

119TH CONGRESS
1ST SESSION

S. 3404

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

DECEMBER 9, 2025

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

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 of 2025”.

6 **SEC. 2. DEFINITIONS.**

7 In this Act:

8 (1) APPROPRIATE CONGRESSIONAL COMMIT-
9 TEES.—The term “appropriate congressional com-
10 mittees” means—

1 (A) the Committee on Commerce, Science,
2 and Transportation and the Committee on
3 Homeland Security and Governmental Affairs
4 of the Senate; and

5 (B) the Committee on Energy and Com-
6 merce, the Committee on Space, Science, and
7 Technology, and the Committee on Homeland
8 Security of the House of Representatives.

9 (2) CLEARINGHOUSE.—The term “clearing-
10 house” means the commercial satellite system cyber-
11 security clearinghouse required to be developed and
12 maintained under section 4(b)(1).

13 (3) COMMERCIAL SATELLITE SYSTEM.—The
14 term “commercial satellite system”—

15 (A) means a system that—

16 (i) is owned or operated by a non-
17 Federal entity that holds a license issued
18 by the United States for business oper-
19 ations; and

20 (ii) is composed of not less than 1
21 earth satellite; and

22 (B) includes—

23 (i) any ground support infrastructure
24 for each satellite in the system; and

1 (ii) any transmission link among and
2 between any satellite in the system and
3 any ground support infrastructure in the
4 system.

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

9 (5) CYBERSECURITY RISK.—The term “cyberse-
10 curity risk” has the meaning given the term in sec-
11 tion 2200 of the Homeland Security Act of 2002 (6
12 U.S.C. 650).

13 (6) CYBERSECURITY THREAT.—The term “cy-
14 bersecurity threat” has the meaning given the term
15 in section 2200 of the Homeland Security Act of
16 2002 (6 U.S.C. 650).

17 (7) SECRETARY.—The term “Secretary” means
18 the Secretary of Commerce.

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-

1 tion to address the cybersecurity of critical infrastructure
2 sectors.

3 (b) REPORT.—Not later than 2 years after the date
4 of enactment of this Act, the Comptroller General of the
5 United States shall report to the appropriate congressional
6 committees on the study conducted under subsection (a),
7 which shall include information—

8 (1) on efforts of the Federal Government, and
9 the effectiveness of those efforts, to—

10 (A) address or improve the cybersecurity of
11 commercial satellite systems; and

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

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

19 (3) on the extent to which commercial satellite
20 systems are reliant on, or relied on by, critical infra-
21 structure;

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

1 (5) on the extent to which Federal agencies are
2 reliant on commercial satellite systems and how Fed-
3 eral agencies mitigate cybersecurity risks associated
4 with those systems;

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

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

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

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

25 (1) the Department of Commerce;

- 1 (2) the Office of the National Cyber Director;
- 2 (3) the Department of Homeland Security;
- 3 (4) the Department of Defense;
- 4 (5) the Department of Transportation;
- 5 (6) the Federal Communications Commission;
- 6 (7) the National Aeronautics and Space Admin-
7 istration;
- 8 (8) the National Executive Committee for
9 Space-Based Positioning, Navigation, and Timing;
- 10 (9) the National Space Council;
- 11 (10) the Department of Justice; and
- 12 (11) the Committee for the Assessment of For-
13 eign Participation in the United States Tele-
14 communications Services Sector.

15 (d) BRIEFING.—Not later than 2 years after the date
16 of enactment of this Act, the Comptroller General of the
17 United States shall provide a briefing to the appropriate
18 congressional committees on the study conducted under
19 subsection (a).

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

1 **SEC. 4. RESPONSIBILITIES OF THE DEPARTMENT OF COM-**
2 **MERCE.**

3 (a) SMALL BUSINESS CONCERN DEFINED.—In this
4 section, the term “small business concern” has the mean-
5 ing given the term in section 3 of the Small Business Act
6 (15 U.S.C. 632).

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

9 (1) IN GENERAL.—Not later than 180 days
10 after the date of enactment of this Act, the Sec-
11 retary, in coordination with the Chair of the Federal
12 Communications Commission and the Director of
13 the Cybersecurity and Infrastructure Security Agen-
14 cy, shall develop and maintain a commercial satellite
15 system cybersecurity clearinghouse.

16 (2) REQUIREMENTS.—The clearinghouse—

17 (A) shall be publicly available online;

18 (B) shall contain publicly available com-
19 mercial satellite system cybersecurity resources,
20 including the voluntary recommendations con-
21 solidated under subsection (c)(1);

22 (C) shall contain appropriate materials for
23 reference by entities that develop, operate, or
24 maintain commercial satellite systems;

25 (D) shall contain materials specifically
26 aimed at assisting small business concerns with

1 the secure development, operation, and mainte-
2 nance of commercial satellite systems; and

3 (E) may contain controlled unclassified in-
4 formation distributed to commercial entities
5 through a process determined appropriate by
6 the Secretary.

7 (3) CONTENT MAINTENANCE.—The Secretary
8 shall maintain current and relevant cybersecurity in-
9 formation on the clearinghouse.

10 (4) EXISTING PLATFORM OR WEBSITE.—To the
11 extent practicable, the Secretary shall establish and
12 maintain the clearinghouse using an online platform,
13 a website, or a capability in existence as of the date
14 of enactment of this Act.

15 (c) CONSOLIDATION OF COMMERCIAL SATELLITE
16 SYSTEM CYBERSECURITY RECOMMENDATIONS.—

17 (1) IN GENERAL.—The Secretary, in coordina-
18 tion with the Secretary of Homeland Security, shall
19 consolidate voluntary cybersecurity recommendations
20 designed to assist in the development, maintenance,
21 and operation of commercial satellite systems.

22 (2) REQUIREMENTS.—The recommendations
23 consolidated under paragraph (1) shall include mate-
24 rials appropriate for a public resource addressing, to
25 the greatest extent practicable, the following:

1 (A) Risk-based, cybersecurity-informed en-
2 gineering, including continuous monitoring and
3 resiliency.

4 (B) Planning for retention or recovery of
5 positive control of commercial satellite systems
6 in the event of a cybersecurity incident.

7 (C) Protection against unauthorized access
8 to vital commercial satellite system functions.

9 (D) Physical protection measures designed
10 to reduce the vulnerabilities of a commercial
11 satellite system's command, control, and telem-
12 etry receiver systems.

13 (E) Protection against jamming, eaves-
14 dropping, hijacking, computer network exploi-
15 tation, spoofing, threats to optical satellite com-
16 munications, and electromagnetic pulse.

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

19 (G) Management of supply chain risks that
20 affect the cybersecurity of commercial satellite
21 systems.

22 (H) Protection against vulnerabilities
23 posed by ownership of commercial satellite sys-
24 tems or commercial satellite system companies
25 by foreign entities.

1 (I) Protection against vulnerabilities posed
2 by locating physical infrastructure, such as sat-
3 ellite ground control systems, in foreign coun-
4 tries.

5 (J) As appropriate, and as applicable pur-
6 suant to the maintenance requirement under
7 subsection (b)(3), relevant findings and rec-
8 ommendations from the study conducted by the
9 Comptroller General of the United States under
10 section 3(a).

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

15 (d) IMPLEMENTATION.—In implementing this sec-
16 tion, the Secretary shall—

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

19 (2) coordinate with—

20 (A) the Secretary of Homeland Security,
21 the Office of the National Cyber Director, the
22 National Space Council, the Chair of the Fed-
23 eral Communications Commission, and the head
24 of any other agency determined appropriate by

1 the Office of the National Cyber Director or the
2 National Space Council; and

3 (B) the heads of appropriate Federal agen-
4 cies with expertise and experience in satellite
5 operations, including the entities described in
6 section 3(c) to enable the alignment of Federal
7 efforts on commercial satellite system cyberse-
8 curity and, to the extent practicable, consist-
9 ency in Federal recommendations relating to
10 commercial satellite system cybersecurity; 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.

16 (e) REPORT.—Not later than 1 year after the date
17 of enactment of this Act, and every 2 years thereafter until
18 the date that is 9 years after the date of enactment of
19 this Act, the Secretary shall submit to the appropriate
20 congressional committees a report summarizing—

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

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

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

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

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

7 (6) any feedback received by the Secretary on
8 the clearinghouse from non-Federal entities.

9 **SEC. 5. STRATEGY.**

10 Not later than 120 days after the date of the enact-
11 ment of this Act, the Secretary, jointly with the National
12 Space Council and the Office of the National Cyber Direc-
13 tor, in coordination with the Secretary of Homeland Secu-
14 rity, the Director of the Office of Space Commerce, the
15 Chair of the Federal Communications Commission, and
16 the heads of other relevant agencies, shall submit to the
17 appropriate congressional committees a strategy for the
18 activities of Federal agencies to address and improve the
19 cybersecurity of commercial satellite systems, which shall
20 include an identification of—

21 (1) proposed roles and responsibilities for rel-
22 evant agencies; and

23 (2) as applicable, the extent to which cybersecu-
24 rity threats to such systems are addressed in Fed-

1 eral and non-Federal critical infrastructure risk
2 analyses and protection plans.

3 **SEC. 6. RULES OF CONSTRUCTION.**

4 Nothing in this Act shall be construed to—

5 (1) designate commercial satellite systems or
6 other space assets as a critical infrastructure sector;
7 or

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

○