February 23, 2021

Dr. Sydney Vergis, Chief
Mobile Source Control Division
California Air Resources Board
1001 I Street
Sacramento, CA 95812

Dear Dr. Vergis:

The National Motor Freight Traffic Association, Inc. (NMFTA) provides the following comments on the *Draft Heavy-Duty Vehicle Inspection and Maintenance (HD I/M) Regulatory Concepts –December 2020* document at https://ww2.arb.ca.gov/sites/default/files/classic/msprog/hdim/meetings/20201217_draft_hdim_reg_concepts.pdf.

NMFTA is a nonprofit membership organization headquartered in Alexandria, Virginia, with a membership consisting of motor carriers operating in interstate, intrastate and foreign commerce. NMFTA's general mission is to promote, advance, and improve the welfare and interests of the motor carrier industry and the motor carriers operating in commerce, both domestically and/or internationally. Other parts of its mission are to research, analyze and distribute information and aggregate data that will be of benefit to the motor carrier industry in the conduct of transportation operations; facilitate education, conduct meetings and seminars, participate and promote its community in legislative matters, develop standards and classifications.

NMFTA feels the draft regulatory concepts document should include explicit cybersecurity requirements as a means to disallow introduction of a 'wide open' internet connection to the vehicular networks to which the Remote OBD (ROBD) devices will be connected. There are recent and significant instances where the mandatory use of Electronic Logging Devices (ELDs) without any cybersecurity requirements resulted in introducing significant risks to heavy vehicle systems. This is evidenced by the publication of the Federal Bureau of Investigation (FBI) Private Industry Notification (PIN) 20200721-001 on *Electronic Logging Device (ELD) Cybersecurity and Best Practices.* It describes an industry and academic study performed on a set of self-certified ELDs identifying a number of security vulnerabilities that could allow an attacker to steal and corrupt data, and in some cases inject commands into a vehicle's electronic control units (ECU) to cause the vehicle to respond in unexpected ways. We can say with confidence borne from the experience in studying ELD vulnerabilities and understanding the numerous risks any type of intrusion has on a vehicle, that the draft legislation should address protections to mitigate cybersecurity risks.

To that end, NMFTA offers the following feedback specific to the current CARB draft version of proposed regulatory concepts:

- VIII.(b)(6)(A)2."The ROBD system shall supply a Client-Side Secure Sockets Layer (SSL) Certificate. This certificate validates the authenticity of the client with an..."
    - We agree that CARB should include this requirement to protect device communication confidentiality because client- side certificates are more secure than passwords. There

should be supporting parts of the draft regulation that detail how to protect the client certificate private keys from disclosure as well as how to update revoked or expired client certificates.

- (VIII.(b)(6)(A)3.) requires server certificates. Like the client side, the regulations should include details on how to update the trust stores on the ROBD devices such that revoked or expired server certificates can be updated.
- VIII.(c)(6)(C)1."The data shall not be altered or tampered with during or prior to electronically submitting to the CARB electronic reporting system approved by the Executive Officer."
    - We believe this is a key location to anchor cybersecurity requirements. To achieve an ROBD that will submit the data without alteration or tampering during or prior to the submission will in turn require that the firmware of the ROBD has not been compromised. In turn, this will require assurances that the firmware has not been exploited; hence requiring a suite of comprehensive security requirements.
- VIII.(c)(6)(D)"Once an internet connection is available, the ROBD system shall submit the encrypted data files to the CARB electronic reporting system approved by the Executive Officer. The internet connection can be satellite, cellular network, Wi-Fi, hot spot, etc."
    - This part of the draft regulatory concepts indicates that the ROBD devices are to be designed to connected to a multitude of wireless internet service providers. This should come with device network security requirements and further motivate the need for a suite of comprehensive security requirements,

NMFTA believes there should be reference to a comprehensive set of security requirements that all ROBD devices must satisfy. NMFTA has produced such a set of requirements for telematics systems which could also apply to ROBDs as well; they can be found at https://github.com/nmfta-repo/nmfta-telematics_security_requirements.

Additionally, we believe that there are fleet privacy issues which could be better addressed in the draft regulatory concepts document.

- VIII.(c)(4)(C)3."Electronic identifiers of the vehicle and its OBD system: The CC-ROBD system shall be capable of detecting any change in the following parameters since the last check: a. E-VIN (item #8 in Table A1) b. Engine serial number and ECU names/IDs (items #9 and #10 in Table A1) c. Software CAL IDs and CVNs (items #6 and #7 in Table A1)"
    - This requirement will force the CC-ROBD providers to store what will be fleet business-sensitive data in their systems. There need to be requirements on segmentation of access controls to the data which may be stored by a single provider for multiple fleets.
- VIII.(c)(5)(C)"File structure: The file shall consist of two sections: the data header, and the CAN Bus data in hexadecimal format."
    - Since the report files will contain CAN data captures, there needs to be a corresponding requirement that only the responses to requests shall be recorded. Otherwise, a lax or malicious implementor could tack on all the CAN Bus traffic during the ROBD operation.
- VIII.(c)(6)(E)2."The ROBD system shall retain the collected OBD data, either in the internal memory of the ROBD tool or in their proprietary database, for at least seven days following a

successful submission to the CARB electronic reporting system approved by the Executive Officer."

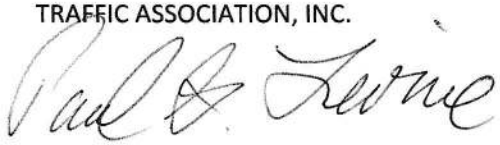
- The servers of the ROBD service providers are thus required to store fleet business-sensitive data and there should, in turn, be data-at-rest confidentiality protections required of the service providers.

Finally, we also offer the following miscellaneous feedback on the draft;

- VIII.(b)(6)(A)1."The serial number of the ROBD tool shall be registered in the electronic reporting system approved by the Executive Officer as a valid testing tool in order to receive authentication to submit data to the electronic reporting system approved by the Executive Officer."
  - What is meant here is authorization, not authentication. It is a common mistake to mix up these two. The draft should use authorization here, not authentication.
- VIII.(c)(6)(C)2."The data file shall be transmitted securely from the ROBD system to the CARB electronic reporting system approved by the Executive Officer.
  3. The data shall be encrypted when sending from the ROBD system to the CARB electronic reporting system approved by the Executive Officer."
  - Part '2.' should be explicit about what 'securely' is meant: confidentiality, integrity, availability, anonymity? Likewise, in part 3, the encryption requirement would (traditionally) offer confidentiality protections – in many cases also integrity protections, but that cannot be assumed and should, rather, be stated explicitly if that is the case here.
- IX.(b)(1)"Applicant shall complete and submit device certification application forms approved by the Executive Officer and other required information for evaluation of the application."
  - We recommend that applicants must also submit a completed checklist of a set of comprehensive cybersecurity requirements. We believe that such a set of requirements is already available for reference and freely licensed use in the telematics security requirements matrix (and questionnaires) available at https://github.com/nmfta-repo/nmfta-telematics_security_requirements.

Sincerely,

NATIONAL MOTOR FREIGHT
TRAFFIC ASSOCIATION, INC.



Paul G. Levine
Executive Director

Ben Gardiner
Senior Cybersecurity Research Engineer