

[DISCUSSION DRAFT]

FEBRUARY 11, 2020

1 **SEC. ____ . CYBERSECURITY RISKS TO MOTOR VEHICLE**
2 **SAFETY.**

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

5 **“§ 30107. Cybersecurity risks to motor vehicle safety**

6 “(a) CYBERSECURITY REPORTS.—Not later than 180
7 days after the date of enactment of this section, a manu-
8 facturer may not sell, offer for sale, introduce or deliver
9 for introduction into commerce, or import into the United
10 States, any [motor vehicle,] *or* [highly automated vehicle,
11 vehicle that performs partial driving automation, or auto-
12 mated driving system] unless such manufacturer has de-
13 veloped, maintains, and executes cybersecurity practices
14 and processes to minimize cybersecurity risks to motor ve-
15 hicle safety.

16 “(b) CYBERSECURITY REQUIREMENTS.—The cyber-
17 security practices and processes required under subsection
18 (a) shall include—

19 “(1) the risk-based prioritized identification, as-
20 sessment, and protection of safety-critical vehicle
21 control systems and the broader transportation eco-

1 system, as appropriate, through the product develop-
2 ment process and entire life-cycle of the vehicle;

3 “(2) a process for taking preventative and cor-
4 rective actions to mitigate against vulnerabilities, in-
5 cluding cybersecurity incident response plans;

6 “(3) the timely detection, assessment, and re-
7 sponse to potential vehicle cybersecurity incidents in
8 the field, including false and spurious messages and
9 malicious vehicle control commands;

10 “(4) facilitating recovery from cybersecurity in-
11 cidents as they occur;

12 “(5) sharing lessons learned across industry
13 through voluntary exchange of information per-
14 taining to cybersecurity incidents, threats, and
15 vulnerabilities;

16 “(6) coordinated cybersecurity vulnerability dis-
17 closure policy or other related practices for collabo-
18 ration with third-party cybersecurity researchers;

19 “(7) the identification of an officer or other in-
20 dividual of the manufacturer as the point of contact
21 with responsibility for the management of cybersecu-
22 rity;

23 “(8) the evaluation of elements of the supply
24 chain to identify and address cybersecurity
25 vulnerabilities;

1 “(9) the use of segmentation and isolation tech-
2 niques in vehicle architecture design, as appropriate;

3 “(10) employee training and supervision for im-
4 plementation and maintenance of the policies and
5 procedures required by this section; and

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

11 “(c) CYBERSECURITY STUDY.—

12 “(1) No later than 2 years after the date of en-
13 actment of this Act, the Secretary of Transpor-
14 tation, in coordination with any other appropriate
15 Federal agency, shall conduct a study on the state
16 of cybersecurity regarding **【motor vehicles,】** *or*
17 **【highly automated vehicles, vehicles that perform**
18 **partial driving automation, or automated driving**
19 **systems】**.

20 “(2) In conducting such study, the Secretary
21 shall—

22 “(A) develop a comprehensive list of Fed-
23 eral agencies with jurisdiction over cybersecu-
24 rity and a brief description of such jurisdiction
25 or expertise of such agencies;

1 “(B) identify all interagency activities tak-
2 ing place among Federal agencies related to cy-
3 bersecurity regarding **【motor vehicles,】** *or*
4 **【highly automated vehicles, vehicles that per-**
5 **form partial driving automation, or automated**
6 **driving systems】**, including working groups or
7 any other relevant coordinated effort;

8 “(C) develop a comprehensive list of pub-
9 lic-private partnerships focused on cybersecurity
10 regarding **【motor vehicles,】** *or* **【highly auto-**
11 **mated vehicles, vehicles that perform partial**
12 **driving automation, or automated driving sys-**
13 **tems】**, as well as any industry-based bodies, in-
14 cluding international bodies, which have devel-
15 oped, or are developing, mandatory or voluntary
16 standards for cybersecurity and that status of
17 such standards;

18 “(D) identify all regulations, guidelines,
19 mandatory standards, voluntary standards, and
20 other policies implemented by each Federal
21 agency identified under this section, as well as
22 all guidelines, mandatory standards, voluntary
23 standards, and other policies implemented by
24 industry-based bodies;

1 “(E) review the current equipment, meas-
2 ures, guidelines, or practices used across the in-
3 dustry to identify, protect, detect, respond to,
4 or recover from cybersecurity incidents affecting
5 the safety of a passenger motor vehicle; and

6 “(F) identify existing cybersecurity re-
7 sources to assist individuals in maintaining
8 awareness of cybersecurity risks due to motor
9 vehicle safety and mechanisms for alerting a
10 human driver or operator regarding cybersecu-
11 rity vulnerabilities.

12 “(3) The Secretary shall submit to the Com-
13 mittee on Energy and Commerce of the House of
14 Representatives and the Committee on Commerce,
15 Science, and Transportation of the Senate a report
16 that contains—

17 “(A) the results of the study conducted
18 under paragraph (1);

19 “(B) recommendations to enable the ex-
20 change of information and lessons learned
21 across the industry regarding cybersecurity inci-
22 dents, threats, and potential vulnerabilities; and

23 “(C) recommendations for legislation or
24 rulemakings needed to address any cybersecu-
25 rity issue to motor vehicle safety related to

1 [motor vehicles,] *or* [highly automated vehi-
2 cles, vehicles that perform partial driving auto-
3 mation, or automated driving systems].

4 [“(d) CYBERSECURITY RULEMAKING.—If the Sec-
5 retary makes a determination under subsection (c) that
6 rulemakings are needed to address any cybersecurity issue
7 to motor vehicle safety [related to [motor vehicles,]
8 *or* [highly automated vehicles, vehicles that perform partial
9 driving automation, or automated driving systems]] the
10 secretary shall complete such rulemakings not later than
11 [___] years after the study is completed.]

12 [“(e) REPORTING REQUIREMENT.—On an annual
13 basis, a manufacturer of a [motor vehicle,] *or* [highly
14 automated vehicle, vehicle that perform partial driving au-
15 tomation, or automated driving system] shall provide the
16 Secretary a detailed description of the practices and proc-
17 esses maintained by the manufacturer to minimize cyber-
18 security risks to motor vehicle safety. Such reports shall
19 be considered privileged and confidential for the purposes
20 of section 552(b)(4) of title 5, United States Code.]

21 [“(f) INSPECTION.—The Secretary may investigate
22 any cybersecurity processes and practice developed, main-
23 tained, and executed by a manufacturer under this section
24 to determine whether a manufacturer has complied, or is

1 complying, with this section, chapter, or a regulation pre-
2 scribed or order issued pursuant to this chapter.】

3 【“(g) CIVIL PENALTY.—Section 30165(a)(1) of title
4 49, United States Code is amended by inserting ‘30107,’
5 after ‘section’.】

6 “(h) DEFINITION.—The term ‘cybersecurity incident’
7 has the meaning given the term ‘significant cyber incident’
8 in Presidential Policy Directive 41 (PPD–41), issued July
9 26, 2016.

10 “(i) CLERICAL AMENDMENT.—The analysis for chap-
11 ter 301 of title 49, United States Code, is amended by
12 inserting after the item relating to section 30107, as
13 added by section 9(b), the following:

“‘30107. Cybersecurity Risk to Motor Vehicle Safety.’”.