

SATELLITE CYBERSECURITY ACT

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND
GOVERNMENTAL AFFAIRS
UNITED STATES SENATE

TO ACCOMPANY

S. 3511

TO REQUIRE A REPORT ON FEDERAL SUPPORT TO
THE CYBERSECURITY OF COMMERCIAL SATELLITE
SYSTEMS, AND FOR OTHER PURPOSES



JUNE 21, 2022.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

THOMAS R. CARPER, Delaware	ROB PORTMAN, Ohio
MAGGIE HASSAN, New Hampshire	RON JOHNSON, Wisconsin
KYRSTEN SINEMA, Arizona	RAND PAUL, Kentucky
JACKY ROSEN, Nevada	JAMES LANKFORD, Oklahoma
ALEX PADILLA, California	MITT ROMNEY, Utah
JON OSSOFF, Georgia	RICK SCOTT, Florida
	JOSH HAWLEY, Missouri

DAVID M. WEINBERG, *Staff Director*

ZACHARY I. SCHRAM, *Chief Counsel*

CHRISTOPHER J. MULKINS, *Director of Homeland Security*

JEFFREY D. ROTHBLUM, *Senior Professional Staff Member*

PAMELA THIESSEN, *Minority Staff Director*

SAM J. MULOPULOS, *Minority Deputy Staff Director*

CARA G. MUMFORD, *Minority Director of Governmental Affairs*

WILLIAM H.W. MCKENNA, *Minority Chief Counsel*

LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 428

117TH CONGRESS }
2d Session }

SENATE

{ REPORT
{ 117-122

SATELLITE CYBERSECURITY ACT

JUNE 21, 2022.—Ordered to be printed

Mr. PETERS, from the Committee on Homeland Security and
Governmental Affairs, submitted the following

R E P O R T

[To accompany S. 3511]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 3511) to require a report on Federal support to the cybersecurity of commercial satellite systems, and for other purposes, having considered the same, reports favorably thereon with an amendment (in the nature of a substitute) and recommends that the bill, as amended, do pass.

CONTENTS

	Page
I. Purpose and Summary	1
II. Background and Need for the Legislation	2
III. Legislative History	4
IV. Section-by-Section Analysis of the Bill, as Reported	4
V. Evaluation of Regulatory Impact	5
VI. Congressional Budget Office Cost Estimate	6
VII. Changes in Existing Law Made by the Bill, as Reported	7

I. PURPOSE AND SUMMARY

S. 3511, the Satellite Cybersecurity Act, requires the Cybersecurity and Infrastructure Security Agency (CISA) to develop a publicly available online clearinghouse of cybersecurity resources, recommendations, and other appropriate materials specific to commercial satellite systems (CSS) owners and operators, including materials tailored for small businesses. The bill also requires CISA to consolidate voluntary cybersecurity recommendations, including recommendations collected from external sources, such as public and private subject matter experts, designed to assist in the development, maintenance, and operation of CSS, and for these rec-

ommendations to be included in the clearinghouse. In implementing the bill, the bill also requires CISA to carry out the implementation as a public-private partnership to the greatest extent practicable, to coordinate with the heads of appropriate federal agencies, and to consult with entities outside the federal government with expertise in CSS or cybersecurity of CSS including private, consensus organizations that develop relevant standards.

Additionally, S. 3511 requires the Comptroller General of the United States, in consultation with other federal agencies, to study and provide a report to Congress on the effectiveness of efforts of the federal government to improve the cybersecurity of CSS and any resources made available by agencies to support the cybersecurity of CSS. The bill requires the report to detail interdependence of critical infrastructure and CSS, the extent to which threats to CSS are part of critical infrastructure risk analyses and protection plans, the extent to which federal agencies rely on CSS, and risks posed by foreign ownership or foreign-located CSS physical infrastructure.

II. BACKGROUND AND NEED FOR THE LEGISLATION

CSS are an essential piece of our economy. The Presidential Memorandum on Space Policy Directive 5 states that space systems are integral to the operation of numerous critical infrastructure sectors and functions, including global communications; position, navigation, and timing; weather monitoring; and “multiple vital national security applications.”¹ Former Acting CISA Director Brandon Wales stated on May 13, 2021 that “secure and resilient space-based assets are critical to our economy, prosperity, and our national security.”² The National Institute of Standards and Technology also notes that CSS are critical to protect, as “[t]he commercial uses of space for research and development, material sciences, communication, and sensing are growing in size, scale, and importance for the future of the U.S. economy.”³

Despite the critical importance of these systems, cybersecurity vulnerabilities in CSS are growing. On November 20, 2021, Gen. David Thompson of U.S. Space Force stated: “the threats [to satellite systems] are really growing and expanding every single day. And it’s really an evolution of activity that’s been happening for a long time.”⁴

Attacks against CSS have also grown over the recent years. Between 2007 and 2008, two American satellites used by the U.S. Geological Survey and NASA to monitor climate and terrain were compromised multiple times.⁵ In 2014, U.S. officials blamed China for a cyberattack that forced the National Oceanic and Atmospheric Administration (NOAA) to cut off public access to imagery data

¹ President Donald Trump, *Memorandum on Space Policy Directive-5 Cybersecurity Principles for Space Systems* (Sep. 4, 2020) (<https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/>).

² Cybersecurity & Infrastructure Security Agency, *CISA Launches a Space Systems Critical Infrastructure Working Group* (May 13, 2021) (<https://www.cisa.gov/news/2021/05/13/cisa-launches-space-systems-critical-infrastructure-working-group>).

³ National Institute of Standards and Technology, *Introduction to Cybersecurity for Commercial Satellite Operations (2nd Draft)* (NISTIR 8270) (Feb. 25, 2022) (<https://csrc.nist.gov/publications/detail/nistir/8270/draft>).

⁴ *A Shadow War in Space is Heating up Fast*, The Washington Post (Nov. 30, 2021) (<https://www.washingtonpost.com/opinions/2021/11/30/space-race-china-david-thompson/>).

⁵ *For Hackers, Space is the Final Frontier*, Vox (July 29, 2021) (<https://www.vox.com/recode/22598437/spacex-hackers-cyberattack-space-force>).

from a satellite network used for weather forecasting.⁶ Most recently, on February 24, 2022, at the onset of the Russian invasion of Ukraine, the KA-SAT communication satellite network, owned by the U.S.-based company Viasat, Inc., was disrupted and caused communication and internet outages within Ukraine, significantly degrading Ukrainian defense forces' command and control, and causing large scale disruption to a German power company's wind turbines.⁷ On March 17, 2022, the Federal Bureau of Investigation (FBI) and CISA released a joint advisory further bringing attention to the cybersecurity threats facing CSS.⁸

While extensive federal and private sector research has led to many cybersecurity standards and resources focused on traditional enterprise information technology, there is a relative lack of easily accessible, consolidated resources focused specifically on securing CSS.⁹ The lack of these resources is of particular concern given the increase in new satellite businesses over the past decade, in part due to the drastic decrease in costs to launch satellites.¹⁰

Small businesses owning and operating satellites have drastically expanded in the past decade as launch prices have dropped.¹¹ While NASA's Space Shuttle would cost \$30,000 per pound to put a satellite into low-earth orbit, private companies have driven down this cost dramatically and increased the frequency of launches.¹² For example, SpaceX can now launch satellites for under \$2,000 per pound and Rocket Lab is licensed to launch rockets every 72 hours.¹³ Multiple market assessments project aggressive growth of the small satellite industry over the next decade.¹⁴ As more businesses enter this market, it is critical that these new satellite owners and operators are aware of common satellite cybersecurity vulnerabilities and the appropriate mitigations.

Historic and recent attacks against satellites, and the severe consequences of a significant attack against satellite systems, makes clear the need for commercial satellite cybersecurity. This bill aims to help address this need by requiring CISA to consolidate voluntary cybersecurity resources, recommendations, and other mate-

⁶*Id.*

⁷*Satellite Outage Caused "Huge Loss in Communications" at War's Outset—Ukrainian Official*, Reuters (Mar. 15, 2022) (<https://www.reuters.com/world/satellite-outage-caused-huge-loss-communications-wars-outset-ukrainian-official-2022-03-15/>); *Satellite Outage Knocks Out Thousands of Enercon's Wind Turbines*, Reuters (Feb. 28, 2022) (<https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28/>).

⁸Cybersecurity and Infrastructure Security Agency and Federal Bureau of Investigation, *Strengthening Cybersecurity of SATCOM Network Providers and Customers* (Mar. 17, 2022) (<https://www.cisa.gov/uscert/sites/default/files/publications/AA22-076-Strengthening-Cybersecurity-of-SATCOM-Network-Providers-and-Customers.pdf>).

⁹Examples of well-established and widely used enterprise information technology standards include the National Institute of Standard and Technology's (NIST) Cybersecurity Framework and the International Organization for Standardization's 27000 family of Standards.

¹⁰*To Cheaply Go: How Falling Launch Costs Fueled a Thriving Economy in Orbit*, NBC News (Apr. 8, 2022) (<https://www.nbcnews.com/science/space/space-launch-costs-growing-business-industry-rcna23488>).

¹¹*Small Rockets Aim for a Big Market*, Smithsonian Magazine (Apr. 2018) (<https://www.smithsonianmag.com/air-space-magazine/milestone-180968351/>); *To Cheaply Go: How Falling Launch Costs Fueled a Thriving Economy in Orbit*, NBC News (Apr. 8, 2022) (<https://www.nbcnews.com/science/space/space-launch-costs-growing-business-industry-rcna23488>).

¹²*Id.*

¹³*Id.*

¹⁴Allied Market Research, *Small Satellite Market Statistics 2030* (<https://www.alliedmarketresearch.com/small-satellite-market>) (accessed May 26, 2022); *The Small Satellite Market is Projected to Grow From USD 3.1 billion in 2021 to USD 7.4 billion by 2026, at a CAGR of 19.4%*, GlobeNewswire (Feb. 28, 2022) (<https://www.globenewswire.com/news-release/2022/02/28/2393562/0/en/The-small-satellite-market-is-projected-to-grow-from-USD-3-1-billion-in-2021-to-USD-7-4-billion-by-2026-at-a-CAGR-of-19-4.html>).

rials for large and small businesses regarding how to secure CSS. To distribute these materials efficiently, this bill requires CISA to create a clearinghouse, and to curate up-to-date satellite cybersecurity information from private industry and federal government experts. This bill also requires the Comptroller General of the United States to study how the federal government supports CSS owners and operators, and the degree to which critical infrastructure and the government relies on CSS today. The study will also examine how the government uses CSS that are owned or operated by foreign entities.

While historically there has been a lack of federal resources dedicated to improving the cybersecurity of CSS, CISA’s Space Systems Critical Infrastructure Working Group, which the agency launched in May 2021, seeks to address this risk by working with the private sector in a public-private partnership to develop cybersecurity resources for CSS owners and operators. This legislation would build upon that work.

III. LEGISLATIVE HISTORY

Senator Gary Peters (D–MI) introduced S. 3511, the Satellite Cybersecurity Act, on January 13, 2022, with Senator John Cornyn (R–TX). The bill was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 3511 at a business meeting on March 30, 2022. During the business meeting, a substitute amendment, as modified, was offered by Senator Peters. The Peters substitute amendment, as modified, extended the original reporting requirement for the study from the Comptroller General from one year to two years; refined the Comptroller General’s agency consultation and coordination requirement; and emphasized the use of a public-private partnership in the implementation of this act. The Peters substitute amendment, as modified, was adopted by voice vote *en bloc* with Senators Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Paul, Lankford, Romney, Scott, and Hawley present.

Senator Ossoff offered an amendment which adds additional requirements to the Comptroller General study and the consolidated recommendations to evaluate the risks associated with foreign ownership and foreign location of CSS equipment. The Ossoff amendment was adopted by voice vote *en bloc* with Senators Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Paul, Lankford, Romney, Scott, and Hawley present.

The Committee ordered the bill, as amended, to be reported favorably by voice vote *en bloc*. Senators present for the vote were: Peters, Carper, Hassan, Sinema, Rosen, Padilla, Ossoff, Paul, Lankford, Romney, Scott, and Hawley.

Consistent with Committee Rule 3(G), the Committee reports the bill with a technical amendment by mutual agreement of the Chairman and Ranking Member.

IV. SECTION-BY-SECTION ANALYSIS OF THE BILL, AS REPORTED

Section 1. Short title

This section designates the name of the bill as the “Satellite Cybersecurity Act.”

Section 2. Definitions

This section defines the terms “commercial satellite system,” “critical infrastructure,” “cybersecurity risk,” and “cybersecurity threat.”

Section 3. Report on commercial satellite cyber security

This section requires a study to be performed by the Comptroller General of the United States concerning the cybersecurity of commercial satellite systems, including the examination of federal government and critical infrastructure reliance on these systems, existing government efforts to support secure system development and operations, and the identification of risks associated with foreign ownership of commercial satellite system companies or infrastructure. The Comptroller General is required to submit a report to Congress no later than two years after enactment of this bill, and provide a briefing on the status of the study one year after enactment.

In carrying out this section, GAO is required to coordinate with the Department of Homeland Security, Department of Commerce, Department of Defense, Department of Transportation, Federal Communications Commission, National Aeronautics and Space Administration, and the National Executive Committee for Space-Based Positioning, Navigation, and Timing.

Section 4. Responsibilities of the Cybersecurity and Infrastructure Agency

Subsection (a) defines the terms “clearinghouse,” “director,” and “small business concern.”

Subsection (b) establishes the Commercial Satellite Cybersecurity Clearinghouse to be developed by the CISA Director. The clearinghouse is to be publicly available and offer voluntary commercial satellite systems cybersecurity resources and recommendations, including materials aimed at assisting small business concerns with the development, operation, and maintenance of commercial satellite systems.

Subsection (c) requires the CISA Director to consolidate voluntary cybersecurity recommendations for commercial satellite systems. The recommendations will address different aspects of CSS development and operations, including protection against unauthorized access, physical protection measures, supply chain risk management, and mitigations against risks posed by foreign entity ownership and maintenance of physical infrastructure in foreign countries.

Subsection (d) requires the CISA Director to carry out the implementation of this bill as a public-private partnership, to the greatest extent practicable. It also requires CISA to coordinate with the heads of appropriate federal agencies and consult with non-federal entities developing commercial satellite systems or supporting the cybersecurity of commercial satellite systems, including private, consensus organizations that develop relevant standards.

V. EVALUATION OF REGULATORY IMPACT

Pursuant to the requirements of paragraph 11(b) of rule XXVI of the Standing Rules of the Senate, the Committee has considered

the regulatory impact of this bill and determined that the bill will have no regulatory impact within the meaning of the rules. The Committee agrees with the Congressional Budget Office's statement that the bill contains no intergovernmental or private-sector mandates as defined in the Unfunded Mandates Reform Act (UMRA) and would impose no costs on state, local, or tribal governments.

VI. CONGRESSIONAL BUDGET OFFICE COST ESTIMATE

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, April 19, 2022.

Hon. GARY C. PETERS,
Chairman, Committee on Homeland Security and Governmental Affairs, U.S. Senate, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the enclosed cost estimate for S. 3511, the Satellite Cybersecurity Act.

If you wish further details on this estimate, we will be pleased to provide them. The CBO staff contact is Aldo Prospero.

Sincerely,

PHILLIP L. SWAGEL,
Director.

Enclosure.

S. 3511, Satellite Cybersecurity Act			
As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on March 30, 2022			
By Fiscal Year, Millions of Dollars	2022	2022-2026	2022-2031
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	*	12	not estimated
Statutory pay-as-you-go procedures apply?	No	Mandate Effects	
Increases on-budget deficits in any of the four consecutive 10-year periods beginning in 2032?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No
* = between zero and \$500,000.			

S. 3511 would require the Cybersecurity and Infrastructure Security Agency (CISA) to disseminate information on cyber safety measures to operators of commercial satellites. Under the bill, CISA would collect security recommendations from the private sector and other federal agencies with expertise in satellite operations.

Using information from CISA about similar information sharing efforts, CBO anticipates that the agency would need six full-time employees to create and manage an online database with cybersecurity resources for satellite operators. CBO estimates that staff salaries and technology costs to publish safety materials would

total \$3 million annually. Accounting for the time needed to hire new employees and prepare the database, CBO estimates that implementing the bill would cost \$12 million over the 2022–2026 period; such spending would be subject to the availability of appropriated funds.

The CBO staff contact for this estimate is Aldo Prospero. The estimate was reviewed by Leo Lex, Deputy Director of Budget Analysis.

VII. CHANGES IN EXISTING LAW MADE BY THE BILL, AS REPORTED

This legislation would make no change in existing law, within the meaning of clauses (a) and (b) of subparagraph 12 of rule XXVI of the Standing Rules of the Senate, because this legislation would not repeal or amend any provision of current law.