(b) EFFECTIVE DATE AND APPLICABILITY.—The amendments made by subsection (a) shall—

(1) take effect with regard to the prohibition under subsection (a)(1)(A) of section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 on such date of enactment; and

(2) take effect with regard to the prohibitions under subsections (a)(1)(B) and (b)(1) of such section two years after such date of enactment.

SA 6136. Mr. PETERS (for himself and Mr. CORNYN) submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

TITLE _____—SATELLITE CYBERSECURITY

SEC. ___01. SHORT TITLE.

This title may be cited as the ''Satellite Cybersecurity Act''.

SEC. ___02. DEFINITIONS.

In this title:

(1) CLEARINGHOUSE.—The term ''clearinghouse'' means the commercial satellite system cybersecurity clearinghouse required to be developed and maintained under section ____04(b)(1) of this title.

(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).

SEC. ___03. 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 Space, Science, and Technology of the House of Representatives on the study conducted under subsection (a), which shall include information on—

(1) efforts of the Federal Government to—

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

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

(2) 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) the extent to which commercial satellite systems and the cybersecurity threats to such systems are addressed in Federal and non-Federal critical infrastructure risk analyses and protection plans;

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

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

(6) as determined appropriate by the Comptroller General of the United States, 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 Department of Homeland Security;

(2) the Department of Commerce;

(3) the Department of Defense;

(4) the Department of Transportation;

(5) the Federal Communications Commission;

(6) the National Aeronautics and Space Administration;

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

(8) 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. ___04. RESPONSIBILITIES OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY.

(a) DEFINITIONS.—In this section:

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

(2) 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.—Subject to the availability of appropriations, 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 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 ____03(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 National Space Council and the head of any other agency determined appropriate by 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 ___03(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.

(e) SUNSET AND REPORT.—

(1) IN GENERAL.—This section shall cease to have force or effect on the date that is 7 years after the date of the enactment of this Act.

(2) REPORT.—Not later than 6 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 Space, Science, and Technology of the House of Representatives a report summarizing—

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

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

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

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

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

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

SEC. ___05. STRATEGY.

Not later than 120 days after the date of the enactment of this Act, the National Space Council, in coordination with the Director of the Office of Space Commerce and the heads of other relevant agencies, shall submit to the Committee on Commerce, Science, and Transportation and the Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Space, Science, and Technology and the Committee on Homeland Security 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. ___06. RULES OF CONSTRUCTION.

Nothing in this title 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 ___03(c) .

SA 6137. Mr. PADILLA (for himself and Mr. TILLIS) submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the end of subtitle G of title X, add the following:

SEC. 1077. TRANSPORTATION DEMAND MANAGEMENT.

Section 101(a) of title 23, United States Code, is amended—

(1) by redesignating paragraphs (32) through (36) as paragraphs (33) through (37), respectively; and

(2) by inserting after paragraph (31) the following:

''(32) TRANSPORTATION DEMAND MANAGEMENT.—The term 'transportation demand management' means the use of strategies to inform and encourage travelers to maximize the efficiency of a transportation system, leading to improved mobility, reduced congestion, and lower vehicle emissions, including strategies that use planning, programs, policies, marketing, communications, incentives, pricing, data, and technology.''.

SA 6138. Mr. SCHATZ (for himself and Ms. HIRONO) submitted an amendment intended to be proposed to amendment SA 5499 submitted by Mr. REED (for himself and Mr. INHOFE) and intended to be proposed to the bill H.R. 7900, to authorize appropriations for fiscal year 2023 for military activities of the Department of Defense, for military construction, and for defense activities of the Department of Energy, to prescribe military personnel strengths for such fiscal year, and for other purposes; which was ordered to lie on the table; as follows:

At the appropriate place, insert the following:

SEC. _____. AIR TOUR AND SPORT PARACHUTING SAFETY IMPROVEMENT.

(a) DEFINITIONS.—In this section:

(1) ADMINISTRATOR.—The term ''Administrator'' means the Administrator of the Federal Aviation Administration.

(2) AIR CARRIER.—The term ''air carrier'' has the meaning given that term in section 40102 of title 49, United States Code.

(3) COMMERCIAL AIR TOUR.—The term ''commercial air tour'' means a flight conducted for compensation or hire in an airplane or helicopter where a purpose of the flight is sightseeing.

(4) COMMERCIAL AIR TOUR OPERATOR.—The term ''commercial air tour operator'' means any person who conducts a commercial air tour.

(5) PARACHUTE OPERATION.—The term ''parachute operation'' has the meaning given that term in section 105.3 of title 14, Code of Federal Regulations (or any successor regulation).

(b) SAFETY MANAGEMENT SYSTEM REQUIREMENTS FOR CERTAIN OPERATORS.—Not later than 24 months after the date of enactment of this section, the Administrator shall issue a final rule requiring each person holding a certificate under part 119 of title 14, Code of Federal Regulations, and authorized to conduct operations in accordance with the provisions of part 135 of title 14, Code of Federal Regulations, to implement a safety management system, as appropriate for the operations.

(c) OTHER SAFETY REQUIREMENTS FOR COMMERCIAL OPERATORS.—

(1) SAFETY REFORMS.—

(A) PART 121 OR PART 135 CERTIFICATE REQUIRED FOR COMMERCIAL AIR TOURS.—

(i) IN GENERAL.—Beginning on the date that is 3 years after the date of enactment of this section, no person may conduct commercial air tours unless that person—

(I) holds a certificate identifying the person as an air carrier or commercial operator under part 119 of title 14, Code of Federal Regulations; and

(II) conducts all commercial air tours under the applicable provisions of part 121 or part 135 of title 14, Code of Federal Regulations.

(ii) EXCLUSION.—Clause (i) shall not apply to a person that conducts fewer than 50 commercial air tours in a calendar year.

(iii) REPORTING REQUIRED.—Beginning on the date that is 3 years after the date of enactment of this section, and every 12 months thereafter, each person that conducts commercial air tours (including any person excluded from the certificate requirement under clause (ii)) shall report to the Administrator the total number of commercial air tours that person conducted during the previous 12 months.

(iv) OTHER TERMS.—The Administrator shall—

(I) revise title 14, Code of Federal Regulations, to include definitions for the terms ''aerial work'' and ''aerial photography'' that are limited to aerial operations performed for compensation or hire with an approved operating certificate; and

(II) to the extent necessary, revise section 119.1(e)(4)(iii) of title 14, Code of Federal Regulations, to conform with the requirements of such definitions.

(B) ADDITIONAL SAFETY REQUIREMENTS.—Not later than 3 years after the date of enactment of this section, the Administrator shall issue new or revised regulations that shall require all certificated commercial air tour operators to incorporate avoidance training for controlled flight into terrain and in-flight loss of control into the training program required under part 121 or 135 of title 14, Code of Federal Regulations, as applicable. The training shall especially address reducing the risk of accidents involving unintentional flight into instrument meteorological conditions to address day, night, and low visibility environments with special attention paid to research available as of the date of enactment of this section on human factors issues involved in such accidents, including but not limited to—

(i) specific terrain, weather, and infrastructure challenges relevant in the local operating environment that increase the risk of such accidents;

(ii) pilot decision-making relevant to the avoidance of instrument meteorological conditions while operating under visual flight rules;

(iii) use of terrain awareness displays;

(iv) spatial disorientation risk factors and countermeasures; and

(v) strategies for maintaining control, including the use of automated systems.

(2) AVIATION RULEMAKING COMMITTEE.—

(A) IN GENERAL.—The Administrator, shall convene an aviation rulemaking committee to review and develop findings and recommendations to inform—

(i) establishing a performance-based standard for flight data monitoring for all commercial air tour operators that reviews all available data sources to identify deviations from established areas of operation and potential safety issues;

(ii) requiring all commercial air tour operators to install flight data recording devices capable of supporting collection and dissemination of the data incorporated in the Flight Operational Quality Assurance Program (or, if an aircraft cannot practically be retrofitted with such equipment, requiring the commercial air tour operator for such aircraft to collect and maintain flight data through alternative methods);