Congress Introduces Legislation for Orbital Data Centers: Analyzing the Cruz–Hickenlooper NEW HORIZON Act

June 12, 2026

Senator Ted Cruz, joined by Senator John Hickenlooper, has introduced the Nodes, Enterprise Workloads, and Hybrid Operations, Resilience, Integration, Zero-Trust, Orbital Networks Act (the "NEW HORIZON Act"). The Act would, for the first time, statutorily direct the Department of Defense ("DoD") to operationally evaluate commercially available orbital data center services and space-based cloud computing capabilities. While the bill is modest in length, its implications for the commercial space industry are anything but. It signals that Congress now views in-orbit computing not as a speculative technology, but as prospective national security infrastructure.

What the Bill Is

The NEW HORIZON Act is a pilot program authorization. It directs the Secretary of Defense, acting through the Director of the Defense Innovation Unit ("DIU"), to carry out an operational pilot program under the existing Hybrid Space Architecture initiative within one year of enactment. The program's mandate is to evaluate the use of commercially available orbital data center services relevant to national security space and joint mission requirements, with the authority sunsetting five years after enactment.

The congressional findings underpinning the bill articulate a problem the industry has long understood: modern national security space missions generate ever-increasing volumes of sensor and platform data, while reliance on ground-based processing introduces latency, bandwidth constraints, and vulnerabilities that degrade operational effectiveness in contested environments. Congress finds that commercial industry is developing the in-space processing, storage, and analytics capabilities that may resolve this bottleneck and an operational pilot is necessary to test military utility through real-world mission use cases before any broader adoption or sustained acquisition.

Notably, the bill also supplies a statutory definition for orbital data centers, something the sector has lacked. An "orbital data center" is defined as a space-based computing, data storage, or networking capability — whether a single spacecraft, hosted payload, or distributed orbital architecture — designed primarily to provide persistent, scalable, or shared in-orbit processing as a distinct operational capability, rather than as a function ancillary to a spacecraft's primary mission. That distinction between dedicated capability and ancillary function will matter considerably as agencies, insurers, and contracting parties begin referencing the term.

What the Bill Outlines

The pilot program is built around seven enumerated purposes, spanning the assessment of military utility, operational integration into existing and planned DoD architectures, and the resilience, latency, security, and mission assurance benefits of in-space data processing. Two purposes warrant particular attention. First, the program must evaluate concepts of operations for the protection and defense of orbital data center assets against kinetic, non-kinetic, and cyber threats. This is an ostensible acknowledgment from the DoD that commercial compute infrastructure in orbit may become

a target. Second, it must evaluate interoperable, commercially provided infrastructure sourced from multiple vendors, a clear congressional preference against single-provider lock-in.

In scope, the Secretary may employ commercial orbital data center services in support of real-world mission scenarios — including intelligence, space domain awareness, command and control, and data transport — and may conduct testing, demonstration, and limited operational employment. The Secretary is directed to encourage competitive participation from non-traditional defense contractors and commercial space providers.

The most consequential provisions for industry are the security requirements. Any orbital data center service processing, storing, or transmitting sensitive or classified information must implement zero-trust architecture, encryption, identity and access management, and insider threat protections; risk-management measures addressing supply chain vulnerabilities and foreign ownership, control, or influence ("FOCI"); redundancy, failover, and rapid reconstitution capabilities; secured telemetry, tracking, and command links with anti-spoofing and anti-jamming protections; hardened ground segments and software supply chains; and workload isolation, tenant separation, and data sovereignty safeguards against cross-tenant or provider access.

The Secretary must consult with the Assistant Secretary of Defense for Space Policy, the service acquisition executives, the Space Force, the National Reconnaissance Office, and the National Geospatial-Intelligence Agency, and must brief the congressional defense committees by December 31, 2028, including recommendations regarding future acquisition and the security requirements for any future program of record.

What It Could Mean for the Industry

For commercial operators, the bill is a door and a filter. The

door is that DIU becomes a statutory front-of-house for orbital compute providers, with congressional direction to draw in non-traditional contractors and an explicit pathway toward programs of record. Whereas the filter is that the security provisions will function as de facto market standards. Providers whose architectures cannot demonstrate zero-trust compliance, FOCI-clean supply chains, and verifiable tenant separation will be structurally excluded from the defense market and, given the gravitational pull of defense requirements on commercial contracting, likely disadvantaged in adjacent commercial markets as well.

Counsel advising orbital infrastructure companies should treat the bill as a compliance roadmap now, not upon enactment. Capital structures should be reviewed for FOCI exposure, vendor agreements for supply chain attestations, and service-level architectures for the isolation and reconstitution capabilities Congress has signaled it expects. The NEW HORIZON Act is a pilot but, in defense acquisition, pilots are how markets are made.

Author: Abdulla Abuwasel
Title: Partner – Transactions
Email: awasel@waselandwasel.com
Profile:
https://waselandwasel.com/about/abdulla-abuwasel/

Lawyers and consultants.
Tier-1 services since 1799.
www.waselandwasel.com
business@waselandwasel.com