

118TH CONGRESS  
1ST SESSION

**S.** \_\_\_\_\_

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

---

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

---

## 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) CLEARINGHOUSE.—The term “clearing-  
9 house” means the commercial satellite system cyber-

1 security clearinghouse required to be developed and  
2 maintained under section 4(b)(1).

3 (2) COMMERCIAL SATELLITE SYSTEM.—The  
4 term “commercial satellite system”—

5 (A) means a system that—

6 (i) is owned or operated by a non-  
7 Federal entity based in the United States;  
8 and

9 (ii) is composed of not less than 1  
10 earth satellite; and

11 (B) includes—

12 (i) any ground support infrastructure  
13 for each satellite in the system; and

14 (ii) any transmission link among and  
15 between any satellite in the system and  
16 any ground support infrastructure in the  
17 system.

18 (3) CRITICAL INFRASTRUCTURE.—The term  
19 “critical infrastructure” has the meaning given the  
20 term in subsection (e) of the Critical Infrastructure  
21 Protection Act of 2001 (42 U.S.C. 5195e(e)).

22 (4) CYBERSECURITY RISK.—The term “cyberse-  
23 curity risk” has the meaning given the term in sec-  
24 tion 2209 of the Homeland Security Act of 2002 (6  
25 U.S.C. 659).

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

5           (6) DIRECTOR.—The term “Director” means  
6           the Director of the Cybersecurity and Infrastructure  
7           Security Agency.

8           (7) SECTOR RISK MANAGEMENT AGENCY.—The  
9           term “sector risk management agency” has the  
10          meaning given the term “Sector-Specific Agency” in  
11          section 2201 of the Homeland Security Act of 2002  
12          (6 U.S.C. 651).

13 **SEC. 3. REPORT ON COMMERCIAL SATELLITE CYBERSECU-**  
14 **RITY.**

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

21          (b) REPORT.—Not later than 2 years after the date  
22          of enactment of this Act, the Comptroller General of the  
23          United States shall report to the Committee on Homeland  
24          Security and Governmental Affairs and the Committee on  
25          Commerce, Science, and Transportation of the Senate and

1 the Committee on Homeland Security and the Committee  
2 on Space, Science, and Technology of the House of Rep-  
3 resentatives on the study conducted under subsection (a),  
4 which shall include information—

5 (1) on efforts of the Federal Government, and  
6 the effectiveness of those efforts, to—

7 (A) address or improve the cybersecurity of  
8 commercial satellite systems; and

9 (B) support related efforts with inter-  
10 national entities or the private sector;

11 (2) on the resources made available to the pub-  
12 lic by Federal agencies to address cybersecurity risks  
13 and threats to commercial satellite systems, includ-  
14 ing resources made available through the clearing-  
15 house;

16 (3) on the extent to which commercial satellite  
17 systems are reliant on, or relied on by, critical infra-  
18 structure;

19 (4) that includes an analysis of how commercial  
20 satellite systems and the threats to those systems  
21 are integrated into Federal and non-Federal critical  
22 infrastructure risk analyses and protection plans;

23 (5) on the extent to which Federal agencies are  
24 reliant on commercial satellite systems and how Fed-

1       eral agencies mitigate cybersecurity risks associated  
2       with those systems;

3           (6) on the extent to which Federal agencies are  
4       reliant on commercial satellite systems that are  
5       owned wholly or in part or controlled by foreign enti-  
6       ties, or that have infrastructure in foreign countries,  
7       and how Federal agencies mitigate associated cyber-  
8       security risks;

9           (7) on the extent to which Federal agencies co-  
10      ordinate or duplicate authorities and take other ac-  
11      tions focused on the cybersecurity of commercial sat-  
12      ellite systems; and

13          (8) as determined appropriate by the Comp-  
14      troller General of the United States, that includes  
15      recommendations for further Federal action to sup-  
16      port the cybersecurity of commercial satellite sys-  
17      tems, including recommendations on information  
18      that should be shared through the clearinghouse.

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

- 23           (1) the Office of the National Cyber Director;  
24           (2) the Department of Homeland Security;  
25           (3) the Department of Commerce;

1 (4) the Department of Defense;

2 (5) the Department of Transportation;

3 (6) the Federal Communications Commission;

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

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

9 (9) the National Space Council.

10 (d) BRIEFING.—Not later than 2 years after the date  
11 of enactment of this Act, the Comptroller General of the  
12 United States shall provide a briefing to the appropriate  
13 congressional committees on the study conducted under  
14 subsection (a).

15 (e) CLASSIFICATION.—The report made under sub-  
16 section (b) shall be unclassified but may include a classi-  
17 fied annex.

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

20 (a) SMALL BUSINESS CONCERN DEFINED.—In this  
21 section, the term “small business concern” has the mean-  
22 ing given the term in section 3 of the Small Business Act  
23 (15 U.S.C. 632).

24 (b) ESTABLISHMENT OF COMMERCIAL SATELLITE  
25 SYSTEM CYBERSECURITY CLEARINGHOUSE.—

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

5           (2) REQUIREMENTS.—The clearinghouse—

6                   (A) shall be publicly available online;

7                   (B) shall contain publicly available com-  
8 mercial satellite system cybersecurity resources,  
9 including the voluntary recommendations con-  
10 solidated under subsection (c)(1);

11                   (C) shall contain appropriate materials for  
12 reference by entities that develop, operate, or  
13 maintain commercial satellite systems;

14                   (D) shall contain materials specifically  
15 aimed at assisting small business concerns with  
16 the secure development, operation, and mainte-  
17 nance of commercial satellite systems; and

18                   (E) may contain controlled unclassified in-  
19 formation distributed to commercial entities  
20 through a process determined appropriate by  
21 the Director.

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

1           (4) EXISTING PLATFORM OR WEBSITE.—To the  
2 extent practicable, the Director shall establish and  
3 maintain the clearinghouse using an online platform,  
4 a website, or a capability in existence as of the date  
5 of enactment of this Act.

6           (c) CONSOLIDATION OF COMMERCIAL SATELLITE  
7 SYSTEM CYBERSECURITY RECOMMENDATIONS.—

8           (1) IN GENERAL.—The Director shall consoli-  
9 date voluntary cybersecurity recommendations de-  
10 signed to assist in the development, maintenance,  
11 and operation of commercial satellite systems.

12           (2) REQUIREMENTS.—The recommendations  
13 consolidated under paragraph (1) shall include mate-  
14 rials appropriate for a public resource addressing, to  
15 the greatest extent practicable, the following:

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

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

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

24           (D) Physical protection measures designed  
25 to reduce the vulnerabilities of a commercial



1 satellite system's command, control, and telem-  
2 etry receiver systems.

3 (E) Protection against jamming, eaves-  
4 dropping, hijacking, computer network exploi-  
5 tation, spoofing, threats to optical satellite com-  
6 munications, and electromagnetic pulse.

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

9 (G) Management of supply chain risks that  
10 affect the cybersecurity of commercial satellite  
11 systems.

12 (H) Protection against vulnerabilities  
13 posed by ownership of commercial satellite sys-  
14 tems or commercial satellite system companies  
15 by foreign entities.

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

20 (J) As appropriate, and as applicable pur-  
21 suant to the maintenance requirement under  
22 subsection (b)(3), relevant findings and rec-  
23 ommendations from the study conducted by the  
24 Comptroller General of the United States under  
25 section 3(a).

1           (K) Any other recommendations to ensure  
2           the confidentiality, availability, and integrity of  
3           data residing on or in transit through commer-  
4           cial satellite systems.

5           (d) IMPLEMENTATION.—In implementing this sec-  
6           tion, the Director shall—

7           (1) to the extent practicable, carry out the im-  
8           plementation in partnership with the private sector;

9           (2) coordinate with—

10           (A) the Office of the National Cyber Direc-  
11           tor, the National Space Council, and the head  
12           of any other agency determined appropriate by  
13           the Office of the National Cyber Director or the  
14           National Space Council; and

15           (B) the heads of appropriate Federal agen-  
16           cies with expertise and experience in satellite  
17           operations, including the entities described in  
18           section 3(c) to enable the alignment of Federal  
19           efforts on commercial satellite system cyberse-  
20           curity and, to the extent practicable, consist-  
21           ency in Federal recommendations relating to  
22           commercial satellite system cybersecurity; and

23           (3) consult with non-Federal entities developing  
24           commercial satellite systems or otherwise supporting  
25           the cybersecurity of commercial satellite systems, in-

1 including private, consensus organizations that develop  
2 relevant standards.

3 (e) REPORT.—Not later than 1 year after the date  
4 of enactment of this Act, and every 2 years thereafter until  
5 the date that is 9 years after the date of enactment of  
6 this Act, the Director shall submit to the Committee on  
7 Homeland Security and Governmental Affairs and the  
8 Committee on Commerce, Science, and Transportation of  
9 the Senate and the Committee on Homeland Security and  
10 the Committee on Space, Science, and Technology of the  
11 House of Representatives a report summarizing—

12 (1) any partnership with the private sector de-  
13 scribed in subsection (d)(1);

14 (2) any consultation with a non-Federal entity  
15 described in subsection (d)(3);

16 (3) the coordination carried out pursuant to  
17 subsection (d)(2);

18 (4) the establishment and maintenance of the  
19 clearinghouse pursuant to subsection (b);

20 (5) the recommendations consolidated pursuant  
21 to subsection (c)(1); and

22 (6) any feedback received by the Director on  
23 the clearinghouse from non-Federal entities.

1 **SEC. 5. STRATEGY.**

2 Not later than 120 days after the date of the enact-  
3 ment of this Act, the National Space Council, jointly with  
4 the Office of the National Cyber Director, in coordination  
5 with the Director of the Office of Space Commerce and  
6 the heads of other relevant agencies, shall submit to the  
7 Committee on Homeland Security and Governmental Af-  
8 fairs and the Committee on Commerce, Science, and  
9 Transportation of the Senate and the Committee on  
10 Homeland Security and the Committee on Space, Science,  
11 and Technology of the House of Representatives a strat-  
12 egy for the activities of Federal agencies to address and  
13 improve the cybersecurity of commercial satellite systems,  
14 which shall include an identification of—

15 (1) proposed roles and responsibilities for rel-  
16 evant agencies; and

17 (2) as applicable, the extent to which cybersecu-  
18 rity threats to such systems are addressed in Fed-  
19 eral and non-Federal critical infrastructure risk  
20 analyses and protection plans.

21 **SEC. 6. RULES OF CONSTRUCTION.**

22 Nothing in this Act shall be construed to—

23 (1) designate commercial satellite systems or  
24 other space assets as a critical infrastructure sector;  
25 or

1           (2) infringe upon or alter the authorities of the  
2           agencies described in section 3(c).

3 **SEC. 7. SECTOR RISK MANAGEMENT AGENCY TRANSFER.**

4           If the President designates an infrastructure sector  
5 that includes commercial satellite systems as a critical in-  
6 frastructure sector pursuant to the process established  
7 under section 9002(b)(3) of the William M. (Mac) Thorn-  
8 berry National Defense Authorization Act for Fiscal Year  
9 2021 (Public Law 116–283; 134 Stat. 4770) and subse-  
10 quently designates a sector risk management agency for  
11 that critical infrastructure sector that is not the Cyberse-  
12 curity and Infrastructure Security Agency, the President  
13 may direct the Director to transfer the authorities of the  
14 Director under section 4 of this Act to the head of the  
15 designated sector risk management agency.