

117TH CONGRESS
2D SESSION

S. 3511

To require a report on Federal support to the cybersecurity of commercial satellite systems, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JANUARY 13 (legislative day, JANUARY 10), 2022

Mr. PETERS (for himself and Mr. CORNYN) introduced the following bill; which was read twice and referred to the Committee on Homeland Security and Governmental Affairs

A BILL

To require a report on Federal support to the cybersecurity of commercial satellite systems, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Satellite Cybersecurity
5 Act”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

8 (1) **COMMERCIAL SATELLITE SYSTEM.**—The
9 term “commercial satellite system” means an earth

1 satellite owned and operated by a non-Federal enti-
 2 ty.

3 (2) CRITICAL INFRASTRUCTURE.—The term
 4 “critical infrastructure” has the meaning given the
 5 term in subsection (e) of the Critical Infrastructure
 6 Protection Act of 2001 (42 U.S.C. 5195e(e)).

7 (3) CYBERSECURITY RISK.—The term “cyberse-
 8 curity risk” has the meaning given the term in sec-
 9 tion 2209 of the Homeland Security Act of 2002 (6
 10 U.S.C. 659).

11 (4) CYBERSECURITY THREAT.—The term “cy-
 12 bersecurity threat” has the meaning given the term
 13 in section 102 of the Cybersecurity Information
 14 Sharing Act of 2015 (6 U.S.C. 1501).

15 **SEC. 3. REPORT ON COMMERCIAL SATELLITE CYBERSECU-**
 16 **RITY.**

17 (a) STUDY.—The Comptroller General of the United
 18 States shall conduct a study on the actions the Federal
 19 Government has taken to support the cybersecurity of
 20 commercial satellite systems, including as part of any ac-
 21 tion to address the cybersecurity of critical infrastructure
 22 sectors.

23 (b) REPORT.—Not later than 1 year after the date
 24 of enactment of this Act, the Comptroller General of the
 25 United States shall report to Congress on the study con-

1 ducted under subsection (a), which shall include informa-
2 tion on—

3 (1) the effectiveness of efforts of the Federal
4 Government in improving the cybersecurity of com-
5 mercial satellite systems;

6 (2) the resources made available to the public
7 by Federal agencies to address cybersecurity threats
8 to commercial satellite systems;

9 (3) the extent to which commercial satellite sys-
10 tems are reliant on or are relied on by critical infra-
11 structure and an analysis of how commercial sat-
12 ellite systems, and the threats to such systems, are
13 integrated into Federal and non-Federal critical in-
14 frastructure risk analyses and protection plans;

15 (4) the extent to which Federal agencies are re-
16 liant on commercial satellite systems and how Fed-
17 eral agencies mitigate cybersecurity risks associated
18 with those systems; and

19 (5) the extent to which Federal agencies coordi-
20 nate or duplicate authorities and take other actions
21 focused on the cybersecurity of commercial satellite
22 systems.

23 (c) CONSULTATION.—In carrying out subsections (a)
24 and (b), the Comptroller General of the United States
25 shall coordinate with—

- 1 (1) the Secretary of Homeland Security;
- 2 (2) the Director of the National Institute of
- 3 Standards and Technology;
- 4 (3) the Secretary of Defense;
- 5 (4) the Federal Communications Commission;
- 6 (5) the National Oceanic and Atmospheric Ad-
- 7 ministration;
- 8 (6) the National Aeronautics and Space Admin-
- 9 istration;
- 10 (7) the Federal Aviation Administration; and
- 11 (8) the head of any other Federal agency deter-
- 12 mined appropriate by the Comptroller General of the
- 13 United States.

14 **SEC. 4. RESPONSIBILITIES OF THE CYBERSECURITY AND**
 15 **INFRASTRUCTURE SECURITY AGENCY.**

16 (a) DEFINITIONS.—In this section:

17 (1) CLEARINGHOUSE.—The term “clearing-

18 house” means the commercial satellite system cyber-

19 security clearinghouse required to be developed and

20 maintained under subsection (b)(1).

21 (2) DIRECTOR.—The term “Director” means

22 the Director of the Cybersecurity and Infrastructure

23 Security Agency.

24 (3) SMALL BUSINESS CONCERN.—The term

25 “small business concern” has the meaning given the

1 term in section 3 of the Small Business Act (15
2 U.S.C. 632).

3 (b) ESTABLISHMENT OF COMMERCIAL SATELLITE
4 SYSTEM CYBERSECURITY CLEARINGHOUSE.—

5 (1) IN GENERAL.—Not later than 180 days
6 after the date of enactment of this Act, the Director
7 shall develop and maintain a commercial satellite
8 system cybersecurity clearinghouse.

9 (2) REQUIREMENTS.—The clearinghouse
10 shall—

11 (A) be publicly available online;

12 (B) contain publicly available commercial
13 satellite system cybersecurity resources, includ-
14 ing the recommendations developed under sub-
15 section (c), and any other materials developed
16 by entities in the Federal Government, for ref-
17 erence by entities that develop commercial sat-
18 ellite systems; and

19 (C) include materials specifically aimed at
20 assisting small business concerns with the se-
21 cure development, operation, and maintenance
22 of commercial satellite systems.

23 (3) CONTENT MAINTENANCE.—The Director
24 shall maintain current and relevant cybersecurity in-
25 formation on the clearinghouse.

1 (4) EXISTING PLATFORM OR WEBSITE.—The
 2 Director may establish and maintain the clearing-
 3 house on an online platform or a website that is in
 4 existence as of the date of enactment of this Act.

5 (c) DEVELOPMENT OF COMMERCIAL SATELLITE SYS-
 6 TEM CYBERSECURITY RECOMMENDATIONS.—

7 (1) IN GENERAL.—The Director shall develop
 8 voluntary cybersecurity recommendations designed
 9 to assist in the development, maintenance, and oper-
 10 ation of commercial satellite systems.

11 (2) REQUIREMENTS.—The recommendations re-
 12 quired under paragraph (1) shall include materials
 13 addressing the following:

14 (A) Risk-based, cybersecurity-informed en-
 15 gineering, including continuous monitoring and
 16 resiliency.

17 (B) Planning for retention or recovery of
 18 positive control of commercial satellite systems
 19 in the event of a cybersecurity incident.

20 (C) Protection against unauthorized access
 21 to vital commercial satellite system functions.

22 (D) Physical protection measures designed
 23 to reduce the vulnerabilities of a commercial
 24 satellite system's command, control, and telem-
 25 etry receiver systems.

1 (E) Protection against communications
2 jamming and spoofing.

3 (F) Security against threats throughout a
4 commercial satellite system's mission lifetime.

5 (G) Management of supply chain risks that
6 affect cybersecurity of commercial satellite sys-
7 tems.

8 (H) As appropriate, the findings and rec-
9 ommendations from the study conducted by the
10 Comptroller General of the United States under
11 section 3(a).

12 (I) Any other recommendations to ensure
13 the confidentiality, availability, and integrity of
14 data residing on or in transit through commer-
15 cial satellite systems.

16 (d) CONSULTATION.—With respect to the collation
17 and development of clearinghouse content under sub-
18 section (b)(2) and the recommendations developed pursu-
19 ant to subsection (c), the Director shall consult with—

20 (1) the heads of appropriate Federal agencies
21 with expertise and experience in satellite operations;
22 and

- 1 (2) non-Federal entities developing commercial
- 2 satellite systems or otherwise supporting the cyber-
- 3 security of commercial satellite systems.

○