AXIOM RESEARCH INSTITUTE

Publication Series: Emerging Infrastructure Security

Commercial Space and the Cybersecurity Governance Deficit

Ground Segment Security, Supply Chain Risk, and Third-Party Dependency Governance

KEY FINDINGS

01 Commercial space is critical infrastructure by function — GPS, imagery, comms, timing — regardless of formal designation

02 The ground station, not the satellite, is the actionable attack surface (Viasat KA-SAT, 2022)

03 Most organizations dependent on commercial space services have never assessed them as vendor risk

04 Standard vendor risk frameworks are not designed to ask the right questions about satellite operators

05 NIST IR 8401 exists and is voluntary — dependent organizations cannot assume operator compliance

Document ARI-2026-003 | Published May 2026 | axiomresearch.institute

About the Axiom Research Institute

The Axiom Research Institute is the independent research and publications division of Axiom Sovereign LLC, a fractional vCISO and GRC consulting firm. The Institute publishes primary research on post-quantum cryptography governance, AI privacy compliance, space cybersecurity, and emerging technology risk management. All publications are grounded in primary regulatory and standards sources and are designed to support practitioners, legal counsel, and executive leadership in navigating complex governance challenges.

About Axiom Sovereign

Axiom Sovereign LLC provides fractional vCISO services, GRC program design and assessment, vendor privacy risk analysis, and AI governance advisory for mid-market organizations in regulated sectors. Principal: Cory Missimore, CISSP, CISM, CISA, CIPP/E, CIPP/US, CIPM, AIGP.

How to Use This Paper

This is a foundational publication. It establishes the Institute's analytical framework and primary source grounding for this topic. Subsequent publications in the series address specific implementation domains and can be used independently or in conjunction with this paper. Implementation guides, assessment instruments, and templates derived from this paper are published separately and reference this document.

Document Number	ARI-2026-003
Publication Series	Emerging Infrastructure Security
Published	May 2026
Version	1.0 — Initial Release
Suggested Citation	Axiom Research Institute. (2026). Commercial Space and the Cybersecurity Governance Deficit (ARI-2026-003).
Distribution	Public — Unrestricted
License	CC BY-NC 4.0 — Non-commercial with attribution

Disclaimer

EXECUTIVE SUMMARY

01

Commercial space is embedded critical infrastructure, not a specialized sector.

GPS timing underpins financial settlement and aviation. Commercial imagery supports defense intelligence. LEO satellite communications provide military and civilian backup connectivity. Space-based weather observation drives aviation routing and emergency management. The organizations operationally dependent on these services span aviation, finance, agriculture, defense, telecommunications, and emergency management — most of whom have not assessed this dependency.

02

The ground station is the attack surface. The Viasat KA-SAT incident proved it.

In February 2022, a VPN misconfiguration in Viasat's ground segment network management infrastructure allowed the GRU to push a destructive payload to tens of thousands of satellite modems across Europe, disrupting Ukrainian military communications and German wind turbine remote management simultaneously. The satellites were never touched.

03

Most dependent organizations have not mapped their commercial space dependencies.

Defense contractors using commercial imagery, financial institutions using GPS timing, agricultural operators using precision navigation, telecoms using LEO broadband backup — none of these organizations typically assess commercial satellite operators as vendor risk. The dependency exists. The assessment does not.

04

NIST IR 8401 provides the assessment framework. It is voluntary and unevenly adopted.

IR 8401 (2022) maps NIST CSF controls to satellite ground operations. No regulatory requirement compels commercial operators to implement it. No mechanism allows dependent organizations to verify compliance without contractual requirements.

05

The governance framework proposed here requires no specialized space expertise.

Dependency identification, risk assessment by category, vendor assessment against IR 8401, and resilience planning apply the same organizational discipline as any third-party risk management program — adapted to a risk domain most programs have missed.

SECTION 1

The Dependency Most Organizations Have Not Mapped

1.1 What Commercial Space Underlies

GPS, operated by the U.S. Space Force, provides positioning, navigation, and timing (PNT) services that are not optional infrastructure for the sectors that depend on them — they are the infrastructure. Civil aviation navigation relies on GPS for en route navigation and precision approach procedures. Financial transaction systems use GPS-derived timing signals for timestamping that ensures settlement sequencing integrity — the DTCC and major exchanges operate GPS timing infrastructure precisely because the financial system cannot function without reliable, precise timekeeping. Emergency response coordination, telecommunications network synchronization, and precision agriculture equipment guidance each have direct GPS dependencies.

Commercial satellite imagery supports defense intelligence analysis, insurance risk modeling, agricultural yield forecasting, disaster response coordination, and urban planning. The commercial imagery market has grown because government satellite capacity cannot keep pace with demand — which means government and defense intelligence consumers are operationally dependent on commercial operators whose security posture is determined by those private companies.

Commercial LEO satellite communications — Starlink, OneWeb, Amazon Project Kuiper — provide broadband connectivity for users without terrestrial infrastructure access and serve as backup communications for government and defense operations. The 2022 conflict in Ukraine demonstrated what happens when a commercial communications constellation becomes operationally critical for military command: the system was designed for commercial consumers and found itself a target in an active conflict.

1.2 Who Is Dependent Without Knowing It

The organizations most exposed to commercial space cybersecurity risk are not space companies. They are organizations that have incorporated commercial space-derived data and services into their operations without assessing those services as a vendor risk category.

> Defense contractors who deliver intelligence products derived from commercial satellite imagery are dependent on the security of commercial imagery providers. A compromise of that provider's ground systems that manipulates imagery before delivery does not register as a cybersecurity incident at the defense contractor. It registers, eventually, as an analytical error — or it does not register at all.

Financial institutions whose settlement infrastructure uses GPS timing are dependent on GPS signal integrity in a way that operational risk programs have not systematically addressed. Agricultural operations

using precision farming equipment have operational dependencies on commercial satellite navigation directly tied to crop yield and seasonal windows. A GPS spoofing event affecting planting equipment at a critical seasonal point is a production disruption with quantifiable financial consequences.

1.3 The Commercial Expansion Created a New Risk Surface

Active satellites in low Earth orbit grew from approximately 5,000 in 2020 to over 9,000 in 2024, driven almost entirely by commercial LEO constellation deployment. Modern commercial satellites are software-defined systems supporting remote update, feature modification, and reconfiguration through ground-to-satellite command links. This creates an attack surface that purpose-built, hardwired satellite platforms did not have. The software update channel is a potential injection vector.

Commercial operators span an enormous range of security maturity. SpaceX has resources commensurate with its scale. Many commercial satellite operators are venture-backed startups whose security programs reflect startup constraints. The supplier ecosystem for commercial space is concentrated: satellite bus platforms, ground station software, and RF components come from a limited number of vendors. A vulnerability in a widely used ground station software platform could affect multiple operators simultaneously — the same supply chain risk mechanism that produced SolarWinds, applied to systems that control satellites.

SECTION 2

The Threat Is Documented

2.1 The Viasat KA-SAT Incident

In February 2022, hours before Russia's military invasion of Ukraine, Viasat's KA-SAT satellite broadband network was attacked in a cyberattack that disabled tens of thousands of satellite modems across Europe and disrupted Ukrainian military and government communications at a moment of operational consequence. CISA, NSA, and the FBI jointly attributed the attack to Russia's GRU in a May 2022 advisory.

The attack was not conducted against the satellites. It was conducted against the ground segment — specifically, a misconfigured VPN appliance that provided access to the network management infrastructure controlling KA-SAT's customer modems. A destructive payload was pushed across the service area, rendering modems inoperable. The space segment was never touched.

> The same advisory documented collateral damage: Enercon, a German wind turbine operator, lost remote management capability for approximately 5,800 turbines because those turbines used KA-SAT connectivity for monitoring and control. Enercon had no relationship with the military users being targeted. Its operational disruption was collateral to an attack on a commercial satellite network it happened to depend on.

The KA-SAT incident establishes three facts directly relevant to governance. First, the ground segment is the effective attack vector — the satellite did not need to be touched. Second, the attack method was not technically exotic; VPN misconfiguration is a common enterprise security failure. Third, collateral damage to non-targeted organizations is predictable from the architecture: commercial satellite networks do not segment traffic by customer security classification.

2.2 GPS Signal Manipulation

GPS jamming degrades signal reception by broadcasting noise on GPS frequency bands. Its effects are documented in EASA safety information bulletins covering GPS signal interference affecting civil aviation in the Eastern Mediterranean, Baltic region, and Middle East — public safety reporting accessible to any aviation operator. GPS spoofing replaces authentic signals with false signals accepted by receivers as legitimate. A sophisticated operation drifts reported position gradually, delaying detection.

The Black Sea spoofing events documented beginning in 2017 caused vessels to report GPS positions inconsistent with their actual locations. The mechanism is not complex — consumer-grade GPS spoofing equipment is commercially available. For organizations with GPS-dependent operations, the governance question is specific: which systems use GPS timing or positioning, what is the consequence of signal degradation or spoofing, does the organization have detection capability, and does an alternate timing or

positioning source exist for critical operations?

2.3 Software Supply Chain

EO 14028 established SBOM requirements for federal software procurement. These requirements have not been extended to commercial satellite systems. Most commercial satellite operators do not require SBOM documentation from their satellite bus vendors or payload software providers. The supply chain visibility becoming standard in enterprise software procurement is absent in space hardware and software procurement. A compromise of any software supply chain input — development kit, embedded library, ground station component — creates a pathway to compromise the space or ground system.

SECTION 3

The Framework Environment and Its Gaps

3.1 NIST IR 8401

NIST IR 8401, Satellite Ground System Cybersecurity Framework Profile (October 2022), is the primary applicable framework for satellite ground operations. It maps NIST CSF categories and subcategories to the specific environment of ground segment operations: command and control systems, network infrastructure, telemetry and mission data processing, and mission planning and scheduling software. The profile is well-constructed and provides a useful assessment baseline for organizations with operational control over ground systems.

> IR 8401 is voluntary. No regulatory requirement compels commercial satellite operators to implement it. No mechanism allows dependent organizations to verify compliance without contractual requirements. An organization that relies on a commercial satellite service has no visibility into the operator's IR 8401 implementation unless the contract requires attestation or third-party audit documentation.

3.2 NIST IR 8270 and Space Policy Directive 5

NIST IR 8270 provides accessible threat landscape orientation and NIST CSF application guidance for commercial operators with limited security resources. Space Policy Directive 5 (September 2020) establishes high-level cybersecurity principles for government space systems and recommends their adoption by commercial operators on a voluntary basis. Voluntary adoption across the commercial sector has been incomplete and unverified.

3.3 The Legislative Direction

The Satellite Cybersecurity Act, reintroduced in December 2025 with bipartisan Senate sponsorship, would direct Commerce in coordination with CISA to develop voluntary cybersecurity guidelines for commercial satellite operators published through NTIA. The Space Infrastructure Act, if enacted, would formally designate space systems as critical infrastructure under the PPD-21 sector framework, bringing commercial space operators within sector-specific plan, council, and information-sharing structures. Both developments point toward greater engagement, not away from it. Organizations with commercial space dependencies should not wait for mandatory regulation.

SECTION 4

The Governance Gap in Dependent Organizations

4.1 Third-Party Vendor Risk and the Space Blind Spot

Third-party vendor risk frameworks — NIST SP 800-161r1, ISO 27001 supplier relationships, FFIEC guidance, HIPAA, CMMC supply chain provisions — are designed primarily with software vendors, cloud service providers, and data processors in mind. Their questionnaires ask about network access, data encryption, access controls, incident response, and regulatory compliance. They do not ask about ground station security, command authentication, software update chain integrity, or GPS dependency.

This creates a structural blind spot. An organization with a mature vendor risk management program — quarterly reviews of cloud providers, formal onboarding for managed service providers — may have zero assessment of its commercial satellite service dependencies. Not because those dependencies were assessed and deemed acceptable. Because the assessment framework was not designed to ask about them.

4.2 What Adequate Assessment Asks

A vendor security questionnaire for a commercial satellite operator should draw from NIST IR 8401 control categories, adapted into a vendor-facing format. Key areas: ground segment network security (network segmentation from corporate IT, access controls, monitoring cadence); command authentication (authentication mechanisms for satellite command uplink, command signing, access logging); software update security (authentication process for ground-to-satellite updates, testing and rollback capability, authorization controls); supply chain (SBOM for ground station software, security assessment of satellite bus software vendors, third-party vendor access controls); and incident response (documented plan for space and ground segment events, customer notification commitments, recovery time objectives).

4.3 Defense Contractors and Supply Chain Integrity

Defense contractors whose work product relies on commercial space services face a specific supply chain integrity problem that CMMC and NIST SP 800-161r1 are designed to address. If a commercial imagery provider's ground systems are compromised and imagery is manipulated before delivery, every analytical product built on that imagery carries the adversary's influence — and the defense contractor may not know. NIST SP 800-161r1's supply chain risk management practices require identification and assessment of supply chain risks including subcontractors and service providers. For contractors using commercial satellite imagery, communications, or GPS-dependent timing in operations touching CUI, the commercial space provider is a supply chain element requiring assessment under that framework.

4.4 GPS Dependency and Business Continuity

Business continuity planning should include a GPS dependency assessment: which systems use GPS timing or positioning, what is the consequence of GPS unavailability or degradation for each, and what alternate timing or positioning source is available. For most organizations, this assessment has not been conducted. Its absence means the continuity plan has an undocumented single point of failure that cannot be addressed because it has not been identified.

SECTION 5

A Governance Framework for Dependent Organizations

5.1 Phase One: Dependency Identification

The starting point is a structured inventory of commercial space dependencies across four categories. Data product dependencies: satellite imagery, satellite-derived weather data, commercial positioning data products. Communications dependencies: satellite broadband services, satellite phone systems, backup communications links. Timing dependencies: GPS or other satellite-derived timing in financial transaction systems, network synchronization, precise timekeeping applications. Navigation dependencies: GPS positioning in equipment guidance, logistics tracking, precision agriculture, fleet management.

The inventory output is a dependency map: commercial space dependencies by category, specific commercial operators providing each service, and operational consequence of loss or degradation. This is the prerequisite for everything that follows. Organizations that have not completed it have not assessed their commercial space risk.

5.2 Phase Two: Risk Assessment by Category

For data product dependencies: supply chain integrity compromise (data manipulated at source), service availability disruption, and data authenticity attacks. For communications dependencies: service disruption (as documented by KA-SAT), interception of unencrypted communications, and injection of false communications. For timing dependencies: GPS jamming and GPS spoofing, requiring identification of alternate timing sources and anomaly detection capability. For navigation dependencies: GPS spoofing and jamming, requiring assessment of detection capability and backup navigation methods.

5.3 Phase Three: Vendor Assessment

For critical-path commercial satellite operators, the NIST IR 8401-derived questionnaire from Section 4.2 should be incorporated into formal vendor risk assessment. For new and renewing contracts with critical-path providers, contract language should require annual security questionnaire completion, notification within a defined timeframe of security incidents affecting service delivery, and SBOM documentation for ground station software components as a condition of contract. A provider that refuses security transparency is providing information about its security posture through that refusal.

5.4 Phase Four: Resilience Planning

For data product dependencies: alternate sources, procedures for operating on degraded data, and escalation criteria for when degraded operations are unacceptable. For communications dependencies: alternate communications paths — terrestrial networks, alternate satellite providers, PSTN fallback — and

procedures for activation. For timing dependencies: alternate timing sources including terrestrial atomic clock references and PTP grandmaster clock infrastructure, and switchover procedures. For navigation dependencies: alternate navigation methods appropriate to the operational context and trained operational staff.

SECTION 6

The Regulatory Trajectory and Its Governance Implications

The regulatory trajectory toward formal critical infrastructure designation for space systems creates governance obligations that organizations with commercial space dependencies should begin addressing now, independent of how the legislative debate resolves. Whether the Space Infrastructure Act passes or not, whether the Satellite Cybersecurity Act produces voluntary guidelines or mandatory requirements, the operational dependencies documented in this paper exist today. The incidents have already occurred. Waiting for regulatory clarity before beginning vendor assessment is the same error organizations make when they wait for a breach before inventorying vendor access.

On SBOM requirements: EO 14028 established software bill of materials requirements for federal software procurement. The same transparency logic applies to commercial satellite ground station software. Organizations with critical-path commercial space dependencies can begin requiring contractual SBOM commitments from their providers now, as a condition of contract renewal, without waiting for regulatory mandate. Early movers in supply chain transparency create leverage in vendor negotiations; late movers accept whatever transparency vendors are willing to offer after a mandate forces it.

On information sharing: the Space ISAC provides a sector-specific threat intelligence mechanism. Organizations with commercial space dependencies that are not themselves space operators should assess whether their commercial service providers participate, and whether that participation produces threat intelligence the dependent organization can act on. The KA-SAT attack was preceded by intelligence collection. Organizations that share threat information through sector mechanisms get that intelligence. Those that don't, don't.

CONCLUSION

The governance gap this paper documents is not primarily a technical gap. It is an assessment gap. The commercial space dependencies are present. The threat environment is documented. The incidents have occurred. What is missing in most dependent organizations is the recognition that commercial space services belong in the vendor risk register, the assessment framework to evaluate them, and the resilience planning to manage the consequences of disruption.

> The organizations that discover their commercial space dependencies through an incident are making the same governance error as organizations that discover a data breach through a regulatory notification. The dependency existed. The risk was assessable. The assessment was not done.

For risk and compliance leaders reading this paper: the starting point is a dependency map. Which of your organization's business processes rely on commercial satellite services — data products, communications, timing, or navigation? If that map does not exist, it is the first deliverable. Everything else in this framework — vendor assessment, resilience planning, contract requirements — depends on knowing what you depend on.

Axiom Research Institute's subsequent publications in this series address the commercial space vendor assessment instrument in detail, GPS resilience planning methodology, and the application of NIST IR 8401 to third-party questionnaire development. Organizations seeking practitioner support for commercial space vendor risk governance may request an initial consultation at axiomsovereign.com.

REFERENCES

National Institute of Standards and Technology. (2022). NIST IR 8401: Satellite Ground System Cybersecurity Framework Profile. U.S. Department of Commerce.

National Institute of Standards and Technology. (2022). NIST IR 8270: Introduction to Cybersecurity for Commercial Satellite Operations. U.S. Department of Commerce.

National Institute of Standards and Technology. (2022). SP 800-161r1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations.

The White House. (2020). Space Policy Directive 5: Cybersecurity Principles for Space Systems.

The White House. (2021). Executive Order 14028: Improving the Nation's Cybersecurity.

Cybersecurity and Infrastructure Security Agency, National Security Agency, & Federal Bureau of Investigation. (2022). Russian State-Sponsored Cyber Actors Target Critical Infrastructure. Joint Advisory AA22-110A.

European Union Aviation Safety Agency. (Multiple years). Safety Information Bulletins: GNSS Signal Interference. EASA.

European Network and Information Security Agency. (2022). ENISA Threat Landscape 2022.

U.S. Department of Homeland Security. (2013). NIPP 2013: Partnering for Critical Infrastructure Security and Resilience.

Department of Defense. (2023). Cybersecurity Maturity Model Certification (CMMC) 2.0 Program. 32 CFR Part 170.

Satellite Cybersecurity Act. (2025). Reintroduced to the U.S. Senate, December 2025.