Cosmonaut Removed from SpaceX Flight Mission for Violation of National Security via the ITAR

December 8, 2025

The recent removal of a cosmonaut from SpaceX's Crew-12 mission has drawn attention not for its diplomatic implications, but for what it signals about the tightening intersection of human spaceflight and national-security regulation. Reports indicate that the cosmonaut was withdrawn following an alleged violation of U.S. export-control rules, specifically, the International Traffic in Arms Regulations ("ITAR").

The cosmonaut allegedly photographed restricted technical materials during training activities at SpaceX facilities in Hawthorne, California. Even a seemingly routine photograph taken within a secure environment can constitute an "export" under ITAR, which defines export to include, *inter alia*, the transfer of controlled technical data to any foreign person, whether or not that transfer occurs outside U.S. territory. As such, the act of capturing and storing sensitive imagery on a personal device may be sufficient to trigger an export-control investigation.

If confirmed, the incident stands as one of the clearest examples thus far that human spaceflight no longer exists outside the perimeter of national-security law. Commercial operators routinely host international astronauts, government partners, researchers, and soon, even private passengers on flight missions. Each individual, regardless of their role,

walks into environments saturated with ITAR-controlled systems and data. The presence of foreign nationals in training facilities, spacecraft assembly buildings, and mission-simulation centers requires companies to build increasingly robust compliance architectures to avoid inadvertent transfers of technical data.

The episode also arrives at a moment when U.S. export-control agencies are actively considering reforms to modernize ITAR and the Export Administration Regulations for the commercial space era. Policymakers have proposed new license exemptions for civil and scientific missions, and revisions to the definitions of spacecraft, launch vehicles, and related equipment. The U.S. Department of State's Directorate of Defense Trade Controls has also announced planned revisions to the ITAR and U.S. Munitions List for 2026. Yet even as regulators contemplate liberalization in some areas, the Crew-12 incident underscores that ITAR's core prohibitions remain formidable.

There is a broader lesson for future spaceflight participants. As commercial missions increasingly include non-career astronauts, civilians, and international passengers, individuals may find themselves documenting their experiences: photographing hardware, recording facilities, posting social media updates, or capturing behind the scenes content for family, research, or personal records. What feels like ordinary documentation may, in a high-technology environment, constitute a regulatory breach. Travelers who are unaccustomed to U.S. export-control regimes may not appreciate the breadth of which "technical data" encompasses. The penalties for unintended violations can be severe, and operators remain responsible for safeguarding access to controlled technology.

General counsel and in-house legal teams can take several concrete steps to harden their facilities against similar breaches. This begins with implementing granular export-control access protocols, including individualized technology

control plans that specify precisely which foreign persons may enter which areas, under what supervision, and with what restrictions on electronic devices. Counsel should also oversee mandatory pre-training for all visitors, regardless of role, explaining the scope of ITAR technical data and the severe consequences of unauthorized documentation. Facility layouts should be reviewed to ensure that controlled hardware is never visible from mixed-access zones, and companies should adopt monitored storage solutions to prevent personal devices from entering sensitive areas. Finally, incident-response procedures must be rehearsed in advance so that any suspected breach is escalated immediately, preserved for regulatory reporting, and contained before it can compromise export-license obligations.

For companies, investors, and governments participating in cross-border space missions, the Crew-12 development is a reminder that export compliance is now inseparable from mission design, astronaut training, facility access management, and passenger education. For passengers, it signals that the legal obligations accompanying space travel extend far beyond launch contracts and liability waivers; they reach into the way one records, describes, and shares the experience itself. Operators and participants alike would be well advised to approach these missions with a heightened awareness of the legal architecture that surrounds them and with cognizance that, in the space industry, even a photograph can carry the weight of national security concern.

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