high risk as described in the certification and accreditation process.

II. Peer-to-Peer (USB, barcoding, alternative electronic solutions)

A. Peer to peer (e.g., USB, Bluetooth) is a possible solution that could work with other solutions. All technologies will have different costs and advantages/disadvantages.
B. An alternative to telematics, such as peer to peer, may or may not be desirable.
C. Refer to risk assessment on FMCSA website for cons for each technology.
D. 2D Barcodes (e.g., QRC)
    1. Pros
        a. Built for file transfer without database connection
        b. Compatible with E-RODs flat-file analysis
        c. High reliability of error detection
    2. Cons
        a. Smudging
        b. Scanning
        c. Character limit
        d. Screen clarity/resolution
        e. Glare
        f. Significant cost to enforcement and industry to implement

g. Power usage
h. Unproven technology in EOBR usage

3. Ask manufacturers to submit comments to MCSAC on viability of this option?

E. USB (mass storage device, not cable)
1. Pros
a. Many states allow
b. Reliable
c. Immediate
d. Cost-effective
e. Universally available and off the shelf hardware
f. [Note: See "Zonar's Response to Qualcomm's Risk Assessment"]
2. Cons
a. Qualcomm Product Security Initiative risk assessment of USB
b. Inconsistent usage among states (e.g., not allowed by some states)
c. USB may become obsolete technology
d. Security threat (e.g., malware)
e. Older legacy systems use USB low-speed interfaces. New USB devices authenticate at high-speed and negotiate down to lower speed, so the cable length may not work. Some older devices will not work under a mandate for USB peer to peer.
3. Limiting the format the data files could take (e.g., text file) would minimize potential for abuse.

F. SD Card
1. Pros
a. Reliable
b. Immediate
c. Cost-effective
d. Universally available and off the shelf hardware
2. Cons
a. Inconsistent usage among states
b. Security threat (e.g., malware)
c. SD is not widely used or accepted field device and would require engineering change and additional cost
d. Limited lifecycle

G. Bluetooth
1. Pros
a. Authentication is possible in specific instances
b. NIST 800-121
c. Cost-effective
d. Communication can be secured and encrypted
e. Universally available and off the shelf hardware
f. Either work with or without integrated Bluetooth in EOBR
i. Requires device drivers for USB. Note: this entails additional cost.
g. Distance limited – security feature that prevents eavesdropping, etc.

2. Cons
    a. Difficult to get a connection
    b. Lack of authentication. Note: no consensus on this point
    c. Malware risk
    d. Pairing with display screens
    e. Law enforcement may not have availability

H. 802.11 (WiFi)
1. Pros
    a. Standard protocols for encryption
    b. NIST 800-48 Revision 1, Guide to Securing Legacy IEEE 802.11 Wireless Network
2. Cons
    a. Management of SSIDs (time and effort)
    b. Not easily used
    c. No common usage for peer to peer environment
    d. Scored lowest for usability in CVSA survey
3. Reference comments from Larry Steinbecker
    a. Higher cost for Wifi hardware than for other means of communication. Need technical resources in addition to hardware.

I. Dedicated short-range communication (DSRC) using transponders (5.9 GHz)
1. Pros
    a. Multiple uses, valuable
    b. May be proven to have robust security model
    c. Agency has set aside bandwidth for this type of communication
    d. Relatively secure data (security would have to be perfect)
2. Cons
    a. Cost
    b. Not being used for HOS applications now; not ready now
    c. Not continental
3. USDOT large safety pilot – evaluate the effectiveness. NHTSA will decide on DSRC mandate based on this.
4. Agency acknowledges other efforts in this area and should place industry on notice that may be moving toward requirement related to DSRC (NHTSA has already moved in this direction).
5. Recommend pilot testing; proof of concept

III. Telematics (web services, credentialing, interface to transmit files, portability of electronic data, streamlining driver data, system response)

A. See "Framework for Telematics Application Services Approach" for discussion on Telematics

B. Need to consider data security throughout process
1. But this may not be a security issue, just a method for data transfer
2. Look at NIST SP 800-95, Guide to Secure Web Services, REST

C. Roadside Compliance Request (RCRs) number
1. Reason for RCR: keep it simple for the enforcement officer
2. RCR could just be for a particular roadside instance

3. When using RCRs, exclude 1s, Is, Ls, 0s, and Os
    a. Make first 2 digits alphas

D. Might only be needed 10% of roadside instances, so need to keep it simple or officers will not use it
E. Driver request for file indicates certification
F. Consider not putting this in rule due to technical content –put it in an Appendix or technical bulletin that is referenced in rule? Need a good change management process.
    1. FMCSA needs to discuss this. An Appendix is part of a regulation. This may be a likely solution.

IV. File Data (authentication, certification of files, digital signatures, ownership of data)

A. Refer to "Framework for Telematics Application Services Approach" for basics/definitions for encryption, authentication
    1. Data at rest addressed by data protection requirements
    2. In the use of Representational State Transfer (REST) web services, the data format should be JavaScript Object Notation (JSON)
B. Examine feasibility of three possible methods of authentication: (1) token-based, (2) telematic, and (3) username/password provision on every device

V. Uniformity of Display

A. Committee recommends uniformity of display (e.g., red/yellow/green screen) that may be useful at the roadside. Some data transfer will still be necessary. See Attachment A for details.
    1. From outside of cab, enable enforcement official to see driver's current available driving hours;
    2. Standardize listing of exceptions relative to yellow or red status to simplify training;
    3. Display driver's name;
    4. Roadside inspection button to display exceptions and any other requirements.
B. Option of calling number for service provider to verify device (i.e., an enforcement request number). List phone number separately on the cab card (i.e., instruction card for EOBR device) rather than on screen.
    1. Consider potential cost of this option
C. Training for enforcement officers should be minimal
D. Requirements for minimum display screen size – should be large enough for officer to see over driver's shoulder
    1. 7-inch (diagonal) minimum if permanently mounted
    2. If smaller, but not less than 2.5 inches, screen should be detachable, removable, or tethered
    3. Devices (i.e., 395.15 devices) that do not meet this criteria should be grandfathered
E. Requirements for minimum text size
F. Graph grids
    1. Default screen with go/no go, available hours
    2. Screen with full compilation of compliance with HOS requirements

3. Details in a graph
    a. Standardization of graph grid display is not necessary. Standardization of basic elements.
4. Export via an authorized data transfer mode to enforcement official

VI. Third-party Certification of EOBR Providers

A. Third-party certification is necessary.
B. Certification process is only about HOS application; it does not encompass the entire operating device. It is not appropriate to build certification process beyond HOS.
    1. Consensus not reached on this point. See "Electronic On-Board Recorders Guiding Principles" presentation.
C. Certification based on an established set of certification criteria that are based in regulation.
D. FMCSA shall promulgate regulations that establish parameters and performance standards for industry manufacturers. Entities who want to enter into the business enter in to MOUs with FMSCA stating that they will commit to follow those parameters. Every provider would need to go through the process. Agency contracts with third party to do certifying. Auditing process consists of determining whether manufacturer is complying with MOU. Third party makes periodic visits to carriers on site. Also use law enforcement as a check on the certification process – would trigger additional on-site visits. Cost relationship is between manufacturer and third-party so Agency is not involved with funding.
    1. Needs to be iterative process to comply with changing standards
    2. This option could be cost-prohibitive. Any change in regulation or equipment updates may require re-certification.
        a. Certification should allow for partial re-certification based on new regulations or equipment upgrades. Full certification test should not be required for equipment upgrade.
    3. Suppliers shall go to one of independent labs as qualified by FMCSA in order to become certified. Which lab does the testing depends on FMCSA's qualification of that lab. This would be most economical for suppliers and customers.
E. Testing criteria would be developed based on regulation and nothing more.
F. The whole process would be multi-step and would include long lead time.
G. Need to recognize that EOBR is an application that is overlaid on a large existing system.
H. FMCSA should consider setting funding aside to get the certification process up and running.
I. EOBR vendors/suppliers discussed previous experiences. Certification could be estimated, based on experience with OEMs, to last from 60-180 days.

VII. Other

A. If a driver is working for multiple carriers, there is concern about transfer/sharing of records
B. Interchangeability of devices between 395.15 and 395.16

Attachment A: Option for Uniformity of Display

Green status means the following:

Green

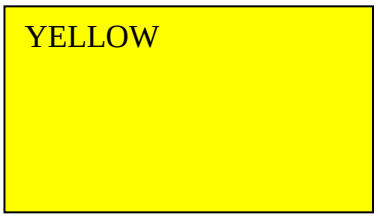
- No HOS violations
- All driver time fully accounted for
- All vehicle movement fully accounted for
- No record annotations (last 8 days)
- No sensor failures (last 8 days)
- No other data abnormalities

Green status display:

- "Diagnostics GREEN" and remaining driving time today: HH:MM

Yellow status means the following:

Yellow



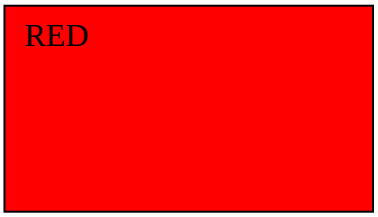
- Data exceptions to be reviewed / explained

Yellow status display:

- "Review Exceptions" and remaining driving time available today: HH:MM
- Gaps in driver log records – (data rules to be specified – e.g., 2 days not accounted for in electronic records)
- Gaps in vehicle movement records (data rules to be specified, e.g., unassigned driving or unexplained vehicle miles without associated driver's driving duty status record)
- Any record annotations in last 8 days (show current record and original version with explanation remarks and who made change)
- Sensor failures (list of sensor failures and time/duration of failure)
- Other data abnormalities (data rules to be specified)
- Daily duty status (graphs and other available displays) and recap of total hours

Red status means the following:

Red



- Suspected violations

Red status display:

- "Suspected Violations" and HOS summary data suspected in violation
- Daily duty status records (e.g., grid graph)
- Data issues that indicate suspected tampering (data rules to be specified – e.g., data indicates significant change in location for driver and vehicle without driving record or co-driver)
- Excessive personal conveyance or yard moves (rules to be specified)

Appendix B: MCSAC Task 11-04 Technical Workgroup Members

- MCSAC Subcommittee Members
    - R.C. Powell, Virginia State Policy (Subcommittee Chairman)
    - Dave Parker, Great West Casualty (MCSAC Chairman)

- Non-MCSAC Subcommittee Members
    - Bill Bland, Rand McNally
    - Alex Capelle, Continental Corporation
    - Tom Cuthbertson, Xata Corp.
    - Amy Daley, J.J. Keller and Associates, Inc.
    - Chinpai Jong, Daimler Trucks North America
        - Surrogate: Fred Gneuchtel, Daimler FleetBoard
    - Dave Kraft, Qualcomm Enterprise Services
    - Jim Angel, PeopleNet
    - Robin Doherty, Verigo, Inc.
    - Carleton Watkins, inthinkc Technology Solutions, Inc.
    - Shaun Kildare, Advocates for Highway and Auto Safety

- FMCSA Members
    - Debbie Freund, FMCSA
    - Toccaro Young, FMCSA
    - Stephen Parker, FMCSA
    - Bunmi Ogunlade, FMCSA
    - Andrew Orndorff, FMCSA
    - Elizabeth Vargas, FMCSA
    - Larry Minor, FMCSA
    - Shannon Watson, FMCSA