Evaluation of Qualcomm’s

“Risk Analysis of USB Communication for EOBRs Rev. 1.4”

# Summary

Zonar’s technical team has reviewed the Qualcomm “Risk Analysis of USB Communication for EOBRs Rev 1.4 and are of the opinion that the issues raised do not create substantial risk.

In this document we evaluate each concern, present explanations why we believe the concern is insignificant, raise questions of Qualcomm’s existing use of USB, and finally conclude that modifying FMCSA’s final ruling regarding this feature is unnecessary.

# Analysis

Zonar is a pioneer in positively encouraging compliance with safety regulations in high liability businesses by making compliance simple, easy, and affordable (electronic vehicle inspection & reporting). The Zonar team of highly experienced professionals from the transportation industry, law enforcement and vehicle development has analyzed the ruling (49 CFR Part 395) as produced by FMCSA to come to the conclusion that at its core the fundamental requirements are:

1. A driver must have a complete record of his logs at all time (1)
2. Upon request a driver must provide this record to law enforcement (1) (2)

Among the various aspects of Part 395 there is no mention of exceptions to these fundamental elements; no exceptions based on weather, location, or radio data connectivity. In the event that network connectivity is not available the ability to write to a mass storage device (“USB Stick”, “JumpDrive™”, “ThumbDrive™”, etc) as presented in the ruling by FMCSA meets the needs of law enforcement without adding appreciable complexity, cost, or risk.

Qualcomm’s statement, “we see no practical reasons why FMCSA should allow transmitting electronic driving records via wired USB connections…” seems to indicate that there will never be an instance where law enforcement cannot receive a copy of the log via wireless mode, yet experience tells us that may frequently be the case. In fact the variability of terrain, weather and law enforcement IT systems make the potential unavailability of wireless transmission a reality. As a provider of compliance systems, Zonar believes these systems need to help provide compliance solutions to the fleets we serve and provide timely information to law enforcement when requested.

## Qualcomm Concern: Lack of Secure Authentication

“Lack of Secure Authentication. USB connection between two devices provides no way of verifying identities of either device.”

In our analysis we feel this is an antiquated philosophy that does not mesh with modern industry practices. All of today’s accepted protocols for secure transmission of sensitive information start with the assumption that the channel is insecure and un-authenticated (3).

“An example attack would be a third party (either a malicious driver or a competitor) connecting a personal laptop to the EOBR in order to retrieve driving records”

This could also be accomplished today by theft of a log book which is typically within easy reach of the driver’s seat. We question the value of a driver’s hours of service records to a third party, however unlike theft of a driver’s written logs, the theft of a digital copy would not place the vehicle out of service.

“Another example would be a malicious motor carrier equipping drivers with USB storage devices containing fake driving records or a malicious driver modifying driving records…At a traffic stop, a driver would connect…not the actual EOBR but a USB device containing these fake records”

Unfortunately we feel this statement is an indication of a lack of understanding of the regulation and can only be answered by citing 395.16 in its entirety. A law enforcement program designed to verify records to 395.16 would be able to easily identify inconsistencies in a driver record. It would be impossible to pre-generate a driver’s log that would be correct at the time of any random inspection. Previously some drivers have attempted to circumvent hours of service (HOS) regulation by maintaining two log books, however experienced and discerning officers are able to spot these discrepancies. Likewise, FMCSA will still require supporting documents to verify on-duty not driving time and all records must accurately match these supporting documents.

“Given realistic budget and time constraints, we don’t envision a software authentication component as a feasible solution”

While Zonar believes that there is not a strict need for encryption or authentication of the file provided to law enforcement per 395.16 Appendix A, we feel the addition of encryption would not put undue stress on development budgets or timelines. Zonar can not speculate on any competitor’s abilities but remotely updating firmware and revoking/reissuing encryption keys should be a relatively simple process for any vendor in the space.

## Qualcomm Concern: Unauthorized Read/Write/Code Execution

“Unauthorized Read/Write/Code Execution. The most common ways of connecting devices via a USB connection do not provide sufficient protection against unauthorized data access on EOBR devises and requires additional security measures”

Any computer system today is under continuous attack, the vast majority of which come through network connections. The amount of access one can gain is directly defined by what is possible. Because a port exists does not mean that one can (or should) be allowed to do something malicious through that port. The responsibility of limiting access through ports should be the vendor’s, especially when said ports already exist on the product they intend to certify.

“The most common ways of connecting devices via a USB connection do not provide sufficient protection against unauthorized access and require additional security measures”

If this is a concern why are USB ports and devices a fundamental part of Qualcomm’s flagship offering in this area? (MCP-200) Based on Qualcomm’s statements they state the presence of USB ports on their device is an existing vulnerability and yet continue to offer those USB ports. We believe their statements and actions are contradictory and incongruent.

## Qualcomm Concern: Malware

“Malware. USB Malware is a highly likely attack vector which can infect or disable a large fraction of both EOBR devices and law enforcement computers”

While USB drives have (just as every other digital information technology) been victim to exploitation for various reasons, and there has been in the past some novel or unique USB based malicious exploitations, fundamentally USB connections are no more dangerous than the web browsers installed on virtually every PC.

In Qualcomm’s document they do not discuss how they plan to address the malware question on the device they wish to certify for EOBR, which is already equipped with a USB port.

“On many computing platforms, such code from a USB device may be executed without the user’s acknowledgment”

In January of 2011, Microsoft published a windows-update that removed the AutoRun/AutoPlay feature for all USB devices for all Windows versions permanently (4). This renders the device no more harmful than any other medium for data transfer.

“Given a large variety of computing platforms used in EOBR devices, QPSI considers malware to be a highly likely attack vector which can infect or disable a large fraction of both EOBR devices and law enforcement computers.”

This statement directly conflicts with generally accepted research showing that variety of computing platforms reduces the likelihood of attack due to the lack of financial incentive or wide enough impact to satisfy the effort (5). The industry refers to this as Security through Diversity, or to put it words most of us would understand: “don’t put all your eggs in one basket” (6). The variety of telematics solutions available should reduce the impact of any exploit to a specific vendor if one were to emerge.

## Physical Limitations of USB Connections

“Physical Limitations of USB Connections. USB 2.0 standard specifies the maximal length of a USB cable to be 16.4 ft (5 meters), which might be insufficient for most intended uses of a USB connection with EOBR devices”

Zonar does not disagree with Qualcomm’s statement regarding the standard but believe the issue does not exist based our understanding of the requirement in the ruling by FMCSA.

From 49 CFR 395 App. A §2.2:

‘Wired. EOBRs must be capable of transferring RODS using the “Universal Serial Bus Specification (Revision 2.0)” (incorporated by reference, see §395.18). Each EOBR device must implement a single USB compliant interface feature a Type A connector. The USB interface must implement the Mass Storage class (08h) for driverless operation.”

Zonar has interpreted this requirement devices are expected to present a Type-A connector (vs plug) as a number of existing telematics devices currently are equipped as such and be able to write the Appendix A specified “flat file” to a portable mass storage device. Our vision is that a law enforcement officer would provide a device for the driver to insert into the EOBR. The officer would be able to observe this operation. The driver then would return the portable storage device that was provided to him. The officer would then be able to evaluate the hours of service records in the safety and comfort of their own vehicle.

Based on the overwhelmingly positive reception of Zonar’s interpretation at the 2011 North American Inspectors Championship (NAIC 2011) hosted by FMCSA & the Commercial Vehicle Safety Alliance (CVSA) we feel this interpretation is the best embodiment of the spirit of the 49 CFR 395.16 USB requirements.

# Conclusion & Recommendations

Zonar believes that the existing ruling by the FMCSA provides a robust framework in which to develop systems that work well with existing technology and infrastructure. While some areas do require clarification, if done so in a timely fashion there should be no issue in deploying 395.16 compliant solutions by the implementation date.

Defining a system for distributing secret keys could be incorporated in the FMCSA systems that are to be installed on law enforcement computers for viewing record of duty status (RODS) files. Our recommendation if the FMCSA deems it necessary to incorporate encryption into the file format would be the use of AES-128 in counter (CTR) mode. (7)

Zonar has presented a defense of USB as proposed by the FMCSA as a viable local method for transfer of RODS data, Zonar also believes that whenever possible, the retrieval of RODS data remotely in the patrol vehicle is preferable, for both convenience and uniformity of experience, and the safety of the officer. When remote network connectivity is available, this should allow a faster inspection time, which would benefit all parties. In the absence of network connectivity USB functionality provides a preferable alternative to placing a vehicle out of service

In Summary:

1. The preferred method of RODS retrieval would be a central FMCSA managed system able to authenticate users and provide data from all telematics vendors. Such a system should store and distribute vendor specific encryption keys if the FMCSA were to adopt an encryption requirement.
2. A local transfer method is essential, such as the use of USB memory devices.
3. Law enforcement should not be required to enter a CMV nor know how to operate the various vendor devices that may be installed.
4. If FMCSA elects to use encryption of the file copied to a USB device to use AES-128 in CTR mode.

# Works Cited

1. *Drivers Declared Out of Service.* **Code of Federal Regulations Title 49.** 395.13, 2010.

2. *Inspection of motor vehicles and intermodal equipment in operation.* **Code of Federal Regulations Title 49.** 396.9, 2010.

3. **Dierks, Tim and Allen, Christopher.** The TLS Protocol. [Online] January 1999. [Cited: August 22, 2011.] http://tools.ietf.org/html/rfc2246. RFC2246.

4. **Microsoft.** Update to the AutoPlay functionality in Windows. *Microsoft Support.* [Online] June 29, 2011. [Cited: August 22, 2011.] http://support.microsoft.com/kb/971029.

5. **Miller, Charlie.** *The Legitimate Vulnerability Market: Inside the Secretive World of 0-day Exploit Sales.* [PDF] s.l. : Independent Security Evaluators, 2007. http://weis2007.econinfosec.org/papers/29.pdf.

6. *Security through Diversity: Leveraging Virtual Machine Technology.* **Williams, D., et al., et al.** 1, s.l. : IEEE Computer Society, 2009, Security & Privacy, Vol. 7, pp. 26-33.

7. *Advanced Encryption Standard.* **National Institute of Standards and Technology.** 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.