AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

Calendar No. 195

118TH CONGRESS *1st Session*	SENATE	REPORT 118–92

SATELLITE CYBERSECURITY ACT

R E P O R T

OF THE

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS UNITED STATES SENATE

TO ACCOMPANY

S. 1425

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

SEPTEMBER 5, 2023.—Ordered to be printed

U.S. GOVERNMENT PUBLISHING OFFICE
39–010 WASHINGTON : 2023

COMMITTEE ON HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

GARY C. PETERS, Michigan, *Chairman*

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

DAVID M. WEINBERG, *Staff Director*
CHRISTOPHER J. MULKINS, *Director of Homeland Security*
JEFFREY D. ROTHBLUM, *Senior Professional Staff Member*
WILLIAM E. HENDERSON III, *Minority Staff Director*
CHRISTINA N. SALAZAR, *Minority Chief Counsel*
KENDAL B. TIGNER, *Minority Professional Staff Member*
LAURA W. KILBRIDE, *Chief Clerk*

Calendar No. 195

118TH CONGRESS *1st Session* | SENATE | REPORT 118–92

SATELLITE CYBERSECURITY ACT

SEPTEMBER 5, 2023.—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. 1425]

[Including cost estimate of the Congressional Budget Office]

The Committee on Homeland Security and Governmental Affairs, to which was referred the bill (S. 1425), 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

I. PURPOSE AND SUMMARY

S. 1425, 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. 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.[1]

Additionally, S. 1425 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.

Finally, S. 1425 requires the National Space Council, jointly with the Office of the National Cyber Director, to develop and provide to Congress a strategy for the activities of federal agencies to address and improve the cybersecurity of CSS.

II. BACKGROUND AND NEED FOR THE LEGISLATION

CSS are an essential piece of our nation's 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."[2] 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."[3] 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."[4]

Despite the critical importance of these systems, cybersecurity vulnerabilities in CSS are growing. On November 20, 2021, Gen. David Thompson of the 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."[5]

---

[1] On March 30, 2022, the Committee approved S. 3511, the *Satellite Cybersecurity Act*. That bill is substantially similar to S. 1425. Accordingly, this committee report is in many respects similar to the committee report for S. 1425. *See* S. Rept. No. 117–122.

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

[3] 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).

[4] 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).

[5] *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/).

Attacks against CSS have also grown in recent years. Between 2007 and 2008, two American satellites used by the U.S. Geological Survey and the National Aeronautics and Space Administration (NASA) to monitor climate and terrain were compromised multiple times. In 2014, U.S. officials blamed China for a cyberattack that forced the National Oceanic and Atmospheric Administration to cut off public access to imagery data 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. This significantly degraded Ukrainian defense forces' command and control, and caused large scale disruption to a German power company's wind turbines.[7] On March 17, 2022, the Federal Bureau of Investigation 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. 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. For example, SpaceX can now launch satellites for under $2,000 per pound and Rocket Lab is licensed to launch rockets every 72 hours.[11] Multiple market assessments project aggressive growth of the small satellite industry over the next decade.[12] As more busi-

---

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

[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/).

[8] Cybersecurity 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).

[9] Examples 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. National Institute of Standards and Technology, *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)* (Apr. 16, 2018) (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf) and International Organization for Standardization, *ISO/IEC 27000 (Fifth Edition)* (Feb. 2018) (https://www.iso.org/standard/73906.html).

[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] Allied 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%*, GlobeNewswwire (Feb. 28, 2022) (https://www.globenewswire.com/news-

Continued

nesses 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 materials 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.[13] This legislation would build upon that work.

III. LEGISLATIVE HISTORY

Senator Gary Peters (D–MI) introduced S. 1425, the *Satellite Cybersecurity Act,* on May 3, 2023, with original cosponsor Senator John Cornyn (R–TX). The bill was referred to the Committee on Homeland Security and Governmental Affairs.

The Committee considered S. 1425 at a business meeting on May 17, 2023. At the business meeting, Chairman Peters offered a substitute amendment making technical edits to the bill. The substitute amendment was adopted by unanimous consent with Senators Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Blumenthal, Paul, Lankford, Romney, and Scott present. The bill, as amended, was ordered reported favorably by roll call vote of 10 yeas to 1 nay, with Senators Peters, Hassan, Sinema, Rosen, Padilla, Ossoff, Blumenthal, Lankford, Romney, and Scott voting in the affirmative, and with Senator Paul voting in the negative. Senators Carper, Johnson, Hawley, and Marshall voted yea by proxy, for the record only.

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 establishes the short title of the bill as the "Satellite Cybersecurity Act."

---

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).

[13] Cybersecurity & Infrastructure Security Agency, *supra* note 3.

Section 2. Definitions

This section defines the terms "clearinghouse," "commercial satellite system," "critical infrastructure," "cybersecurity risk," "cybersecurity threat," "Director," and "sector risk management agency."

Section 3. Report on commercial satellite cybersecurity

Subsection (a) establishes a study, to be completed within two years by the Comptroller General of the United States, on the federal government's efforts and resources to support the cybersecurity of commercial satellite systems, including as part of any action to address the cybersecurity of critical infrastructure sectors.

Subsections (b)–(e) require the Comptroller General of the United States to coordinate with appropriate federal agencies and organizations, require the report be unclassified, but may include a classified annex, and require briefing the appropriate congressional committees on the Comptroller General's findings.

Section 4. Responsibilities of the cybersecurity and infrastructure agency

Subsection (a) defines the term "small business concern."

Subsection (b) establishes a commercial satellite cybersecurity clearinghouse to be developed and maintained 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 and exploitation, 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 in partnership with the private sector, to the 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.

Subsection (e) requires the CISA Director report on the implementation of the clearinghouse to the Senate Committee on Homeland Security and Governmental Affairs; Senate Committee on Commerce, Science and Transportation; House Committee on Homeland Security; and House Committee on Science, Space, and Technology.

Section 5. Strategy

This section requires that 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, submit a strategy for the activities of federal agencies to address and improve the cybersecurity of commer-

cial satellite systems to the Senate Committee on Homeland Security and Governmental Affairs; Senate Committee on Commerce, Science and Transportation; House Committee on Homeland Security; and House Committee on Science, Space, and Technology.

Section 6. Rules of construction

This section establishes that nothing in this Act shall be construed to designate commercial satellite systems or other space assets as a critical infrastructure sector, or to infringe upon or alter the authorities of the other federal agencies.

Section 7. Sector risk management agency transfer

This section allows the President to transfer the clearinghouse authority from CISA to another sector risk management agency if the President first 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, and then subsequently designates a sector risk management agency for that critical infrastructure sector that is not CISA.

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

S. 1425, Satellite Cybersecurity Act
As ordered reported by the Senate Committee on Homeland Security and Governmental Affairs on May 17, 2023

By Fiscal Year, Millions of Dollars	2023	2023-2028	2023-2033
Direct Spending (Outlays)	0	0	0
Revenues	0	0	0
Increase or Decrease (-) in the Deficit	0	0	0
Spending Subject to Appropriation (Outlays)	0	14	not estimated

Increases *net direct spending* in any of the four consecutive 10-year periods beginning in 2034?	No	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 2034?	No	Contains intergovernmental mandate?	No
		Contains private-sector mandate?	No

S. 1425 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 $14 million over the 2023–2028 period; such spending would be subject to the availability of appropriated funds.

The costs of the legislation, detailed in Table 1, fall within budget function 050 (national defense).

TABLE 1.—ESTIMATED INCREASES IN SPENDING SUBJECT TO APPROPRIATION UNDER S. 1425

	By fiscal year, millions of dollars—						
	2023	2024	2025	2026	2027	2028	2023–2028
Estimated Authorization	0	2	3	3	3	3	14
Estimated Outlays	0	2	3	3	3	3	14

The CBO staff contact for this estimate is Aldo Prosperi. The estimate was reviewed by Chad Chirico, Director of Budget Analysis.

PHILLIP L. SWAGEL,
Director, Congressional Budget Office.

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.

○