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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

~~**SECTION 1. SHORT TITLE.**~~

~~This Act may be cited as the "Satellite Cybersecurity Act".~~

SEC. 2. DEFINITIONS.

In this Act:

(1) CLEARINGHOUSE.—The term ''clearinghouse'' means the commercial satellite system cybersecurity clearinghouse required to be developed and maintained under section 4(b)(1).

(2) COMMERCIAL SATELLITE SYSTEM.—The term ''commercial satellite system''—

(A) means a system that—

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

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

(B) includes—

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

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

(3) CRITICAL INFRASTRUCTURE.—The term ''critical infrastructure'' has the meaning given the term in subsection (e) of the Critical Infrastructure Protection Act of 2001 (42 U.S.C. 5195c(e)).

(4) CYBERSECURITY RISK.—The term ''cybersecurity risk'' has the meaning given the term in section 2209 of the Homeland Security Act of 2002 (6 U.S.C. 659).

(5) CYBERSECURITY THREAT.—The term ''cybersecurity threat'' has the meaning given the term in section 102 of the Cybersecurity Information Sharing Act of 2015 (6 U.S.C. 1501).

(6) DIRECTOR.—The term ''Director'' means the Director of the Cybersecurity and Infrastructure Security Agency.

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

SEC. 3. REPORT ON COMMERCIAL SATELLITE CYBERSECURITY.

(a) STUDY.—The Comptroller General of the United States shall conduct a study on the actions the Federal Government has taken to support the cybersecurity of commercial satellite systems, including as part of any action to address the cybersecurity of critical infrastructure sectors.

(b) REPORT.—Not later than 2 years after the date of enactment of this Act, the Comptroller General of the United States shall report to the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives on the study conducted under subsection (a), which shall include information—

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

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

(B) support related efforts with international entities or the private sector;

(2) on the resources made available to the public by Federal agencies to address cybersecurity risks and threats to commercial satellite systems, including resources made available through the clearinghouse;

(3) on the extent to which commercial satellite systems are reliant on, or relied on by, critical infrastructure;

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

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

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

(6) on the extent to which Federal agencies are reliant on commercial satellite systems that are owned wholly or in part or controlled by foreign entities, or that have infrastructure in foreign countries, and how Federal agencies mitigate associated cybersecurity risks;

(7) on the extent to which Federal agencies coordinate or duplicate authorities and take other actions focused on the cybersecurity of commercial satellite systems; and

(8) as determined appropriate by the Comptroller General of the United States, that includes recommendations for further Federal action to support the cybersecurity of commercial satellite systems, including recommendations on information that should be shared through the clearinghouse.

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

shall coordinate with appropriate Federal agencies and organizations, including—

(1) the Office of the National Cyber Director;

(2) the Department of Homeland Security;

(3) the Department of Commerce;

(4) the Department of Defense;

(5) the Department of Transportation;

(6) the Federal Communications Commission;

(7) the National Aeronautics and Space Administration;

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

(9) the National Space Council.

(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 subsection (b) shall be unclassified but may include a classified annex.

SEC. 4. RESPONSIBILITIES OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

(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).

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

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

(2) REQUIREMENTS.—The clearinghouse—

(A) shall be publicly available online;

(B) shall contain publicly available commercial satellite system cybersecurity resources, including the voluntary recommendations consolidated under subsection (c)(1);

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

(D) shall contain materials specifically 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 Director.

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

(4) EXISTING PLATFORM OR WEBSITE.—To the extent practicable, the Director 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 Director 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:

(A) Risk-based, cybersecurity-informed engineering, including continuous monitoring and resiliency.

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

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

(D) Physical protection measures designed to reduce the vulnerabilities of a commercial satellite system's command, control, and telemetry receiver systems.

(E) Protection against jamming, eavesdropping, hijacking, computer network exploitation, spoofing, threats to optical satellite communications, and electromagnetic pulse.

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

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

(H) Protection against vulnerabilities posed by ownership of commercial satellite systems or commercial satellite system companies by foreign entities.

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

ellite ground control systems, in foreign countries.

(J) As appropriate, and as applicable pursuant to the maintenance requirement under subsection (b)(3), relevant findings and recommendations from the study conducted by the Comptroller General of the United States under section 3(a).

(K) Any other recommendations to ensure the confidentiality, availability, and integrity of data residing on or in transit through commercial satellite systems.

(d) IMPLEMENTATION.—In implementing this section, the Director shall—

(1) to the extent practicable, carry out the implementation in partnership with the private sector;

(2) coordinate with—

(A) the Office of the National Cyber Director, the National Space Council, and the head of any other agency determined appropriate by the Office of the National Cyber Director or the National Space Council; and

(B) the heads of appropriate Federal agencies with expertise and experience in satellite operations, including the entities described in

section 3(c) to enable the alignment of Federal efforts on commercial satellite system cybersecurity and, to the extent practicable, consistency in Federal recommendations relating to commercial satellite system cybersecurity; and

(3) consult with non-Federal entities developing commercial satellite systems or otherwise supporting the cybersecurity of commercial satellite systems, including private, consensus organizations that develop relevant standards.

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

(1) any partnership with the private sector described in subsection (d)(1);

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

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

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

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

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

SEC. 5. STRATEGY.

Not later than 120 days after the date of the enactment of this Act, the National Space Council, jointly with the Office of the National Cyber Director, in coordination with the Director of the Office of Space Commerce and the heads of other relevant agencies, shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives a strategy for the activities of Federal agencies to address and improve the cybersecurity of commercial satellite systems, which shall include an identification of—

(1) proposed roles and responsibilities for relevant agencies; and

(2) as applicable, the extent to which cybersecurity threats to such systems are addressed in Fed-

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

SEC. 6. RULES OF CONSTRUCTION.

Nothing in this Act shall be construed to—

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

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

SEC. 7. SECTOR RISK MANAGEMENT AGENCY TRANSFER.

If the President designates an infrastructure sector that includes commercial satellite systems as a critical infrastructure sector pursuant to the process established under section 9002(b)(3) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (Public Law 116–283; 134 Stat. 4770) and subsequently designates a sector risk management agency for that critical infrastructure sector that is not the Cybersecurity and Infrastructure Security Agency, the President may direct the Director to transfer the authorities of the Director under section 4 of this Act to the head of the designated sector risk management agency.

SECTION 1. SHORT TITLE.

This Act may be cited as the "Satellite Cybersecurity Act".

SEC. 2. DEFINITIONS.

In this Act:

(1) CLEARINGHOUSE.—The term "clearinghouse" means the commercial satellite system cybersecurity clearinghouse required to be developed and maintained under section 4(b)(1).

(2) COMMERCIAL SATELLITE SYSTEM.—The term "commercial satellite system"—

(A) means a system that—

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

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

(B) includes—

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

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

(3) CRITICAL INFRASTRUCTURE.—The term "critical infrastructure" has the meaning given the term in subsection (e) of the Critical Infrastructure Protection Act of 2001 (42 U.S.C. 5195c).

(4) CYBERSECURITY RISK.—The term "cybersecurity risk" has the meaning given the term in sec-

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

(5) CYBERSECURITY THREAT.—The term "cybersecurity threat" has the meaning given the term in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

(6) DIRECTOR.—The term "Director" means the Director of the Cybersecurity and Infrastructure Security Agency.

(7) SECTOR RISK MANAGEMENT AGENCY.—The term "sector risk management agency" has the meaning given the term "Sector Risk Management Agency" in section 2200 of the Homeland Security Act of 2002 (6 U.S.C. 650).

SEC. 3. REPORT ON COMMERCIAL SATELLITE CYBERSECURITY.

(a) STUDY.—The Comptroller General of the United States shall conduct a study on the actions the Federal Government has taken to support the cybersecurity of commercial satellite systems, including as part of any action to address the cybersecurity of critical infrastructure sectors.

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

Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives on the study conducted under subsection (a), which shall include information—

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

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

(B) support related efforts with international entities or the private sector;

(2) on the resources made available to the public by Federal agencies to address cybersecurity risks and threats to commercial satellite systems, including resources made available through the clearinghouse;

(3) on the extent to which commercial satellite systems are reliant on, or relied on by, critical infrastructure;

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

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

eral agencies mitigate cybersecurity risks associated with those systems;

(6) on the extent to which Federal agencies are reliant on commercial satellite systems that are owned wholly or in part or controlled by foreign entities, or that have infrastructure in foreign countries, and how Federal agencies mitigate associated cybersecurity risks;

(7) on the extent to which Federal agencies coordinate or duplicate authorities and take other actions focused on the cybersecurity of commercial satellite systems; and

(8) as determined appropriate by the Comptroller General of the United States, that includes recommendations for further Federal action to support the cybersecurity of commercial satellite systems, including recommendations on information that should be shared through the clearinghouse.

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

(1) the Office of the National Cyber Director;

(2) the Department of Homeland Security;

(3) the Department of Commerce;

(4) the Department of Defense;

(5) the Department of Transportation;

(6) the Federal Communications Commission;

(7) the National Aeronautics and Space Administration;

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

(9) the National Space Council.

(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 subsection (b) shall be unclassified but may include a classified annex.

SEC. 4. RESPONSIBILITIES OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

(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).

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

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

(2) REQUIREMENTS.—The clearinghouse—

(A) shall be publicly available online;

(B) shall contain publicly available commercial satellite system cybersecurity resources, including the voluntary recommendations consolidated under subsection (c)(1);

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

(D) shall contain materials specifically 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 Director.

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

(4) EXISTING PLATFORM OR WEBSITE.—To the extent practicable, the Director 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 Director 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:

(A) Risk-based, cybersecurity-informed engineering, including continuous monitoring and resiliency.

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

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

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

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

(E) Protection against jamming, eavesdropping, hijacking, computer network exploitation, spoofing, threats to optical satellite communications, and electromagnetic pulse.

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

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

(H) Protection against vulnerabilities posed by ownership of commercial satellite systems or commercial satellite system companies by foreign entities.

(I) Protection against vulnerabilities posed by locating physical infrastructure, such as satellite ground control systems, in foreign countries.

(J) As appropriate, and as applicable pursuant to the maintenance requirement under subsection (b)(3), relevant findings and recommendations from the study conducted by the Comptroller General of the United States under section 3(a).

(K) Any other recommendations to ensure the confidentiality, availability, and integrity of data residing on or in transit through commercial satellite systems.

(d) IMPLEMENTATION.—In implementing this section, the Director shall—

(1) to the extent practicable, carry out the implementation in partnership with the private sector;

(2) coordinate with—

(A) the Office of the National Cyber Director, the National Space Council, and the head of any other agency determined appropriate by the Office of the National Cyber Director or the National Space Council; and

(B) the heads of appropriate Federal agencies with expertise and experience in satellite operations, including the entities described in section 3(c), to enable—

(i) the alignment of Federal efforts on commercial satellite system cybersecurity; and

(ii) to the extent practicable, consistency in Federal recommendations relating to commercial satellite system cybersecurity; and

(3) consult with non-Federal entities developing commercial satellite systems or otherwise supporting the cybersecurity of commercial satellite systems, including private, consensus organizations that develop relevant standards.

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

(1) any partnership with the private sector described in subsection (d)(1);

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

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

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

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

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

SEC. 5. STRATEGY.

Not later than 120 days after the date of the enactment of this Act, the National Space Council, jointly with the Office of the National Cyber Director, in coordination with the Director of the Office of Space Commerce and the heads of other relevant agencies, shall submit to the Committee on Homeland Security and Governmental Affairs and the Committee on Commerce, Science, and Transportation of the Senate and the Committee on Homeland Security and the Committee on Science, Space, and Technology of the House of Representatives a strategy for the activities of Federal agencies to address and improve the cybersecurity of commercial satellite systems, which shall include an identification of—

(1) proposed roles and responsibilities for relevant agencies; and

(2) as applicable, the extent to which cybersecurity threats to such systems are addressed in Federal and non-Federal critical infrastructure risk analyses and protection plans.

SEC. 6. RULES OF CONSTRUCTION.

Nothing in this Act shall be construed to—

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

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

SEC. 7. SECTOR RISK MANAGEMENT AGENCY TRANSFER.

If the President designates an infrastructure sector that includes commercial satellite systems as a critical infrastructure sector pursuant to the process established under section 9002(b)(3) of the William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021 (6 U.S.C. 652a(b)(3)) and subsequently designates a sector risk management agency for that critical infrastructure sector that is not the Cybersecurity and Infrastructure Security Agency, the President may direct the Director to transfer the authorities of the Director under section 4 of this Act to the head of the designated sector risk management agency.

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