

The FAA Joins the Global Air Taxi Race: New Rules for eVTOLs and Supersonic Flight by 2027

July 28, 2026

At the Farnborough Airshow on 21 July 2026, the FAA announced that it would move to certify electric air taxis, civil supersonic aircraft, expanded drone operations, and commercial space launches, and that it would avoid being “too prescriptive” and let industry drive innovation.

Since 1973, 14 CFR § 91.817 has prohibited operating a civil aircraft over the United States above true Mach 1 speed. The only exception is a Special Flight Authorization for research and testing in isolated areas. The rule sits on the FAA’s noise authority at 49 U.S.C. § 44715 and safety authority at § 44701. The FAA adopted it because the sonic boom measurement and mitigation technology of the era could not control overpressure at the source, so the FAA instead banned the speed outright.

Concorde is the most infamous example which absorbed the cost as the Anglo-French airliner entered service in 1976 and cruised at Mach 2, but § 91.817 forced it subsonic over US land. That confined the Concorde to transatlantic routes, and only London to New York turned a consistent profit. Fuel burn, the fatal 2000 Air France crash, and collapsing demand after 2001 resulted in the fleet’s retirement in 2003. No civil supersonic aircraft has carried a paying passenger since.

The reversal began in June 2025 with Executive Order 14304, titled “Leading the World in Supersonic Flight,” directing the

FAA to repeal the overland prohibition within 180 days, set an interim noise-based certification standard, and revise § 91.818. The FAA issued the notice of proposed rulemaking “Enabling Supersonic Overland Flight” (Docket FAA-2026-6935) in the Federal Register on 2 July 2026, replacing the Mach-based ban with a performance standard. The FAA targets final rules, including a companion takeoff and landing noise rule, by mid-2027.

Under the Administrative Procedure Act, the FAA may repeal its own rule through notices and comment provided it gives a reasoned explanation for abandoning the premises that justified it. The record does that, citing advancements in boom-shaping and acoustic modeling since 1973. The House passed the Supersonic Aviation Modernization Act (H.R. 3410) in March 2026; Senate passage would codify the standard and remove the deference exposure left by Loper Bright.

Air taxis follow the same method. Electric vertical takeoff and landing aircraft (“eVTOLs”), functioning as a quiet, green hybrid between a helicopter and a small plane, are certified as a special class; the FAA’s integration pilot programme, launched in March 2026, now covers eight companies across 26 states and is generating the data certification and community acceptance required for nationwide eVTOLS. The commercial value for these aircraft is the routes that they make possible: short intra-city flights for the air taxis, and long city-to-city routes for the supersonic jets. The most illustrative example is New York to Los Angeles; overland supersonic flights could cover the route in under two and a half hours, whereas Concorde never could because of the 1973 ban.

The air taxi and supersonic rules are not separate developments. Taken together, they show the FAA building a single framework for point-to-point travel via short vertical flights within cities, supersonic flights between them, and eventually suborbital launches between distant points, which

the FAA's Office of Commercial Space Transportation already licenses under 51 U.S.C. chapter 509. All three rely on the same shift. Instead of banning the category of flight outright, the FAA sets a measurable limit on noise, safety, and sonic boom overpressure and clears any operator who meets it. If the FAA keeps that approach in its 2027 final rules, it becomes the certification model for point-to-point transportation for the next decade.

The race is already global and running rapidly. China's EHang holds the world's first eVTOL type certificate and has carried paying passengers on its autonomous EH216-S in Guangzhou and Hefei, adding a Shenzhen to Hong Kong route in January 2026. The UAE granted Joby Aviation a six-year exclusive with Dubai's Road and Transport Authority and Archer have a parallel Abu Dhabi program, both targeting commercial service in late 2026 or early 2027. The UK is slower but deliberate with the Civil Aviation Authority targeting initial commercial passenger eVTOL flights by end-2028 or early 2029. For operators and investors, the optimal route is pursuing certification in the jurisdiction offering the most expeditious pathway, accumulating a demonstrable operational record, and leveraging that record within the US framework as the FAA finalizes its rules by mid-2027. The variable to watch is which standard each regulator adopts and whether there is reciprocal recognition of another authority's approvals.

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

China's Space Momentum: The Long March 10B Catch, a State-Curated Consortium, and a Bifurcating Market

July 28, 2026

On 10 July 2026, China became only the second nation, after the United States, to recover an orbital-class booster under control, and the first anywhere to do so with a net rather than landing legs. The state-owned China Academy of Launch Vehicle Technology intends to re-fly the same stage before year's end.

The engineering is novel, but the more consequential story is legal and commercial. Reusability is the mechanism through which SpaceX collapsed launch costs and captured most of the world's orbital launches. Net capture removes landing-leg mass from the vehicle and shifts it to the recovery infrastructure, freeing payload and, if it scales, lowering cost per kilogram. A credible second source of low-cost, high-cadence launch would cause ripples across the commercial launch market.

A state-curated commercial base

The timing of the booster is not coincidental. On 1 July 2026, a body under the China State Administration of Science, Technology and Industry for National Defense published the membership of the national commercial space consortium established at China's Space Day in April 2025. The roster runs to 271 vetted entities across nine groups, from launch and satellite manufacturing to ground segment and financial services. Because membership followed voluntary application and deliberate vetting, the list functions as a signal of

which players the state treats as serious and which domains it intends to back: direct-to-device and non-terrestrial networks as a full value chain, commercial human spaceflight, hypersonic spaceplanes, and orbital compute.

The membership captures the state-commercial hybrid that defines Chinese “new space,” pairing state-linked launch arms with venture-backed firms that have independently reached orbit, alongside satellite operators. Whilst officially a coordination mechanism for policy, standards, and supply-demand matching, China has not yet enacted a dedicated national space law and thus the consortium, paired with China National Space Administration’s November 2025 action plan on commercial space, operates as an interim instrument for steering the sector and curating its industrial base. For counterparties, it also clarifies which Chinese entities are established, state-endorsed, and, almost uniformly, dual-use.

Two blocs, two legal regimes

The same rocket technology that is used by the Long March 10B supports the Long March 10A, the vehicle designed to carry China’s crew spacecraft and lander to the Moon before 2030 and eventually to the International Lunar Research Station (“ILRS”). The ILRS, led by China and Russia, is the rival to the U.S.-led Artemis Accords. It has become a real consortium, drawing in about seventeen countries and international organizations and more than fifty research institutions, including Pakistan, the UAE, Senegal, Venezuela, and Turkey. The Artemis Accords, by comparison, have sixty-six signatories. Two camps are taking shape, each with its own rockets, partners, and view of the law.

Export control is the force consolidating them. The Wolf Amendment bars NASA from bilateral cooperation with China, while International Traffic in Arms Regulations and the Export Administration Regulations restrict the flow of launch, satellite, and component technology, turning bloc affiliation

into a threshold commercial decision. Entities wishing to work across both, as several Gulf states presently do, face a genuine compliance tightrope, sharpened by the dual-use character of the newly named Chinese consortium. Critically, Artemis and ILRS advance competing interpretations of the Outer Space Treaty's non-appropriation principle, of "safety zones," and of resource-utilization rights that China will begin to test in 2028.

The takeaway

China's momentum is compounding vis-à-vis a recovered booster, a crewed lunar architecture behind it, and a state-curated commercial base beneath it. The result is a structurally bifurcated market in which launch access, partnership eligibility, financing, insurance, and dispute resolution increasingly depend on which side of an export-control line a venture sits. For governments building space agencies and corporations structuring cross-border ventures, the decisive questions have become substantial questions of law.

Author: Abdulla Abuwaseel

Title: Partner – Transactions

Email: awaseel@waselandwaseel.com

Profile:

<https://waselandwaseel.com/about/abdulla-abuwaseel/>

Lawyers and consultants.

Tier-1 services since 1799.

www.waselandwaseel.com

business@waselandwaseel.com

From Part 25 to Part 100: The FCC's Space Licensing Overhaul Reaches Its Decisive

Stage

July 28, 2026

On 1 July 2026, the Federal Communications Commission (“FCC”) released the tentative agenda for the FCC’s Open Meeting scheduled for 22 July 2026. Among the items is *Space Modernization for the 21st Century* (SB Docket No. 25-306), a Report and Order and Further Notice of Proposed Rulemaking (“FNPRM”) that would overhaul how the FCC licenses space and earth stations. The centerpiece is a proposal to sunset Part 25 of the FCC’s rules and replace it with an entirely new rule part, Part 100, built around what the FCC calls a “licensing assembly line.”

This is the resolution stage of a proceeding that opened in October 2025. The FCC adopted the underlying Notice of Proposed Rulemaking (“NPRM”), designated FCC 25,69, on 28 October 2025; comments closed on 20 January 2026 and reply comments on 18 February 2026. The 22 July item would convert those proposals into binding rules, while the accompanying Further Notice seeks comment on additional changes that build on the new Part 100. If adopted, it would represent the most significant restructuring of US commercial space licensing in decades.

The Current Framework: Part 25 Under Strain

Part 25, titled “Satellite Communications,” has governed satellite and earth station licensing for decades. It sits within Subchapter B (Common Carrier Services) and has been revised repeatedly and piecemeal as the industry evolved. Its architecture reflects an earlier era: a small field of largely quasi-governmental, geostationary orbit (“GSO”) operators, reviewed through narrative-heavy, discretionary, case-by-case adjudication.

That model has struggled to scale with the industry. The FCC received circa 290 space station applications and circa 2,680 earth station applications in 2024, compared with 124 and 974 respectively in 2016, tracking a more than ten-fold rise in objects launched into orbit over the past decade. In conjunction, applications have grown more complex and non-traditional, spanning large non-geostationary orbit constellations (“NGSO”), direct-to-device services, Earth observation, in-space servicing, and lunar missions that fit awkwardly within the existing taxonomy.

The strain shows up as delay and unpredictability. Timelines for acting on some applications can run to years and staff spend disproportionate resources sifting through non-standardized materials to establish completeness. The subjective requirements produce inconsistent levels of review and frequent back-and-forth between applicants and the FCC. Given the capital-intensive nature of the industry, where financing depends on speed and demonstrated progress, that uncertainty carries real cost.

The Proposed Overhaul: Part 100 and the “Licensing Assembly Line”

The reform is organized around four statutory review concerns the FCC has identified as the proper focus of its public-interest analysis: harmful interference, spectrum efficiency, space safety, and foreign ownership. Everything else in the process is designed to move applications toward a decision on those questions as efficiently as possible.

A new rule part. Part 100 would be titled “Space and Earth Station Services” and relocated to Subchapter D (Safety and Special Radio Services), reflecting that not all licensees are common carriers but all use radio services. It would be organized into four subparts (General; Applications and Licenses; Operational Rules; and Compliance), separating application requirements from operating obligations and

enforcement.

Modular applications and “presumed acceptable” criteria. The assembly line moves applications through three phases: a modular application phase, a processing phase, and a decision phase. Applicants would complete only the modules relevant to their request. For space stations, the FCC proposed condensing requirements into three areas (general applicant information, orbital information, and frequency information) and replacing the current Schedule S with a new Schedule O for orbital data and Schedule F for frequency data on FCC Form 312. The framework shifts from prescriptive design mandates and narrative demonstrations toward standardized, performance-based certifications. Applications certifying compliance with bright-line criteria would be “presumed acceptable,” meaning presumed to serve the public interest, and routed for expedited processing, with defined exceptions reserved for targeted review.

Timelines, conditional grants, and processing rounds. Part 100 would establish review timelines, shorten public notice periods, and permit certain conditional grants so applicants can begin planning earlier. For NGS0 systems, the FCC proposed restructuring processing rounds into annual, band-specific rounds in which co-filers share equal spectrum priority (subject to a sunset), and expanding eligibility for first-come, first-served treatment.

Milestones, bonds, and license terms. The proposal would eliminate milestone requirements for GS0 systems and align NGS0 milestones with International Telecommunication Union benchmarks, including a first-satellite milestone followed by staged deployment obligations. Surety bonds would be removed for GS0 stations and certain NGS0 stations, and milestones simplified. License terms for most space and earth stations would extend to 20 years, and the list of modifications permitted without prior approval would expand.

Earth stations. The framework would shift predominantly to nationwide, non-site-based blanket licensing and introduce a new “[i]mmovable” earth station category modeled on the 70/80/90 GHz site-registration regime, available to fixed stations that certify compliance with bright-line criteria.

Space safety. In exchange for streamlined entry, operators would take on affirmative safety obligations, including sharing ephemeris data with approved space situational awareness services and filing periodic space safety reports.

Implications for Industry

The FCC has openly positioned the reform as a competitiveness strategy, aiming to make the US the destination of choice for licensing and operating space systems as other nations compete for the same investment. The certification-and-presumption model rewards applicants who can map their systems onto bright-line criteria with fast, predictable grants, an advantage for well-advised operators and a meaningful reduction in regulatory latency across the ecosystem.

With that said, the trade-offs merit close attention. A move from discretionary review to bright-line certification shifts risk onto the applicant: certifications carry compliance and enforcement exposure, and the FCC has signaled a robust back end, including automatic termination for failure to meet operational deadlines or milestones, revocation, forfeitures, and penalties for materially false statements. The reform effectively trades front-loaded scrutiny for back-loaded accountability.

The impact is broad, reaching operators, service providers, and manufacturers, and, because it governs US market access, foreign entities seeking to serve or partner in the US. Several issues remain genuinely contested and will shape how favorable the final rules prove in practice. On transition, the FCC proposed applying Part 100’s procedural rules

prospectively to all licensees, including existing ones, while preserving the substantive obligations embedded in current authorizations, and it sought comment on how pending applications would be handled at the effective date. Existing licensees should not assume their current authorizations are fully insulated from the new regime.

What's Next

The 22 July meeting is a consideration date rather than a foregone conclusion; the draft text remains subject to change, and the Report and Order may adopt the NPRM's proposals with modifications informed by the comment record. If adopted, the new rules would take effect following Federal Register publication, with the revised Form 312 schedules also subject to Paperwork Reduction Act review before they can be required. The accompanying Further Notice would open a fresh comment cycle on further refinements built on Part 100, so the proceeding will continue well past July.

For anyone active in, or seeking to enter, the US space sector, the practical steps are assessing how current and planned systems would map onto the presumed-acceptable criteria and modular application structure, evaluating the compliance exposure that comes with a certification-based regime, and monitoring the Further Notice for the next round of proposed changes.

Author: Abdulla Abuwaseel

Title: Partner – Transactions

Email: awaseel@waselandwaseel.com

Profile:

<https://waselandwaseel.com/about/abdulla-abuwaseel/>

Lawyers and consultants.

Tier-1 services since 1799.

www.waselandwaseel.com

business@waselandwaseel.com

Anthropic's Fable 5 Directive: Overnight Export Control Authority and Its Implications for the Commercial Space Industry

July 28, 2026

On the evening of June 12, 2026, Anthropic received a directive from the United States government at 5:21 p.m. Eastern Time. The instruction was unambiguous: suspend all access to Fable 5 and Mythos 5 for any foreign national, whether residing inside or outside the United States, including Anthropic's own employees who are non-U.S. citizens. Within hours, both models went offline for every customer worldwide. No advance notice. No transitional period. No grandfathering of existing contracts. A commercial product generating active revenue was switched off overnight.

The government's stated rationale was the discovery of a jailbreak technique capable of bypassing Fable 5's safeguards and, in particular, those designed to prevent access to the advanced cybersecurity capabilities embedded in Mythos, the underlying frontier model. The directive cited national security authorities but provided no further specifics. Anthropic responded with transparency, publicly noting that its own review of the demonstrated jailbreak found only minor, previously known vulnerabilities discoverable through other publicly available models. The company characterized the shutdown as a misunderstanding and committed to restoring access promptly.

The legal mechanism at work here is not novel. What is

remarkable is its application at this scale and speed to a consumer-facing AI platform.

Legal Architecture

The Export Administration Regulations (“EAR”) have for decades governed the transfer of dual-use technology which are items with both civilian and military applications. Under the EAR, the release of controlled technology or source code to a foreign national within the United States constitutes a deemed export to that person’s home country. This means that domestic access, not merely cross-border transfer, can trigger export control obligations.

The regulatory landscape governing advanced AI specifically has been in considerable flux. In January 2025, the Commerce Department’s Bureau of Industry and Security issued an interim final rule called the Framework for Artificial Intelligence Diffusion. The rule would have introduced new controls and extended U.S. export control jurisdiction to foreign-made items that are the direct product of U.S. technology, regardless of where they are accessed. That rule never took effect and was rescinded on grounds that it was overly bureaucratic, stifled American innovation, and undermined U.S. diplomatic relations. Whilst a replacement rule has yet to be promulgated, the EAR framework, including its longstanding dual-use technology controls and deemed export provisions, remains operative.

What the Fable 5 episode illustrates is that the legal architecture already in place, without any frontier-specific AI rule, is sufficient for the government to suspend access to a commercial AI product overnight. The authority does not depend on a new regulation tailored to AI. It derives from the broad scope of existing national security authorities. The Fable 5 directive is a demonstration of what that authority can do.

A Lesson for Commercial Space Industry

The commercial space industry operates under an analogous, and in some respects more demanding, regulatory framework. Space-related technologies sit at the intersection of the EAR and the International Traffic in Arms Regulations ("ITAR"). The U.S. Munitions List, against which ITAR is enforced, has historically encompassed satellites, launch vehicles, propulsion systems, guidance technologies, and related software.

A commercial space operator providing satellite imagery services, orbital data relay, or launch support to an international customer base is, structurally, in the same position as Anthropic was before June 12. Whilst the service is U.S.-origin technology, it is accessible to foreign nationals and the government retains plenary authority to suspend that access, unilaterally, upon a determination of national security concern.

History has already furnished a sobering illustration of how swiftly that authority can reshape an industry. In the mid-1990s, Hughes Electronics and Loral Space & Communications both faced severe legal consequences after sharing technical analysis with Chinese engineers following the catastrophic failure of Chinese rockets carrying their satellites during launches. The State Department alleged that both companies had transferred sensitive technical data to Chinese engineers without prior government authorization and U.S. officials concluded the data could be used to improve the accuracy and reliability of Chinese ballistic missiles. The charges against Hughes and Boeing Satellite Systems (which had acquired Hughes' satellite division in 2000) were issued in a 2002 letter alleging 123 violations of the Arms Export Control Act and the ITAR. Hughes and Boeing ultimately settled for \$32 million.

The political and regulatory fallout from this instance was

substantial and enduring. Congress enacted a new national defense authorization related act, which transferred jurisdiction over all satellite exports from the Department of Commerce back to the Department of State, placing them squarely under the U.S. Munitions List and the more restrictive ITAR licensing regime. This restructuring remained in force for over a decade, constraining the commercial satellite industry's competitiveness until Congress repealed the relevant provisions in the National Defense Authorization Act for Fiscal Year 2013. Comparably, whilst that episode unfolded over months of investigation, the Fable 5 directive unfolded in hours.

Takeaway

What June 12, 2026, demonstrated is that the U.S. government has both the legal authority and the operational willingness to issue a technology access suspension directive without advance notice, without detailed justification, and without a transitional framework. Moreover, a commercial technology company has no practical mechanism to resist compliance before acting. Anthropic had no meaningful avenue to contest the directive before complying. Its customers had no recourse. Its foreign national employees could not continue working with the affected models.

For commercial space operators, this scenario should prompt an honest inventory of risk. A satellite imagery company serving defense-adjacent customers in mixed-nationality jurisdictions. A launch service provider whose operations involve foreign nationals at mission control. An on-orbit servicing company whose telemetry systems constitute controlled technology. Any of these entities could, upon a government determination, find their operational licenses suspended, their services cut off, and their revenue interrupted with no more notice than Anthropic received. Advanced technology sectors operating at the frontier are, in the eyes of U.S. national security law, custodians of controlled capabilities. The government's

authority to restrict access to those capabilities is broad and immediate, and not dependent on commercial inconvenience. Commercial space companies would be wise to internalize that reality now, before a directive arrives at 5:21 in the afternoon with no advance notice and no specific explanation.

Author: Abdulla Abuwaseel

Title: Partner – Transactions

Email: awaseel@waselandwaseel.com

Profile:

<https://waselandwaseel.com/about/abdulla-abuwaseel/>

Lawyers and consultants.

Tier-1 services since 1799.

www.waselandwaseel.com

business@waselandwaseel.com

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

July 28, 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 sunseting 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 Abuwaseel **Lawyers and consultants.**
Title: Partner – Transactions Tier-1 services since 1799.
Email: awasel@waselandwasel.com www.waselandwasel.com
Profile: business@waselandwasel.com
<https://waselandwasel.com/about/abdulla-abuwaseel/>

Environmental Liability in Commercial Space Launches: Examining the South Texas Mass Tort Case Against SpaceX

July 28, 2026

On April 30, 2026, eighty plaintiffs filed a federal complaint in the U.S. District Court for the Southern District of Texas against Space Exploration Technologies Corp. (“SpaceX”). The case, [*Aguilar et al. v. Space Exploration Technologies Corp., No. 1:26-cv-00485*](#), alleges that repeated Starship launch and landing operations at the Starbase facility in Cameron County have caused structural damage to homes across Port Isabel, South Padre Island, and Laguna Vista. Asserting claims of negligence, gross negligence, and trespass under the exclusive federal jurisdiction of the Commercial Space Launch Act (“CSLA”), the case has the potential to reshape the legal relationship between commercial launch operators and neighboring communities.

The Complaint

The plaintiffs are homeowners residing roughly six to twenty-two miles from Starbase’s launch pads. The complaint alleges

that eleven Starship/Super Heavy test flights between April 2023 and October 2025, together with earlier sub-orbital tests and static firings, subjected their properties to intense acoustic energy. The complaint relies on peer-reviewed research by Brigham Young University scientists whose field measurements during the fifth and sixth test flights recorded maximum unweighted sound levels exceeding a threshold that SpaceX's own assessments and FAA environmental reviews recognize as the onset of structural damage risk. Sonic boom overpressures near and exceeding such a threshold were recorded at the closest locations, which is generally associated with windows shattering and superficial structural damage.

Critically, the complaint draws on SpaceX's own regulatory submissions, including a 2024 corporate statement acknowledging a "gap in data" regarding acoustic prediction for its Raptor engines. The plaintiffs frame this as evidence that SpaceX has been operating at the frontier of acoustic science while conducting the most powerful rocket launches in history, establishing both foreseeability and conscious indifference to risk.

Legal Claims and Statutory Framework

The complaint asserts three causes of action. First, the negligence claim alleges that SpaceX failed to conduct adequate pre- and post-launch studies and proceeded despite a high likelihood of property damage. Second, the gross negligence claim seeks exemplary damages, arguing that SpaceX had actual awareness of acoustic risks, especially after the inaugural April 2023 test destroyed its own launch pad, yet continued with conscious indifference. Lastly, the trespass claim contends that SpaceX intentionally caused acoustic energy to enter the plaintiffs' properties without consent, resulting in physical harm.

Jurisdiction rests on 51 U.S.C. § 50914(g), which grants

federal courts exclusive jurisdiction over third-party property damage claims arising from licensed launch activities. This provision confirms that the CSLA contemplates such suits but does not immunize the licensee. SpaceX is required under the statute to carry up to \$500 million in third-party liability insurance, and the FAA's 2022 environmental assessment explicitly stated that SpaceX would be responsible for resolving structural damages caused by sonic booms.

Potential Legal Consequences

The outcome will turn on causation: whether the plaintiffs can demonstrate that launch-generated acoustic energy, rather than pre-existing deficiencies or other factors, caused their alleged damages. The complaint does not itemize specific harm to each property, which will demand expert engineering and acoustic testimony. SpaceX may challenge the causal link and argue for regulatory compliance.

However, regulatory compliance is not typically a complete defense to tort claims under Texas law; an FAA launch license does not, by itself, insulate a licensee from negligence or trespass liability. The gross negligence claim, if successful, could expose SpaceX to exemplary damages well beyond compensatory relief. The plaintiffs' strategy of grounding their case in SpaceX's own admissions and peer-reviewed acoustic data gives it a scientific credibility that may prove difficult to overcome at summary judgment.

Industry Implications

The ripple effects of this case will likely extend well beyond South Texas. The FAA authorized up to 25 Starship launches per year from Boca Chica in 2025, and similar acoustic concerns have been flagged at Cape Canaveral, Florida, where SpaceX is building another Starship launch site. A substantial damages award or a judicially imposed constraint could prompt a

reassessment of how launch site proximity to residential communities is evaluated during environmental review.

The case also exposes a gap in the CSLA framework: while the statute requires insurance and channels claims to federal court, it does not establish a dedicated compensation mechanism for communities chronically affected by launch operations (e.g., like airport regimes or military installations). As vehicles grow more powerful and cadences increase, policymakers may need to reconsider whether this framework adequately balances interest in space access with the existing property rights of neighboring populations. For operators planning new or expanded sites, this lawsuit is a timely reminder to integrate acoustic modeling and community engagement from the outset.

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

Civilian Space Facilities in an Era of Armed Conflict: Dual Use Military Targets

July 28, 2026

The strikes conducted against the IRGC Aerospace Force Headquarters in Tehran in March 2026, followed days later by the bombing of a building at the Iran University of Science and Technology (“IUST”) on March 28, have introduced a crucial question for the global commercial space industry: at what

point does a civilian aerospace facility lose the protection its designation is understood to afford it?

The answer, as these events demonstrate, carries direct and immediate consequences for every private company, university research program, and commercial operator that shares infrastructure, personnel, or technology with a state-affiliated space program operating in a contested geopolitical environment.

The justification advanced for the Aerospace Headquarters strike was that the facility served simultaneously as a research center for civilian satellite operations and as a command-and-control node for military satellite programs, including those assessed to have provided surveillance and intelligence capabilities over a wide regional theater. The core assertion was function, not designation. Whether or not one accepts that characterization, the doctrinal logic underlying it is well-established: a facility's protected status under international law is determined by what it does, not by how it is labeled. The moment a civilian asset makes an effective contribution to military action and its destruction offers a definite military advantage, its civilian character becomes legally contestable.

The IUST situation is more layered and, for the international academic and commercial space community, more immediately concerning. Founded in 1929 as Iran's first institution to train engineers, IUST is a ranked technical university with thousands of students across dozens of fields of engineering and science; an institution whose civilian educational mission is not in reasonable dispute. Yet, the IUST faculty have conducted research with direct applications for unmanned aerial vehicles and, in 2022, the Japanese government listed the university as an entity of concern for proliferation relating to missiles and nuclear weapons. More concretely, the Zafar satellite project was developed by IUST in direct partnership with the Iranian Space Agency, a joint venture

that exemplifies the close collaboration between Iran's academic institutions and its governmental space bodies.

This is the dual-use problem made operational and inescapable. The same department that produces graduate engineers for a country's commercial aerospace sector also advances propulsion and systems research that feeds its state satellite program. The same laboratory that publishes peer-reviewed papers on orbital mechanics may contribute to launch vehicle development whose applications extend well beyond scientific inquiry. Civilian designation, in this context, functions as a starting presumption, rather than a permanent shield once thought to have existed.

The Chamran-1 satellite, launched in 2024 and developed at facilities that have since been destroyed, was characterized as a research and technology demonstration mission. The distinction between a research asset and an operational intelligence platform, it turns out, was one of framing rather than function. That gap, between what a facility or satellite is called and what it materially enables, is precisely where the commercial space industry's legal exposure now lives.

The consequences are significant and practical. Export control regimes, from the U.S. International Traffic in Arms Regulations to the EU Dual-Use Regulation, already require licensing determinations that assess whether a given technology could serve military ends in the hands of the recipient state or institution. What the current conflict has demonstrated is that the same analysis must now be applied at the facility and institutional level. A ground station that processes both civilian and military satellite telemetry, a university department that collaborates with both private launch operators and a state defense ministry, and a space research center that hosts both commercial payload integration and command-and-control infrastructure for a state constellation are all, under the targeting logic now being applied in practice, facilities whose protected status is

genuinely uncertain.

For commercial operators with supply chains, personnel exchanges, or data-sharing arrangements that touch state-affiliated aerospace programs in conflict-prone jurisdictions, the exposure is a test. Insurance underwriters are already reviewing war-risk exclusion clauses in light of the recent strikes. Technology transfer counterparties face renewed scrutiny from export control authorities examining whether components supplied to ostensibly civilian programs ultimately served infrastructure now treated as a military objective. Foreign academic institutions that maintained research partnerships with IUST, a university that appears in multiple government proliferation-concern registries while simultaneously ranking among the top technical universities in Asia, now confront the uncomfortable possibility that their cooperation agreements linked them, however indirectly, to infrastructure that has been bombed.

The lesson the commercial space industry must draw from March 2026 is this: civilian designation is not self-executing. It must be earned, maintained, and verifiable through a facility's actual function, not merely its stated purpose. In a conflict environment where space is an active warfighting domain and dual-use infrastructure is a recognized and contested military objective, the burden of demonstrating civilian character has, in practice, shifted toward the operator. Companies, universities, and research institutions that have not yet audited their institutional relationships with state-affiliated space programs should do so now as a matter of legal caution and institutional survival.

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

Geopolitical Tensions and Force Majeure in the Commercial Space Economy

July 28, 2026

The commercial space industry operates at the precise intersection of private enterprise and state sovereignty. It is therefore uniquely vulnerable when those sovereignties come into direct conflict. The escalating geopolitical tensions between the United States and the Islamic Republic of Iran present a case study in how diplomatic friction translates, with considerable legal consequence, into force majeure events across commercial space contracts. As practitioners advising operators, investors, and institutions in this sector, it is necessary to examine this phenomenon not as a distant geopolitical abstraction but as an active and pressing contractual reality.

The Legal Architecture of Force Majeure in Space Commerce

In commercial space agreements, force majeure clauses typically enumerate government actions, export license denials, sanctions regimes, and regulatory prohibitions as qualifying triggering events. The breadth of such clauses matters enormously, because in the space industry, performance is invariably conditioned upon a layered web of regulatory approvals.

The commercial space industry is structurally more susceptible to geopolitically induced force majeure than most other sectors, for three reasons. First, performance under space contracts requires regulatory approvals from multiple

sovereign jurisdictions, any one of which may be revoked for reasons entirely unrelated to commercial conduct. Second, the technology involved is dual-use by nature; the same propulsion system that services a commercial telecommunications satellite may fall within the scope of munitions controls. Third, insurance and financing arrangements in the sector are often conditioned on export compliance clearances, such that a sanctions escalation can trigger defaults across an entire capital structure simultaneously.

When geopolitical tensions intensify, as they have periodically, the United States government has expanded the scope of secondary sanctions, tightened technology transfer controls, and revoked or withheld export licenses for satellite components, launch services, and ground station technology.

The AsiaSat Precedent: Geopolitics as a Contractual Trigger

The most instructive case study currently before the industry is the AsiaSat dispute with India. India's National Space Promotion and Authorisation Centre decided to withdraw authorization for AsiaSat's AS-5 and AS-7 satellites beyond March 31, 2026, citing national security concerns stemming from AsiaSat's significant Chinese government ownership through CITIC Group Corporation. The decision was not a commercial judgment, but a sovereign geopolitical act directed at the ownership structure behind the operator.

The downstream contractual consequences were immediate. AsiaSat's current permission expires at the end of March, forcing broadcasters to migrate to other satellites or face channel blackouts. Without this approval, AsiaSat cannot legally provide satellite capacity in India, effectively forcing broadcasters to look for alternative transmission arrangements. Broadcasters including Zee Entertainment Enterprises and JioStar, part of Reliance Industries, must now move their services; Zee has already switched to Intelsat and

ISRO's GSAT satellites.

The contractual dispute that followed is where the case becomes jurisprudentially significant. AsiaSat has issued a "trigger notice" to the Indian government under a bilateral investment treaty, formally signaling a potential legal challenge, and has simultaneously sent arbitration notices to broadcasters including JioStar and Zee, initiating dispute-resolution proceedings. AsiaSat's commercial position is that its agreements were not India-specific as its contracts were not limited to India and customers could continue to use the same bandwidth to provide services elsewhere. The broadcasters reject that framing entirely.

India's 2024 guidelines further require foreign satellite operators to operate through Indian entities and factor in geopolitical ties, while limiting service approvals to a satellite's operational life or five years, whichever is earlier. The regulatory architecture, in other words, was designed to give geopolitical considerations dispositive weight over commercial continuity. AsiaSat's decision to pursue a bilateral investment treaty claim presents a significant legal hurdle, as India does not have a direct BIT with Hong Kong for investment protection beyond tax matters, and enforcing BIT claims against governments is known to be difficult and lengthy.

The Iran Parallel: An Active and Unfolding Crisis

The AsiaSat dispute illustrates what happens when geopolitics terminates a satellite operator's market access. The U.S.-Iran tensions present the same structural risk, with broader contractual exposure across the entire space value chain.

Since the tensions between the U.S. and Iran commenced, a number of oil and commodities companies have invoked force majeure. QatarEnergy, which operates the world's largest liquefied natural gas export facility, declared force majeure

to avoid penalties for missing contracted deliveries. Aluminium Bahrain similarly suspended deliveries to some customers, citing risks of shipping through the Strait of Hormuz. The contractual mechanisms being invoked across these commodity sectors are identical to those embedded in commercial space agreements.

For the space industry specifically, the pathways of exposure are distinct from commodities but no less severe. U.S. export control law, principally the Export Administration Regulations and the International Traffic in Arms Regulations, imposes comprehensive restrictions on the transfer of space technology to designated adversary nations. Iran remains among the most heavily sanctioned jurisdictions globally. Common triggering events such as “acts of war,” may capture Iran-related disruptions, but the more difficult question will arise for supply chain failures that are not directly caused by war or government-mandated embargo but are instead the downstream economic consequence of regional conflict. Launch service agreements, satellite manufacturing contracts, spectrum coordination, and orbital insurance arrangements are all vulnerable to this secondary contagion.

Sanctions and export controls relating to the Iran conflict may independently prohibit performance and may or may not qualify as force majeure under the governing law. A sovereign ban that is itself a breach of sanctions does not automatically become force majeure. This creates a compounded risk for operators: the very act of attempting to invoke force majeure may expose them to sanctions liability if the performance they are excusing was already legally prohibited.

A deterioration of U.S.-Iran relations, whether manifesting as a military confrontation in the Persian Gulf, a further Iranian nuclear escalation, or a fresh round of maximum-pressure sanctions designations, would predictably generate force majeure claims across several categories of space commercial agreement: satellite manufacturing contracts

involving Iranian-backed investment entities; launch services agreements where trajectories or ground stations fall within OFAC-designated operational theaters; orbital slot licensing disputes where spectrum coordination through the International Telecommunication Union implicates sanctioned state entities; and, as the AsiaSat case demonstrates, capacity lease agreements where the nexus to a geopolitically disfavored ownership structure supplies the regulatory trigger.

Drafting Against Geopolitical Risk

Competent space counsel should treat geopolitical risk as a drafting imperative rather than a boilerplate contingency.

Force majeure clauses in commercial space agreements should specifically enumerate sanctions regime changes, export license revocations, and government-mandated service terminations as qualifying events, while simultaneously specifying the notice obligations, mitigation duties, and termination rights that flow from each. The AsiaSat dispute has illustrated that an operator's failure to anticipate and contractually allocate this risk can leave it in the position of asserting arbitration claims against counterparties who have no commercially viable choice but to comply with the regulatory mandate they have been issued.

The commercial space sector has long prided itself on its capacity to transcend political borders. The legal realities of geopolitics suggest that this aspiration, however worthy, must be balanced against rigorous contractual foresight.

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

Musk Announces SpaceX to Build Self-Growing City on the Moon Within 10 Years

July 28, 2026

It is not unbeknown to the public that NASA, for over a decade now, has been working to get humans back on the Moon. This has been a long and challenging journey that has successfully culminated in the Artemis II launch to the Moon this year. On the other side of the aisle, SpaceX and Musk have publicly stood ground on their desire to push the journey just a few kilometers further to Mars instead. However, on 8 February 2026, via X (formerly, Twitter), Musk announced:

“[...] SpaceX has already shifted focus to building a self-growing city on the Moon, as we can potentially achieve that in less than 10 years, whereas Mars would take 20+ years [...] That said, SpaceX will also strive to build a Mars city and begin doing so in about 5 to 7 years, but the overriding priority is securing the future of civilization and the Moon is faster.”

(emphasis added)

The phrasing matters. Musk did not describe a “base,” a “camp,” or even a “permanent presence.” He chose “self-growing city” a term that, in space systems language, implies a settlement that can expand its own capacity faster than Earth can sustain it through resupply. In other words, the decisive milestone is poised to be the point at which the city can manufacture, repair, and reproduce the core inputs of life and industry on-site, with Earth shifting from a lifeline to a partner.

This emphasis on speed is also crucial. In the expanded

announcement, Musk explicitly contrasted lunar cadence with Martian cadence because the former provides frequent launch opportunities and short transit times allowing rapid iteration, while Mars imposes long windows between optimal departures and months-long transfers. The Moon, in Musk's framing, is simply the faster pathway to the larger objective, reducing the risk that a disruption on Earth can strand an off-world population before it is self-sufficient.

What a “self-growing city” would actually mean

A credible “self-growing” settlement is less a single project than a layered stack of capabilities that compound over time.

First, a survivable envelope or atmosphere. A city would begin with pressurized volume, radiation protection, thermal control, and redundancy. On the Moon that likely means habitats that are either buried, barriered, or shielded with regolith. Engineering for sustained occupancy is necessary to turn temporary infrastructure into long-term habitat.

Second, reliable power at city scale. Early lunar outposts can run on solar with storage; a city that grows needs power that is both scalable and resilient through lunar night, dust, and operational contingencies. That can mean distributed solar fields, large-scale storage, and, notably, nuclear surface power (see more on the plans for this [here](#)). The commercial point is that power becomes the first utility market of the lunar economy, and everything else prices off it.

Third, closed-loop life support and food production. “Self-growing” implies that water, oxygen, and consumables are not flown in as a permanent operating model. A settlement can still import specialty components, medicines, and high-value electronics but it cannot depend indefinitely on routine shipments of basic life inputs without remaining fragile by design.

Fourth, industrial metabolism by extraction, processing, and

manufacturing. This is where “city” plays a critical role in an envisioned lunar economy. A lunar settlement that grows must be able to produce increasing quantities of:

- structural materials (regolith-based bricks, sintered surfaces, composites),
- spare parts and tools (additive manufacturing),
- propellants and volatiles if polar ice is exploited, and
- replacement infrastructure (power hardware, pressure shells, mobility platforms).

In practical terms, “self-growing” means establishing an industrial base: each new machine, habitat module, or power unit increases the settlement’s ability to build the next one.

Fifth, governance by logistics. A lunar city will function as a managed system: inventory control, redundancy planning, maintenance cycles, and emergency protocols will be as central as rockets. The romantic imagery of flags and footprints matters less than the operational question of whether the settlement can survive a sustained interruption of Earth resupply.

Why the Moon becomes strategically attractive

Musk’s core argument is speed. The Moon is close enough to allow rapid learning cycles (launch, land, test, fix, repeat) on timelines that resemble industrial development rather than expeditionary exploration.

That matters because establishment of a large-scale settlement will not be a single “mission.” It will be an accumulation of failures and successes: life support anomalies, dust mitigation, thermal shock, power reliability, human factors, medical contingencies. A two-day transit and frequent windows change the economics of failure.

It also matters because NASA’s own lunar return effort remains on a near-term timetable. As of early February 2026, NASA

indicated Artemis II is targeting no earlier than March 2026 following issues identified during a fueling test. Against that backdrop, a public SpaceX narrative that the Moon is the near-term priority signals an alignment with where the most immediate institutional demand sits.

What this shift means for the industry

If SpaceX truly prioritizes a lunar city three effects follow across the market.

1) The lunar economy becomes real and fast.

A city implies persistent demand for cargo, construction, power, comms, navigation, mobility, and surface operations. That demand creates bankable markets for companies that are not launch providers: mining and excavation, robotics, thermal systems, pressure vessel manufacturing, radiation shielding, surface mobility, and autonomous operations.

2) “Cislunar logistics” becomes the main arena of competition. A high-value advantage of establishing a lunar settlement is cadence. Any actor that can move mass routinely will set the tempo for everyone else. Musk’s own commentary places “millions of tons” and scale at the center of the ambition. The competitive response will not only come from rival launch systems, but from anyone building cislunar transportation, depots, tugs, and surface freight capacity.

3) Regulation, liability, and contract standards will tighten. A city forces the legal questions to mature. Risk will address launch and reentry, but expand to long-duration habitation, industrial activity, and sustained operations in proximity to other actors. That pushes regulators and contracting authorities toward stricter requirements on safety cases, mission assurance, spectrum discipline, debris and traffic coordination, and insurance coverage tailored to continuous lunar operations.

It also changes the commercial posture of space law. The legal

work shifts towards operational governance rather than mission approval: how activity is coordinated, how safety zones are treated in practice, how responsibility is allocated across operators and contractors, and how disputes are resolved when operations become continuous rather than episodic.

Conclusion

This is not a retreat from Mars so much as a recalibration of sequencing. Musk still describes Mars as a continuing objective, with work beginning in the five-to-seven-year range, but with the Moon as the overriding priority because it is faster.

If the Moon becomes the proving ground for genuine self-sufficiency via energy independence, industrial reproduction, and survivable logistics, then the lunar decade will be the architectural foundation for everything that follows.

So that means that we are all heading to the Moon, SpaceX included.

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

Russian Spy Satellites Intercepting European Satellite Communications

July 28, 2026

European space security officials are increasingly concerned that two Russian “inspector” satellites have been used to collect communications associated with multiple European satellites, including traffic linked to government and military users. This has evidently been a sustained pattern over several years, with the alleged consequence being intelligence collection and a clearer mapping of how European satellite services could be constrained or disrupted in crisis conditions.

Such activity risks compromising sensitive information transmitted by the satellites but could also allow manipulation of the satellite flight paths or even lead to accidents.

What is reported to have happened

The reporting attributes the assessment to European security and intelligence officials who have been tracking two Russian spacecraft commonly referred to as Luch-1 and Luch-2. Officials reportedly believe these spacecraft were able to intercept communications from at least a dozen European satellites. The reporting also notes close approaches to a wider set of satellites over a multi-year period, which, if accurate, would reflect deliberate station-keeping near targets rather than incidental co-location in geostationary orbit.

A key technical qualifier is that interception risk is not uniform. A close look points to legacy vulnerabilities, including the fact that some older satellites may still rely on weak or unencrypted command links, creating exposure not only for confidentiality but also for command authentication and operational integrity.

None of this requires assuming a “weapon” in orbit. Persistent proximity operations, combined with modern signals-intelligence payloads, can be sufficient to collect metadata,

waveform characteristics, traffic volumes, and in some cases content, depending on encryption and link discipline. Even where encryption holds, the collector learns usage patterns, the contours of the ground segment, and system behavior under stress.

Why proximity operations matter commercially

Geostationary orbit is a commercial operating environment. Many satellites carry mixed traffic of commercial connectivity, leased capacity, and governmental payloads or services. That makes “space security” inseparable from commercial service continuity and contract performance.

Three immediate consequences follow.

First, security standards will move from guidance to gating. Encryption, authenticated command and telemetry, and disciplined key management are no longer features that win competitive bids. They are baseline conditions for eligibility, particularly for government and critical-infrastructure customers.

Second, underwriting and financing will harden around cyber-physical risk. The market already prices launch and debris risk. Persistent proximity and interception concerns introduce a more political category: contested-domain operating risk. That tends to produce tighter warranties, more onerous security representations, and narrower coverage around interference events.

Third, customers will demand assurance, not only service levels. Expect procurement language to expand beyond uptime and throughput into incident response timelines, sovereign control of command chains, ground segment resilience, and demonstrable ability to maintain service under interference conditions.

These pressures are intensified by Europe’s parallel policy

direction toward sovereign secure connectivity. In January 2026, public statements from the European Commission described the commencement of GOVSATCOM operations, explicitly framed as secure and encrypted governmental satellite communications under European control.

The legal consequences: duties exist, but enforcement is political

The legal framework for outer space has not suddenly become obsolete. It is, however, strained by conduct that sits *below* the threshold of overt attack while still producing strategic harm.

Under the Outer Space Treaty, States must conduct activities with “due regard” to the corresponding interests of other States, and where a State has reason to believe an activity would cause “potentially harmful interference,” it should undertake appropriate international consultations. This is not a direct prohibition on collection, and it does not neatly capture intelligence operations. It does, however, create a lawful diplomatic pathway: if proximity operations are credibly framed as creating a risk of harmful interference or unsafe behavior, consultations are the treaty-based mechanism to press the issue.

Separately, Article VI’s responsibility principle matters in today’s mixed government-commercial architecture: States bear international responsibility for national activities in outer space, including those by non-governmental entities, and must authorize and continuously supervise such activities. In practical terms, this pushes European regulators toward more explicit security supervision of licensed operators whose systems carry government traffic, and it strengthens the policy case for security conditions in licensing and procurement.

The radio layer adds another legal and regulatory vocabulary.

The International Telecommunication Union radio regime is designed to prevent harmful interference and imposes obligations on administrations regarding stations under their responsibility. If interception evolves into jamming, spoofing, or service disruption, that framework provides process and terminology even when remedies remain political.

The limiting factor across these regimes is attribution and proof. Legal consequences scale with confidence. That reality will drive investment in independent tracking, data fusion, and evidentiary discipline, because sustaining a position in a diplomatic, regulatory, or legal forum matters.

Strategic meaning: below-threshold pressure becomes normal

The most consequential implication is not that satellites can be listened to. It is that space is being treated as a continuously contested domain, and that this contest is increasingly conducted through activity that stays below the threshold of overt interference.

For operators, the lesson is straightforward: resilience must be engineered and contractually demonstrated.

For governments, the implication is equally clear: the line between commercial service and national capability is thin, and it will continue to thin. Hybrid payloads, shared capacity, and multi-use constellations bring efficiency, but they also bring shared exposure.

For Europe, this incident reporting will likely accelerate three tracks already underway: (1) hardening of legacy systems and uplink security practices; (2) procurement and licensing reforms that make security a condition of market access; and (3) sovereign and allied connectivity architectures that reduce single points of failure and impose higher security baselines.

The diplomatic posture should remain measured. The objective

is to reduce strategic ambiguity, raise the cost of intrusive behavior through collective standards and coordinated responses, and ensure that Europe's commercial satellite market remains credible to the customers who depend on it.

In short, the future will not be defined by a single episode of proximity collection. It will be defined by whether Europe treats this as an intelligence curiosity, or as a governance and market-structure inflection point.

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