

Calendar No. 195

118TH CONGRESS
1ST SESSION**S. 1425****[Report No. 118–92]**

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

MAY 3, 2023

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

SEPTEMBER 5, 2023

Reported by Mr. PETERS, 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~~”.

1 **SEC. 2. DEFINITIONS.**

2 In this Act:

3 (1) **CLEARINGHOUSE.**—The term “clearing-
4 house” means the commercial satellite system cyber-
5 security clearinghouse required to be developed and
6 maintained under section 4(b)(1).

7 (2) **COMMERCIAL SATELLITE SYSTEM.**—The
8 term “commercial satellite system”—

9 (A) means a system that—

10 (i) is owned or operated by a non-
11 Federal entity based in the United States;
12 and

13 (ii) is composed of not less than 1
14 earth satellite; and

15 (B) includes—

16 (i) any ground support infrastructure
17 for each satellite in the system; and

18 (ii) any transmission link among and
19 between any satellite in the system and
20 any ground support infrastructure in the
21 system.

22 (3) **CRITICAL INFRASTRUCTURE.**—The term
23 “critical infrastructure” has the meaning given the
24 term in subsection (e) of the Critical Infrastructure
25 Protection Act of 2001 (42 U.S.C. 5195e(e)).

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

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

9 (6) **DIRECTOR.**—The term “Director” means
10 the Director of the Cybersecurity and Infrastructure
11 Security Agency.

12 (7) **SECTOR RISK MANAGEMENT AGENCY.**—The
13 term “sector risk management agency” has the
14 meaning given the term “Sector-Specific Agency” in
15 section 2201 of the Homeland Security Act of 2002
16 (6 U.S.C. 651).

17 **SEC. 3. REPORT ON COMMERCIAL SATELLITE CYBERSECU-**
18 **RITY.**

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

1 (b) REPORT.—Not later than 2 years after the date
2 of enactment of this Act, the Comptroller General of the
3 United States shall report to the Committee on Homeland
4 Security and Governmental Affairs and the Committee on
5 Commerce, Science, and Transportation of the Senate and
6 the Committee on Homeland Security and the Committee
7 on Science, Space, and Technology of the House of Rep-
8 resentatives 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 lie 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 (e) 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 Office of the National Cyber Director;

4 (2) the Department of Homeland Security;

5 (3) the Department of Commerce;

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 and

14 (9) the National Space Council.

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 CYBERSECURITY AND**
 2 **INFRASTRUCTURE SECURITY AGENCY.**

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 Director
 11 shall develop and maintain a commercial satellite
 12 system cybersecurity clearinghouse.

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

14 (A) shall be publicly available online;

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

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

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

1 ~~(E)~~ may contain controlled unclassified in-
 2 formation distributed to commercial entities
 3 through a process determined appropriate by
 4 the Director.

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

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

13 ~~(e)~~ CONSOLIDATION OF COMMERCIAL SATELLITE
 14 SYSTEM CYBERSECURITY RECOMMENDATIONS.—

15 ~~(1)~~ IN GENERAL.—The Director shall consoli-
 16 date voluntary cybersecurity recommendations de-
 17 signed to assist in the development, maintenance,
 18 and operation of commercial satellite systems.

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

23 (A) Risk-based, cybersecurity-informed en-
 24 gineering, including continuous monitoring and
 25 resiliency.

1 (B) Planning for retention or recovery of
2 positive control of commercial satellite systems
3 in the event of a cybersecurity incident.

4 (C) Protection against unauthorized access
5 to vital commercial satellite system functions.

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

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

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

16 (G) Management of supply chain risks that
17 affect the cybersecurity of commercial satellite
18 systems.

19 (H) Protection against vulnerabilities
20 posed by ownership of commercial satellite sys-
21 tems or commercial satellite system companies
22 by foreign entities.

23 (I) Protection against vulnerabilities posed
24 by locating physical infrastructure, such as sat-

1 elite ground control systems, in foreign coun-
2 tries.

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

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

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

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

17 (2) coordinate with—

18 ~~(A)~~ the Office of the National Cyber Direc-
19 tor, the National Space Council, and the head
20 of any other agency determined appropriate by
21 the Office of the National Cyber Director or the
22 National Space Council; and

23 ~~(B)~~ the heads of appropriate Federal agen-
24 cies with expertise and experience in satellite
25 operations, including the entities described in

1 section 3(c) to enable the alignment of Federal
2 efforts on commercial satellite system cyberse-
3 curity and, to the extent practicable, consist-
4 ency in Federal recommendations relating to
5 commercial satellite system cybersecurity; and
6 (3) consult with non-Federal entities developing
7 commercial satellite systems or otherwise supporting
8 the cybersecurity of commercial satellite systems, in-
9 cluding private, consensus organizations that develop
10 relevant standards.

11 (e) REPORT.—Not later than 1 year after the date
12 of enactment of this Act, and every 2 years thereafter until
13 the date that is 9 years after the date of enactment of
14 this Act, the Director shall submit to the Committee on
15 Homeland Security and Governmental Affairs and the
16 Committee on Commerce, Science, and Transportation of
17 the Senate and the Committee on Homeland Security and
18 the Committee on Science, Space, and Technology of the
19 House of Representatives a report summarizing—

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

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

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

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

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

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

7 **SEC. 5. STRATEGY.**

8 Not later than 120 days after the date of the enact-
9 ment of this Act, the National Space Council, jointly with
10 the Office of the National Cyber Director, in coordination
11 with the Director of the Office of Space Commerce and
12 the heads of other relevant agencies, shall submit to the
13 Committee on Homeland Security and Governmental Af-
14 fairs and the Committee on Commerce, Science, and
15 Transportation of the Senate and the Committee on
16 Homeland Security and the Committee on Science, Space,
17 and Technology of the House of Representatives a strat-
18 egy for the activities of Federal agencies to address and
19 improve the cybersecurity of commercial satellite systems,
20 which shall 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).

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

11 If the President designates an infrastructure sector
12 that includes commercial satellite systems as a critical in-
13 frastructure sector pursuant to the process established
14 under section 9002(b)(3) of the William M. (Mac) Thorn-
15 berry National Defense Authorization Act for Fiscal Year
16 2021 (Public Law 116–283; 134 Stat. 4770) and subse-
17 quently designates a sector risk management agency for
18 that critical infrastructure sector that is not the Cyberse-
19 curity and Infrastructure Security Agency, the President
20 may direct the Director to transfer the authorities of the
21 Director under section 4 of this Act to the head of the
22 designated sector risk management agency.

23 **SECTION 1. SHORT TITLE.**

24 *This Act may be cited as the “Satellite Cybersecurity*
25 *Act”.*

1 **SEC. 2. DEFINITIONS.**

2 *In this Act:*

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

7 (2) *COMMERCIAL SATELLITE SYSTEM.*—*The term*
8 *“commercial satellite system”*—

9 (A) *means a system that—*

10 (i) *is owned or operated by a non-Fed-*
11 *eral entity based in the United States; and*

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

14 (B) *includes—*

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

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

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

25 (4) *CYBERSECURITY RISK.*—*The term “cyberse-*
26 *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 (5) *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 (6) *DIRECTOR.—The term “Director” means the*
8 *Director of the Cybersecurity and Infrastructure Se-*
9 *curity Agency.*

10 (7) *SECTOR RISK MANAGEMENT AGENCY.—The*
11 *term “sector risk management agency” has the mean-*
12 *ing given the term “Sector Risk Management Agency”*
13 *in section 2200 of the Homeland Security Act of 2002*
14 *(6 U.S.C. 650).*

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 Gov-*
19 *ernment has taken to support the cybersecurity of commer-*
20 *cial satellite systems, including as part of any action to*
21 *address the cybersecurity of critical infrastructure sectors.*

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

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

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

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

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

12 (2) *on the resources made available to the public*
13 *by Federal agencies to address cybersecurity risks and*
14 *threats to commercial satellite systems, including re-*
15 *sources made available through the clearinghouse;*

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 are*
21 *integrated into Federal and non-Federal critical in-*
22 *frastructure 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 cyberse-*
8 *curity 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 rec-*
15 *ommendations for further Federal action to support*
16 *the cybersecurity of commercial satellite systems, in-*
17 *cluding recommendations on information that should*
18 *be shared through the clearinghouse.*

19 *(c) CONSULTATION.—In carrying out subsections (a)*
20 *and (b), the Comptroller General of the United States shall*
21 *coordinate with appropriate Federal agencies and organiza-*
22 *tions, 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 Space-*
7 *Based Positioning, Navigation, and Timing; and*

8 (9) *the National Space Council.*

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

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

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

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

23 (b) *ESTABLISHMENT OF COMMERCIAL SATELLITE SYS-*
24 *TEM CYBERSECURITY CLEARINGHOUSE.*—

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

22 (3) *CONTENT MAINTENANCE.*—The Director shall
23 maintain current and relevant cybersecurity informa-
24 tion 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 SYS-*
7 *TEM CYBERSECURITY RECOMMENDATIONS.*—

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

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

16 (A) *Risk-based, cybersecurity-informed engi-*
17 *neering, 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 sat-*

1 *ellite system's command, control, and telemetry*
2 *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 posed*
13 *by ownership of commercial satellite systems or*
14 *commercial satellite system companies by foreign*
15 *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 section,*
6 *the Director shall—*

7 (1) *to the extent practicable, carry out the imple-*
8 *mentation 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 of*
12 *any other agency determined appropriate by the*
13 *Office of the National Cyber Director or the Na-*
14 *tional Space Council; and*

15 (B) *the heads of appropriate Federal agen-*
16 *cies with expertise and experience in satellite op-*
17 *erations, including the entities described in sec-*
18 *tion 3(c), to enable—*

19 (i) *the alignment of Federal efforts on*
20 *commercial satellite system cybersecurity;*
21 *and*

22 (ii) *to the extent practicable, consist-*
23 *ency in Federal recommendations relating*
24 *to commercial satellite system cybersecurity;*
25 *and*

1 (3) *consult with non-Federal entities developing*
2 *commercial satellite systems or otherwise supporting*
3 *the cybersecurity of commercial satellite systems, in-*
4 *cluding private, consensus organizations that develop*
5 *relevant standards.*

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

15 (1) *any partnership with the private sector de-*
16 *scribed in subsection (d)(1);*

17 (2) *any consultation with a non-Federal entity*
18 *described in subsection (d)(3);*

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

21 (4) *the establishment and maintenance of the*
22 *clearinghouse pursuant to subsection (b);*

23 (5) *the recommendations consolidated pursuant*
24 *to subsection (c)(1); and*

1 (6) *any feedback received by the Director on the*
2 *clearinghouse from non-Federal entities.*

3 **SEC. 5. STRATEGY.**

4 *Not later than 120 days after the date of the enactment*
5 *of this Act, the National Space Council, jointly with the*
6 *Office of the National Cyber Director, in coordination with*
7 *the Director of the Office of Space Commerce and the heads*
8 *of other relevant agencies, shall submit to the Committee*
9 *on Homeland Security and Governmental Affairs and the*
10 *Committee on Commerce, Science, and Transportation of*
11 *the Senate and the Committee on Homeland Security and*
12 *the Committee on Science, Space, and Technology of the*
13 *House of Representatives a strategy for the activities of Fed-*
14 *eral agencies to address and improve the cybersecurity of*
15 *commercial satellite systems, which shall include an identi-*
16 *fication of—*

17 (1) *proposed roles and responsibilities for rel-*
18 *evant agencies; and*

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

23 **SEC. 6. RULES OF CONSTRUCTION.**

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

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

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

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

7 *If the President designates an infrastructure sector*
8 *that includes commercial satellite systems as a critical in-*
9 *frastructure sector pursuant to the process established under*
10 *section 9002(b)(3) of the William M. (Mac) Thornberry Na-*
11 *tional Defense Authorization Act for Fiscal Year 2021 (6*
12 *U.S.C. 652a(b)(3)) and subsequently designates a sector risk*
13 *management agency for that critical infrastructure sector*
14 *that is not the Cybersecurity and Infrastructure Security*
15 *Agency, the President may direct the Director to transfer*
16 *the authorities of the Director under section 4 of this Act*
17 *to the head of the designated sector risk management agen-*
18 *cy.*

Calendar No. 195

118TH CONGRESS
1ST Session

S. 1425

[Report No. 118-92]

A BILL

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

SEPTEMBER 5, 2023

Reported with an amendment