

119TH CONGRESS
2D SESSION

S. 4693

To require the Secretary of Defense to carry out an operational pilot program under the Hybrid Space Architecture initiative to evaluate the use of commercially available orbital data center services and space-based cloud computing capabilities relevant to national security space and joint mission requirements, and for other purposes.

IN THE SENATE OF THE UNITED STATES

JUNE 4, 2026

Mr. CRUZ (for himself and Mr. HICKENLOOPER) introduced the following bill;
which was read twice and referred to the Committee on Armed Services

A BILL

To require the Secretary of Defense to carry out an operational pilot program under the Hybrid Space Architecture initiative to evaluate the use of commercially available orbital data center services and space-based cloud computing capabilities relevant to national security space and joint mission requirements, 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 “Nodes, Enterprise
5 Workloads, and Hybrid Operations, Resilience, Integra-

1 tion, Zero-Trust, Orbital Networks Act” or the “NEW
2 HORIZON Act”.

3 **SEC. 2. OPERATIONAL PILOT PROGRAM ON ORBITAL DATA**
4 **CENTER SERVICES.**

5 (a) FINDINGS.—Congress makes the following find-
6 ings:

7 (1) Modern national security space missions
8 generate increasing volumes of data from space-
9 based sensors, platforms, and constellations, placing
10 growing demands on terrestrial data transport, proc-
11 essing, and analysis infrastructure.

12 (2) Reliance on ground-based data processing
13 can introduce latency, bandwidth constraints, and
14 vulnerabilities that may degrade the timeliness, resil-
15 ience, and effectiveness of military and intelligence
16 operations in contested environments.

17 (3) Commercial industry is developing orbital
18 data center and space-based cloud computing capa-
19 bilities that enable in-space data processing, storage,
20 and analytics, which may reduce latency, enhance re-
21 silience, and improve mission outcomes.

22 (4) The Department of Defense has identified
23 the need for hybrid architectures that integrate
24 space, terrestrial, and commercial capabilities to
25 support joint and national security missions.

1 (5) An operational pilot program is necessary to
2 evaluate the military utility, operational integration,
3 and transition potential of orbital data center serv-
4 ices through real-world mission use cases before any
5 broader adoption or sustained acquisition.

6 (6) Maintaining a competitive and resilient do-
7 mestic industrial base for orbital infrastructure, in-
8 cluding satellite platforms, communications systems,
9 and in-space computing capabilities, is important to
10 accelerating innovation and supporting operational
11 resilience.

12 (b) PILOT PROGRAM.—

13 (1) IN GENERAL.—Not later than 1 year after
14 the date of the enactment of this Act, the Secretary
15 of Defense (referred to in this Act as the “Sec-
16 retary”), acting through the Director of the Defense
17 Innovation Unit, shall carry out an operational pilot
18 program under the Hybrid Space Architecture initia-
19 tive to evaluate the use of commercially available or-
20 bital data center services and space-based cloud
21 computing capabilities relevant to national security
22 space and joint mission requirements.

23 (2) PURPOSES.—The purposes of the pilot pro-
24 gram shall be—

1 (A) to assess the military utility of orbital
2 data center and space-based cloud computing
3 services;

4 (B) to evaluate the operational integration
5 of such services into existing and planned De-
6 partment of Defense space and joint architec-
7 tures;

8 (C) to examine the resilience, latency, secu-
9 rity, and mission assurance benefits of in-space
10 data processing;

11 (D) to inform the potential transition of
12 such services into sustained programs of record
13 or operational use;

14 (E) to evaluate concepts of operations for
15 the protection and defense of orbital data cen-
16 ter assets against kinetic, nonkinetic, and cyber
17 threats;

18 (F) to assess the asset protection strate-
19 gies and vulnerabilities of orbital data center in-
20 frastructure; and

21 (G) to evaluate the integration and oper-
22 ational performance of interoperable, commer-
23 cially provided orbital infrastructure compo-
24 nents sourced from multiple vendors across the
25 hybrid space architecture ecosystem.

1 (3) SCOPE.—In carrying out the pilot program,
2 the Secretary may—

3 (A) employ commercially available orbital
4 data center services in support of real-world
5 mission scenarios, including intelligence, space
6 domain awareness, command and control, data
7 transport, and other national security applica-
8 tions;

9 (B) conduct testing, demonstration, and
10 limited operational employment necessary to as-
11 sess technical performance and operational via-
12 bility; and

13 (C) support integration activities required
14 to evaluate interoperability with the Depart-
15 ment of Defense’s space, ground, and network
16 systems.

17 (4) ACQUISITION AUTHORITY.—The Secretary
18 shall encourage competitive participation from a di-
19 verse set of nontraditional defense contractors and
20 commercial space providers.

21 (5) SECURITY AND RESILIENCE MEASURES FOR
22 SENSITIVE AND CLASSIFIED INFORMATION.—In car-
23 rying out the pilot program, the Secretary shall en-
24 sure that any orbital data center services used to

1 process, store, or transmit sensitive or classified in-
2 formation have in place—

3 (A) cybersecurity protections, including
4 zero-trust architecture, encryption, identity and
5 access management, continuous monitoring, and
6 protections against insider threats;

7 (B) risk-management measures—

8 (i) to address supply chain
9 vulnerabilities and foreign ownership, con-
10 trol, or influence; and

11 (ii) that achieve compliance with ap-
12 plicable Department of Defense cybersecu-
13 rity and authorization requirements;

14 (C) resilience and mission assurance capa-
15 bilities, including redundancy, failover, oper-
16 ation in degraded or contested environments,
17 and rapid reconstitution or replacement capa-
18 bilities;

19 (D) protections against cyber, electronic
20 warfare, counterspace, and other nonkinetic
21 threats;

22 (E) secure telemetry, tracking, and com-
23 mand links and associated command-and-con-
24 trol systems, including authenticated command
25 uplinks, encrypted telemetry and data links,

1 anti-spoofing and anti-jamming protections, re-
2 silient cryptographic key management, pro-
3 tected timing and navigation inputs, and secure
4 software and firmware update mechanisms;

5 (F) protections for associated ground sys-
6 tems, mission operations centers, terrestrial
7 network connections, software supply chains,
8 and user access interfaces, including segmenta-
9 tion, continuous monitoring, access controls,
10 encryption, and resilience against cyber intru-
11 sion, disruption, and unauthorized access; and

12 (G) protections to ensure workload isola-
13 tion, tenant separation, and data sovereignty
14 for sensitive or classified information processed,
15 stored, or transmitted through orbital data cen-
16 ter services, including safeguards against unau-
17 thorized cross-tenant, cross-domain, or provider
18 access.

19 (6) INTEGRATION AND INTEROPERABILITY.—

20 The Secretary shall ensure that any orbital data
21 center services evaluated under the pilot program
22 are interoperable with existing Department of De-
23 fense command, control, communications, and intel-
24 ligence systems.

1 (7) CONSULTATION.—In carrying out the pilot
2 program, the Secretary, acting through the Director
3 of the Defense Innovation Unit, shall consult with—

4 (A) the Assistant Secretary of Defense for
5 Space Policy;

6 (B) service acquisition executives (as de-
7 fined in section 101 of title 10, United States
8 Code);

9 (C) the Space Force and other military de-
10 partments with potential operational interest or
11 transition pathways;

12 (D) the National Reconnaissance Office;

13 (E) the National Geospatial-Intelligence
14 Agency; and

15 (F) such other individuals and organiza-
16 tions as the Secretary considers appropriate.

17 (8) BRIEFING.—Not later than December 31,
18 2028, the Secretary shall provide the congressional
19 defense committees (as defined in section 101 of
20 title 10, United States Code) with a briefing on—

21 (A) execution of the pilot program;

22 (B) operational use cases evaluated;

23 (C) lessons learned from operational em-
24 ployment;

1 (D) recommendations regarding future ac-
2 quisition or operational use of orbital data cen-
3 ter services;

4 (E) cybersecurity risks, insider threat
5 vulnerabilities, and mitigation measures;

6 (F) resilience against counterspace threats
7 and contested space environments;

8 (G) commercial provider risks, including
9 supply chain and foreign ownership concerns;
10 and

11 (H) recommendations for security, resil-
12 ience, and acquisition requirements for any fu-
13 ture program of record.

14 (c) TERMINATION.—The authority to carry out the
15 pilot program under this section shall terminate on the
16 date that is five years after the date of the enactment of
17 this Act.

18 (d) ORBITAL DATA CENTER DEFINED.—In this sec-
19 tion, the term “orbital data center” means a space-based
20 computing, data storage, or networking capability, includ-
21 ing 1 or more spacecraft, hosted payloads, or distributed
22 orbital architectures, designed primarily to provide per-
23 sistent, scalable, or shared in-orbit processing, analysis,
24 storage, fusion, routing, or dissemination of data as a dis-
25 tinct operational capability, rather than as a function an-

1 cillary to the primary mission of a spacecraft, prior to
2 transmission to terrestrial or other external infrastruc-
3 ture, including to reduce latency, mitigate bandwidth con-
4 straints, improve operational resilience, or support time-
5 sensitive missions.

○