119TH CONGRESS
2D SESSION

S. _____

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

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

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.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the ''Nodes, Enterprise Workloads, and Hybrid Operations, Resilience, Integra-

tion, Zero-Trust, Orbital Networks Act'' or ''NEW HORIZON Act''.

SEC. 2. OPERATIONAL PILOT PROGRAM ON ORBITAL DATA CENTER SERVICES.

(a) FINDINGS.—Congress makes the following findings:

(1) Modern national security space missions generate increasing volumes of data from space-based sensors, platforms, and constellations, placing growing demands on terrestrial data transport, processing, and analysis infrastructure.

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

(3) Commercial industry is developing orbital data center and space-based cloud computing capabilities that enable in-space data processing, storage, and analytics, which may reduce latency, enhance resilience, and improve mission outcomes.

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

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

(6) Maintaining a competitive and resilient domestic industrial base for orbital infrastructure, including satellite platforms, communications systems, and in-space computing capabilities, is important to accelerating innovation and supporting operational resilience.

(b) PILOT PROGRAM.—

(1) IN GENERAL.—Not later than 1 year after the date of the enactment of this Act, the Secretary of Defense (referred to in this Act as the ''Secretary''), acting through the Director of the Defense Innovation Unit, shall 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.

(2) PURPOSES.—The purposes of the pilot program shall be—

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

(B) to evaluate the operational integration of such services into existing and planned Department of Defense space and joint architectures;

(C) to examine the resilience, latency, security, and mission assurance benefits of in-space data processing;

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

(E) to evaluate concepts of operations for the protection and defense of orbital data center assets against kinetic, nonkinetic, and cyber threats;

(F) to assess the asset protection strategies and vulnerabilities of orbital data center infrastructure; and

(G) to evaluate the integration and operational performance of interoperable, commercially provided orbital infrastructure components sourced from multiple vendors across the hybrid space architecture ecosystem.

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

(A) employ commercially available orbital data center services in support of real-world mission scenarios, including intelligence, space domain awareness, command and control, data transport, and other national security applications;

(B) conduct testing, demonstration, and limited operational employment necessary to assess technical performance and operational viability; and

(C) support integration activities required to evaluate interoperability with the Department of Defense's space, ground, and network systems.

(4) ACQUISITION AUTHORITY.—The Secretary shall encourage competitive participation from a diverse set of nontraditional defense contractors and commercial space providers .

(5) SECURITY AND RESILIENCE MEASURES FOR SENSITIVE AND CLASSIFIED INFORMATION.—In carrying out the pilot program, the Secretary shall ensure that any orbital data center services used to

process, store, or transmit sensitive or classified information have in place—

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

(B) risk-management measures—

(i) to address supply chain vulnerabilities and foreign ownership, control, or influence; and

(ii) that achieve compliance with applicable Department of Defense cybersecurity and authorization requirements;

(C) resilience and mission assurance capabilities, including redundancy, failover, operation in degraded or contested environments, and rapid reconstitution or replacement capabilities;

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

(E) secure telemetry, tracking, and command links and associated command-and-control systems, including authenticated command uplinks, encrypted telemetry and data links,

anti-spoofing and anti-jamming protections, resilient cryptographic key management, protected timing and navigation inputs, and secure software and firmware update mechanisms;

(F) protections for associated ground systems, mission operations centers, terrestrial network connections, software supply chains, and user access interfaces, including segmentation, continuous monitoring, access controls, encryption, and resilience against cyber intrusion, disruption, and unauthorized access; and

(G) protections to ensure workload isolation, tenant separation, and data sovereignty for sensitive or classified information processed, stored, or transmitted through orbital data center services, including safeguards against unauthorized cross-tenant, cross-domain, or provider access.

(6) INTEGRATION AND INTEROPERABILITY.—The Secretary shall ensure that any orbital data center services evaluated under the pilot program are interoperable with existing Department of Defense command, control, communications, and intelligence systems.

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

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

(B) service acquisition executives (as defined in section 101 of title 10, United States Code);

(C) the Space Force and other military departments with potential operational interest or transition pathways;

(D) the National Reconnaissance Office;

(E) the National Geospatial-Intelligence Agency; and

(F) such other individuals and organizations as the Secretary considers appropriate.

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

(A) execution of the pilot program;

(B) operational use cases evaluated;

(C) lessons learned from operational employment;

(D) recommendations regarding future acquisition or operational use of orbital data center services;

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

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

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

(H) recommendations for security, resilience, and acquisition requirements for any future program of record.

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

(d) ORBITAL DATA CENTER DEFINED.—In this section, the term ''orbital data center'' means a space-based computing, data storage, or networking capability, including 1 or more spacecraft, hosted payloads, or distributed orbital architectures, designed primarily to provide persistent, scalable, or shared in-orbit processing, analysis, storage, fusion, routing, or dissemination of data as a distinct operational capability, rather than as a function an-

cillary to the primary mission of a spacecraft, prior to transmission to terrestrial or other external infrastructure, including to reduce latency, mitigate bandwidth constraints, improve operational resilience, or support time-sensitive missions.