

117TH CONGRESS
2D SESSION

H. R. 7629

To require a report on Federal support to the cybersecurity of commercial satellite systems, establish a commercial satellite system cybersecurity clearinghouse in the Cybersecurity and Infrastructure Security Agency, and for other purposes.

IN THE HOUSE OF REPRESENTATIVES

APRIL 28, 2022

Mr. MALINOWSKI (for himself and Mr. GARBARINO) introduced the following bill; which was referred to the Committee on Homeland Security, and in addition to the Committee on Science, Space, and Technology, for a period to be subsequently determined by the Speaker, in each case for consideration of such provisions as fall within the jurisdiction of the committee concerned

A BILL

To require a report on Federal support to the cybersecurity of commercial satellite systems, establish a commercial satellite system cybersecurity clearinghouse in the Cybersecurity and Infrastructure Security Agency, and for other purposes.

1 *Be it enacted by the Senate and House of Representa-*
2 *tives of the United States of America in Congress assembled,*

3 **SECTION 1. SHORT TITLE.**

4 This Act may be cited as the “Satellite Cybersecurity
5 Act”.

1 **SEC. 2. REPORT ON COMMERCIAL SATELLITE CYBERSECURITY;**
2 **CISA COMMERCIAL SATELLITE SYSTEM**
3 **CYBERSECURITY CLEARINGHOUSE.**

4 (a) STUDY.—

5 (1) IN GENERAL.—The Comptroller General of
6 the United States shall conduct a study on the ac-
7 tions the Federal Government has taken to support
8 the cybersecurity of commercial satellite systems, in-
9 cluding as part of any action to address the cyberse-
10 curity of critical infrastructure sectors.

11 (2) REPORT.—Not later than two years after
12 the date of the enactment of this Act, the Comp-
13 troller General of the United States shall report to
14 Congress on the study conducted under paragraph
15 (1), which shall include information on—

16 (A) the effectiveness of efforts of the Fed-
17 eral Government in improving the cybersecurity
18 of commercial satellite systems;

19 (B) the resources made available to the
20 public, as of the date of the enactment of this
21 Act, by Federal agencies to address cybersecu-
22 rity risks and cybersecurity threats to commer-
23 cial satellite systems;

24 (C) the extent to which commercial sat-
25 ellite systems are reliant on or are relied on by
26 critical infrastructure and an analysis of how

1 commercial satellite systems, and the cybersecu-
2 rity threats to such systems, are integrated into
3 Federal and non-Federal critical infrastructure
4 risk analyses and protection plans;

5 (D) the extent to which Federal agencies
6 are reliant on commercial satellite systems and
7 how Federal agencies mitigate cybersecurity
8 risks associated with those systems; and

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

13 (3) CONSULTATION.—In carrying out para-
14 graphs (1) and (2), the Comptroller General of the
15 United States shall coordinate with appropriate Fed-
16 eral agencies, including—

17 (A) the Department of Homeland Security;

18 (B) the Department of Commerce;

19 (C) the Department of Defense;

20 (D) the Department of Transportation;

21 (E) the Federal Communications Commis-

22 sion;

23 (F) the National Aeronautics and Space

24 Administration; and

1 (G) the National Executive Committee for
2 Space-Based Positioning, Navigation, and Tim-
3 ing.

4 (4) BRIEFING.—Not later than one year after
5 the date of the enactment of this Act, the Comp-
6 troller General of the United States shall provide a
7 briefing to Congress relating to carrying out para-
8 graphs (1) and (2).

9 (5) CLASSIFICATION.—The report under para-
10 graph (2) shall be unclassified but may include a
11 classified annex.

12 (b) CISA COMMERCIAL SATELLITE SYSTEM CYBER-
13 SECURITY CLEARINGHOUSE.—

14 (1) ESTABLISHMENT.—

15 (A) IN GENERAL.—Not later than 180
16 days after the date of the enactment of this
17 Act, the Director shall establish a commercial
18 satellite system cybersecurity clearinghouse.

19 (B) REQUIREMENTS.—The clearinghouse
20 shall—

21 (i) be publicly available online;

22 (ii) contain current, relevant, and
23 publicly available commercial satellite sys-
24 tem cybersecurity resources, including the
25 recommendations consolidated under para-

1 graph (2), and any other appropriate ma-
2 terials for reference by entities that de-
3 velop commercial satellite systems; and

4 (iii) include materials specifically
5 aimed at assisting small business concerns
6 with the secure development, operation,
7 and maintenance of commercial satellite
8 systems.

9 (C) EXISTING PLATFORM OR WEBSITE.—

10 The Director may establish the clearinghouse
11 on an online platform or a website that is in ex-
12 istence as of the date of the enactment of this
13 Act.

14 (2) CONSOLIDATION OF COMMERCIAL SAT-
15 ELLITE SYSTEM CYBERSECURITY RECOMMENDA-
16 TIONS.—

17 (A) IN GENERAL.—The Director shall con-
18 solidate voluntary cybersecurity recommenda-
19 tions designed to assist in the development,
20 maintenance, and operation of commercial sat-
21 ellite systems.

22 (B) REQUIREMENTS.—The recommenda-
23 tions consolidated under subparagraph (A) shall
24 include, to the greatest extent practicable, ma-
25 terials addressing the following:

1 (i) Risk-based, cybersecurity-informed
2 engineering, including continuous moni-
3 toring and resiliency.

4 (ii) Planning for retention or recovery
5 of positive control of commercial satellite
6 systems in the event of a cybersecurity in-
7 cident.

8 (iii) Protection against unauthorized
9 access to vital commercial satellite system
10 functions.

11 (iv) Physical protection measures de-
12 signed to reduce the vulnerabilities of a
13 commercial satellite system's command,
14 control, or telemetry receiver systems.

15 (v) Protection against jamming or
16 spoofing.

17 (vi) Security against threats through-
18 out a commercial satellite system's mission
19 lifetime.

20 (vii) Management of supply chain
21 risks that affect the cybersecurity of com-
22 mercial satellite systems.

23 (viii) As appropriate, and as applica-
24 ble pursuant to the requirement under
25 paragraph (1)(b)(ii) (relating to the clear-

1 inghouse containing current, relevant, and
2 publicly available commercial satellite sys-
3 tem cybersecurity resources), the findings
4 and recommendations from the study con-
5 ducted by the Comptroller General of the
6 United States under subsection (a)(1).

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

11 (3) IMPLEMENTATION.—In implementing this
12 subsection, the Director shall—

13 (A) to the extent practicable, carry out
14 such implementation as a public-private part-
15 nership;

16 (B) coordinate with the heads of appro-
17 priate Federal agencies with expertise and expe-
18 rience in satellite operations, including the enti-
19 ties described in subsection (a)(3); and

20 (C) consult with non-Federal entities devel-
21 oping commercial satellite systems or otherwise
22 supporting the cybersecurity of commercial sat-
23 ellite systems, including private, consensus or-
24 ganizations that develop relevant standards.

25 (c) DEFINITIONS.—In this section:

1 (1) CLEARINGHOUSE.—The term “clearing-
2 house” means the commercial satellite system cyber-
3 security clearinghouse required to be developed and
4 maintained under subsection (b)(1).

5 (2) COMMERCIAL SATELLITE SYSTEM.—The
6 term “commercial satellite system” means an earth
7 satellite owned and operated by a non-Federal enti-
8 ty.

9 (3) CRITICAL INFRASTRUCTURE.—The term
10 “critical infrastructure” has the meaning given such
11 term in section 1016(e) of Public Law 107–56 (42
12 U.S.C. 5195c(e)).

13 (4) CYBERSECURITY RISK.—The term “cyberse-
14 curity risk” has the meaning given such term in sec-
15 tion 2209 of the Homeland Security Act of 2002 (6
16 U.S.C. 659).

17 (5) CYBERSECURITY THREAT.—The term “cy-
18 bersecurity threat” has the meaning given such term
19 in section 102 of the Cybersecurity Information
20 Sharing Act of 2015 (6 U.S.C. 1501).

21 (6) DIRECTOR.—The term “Director” means
22 the Director of the Cybersecurity and Infrastructure
23 Security Agency.

24 (7) SMALL BUSINESS CONCERN.—The term
25 “small business concern” has the meaning given the

1 term in section 3 of the Small Business Act (15
2 U.S.C. 632).

○