

## Calendar No. 560

119TH CONGRESS  
2D SESSION**S. 3404****[Report No. 119–141]**

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

SEPTEMBER 14, 2026

Reported by Mr. CRUZ, with an amendment

[Strike out all after the enacting clause and insert the part printed in italic]

**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~~”.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) ~~APPROPRIATE CONGRESSIONAL COMMIT-~~  
 4 ~~TEES.~~—The term “appropriate congressional com-  
 5 mittees” means—

6 (A) the Committee on Commerce, Science,  
 7 and Transportation and the Committee on  
 8 Homeland Security and Governmental Affairs  
 9 of the Senate; and

10 (B) the Committee on Energy and Com-  
 11 merce, the Committee on Space, Science, and  
 12 Technology, and the Committee on Homeland  
 13 Security of the House of Representatives.

14 (2) ~~CLEARINGHOUSE.~~—The term “clearing-  
 15 house” means the commercial satellite system cyber-  
 16 security clearinghouse required to be developed and  
 17 maintained under section 4(b)(1).

18 (3) ~~COMMERCIAL SATELLITE SYSTEM.~~—The  
 19 term “commercial satellite system”—

20 (A) means a system that—

21 (i) is owned or operated by a non-  
 22 Federal entity that holds a license issued  
 23 by the United States for business oper-  
 24 ations; and

25 (ii) is composed of not less than 1  
 26 earth satellite; and

1 (B) includes—

2 (i) any ground support infrastructure  
3 for each satellite in the system; and

4 (ii) any transmission link among and  
5 between any satellite in the system and  
6 any ground support infrastructure in the  
7 system.

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

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

16 (6) CYBERSECURITY THREAT.—The term “cy-  
17 bersecurity threat” has the meaning given the term  
18 in section 2200 of the Homeland Security Act of  
19 2002 (6 U.S.C. 650).

20 (7) SECRETARY.—The term “Secretary” means  
21 the Secretary of Commerce.

22 **SEC. 3. REPORT ON COMMERCIAL SATELLITE CYBERSECU-**  
23 **RITY.**

24 (a) STUDY.—The Comptroller General of the United  
25 States shall conduct a study on the actions the Federal

1 Government has taken to support the cybersecurity of  
 2 commercial satellite systems; including as part of any ac-  
 3 tion to address the cybersecurity of critical infrastructure  
 4 sectors.

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

10 (1) on efforts of the Federal Government, and  
 11 the effectiveness of those efforts, to—

12 (A) address or improve the cybersecurity of  
 13 commercial satellite systems; and

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

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

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

24 (4) that includes an analysis of how commercial  
 25 satellite systems and the threats to those systems

1 are integrated into Federal and non-Federal critical  
2 infrastructure risk analyses and protection plans;

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

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

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

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

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

1 shall coordinate with appropriate Federal agencies and or-  
 2 ganizations, including—

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

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

23       (e) CLASSIFICATION.—The report made under sub-  
 24 section (b) shall be unclassified but may include a classi-  
 25 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

the secure development, operation, and maintenance of commercial satellite systems; and

~~(E)~~ may contain controlled unclassified information distributed to commercial entities through a process determined appropriate by the Secretary.

~~(3)~~ CONTENT MAINTENANCE.—The Secretary shall maintain current and relevant cybersecurity information on the clearinghouse.

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

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

~~(1)~~ IN GENERAL.—The Secretary, in coordination with the Secretary of Homeland Security, shall consolidate voluntary cybersecurity recommendations designed to assist in the development, maintenance, and operation of commercial satellite systems.

~~(2)~~ REQUIREMENTS.—The recommendations consolidated under paragraph (1) shall include materials appropriate for a public resource addressing, to 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(e) 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 ~~(e)~~(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(e).

10   **SECTION 1. SHORT TITLE.**

11       *This Act may be cited as the “Satellite Cybersecurity*  
12   *Act of 2025”.*

13   **SEC. 2. DEFINITIONS.**

14       *In this Act:*

15           (1) *APPROPRIATE CONGRESSIONAL COMMIT-*  
16       *TEES.—The term “appropriate congressional commit-*  
17       *tees” means—*

18                   (A) *the Committee on Commerce, Science,*  
19                   *and Transportation and the Committee on*  
20                   *Homeland Security and Governmental Affairs of*  
21                   *the Senate; and*

22                   (B) *the Committee on Energy and Com-*  
23                   *merce, the Committee on Space, Science, and*  
24                   *Technology, and the Committee on Homeland*  
25                   *Security of the House of Representatives.*

1           (2) *CLEARINGHOUSE*.—The term “clearinghouse”  
 2           means the commercial satellite system cybersecurity  
 3           clearinghouse required to be developed and main-  
 4           tained under section 4(b)(1).

5           (3) *COMMERCIAL SATELLITE SYSTEM*.—The term  
 6           “commercial satellite system”—

7                   (A) means a system that—

8                           (i) is owned or operated by a non-Fed-  
 9                           eral entity that holds a license issued by the  
 10                          United States for business operations; and

11                          (ii) is composed of not less than 1  
 12                          earth satellite; and

13                   (B) includes—

14                           (i) any ground support infrastructure  
 15                           for each satellite in the system; and

16                           (ii) any transmission link among and  
 17                           between any satellite in the system and any  
 18                           ground support infrastructure in the sys-  
 19                           tem.

20           (4) *CRITICAL INFRASTRUCTURE*.—The term  
 21           “critical infrastructure” has the meaning given the  
 22           term in subsection (e) of the Critical Infrastructures  
 23           Protection Act of 2001 (42 U.S.C. 5195c(e)).

24           (5) *CYBERSECURITY RISK*.—The term “cyberse-  
 25           curity risk” has the meaning given the term in sec-

1        *tion 2200 of the Homeland Security Act of 2002 (6*  
 2        *U.S.C. 650).*

3            (6) *CYBERSECURITY THREAT.*—*The term “cyber-*  
 4        *security threat” has the meaning given the term in*  
 5        *section 2200 of the Homeland Security Act of 2002 (6*  
 6        *U.S.C. 650).*

7            (7) *SECRETARY.*—*The term “Secretary” means*  
 8        *the Secretary of Commerce.*

9        **SEC. 3. REPORT ON COMMERCIAL SATELLITE CYBERSECU-**  
 10        **RITY.**

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

16        (b) *REPORT.*—*Not later than 2 years after the date*  
 17        *of enactment of this Act, the Comptroller General of the*  
 18        *United States shall report to the appropriate congressional*  
 19        *committees on the study conducted under subsection (a),*  
 20        *which—*

21            (1) *shall include—*

22            (A) *information on efforts of the Federal*  
 23            *Government, and the effectiveness of those efforts,*  
 24            *to—*

1                   (i) address or improve the cybersecu-  
2                   rity of commercial satellite systems; and

3                   (ii) support related efforts with inter-  
4                   national entities or the private sector;

5                   (B) information on the resources made  
6                   available to the public by Federal agencies to ad-  
7                   dress cybersecurity risks and threats to commer-  
8                   cial satellite systems, including resources made  
9                   available through the clearinghouse;

10                  (C) information on the extent to which com-  
11                  mercial satellite systems are reliant on, or relied  
12                  on by, critical infrastructure;

13                  (D) an analysis of how commercial satellite  
14                  systems and the threats to those systems are inte-  
15                  grated into critical infrastructure risk analyses  
16                  and protection plans;

17                  (E) information on the extent to which Fed-  
18                  eral agencies are reliant on commercial satellite  
19                  systems and how Federal agencies mitigate cy-  
20                  bersecurity risks associated with those systems;

21                  (F) information on the extent to which Fed-  
22                  eral agencies are reliant on commercial satellite  
23                  systems that are owned wholly or in part or con-  
24                  trolled by foreign entities, or that have infra-

1           *structure in foreign countries, and how Federal*  
 2           *agencies mitigate associated cybersecurity risks;*

3           *(G) information on the extent to which Fed-*  
 4           *eral agencies coordinate or duplicate authorities*  
 5           *and take other actions focused on the cybersecu-*  
 6           *rity of commercial satellite systems; and*

7           *(H) as determined appropriate by the*  
 8           *Comptroller General of the United States, rec-*  
 9           *ommendations to support the cybersecurity of*  
 10          *commercial satellite systems, including rec-*  
 11          *ommendations on information that should be*  
 12          *shared through the clearinghouse; and*

13          *(2) shall not include recommendations described*  
 14          *in paragraph (1)(H) for new or changing authorities*  
 15          *or regulations for Federal agencies.*

16          *(c) CONSULTATION.—In carrying out subsections (a)*  
 17          *and (b), the Comptroller General of the United States shall*  
 18          *coordinate with appropriate Federal agencies and organiza-*  
 19          *tions, including—*

20                 *(1) the Department of Commerce;*

21                 *(2) the Office of the National Cyber Director;*

22                 *(3) the Department of Homeland Security;*

23                 *(4) the Department of Defense;*

24                 *(5) the Department of Transportation;*

25                 *(6) the Federal Communications Commission;*

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

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

19 *SEC. 4. RESPONSIBILITIES OF THE DEPARTMENT OF COM-*  
20 *MERCE.*

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

1       **(b) ESTABLISHMENT OF COMMERCIAL SATELLITE SYS-**  
 2       **TEM CYBERSECURITY CLEARINGHOUSE.—**

3               **(1) IN GENERAL.—***Not later than 180 days after*  
 4       *the date of enactment of this Act, the Secretary, in co-*  
 5       *ordination with the Secretary of Homeland Security,*  
 6       *shall develop and maintain a commercial satellite*  
 7       *system cybersecurity clearinghouse for the purpose of*  
 8       *serving as a repository for publicly available re-*  
 9       *sources, guidance, frameworks, voluntary rec-*  
 10       *ommendations, and tools.*

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

12                       **(A)** *shall be publicly available online;*

13                       **(B)** *shall contain publicly available com-*  
 14       *mercial satellite system cybersecurity resources,*  
 15       *including the voluntary recommendations con-*  
 16       *solidated under subsection (c)(1);*

17                       **(C)** *shall contain appropriate materials for*  
 18       *reference by entities that develop, operate, or*  
 19       *maintain commercial satellite systems;*

20                       **(D)** *shall contain materials specifically*  
 21       *aimed at assisting small business concerns with*  
 22       *the secure development, operation, and mainte-*  
 23       *nance of commercial satellite systems;*

24                       **(E)** *may contain controlled unclassified in-*  
 25       *formation distributed to commercial entities*

1           *through a process determined appropriate by the*  
 2           *Secretary; and*

3           *(F) may not contain sensitive security or*  
 4           *proprietary information in the absence of the es-*  
 5           *tablishment and use of a gateway to limit access*  
 6           *to approved users, as determined by the Sec-*  
 7           *retary.*

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

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

16          (c) *CONSOLIDATION OF COMMERCIAL SATELLITE SYS-*  
 17          *TEM CYBERSECURITY RECOMMENDATIONS.—*

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

23           (2) *REQUIREMENTS.—The recommendations con-*  
 24           *solidated under paragraph (1) shall include materials*

1        *appropriate for a public resource addressing, to the*  
2        *greatest extent practicable, the following:*

3                *(A) Risk-based, cybersecurity-informed engi-*  
4                *neering, including continuous monitoring and*  
5                *resiliency.*

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

9                *(C) Protection against unauthorized access*  
10               *to vital commercial satellite system functions.*

11               *(D) Physical protection measures designed*  
12               *to reduce the vulnerabilities of a commercial sat-*  
13               *ellite system's command, control, and telemetry*  
14               *receiver systems.*

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

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

21               *(G) Management of supply chain risks that*  
22               *affect the cybersecurity of commercial satellite*  
23               *systems.*

24               *(H) Protection against vulnerabilities posed*  
25               *by ownership of commercial satellite systems or*

1        *commercial satellite system companies by foreign*  
 2        *entities.*

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

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

13               *(K) Any other recommendations to ensure*  
 14       *the confidentiality, availability, and integrity of*  
 15       *data residing on or in transit through commer-*  
 16       *cial satellite systems only for the purpose de-*  
 17       *scribed in subsection (b)(1).*

18        *(d) IMPLEMENTATION.—In implementing this section,*  
 19       *the Secretary shall—*

20               *(1) to the extent practicable, carry out the imple-*  
 21       *mentation in partnership with the private sector;*

22               *(2) coordinate with—*

23               *(A) the Secretary of Homeland Security, the*  
 24       *Office of the National Cyber Director, the Na-*  
 25       *tional Space Council, the Director of the Na-*

1            *tional Institute of Standards and Technology,*  
 2            *and the head of any other agency with expertise*  
 3            *relating to cybersecurity or satellite communica-*  
 4            *tions determined appropriate by the Secretary;*  
 5            *and*

6            *(B) the heads of appropriate Federal agen-*  
 7            *cies with expertise and experience in satellite op-*  
 8            *erations, including the entities described in sec-*  
 9            *tion 3(c) to enable the alignment of Federal ef-*  
 10           *forts on commercial satellite system cybersecurity*  
 11           *and, to the extent practicable, consistency in*  
 12           *Federal recommendations relating to commercial*  
 13           *satellite system cybersecurity; and*

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

19           *(e) REPORT.—Not later than 1 year after the date of*  
 20           *enactment of this Act, and every 2 years thereafter until*  
 21           *the date that is 9 years after the date of enactment of this*  
 22           *Act, the Secretary shall submit to the appropriate congres-*  
 23           *sional committees a report summarizing—*

24           *(1) the general status of any partnership with*  
 25           *the private sector described in subsection (d)(1);*

1           (2) *the results of consultations with a non-Fed-*  
 2           *eral entity described in subsection (d)(3);*

3           (3) *the coordination carried out pursuant to sub-*  
 4           *section (d)(2);*

5           (4) *the establishment and maintenance of the*  
 6           *clearinghouse pursuant to subsection (b);*

7           (5) *the recommendations consolidated pursuant*  
 8           *to subsection (c)(1); and*

9           (6) *general feedback received by the Secretary on*  
 10          *the clearinghouse from non-Federal entities, including*  
 11          *overall trends and any proposed changes to the clear-*  
 12          *inghouse as a result of the feedback.*

13 **SEC. 5. STRATEGY.**

14          *Not later than 120 days after the date of the enactment*  
 15          *of this Act, the Secretary, jointly with the National Space*  
 16          *Council and the Office of the National Cyber Director, in*  
 17          *coordination with the Secretary of Homeland Security, the*  
 18          *Director of the Office of Space Commerce, the Director of*  
 19          *the Office of Science and Technology Policy, and the heads*  
 20          *of other relevant agencies, shall submit to the appropriate*  
 21          *congressional committees a strategy to support coordina-*  
 22          *tion, information sharing, and voluntary best practices*  
 23          *among Federal agencies and private sector stakeholders re-*  
 24          *lating to the cybersecurity of commercial satellite systems,*  
 25          *which shall include an identification of—*

1           (1) *proposed coordination roles among relevant*  
 2           *agencies; and*

3           (2) *as applicable, the extent to which cybersecu-*  
 4           *rity threats to commercial satellite systems are ad-*  
 5           *dressed in—*

6                     (A) *critical infrastructure risk analyses and*  
 7                     *protection plans; and*

8                     (B) *activities relating to commercial sat-*  
 9                     *ellite systems.*

10 **SEC. 6. RULES OF CONSTRUCTION.**

11       *Nothing in this Act shall be construed to—*

12           (1) *designate commercial satellite systems or*  
 13           *other space assets as a critical infrastructure sector;*

14           (2) *infringe upon or alter the authorities of the*  
 15           *agencies described in section 3(c);*

16           (3) *authorize the development or implementation*  
 17           *of any rulemaking or regulatory requirement, includ-*  
 18           *ing by way of enforcement action or condition on any*  
 19           *license or permit for a commercial satellite system; or*

20           (4) *modify or expand existing authorities of the*  
 21           *Committee on Foreign Investment in the United*  
 22           *States or the Committee for the Assessment of Foreign*  
 23           *Participation in the United States Telecommuni-*  
 24           *cations Service Sector.*

Calendar No. 560

119<sup>TH</sup> CONGRESS  
2D Session

**S. 3404**

[Report No. 119-141]

**A BILL**

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

SEPTEMBER 14, 2026

Reported with an amendment