117TH CONGRESS
2D SESSION

S. _____

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

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

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) COMMERCIAL SATELLITE SYSTEM.—The term ''commercial satellite system'' means an earth

satellite owned and operated by a non-Federal entity.

(2) 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)).

(3) 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).

(4) 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).

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 1 year after the date of enactment of this Act, the Comptroller General of the United States shall report to Congress on the study con-

ducted under subsection (a), which shall include information on—

(1) the effectiveness of efforts of the Federal Government in improving the cybersecurity of commercial satellite systems;

(2) the resources made available to the public by Federal agencies to address cybersecurity threats to commercial satellite systems;

(3) the extent to which commercial satellite systems are reliant on or are relied on by critical infrastructure and an analysis of how commercial satellite systems, and the threats to such systems, are integrated into Federal and non-Federal critical infrastructure risk analyses and protection plans;

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

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

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

(1) the Secretary of Homeland Security;

(2) the Director of the National Institute of Standards and Technology;

(3) the Secretary of Defense;

(4) the Federal Communications Commission;

(5) the National Oceanic and Atmospheric Administration;

(6) the National Aeronautics and Space Administration;

(7) the Federal Aviation Administration; and

(8) the head of any other Federal agency determined appropriate by the Comptroller General of the United States.

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

(a) DEFINITIONS.—In this section:

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

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

(3) SMALL BUSINESS CONCERN.—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 shall—

(A) be publicly available online;

(B) contain publicly available commercial satellite system cybersecurity resources, including the recommendations developed under subsection (c), and any other materials developed by entities in the Federal Government, for reference by entities that develop commercial satellite systems; and

(C) include materials specifically aimed at assisting small business concerns with the secure development, operation, and maintenance of commercial satellite systems.

(3) CONTENT MAINTENANCE.—The Director shall [maintain the content on the clearinghouse to maintain current and relevant cybersecurity informa-

tion.--note: just change to simply ''maintain current and relevant cybersecurity information on the clearinghouse''?❱

(4) EXISTING PLATFORM OR WEBSITE.—The Director may establish and maintain the clearinghouse on an online platform or a website that is in existence as of the date of enactment of this Act.

(c) DEVELOPMENT OF COMMERCIAL SATELLITE SYSTEM CYBERSECURITY RECOMMENDATIONS.—

(1) IN GENERAL.—The Director shall develop voluntary cybersecurity recommendations designed to assist in the development, maintenance, and operation of commercial satellite systems.

(2) REQUIREMENTS.—The recommendations required under paragraph (1) shall include materials addressing 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 communications jamming and spoofing.

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

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

(H) As appropriate, the findings and recommendations from the study conducted by the Comptroller General of the United States under section 3(a).

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

(d) CONSULTATION.—With respect to the collation and development of clearinghouse content under subsection (b)(2) and the recommendations developed pursuant to subsection (c), the Director shall consult with—

(1) the heads of appropriate Federal agencies with expertise and experience in satellite operations; and

(2) non-Federal entities developing commercial satellite systems or otherwise supporting the cybersecurity of commercial satellite systems.