

Calendar No. 428

117TH CONGRESS
2^D SESSION**S. 3511****[Report No. 117–122]**

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

JUNE 21, 2022

Reported by Mr. PETERS, with an amendment

[Strike out all after the enacting clause and insert the part printed in *italics*]**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”.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) **COMMERCIAL SATELLITE SYSTEM.**—The
4 term “commercial satellite system” means an earth
5 satellite owned and operated by a non-Federal enti-
6 ty.

7 (2) **CRITICAL INFRASTRUCTURE.**—The term
8 “critical infrastructure” has the meaning given the
9 term in subsection (c) of the Critical Infrastructure
10 Protection Act of 2001 (42 U.S.C. 5195e(c)).

11 (3) **CYBERSECURITY RISK.**—The term “cyberse-
12 curity risk” has the meaning given the term in sec-
13 tion 2209 of the Homeland Security Act of 2002 (6
14 U.S.C. 659).

15 (4) **CYBERSECURITY THREAT.**—The term “cy-
16 bersecurity threat” has the meaning given the term
17 in section 102 of the Cybersecurity Information
18 Sharing Act of 2015 (6 U.S.C. 1501).

19 **SEC. 3. REPORT ON COMMERCIAL SATELLITE CYBERSECU-**
20 **RITY.**

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

1 (b) REPORT.—Not later than 1 year after the date
2 of enactment of this Act, the Comptroller General of the
3 United States shall report to Congress on the study con-
4 ducted under subsection (a), which shall include informa-
5 tion on—

6 (1) the effectiveness of efforts of the Federal
7 Government in improving the cybersecurity of com-
8 mercial satellite systems;

9 (2) the resources made available to the public
10 by Federal agencies to address cybersecurity threats
11 to commercial satellite systems;

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

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

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

1 (e) CONSULTATION.—In carrying out subsections (a)
 2 and (b), the Comptroller General of the United States
 3 shall coordinate with—

4 (1) the Secretary of Homeland Security;

5 (2) the Director of the National Institute of
 6 Standards and Technology;

7 (3) the Secretary of Defense;

8 (4) the Federal Communications Commission;

9 (5) the National Oceanic and Atmospheric Ad-
 10 ministration;

11 (6) the National Aeronautics and Space Admin-
 12 istration;

13 (7) the Federal Aviation Administration; and

14 (8) the head of any other Federal agency deter-
 15 mined appropriate by the Comptroller General of the
 16 United States.

17 **SEC. 4. RESPONSIBILITIES OF THE CYBERSECURITY AND**
 18 **INFRASTRUCTURE SECURITY AGENCY.**

19 (a) DEFINITIONS.—In this section:

20 (1) CLEARINGHOUSE.—The term “clearing-
 21 house” means the commercial satellite system cyber-
 22 security clearinghouse required to be developed and
 23 maintained under subsection (b)(1).

1 (2) DIRECTOR.—The term “Director” means
2 the Director of the Cybersecurity and Infrastructure
3 Security Agency.

4 (3) SMALL BUSINESS CONCERN.—The term
5 “small business concern” has the meaning given the
6 term in section 3 of the Small Business Act (15
7 U.S.C. 632).

8 (b) ESTABLISHMENT OF COMMERCIAL SATELLITE
9 SYSTEM CYBERSECURITY CLEARINGHOUSE.—

10 (1) IN GENERAL.—Not later than 180 days
11 after the date of enactment of this Act, the Director
12 shall develop and maintain a commercial satellite
13 system cybersecurity clearinghouse.

14 (2) REQUIREMENTS.—The clearinghouse
15 shall—

16 (A) be publicly available online;

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

24 (C) include materials specifically aimed at
25 assisting small business concerns with the se-

1 cure development, operation, and maintenance
2 of commercial satellite systems.

3 ~~(3) CONTENT MAINTENANCE.—~~The Director
4 shall maintain current and relevant cybersecurity in-
5 formation on the clearinghouse.

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

10 ~~(c) DEVELOPMENT OF COMMERCIAL SATELLITE SYS-~~
11 ~~TEM CYBERSECURITY RECOMMENDATIONS.—~~

12 ~~(1) IN GENERAL.—~~The Director shall develop
13 voluntary cybersecurity recommendations designed
14 to assist in the development, maintenance, and oper-
15 ation of commercial satellite systems.

16 ~~(2) REQUIREMENTS.—~~The recommendations re-
17 quired under paragraph ~~(1)~~ shall include materials
18 addressing the following:

19 ~~(A) Risk-based, cybersecurity-informed en-~~
20 ~~gineering, including continuous monitoring and~~
21 ~~resiliency.~~

22 ~~(B) Planning for retention or recovery of~~
23 ~~positive control of commercial satellite systems~~
24 ~~in the event of a cybersecurity incident.~~

1 (C) Protection against unauthorized access
2 to vital commercial satellite system functions.

3 (D) Physical protection measures designed
4 to reduce the vulnerabilities of a commercial
5 satellite system's command, control, and telem-
6 etry receiver systems.

7 (E) Protection against communications
8 jamming and spoofing.

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

11 (G) Management of supply chain risks that
12 affect cybersecurity of commercial satellite sys-
13 tems.

14 (H) As appropriate, the findings and rec-
15 ommendations from the study conducted by the
16 Comptroller General of the United States under
17 section 3(a).

18 (I) Any other recommendations to ensure
19 the confidentiality, availability, and integrity of
20 data residing on or in transit through commer-
21 cial satellite systems.

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

1 (1) the heads of appropriate Federal agencies
 2 with expertise and experience in satellite operations;
 3 and

4 (2) non-Federal entities developing commercial
 5 satellite systems or otherwise supporting the cyber-
 6 security of commercial satellite systems.

7 **SECTION 1. SHORT TITLE.**

8 *This Act may be cited as the “Satellite Cybersecurity*
 9 *Act”.*

10 **SEC. 2. DEFINITIONS.**

11 *In this Act:*

12 (1) *COMMERCIAL SATELLITE SYSTEM.*—*The term*
 13 *“commercial satellite system” means an earth satellite*
 14 *owned and operated by a non-Federal entity.*

15 (2) *CRITICAL INFRASTRUCTURE.*—*The term*
 16 *“critical infrastructure” has the meaning given the*
 17 *term in subsection (e) of the Critical Infrastructure*
 18 *Protection Act of 2001 (42 U.S.C. 5195c(e)).*

19 (3) *CYBERSECURITY RISK.*—*The term “cyberse-*
 20 *curity risk” has the meaning given the term in sec-*
 21 *tion 2209 of the Homeland Security Act of 2002 (6*
 22 *U.S.C. 659).*

23 (4) *CYBERSECURITY THREAT.*—*The term “cyber-*
 24 *security threat” has the meaning given the term in*

1 *section 102 of the Cybersecurity Information Sharing*
2 *Act of 2015 (6 U.S.C. 1501).*

3 **SEC. 3. REPORT ON COMMERCIAL SATELLITE CYBERSECU-**
4 **RITY.**

5 (a) *STUDY.*—*The Comptroller General of the United*
6 *States shall conduct a study on the actions the Federal Gov-*
7 *ernment has taken to support the cybersecurity of commer-*
8 *cial satellite systems, including as part of any action to*
9 *address the cybersecurity of critical infrastructure sectors.*

10 (b) *REPORT.*—*Not later than 2 years after the date*
11 *of enactment of this Act, the Comptroller General of the*
12 *United States shall report to Congress on the study con-*
13 *ducted under subsection (a), which shall include informa-*
14 *tion on—*

15 (1) *the effectiveness of efforts of the Federal Gov-*
16 *ernment in improving the cybersecurity of commer-*
17 *cial satellite systems;*

18 (2) *the resources made available to the public, as*
19 *of the date of enactment of this Act, by Federal agen-*
20 *cies to address cybersecurity risks and threats to com-*
21 *mercial satellite systems;*

22 (3) *the extent to which commercial satellite sys-*
23 *tems are reliant on or are relied on by critical infra-*
24 *structure and an analysis of how commercial satellite*
25 *systems, and the threats to such systems, are inte-*

1 *grated into Federal and non-Federal critical infra-*
2 *structure risk analyses and protection plans;*

3 *(4) the extent to which Federal agencies are reli-*
4 *ant on commercial satellite systems and how Federal*
5 *agencies mitigate cybersecurity risks associated with*
6 *those systems;*

7 *(5) the extent to which Federal agencies are reli-*
8 *ant on commercial satellite systems owned wholly or*
9 *in part or controlled by foreign entities, and how*
10 *Federal agencies mitigate associated cybersecurity*
11 *risks;*

12 *(6) the extent to which Federal agencies are reli-*
13 *ant on commercial satellite systems with physical*
14 *structures, such as satellite ground control systems, in*
15 *foreign countries, and how Federal agencies mitigate*
16 *associated cybersecurity risks; and*

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

21 *(c) CONSULTATION.—In carrying out subsections (a)*
22 *and (b), the Comptroller General of the United States shall*
23 *coordinate with appropriate Federal agencies, including—*

24 *(1) the Department of Homeland Security;*

25 *(2) the Department of Commerce;*

1 (3) *the Department of Defense;*

2 (4) *the Department of Transportation;*

3 (5) *the Federal Communications Commission;*

4 (6) *the National Aeronautics and Space Admin-*
5 *istration; and*

6 (7) *the National Executive Committee for Space-*
7 *Based Positioning, Navigation, and Timing.*

8 (d) *BRIEFING.*—*Not later than 1 year after the date*
9 *of enactment of this Act, the Comptroller General of the*
10 *United States shall provide a briefing to the appropriate*
11 *congressional committees.*

12 (e) *CLASSIFICATION.*—*The report made under sub-*
13 *section (b) shall be unclassified but may include a classified*
14 *annex.*

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

17 (a) *DEFINITIONS.*—*In this section:*

18 (1) *CLEARINGHOUSE.*—*The term “clearinghouse”*
19 *means the commercial satellite system cybersecurity*
20 *clearinghouse required to be developed and main-*
21 *tained under subsection (b)(1).*

22 (2) *DIRECTOR.*—*The term “Director” means the*
23 *Director of the Cybersecurity and Infrastructure Se-*
24 *curity Agency.*

1 (3) *SMALL BUSINESS CONCERN.*—*The term*
 2 *“small business concern” has the meaning given the*
 3 *term in section 3 of the Small Business Act (15*
 4 *U.S.C. 632).*

5 (b) *ESTABLISHMENT OF COMMERCIAL SATELLITE SYS-*
 6 *TEM CYBERSECURITY CLEARINGHOUSE.*—

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

11 (2) *REQUIREMENTS.*—*The clearinghouse shall—*

12 (A) *be publicly available online;*

13 (B) *contain publicly available commercial*
 14 *satellite system cybersecurity resources, including*
 15 *the recommendations consolidated under sub-*
 16 *section (c)(1), and any other appropriate mate-*
 17 *rials for reference by entities that develop com-*
 18 *mercial satellite systems; and*

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

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

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

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

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

11 (2) *REQUIREMENTS.*—*The recommendations con-*
 12 *solidated under paragraph (1) shall include, to the*
 13 *greatest extent practicable, materials addressing the*
 14 *following:*

15 (A) *Risk-based, cybersecurity-informed engi-*
 16 *neering, including continuous monitoring and*
 17 *resiliency.*

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

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

23 (D) *Physical protection measures designed*
 24 *to reduce the vulnerabilities of a commercial sat-*

1 *ellite system's command, control, and telemetry*
2 *receiver systems.*

3 *(E) Protection against jamming and spoof-*
4 *ing.*

5 *(F) Security against threats throughout a*
6 *commercial satellite system's mission lifetime.*

7 *(G) Management of supply chain risks that*
8 *affect the cybersecurity of commercial satellite*
9 *systems.*

10 *(H) Protection against vulnerabilities posed*
11 *by ownership of commercial satellite systems or*
12 *commercial satellite system companies by foreign*
13 *entities.*

14 *(I) Protection against vulnerabilities posed*
15 *by locating physical infrastructure, such as sat-*
16 *ellite ground control systems, in foreign coun-*
17 *tries.*

18 *(J) As appropriate, and as applicable pur-*
19 *suant to the maintenance requirement under*
20 *subsection (b)(3), the findings and recommenda-*
21 *tions from the study conducted by the Comp-*
22 *troller General of the United States under section*
23 *3(a).*

24 *(K) Any other recommendations to ensure*
25 *the confidentiality, availability, and integrity of*

1 *data residing on or in transit through commer-*
2 *cial satellite systems.*

3 (d) *IMPLEMENTATION.*—*In implementing this Act, the*
4 *Director shall—*

5 (1) *to the extent practicable, carry out the imple-*
6 *mentation as a public-private partnership;*

7 (2) *coordinate with the heads of appropriate*
8 *Federal agencies with expertise and experience in sat-*
9 *ellite operations, including the entities described in*
10 *section 3(c); and*

11 (3) *consult with non-Federal entities developing*
12 *commercial satellite systems or otherwise supporting*
13 *the cybersecurity of commercial satellite systems, in-*
14 *cluding private, consensus organizations that develop*
15 *relevant standards.*

Calendar No. 428

117TH CONGRESS
2D Session

S. 3511

[Report No. 117-122]

A BILL

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

JUNE 21, 2022

Reported with an amendment