[DISCUSSION DRAFT]

FEBRUARY 11, 2020

SEC. ___. CYBERSECURITY RISKS TO MOTOR VEHICLE SAFETY.

Subchapter I of chapter 301 of title 49, United States Code, is amended by adding at the end the following:

"§ 30107. Cybersecurity risks to motor vehicle safety

"(a) CYBERSECURITY REPORTS.—Not later than 180 days after the date of enactment of this section, a manufacturer may not sell, offer for sale, introduce or deliver for introduction into commerce, or import into the United States, any [motor vehicle,] *or* [highly automated vehicle, vehicle that performs partial driving automation, or automated driving system] unless such manufacturer has developed, maintains, and executes cybersecurity practices and processes to minimize cybersecurity risks to motor vehicle safety.

"(b) CYBERSECURITY REQUIREMENTS.—The cybersecurity practices and processes required under subsection (a) shall include—

"(1) the risk-based prioritized identification, assessment, and protection of safety-critical vehicle control systems and the broader transportation eco-

system, as appropriate, through the product development process and entire life-cycle of the vehicle;

''(2) a process for taking preventative and corrective actions to mitigate against vulnerabilities, including cybersecurity incident response plans;

''(3) the timely detection, assessment, and response to potential vehicle cybersecurity incidents in the field, including false and spurious messages and malicious vehicle control commands;

''(4) facilitating recovery from cybersecurity incidents as they occur;

''(5) sharing lessons learned across industry through voluntary exchange of information pertaining to cybersecurity incidents, threats, and vulnerabilities;

''(6) coordinated cybersecurity vulnerability disclosure policy or other related practices for collaboration with third-party cybersecurity researchers;

''(7) the identification of an officer or other individual of the manufacturer as the point of contact with responsibility for the management of cybersecurity;

''(8) the evaluation of elements of the supply chain to identify and address cybersecurity vulnerabilities;

''(9) the use of segmentation and isolation techniques in vehicle architecture design, as appropriate;

''(10) employee training and supervision for implementation and maintenance of the policies and procedures required by this section; and

''(11) considering consistency and alignment with the cybersecurity risk management approach described in section 2(e) of the National Institute of Standards and Technology Act (15 U.S.C. 272(e)) or international consensus cybersecurity standards.

''(c) CYBERSECURITY STUDY.—

''(1) No later than 2 years after the date of enactment of this Act, the Secretary of Transportation, in coordination with any other appropriate Federal agency, shall conduct a study on the state of cybersecurity regarding [motor vehicles,] *or* [highly automated vehicles, vehicles that perform partial driving automation, or automated driving systems].

''(2) In conducting such study, the Secretary shall—

''(A) develop a comprehensive list of Federal agencies with jurisdiction over cybersecurity and a brief description of such jurisdiction or expertise of such agencies;

"(B) identify all interagency activities taking place among Federal agencies related to cybersecurity regarding [motor vehicles,] *or* [highly automated vehicles, vehicles that perform partial driving automation, or automated driving systems], including working groups or any other relevant coordinated effort;

"(C) develop a comprehensive list of public-private partnerships focused on cybersecurity regarding [motor vehicles,] *or* [highly automated vehicles, vehicles that perform partial driving automation, or automated driving systems], as well as any industry-based bodies, including international bodies, which have developed, or are developing, mandatory or voluntary standards for cybersecurity and that status of such standards;

"(D) identify all regulations, guidelines, mandatory standards, voluntary standards, and other policies implemented by each Federal agency identified under this section, as well as all guidelines, mandatory standards, voluntary standards, and other policies implemented by industry-based bodies;

"(E) review the current equipment, measures, guidelines, or practices used across the industry to identify, protect, detect, respond to, or recover from cybersecurity incidents affecting the safety of a passenger motor vehicle; and

"(F) identify existing cybersecurity resources to assist individuals in maintaining awareness of cybersecurity risks due to motor vehicle safety and mechanisms for alerting a human driver or operator regarding cybersecurity vulnerabilities.

"(3) The Secretary shall submit to the Committee on Energy and Commerce of the House of Representatives and the Committee on Commerce, Science, and Transportation of the Senate a report that contains—

"(A) the results of the study conducted under paragraph (1);

"(B) recommendations to enable the exchange of information and lessons learned across the industry regarding cybersecurity incidents, threats, and potential vulnerabilities; and

"(C) recommendations for legislation or rulemakings needed to address any cybersecurity issue to motor vehicle safety related to

[motor vehicles,] *or* [highly automated vehicles, vehicles that perform partial driving automation, or automated driving systems].

[''(d) CYBERSECURITY RULEMAKING.—If the Secretary makes a determination under subsection (c) that rulemakings are needed to address any cybersecurity issue to motor vehicle safety [related to [motor vehicles,] *or*[highly automated vehicles, vehicles that perform partial driving automation, or automated driving systems]] the secretary shall complete such rulemakings not later than [__] years after the study is completed.]

[''(e) REPORTING REQUIREMENT.—On an annual basis, a manufacturer of a [motor vehicle,] *or* [highly automated vehicle, vehicle that perform partial driving automation, or automated driving system] shall provide the Secretary a detailed description of the practices and processes maintained by the manufacturer to minimize cybersecurity risks to motor vehicle safety. Such reports shall be considered privileged and confidential for the purposes of section 552(b)(4)of title 5, United States Code.]

[''(f) INSPECTION.—The Secretary may investigate any cybersecurity processes and practice developed, maintained, and executed by a manufacturer under this section to determine whether a manufacturer has complied, or is

complying, with this section, chapter, or a regulation prescribed or order issued pursuant to this chapter.]

[''(g) CIVIL PENALTY.—Section 30165(a)(1) of title 49, United States Code is amended by inserting '30107,' after 'section'.]

''(h) DEFINITION.—The term 'cybersecurity incident' has the meaning given the term 'significant cyber incident' in Presidential Policy Directive 41 (PPD–41), issued July 26, 2016.

''(i) CLERICAL AMENDMENT.—The analysis for chapter 301 of title 49, United States Code, is amended by inserting after the item relating to section 30107, as added by section 9(b), the following:

''''30107. Cybersecurity Risk to Motor Vehicle Safety.'.''.