Peters_ANS (as modified)

AMENDMENT NO._____ Calendar No._____

Purpose: In the nature of a substitute.

IN THE SENATE OF THE UNITED STATES—119th Cong., 2d Sess.

S. 3404

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

Referred to the Committee on _____ and ordered to be printed

Ordered to lie on the table and to be printed

AMENDMENT IN THE NATURE OF A SUBSTITUTE intended to be proposed by Mr. PETERS

Viz:

Strike all after the enacting clause and insert the following:

SECTION 1. SHORT TITLE.

This Act may be cited as the "Satellite Cybersecurity Act of 2025".

SEC. 2. DEFINITIONS.

In this Act:

(1) APPROPRIATE CONGRESSIONAL COMMITTEES.—The term "appropriate congressional committees" means—

(A) the Committee on Commerce, Science, and Transportation and the Committee on

Homeland Security and Governmental Affairs of the Senate; and

(B) the Committee on Energy and Commerce, the Committee on Space, Science, and Technology, and the Committee on Homeland Security of the House of Representatives.

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

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

(A) means a system that—

(i) is owned or operated by a non-Federal entity that holds a license issued by the United States for business operations; 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.

(4) 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)).

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

(6) 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).

(7) SECRETARY.—The term "Secretary" means the Secretary of Commerce.

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 appropriate congressional committees on the study conducted under subsection (a), which—

(1) shall include—

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

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

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

(B) information 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;

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

(D) an analysis of how commercial satellite systems and the threats to those systems are integrated into critical infrastructure risk analyses and protection plans;

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

(F) information 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;

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

(H) as determined appropriate by the Comptroller General of the United States, recommendations to support the cybersecurity of commercial satellite systems, including recommendations on information that should be shared through the clearinghouse; and

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

(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 Department of Commerce;

(2) the Office of the National Cyber Director;

(3) the Department of Homeland Security;

(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;

(9) the National Space Council;

(10) the Office of Science and Technology Policy;

(11) the Department of Justice ; and

(12) the Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector.

(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 DEPARTMENT OF COMMERCE.

(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 Secretary, in coordination with the Secretary of Homeland Security, shall develop and maintain a commercial satellite system cybersecurity clearinghouse for the purpose of serving as a repository for publicly available resources, guidance, frameworks, voluntary recommendations, and tools.

(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;

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

(F) may not contain sensitive security or proprietary information in the absence of the establishment and use of a gateway to limit access to approved users, as determined 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:

(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 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 only for the purpose described in subsection (b)(1).

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

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

(2) coordinate with—

(A) the Secretary of Homeland Security, the Office of the National Cyber Director, the National Space Council, the Director of the National Institute of Standards and Technology, and the head of any other agency with expertise relating to cybersecurity or satellite communications determined appropriate by the Secretary ; 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 cyberse-

curity 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.

(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 Secretary shall submit to the appropriate congressional committees a report summarizing—

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

(2) the results of consultations 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) general feedback received by the Secretary on the clearinghouse from non-Federal entities, in-

cluding overall trends and any proposed changes to the clearinghouse as a result of the feedback.

SEC. 5. STRATEGY.

Not later than 120 days after the date of the enactment of this Act, the Secretary, jointly with the National Space Council and the Office of the National Cyber Director, in coordination with the Secretary of Homeland Security, the Director of the Office of Space Commerce, the Director of the Office of Science and Technology Policy, and the heads of other relevant agencies, shall submit to the appropriate congressional committees a strategy to support coordination, information sharing, and voluntary best practices among Federal agencies and private sector stakeholders relating to the cybersecurity of commercial satellite systems, which shall include an identification of—

(1) proposed coordination roles among relevant agencies; and

(2) as applicable, the extent to which cybersecurity threats to commercial satellite systems are addressed in—

(A) critical infrastructure risk analyses and protection plans; and

(B) activities relating to commercial satellite systems.

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;

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

(3) authorize the development or implementation of any rulemaking or regulatory requirement, including by way of enforcement action or condition on any license or permit for a commercial satellite system; or

(4) modify or expand existing authorities of the Committee on Foreign Investment in the United States or the Committee for the Assessment of Foreign Participation in the United States Telecommunications Service Sector.