Securing space

Cyber security for low earth orbit satellite communications





Australian Government

Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre



Australian Space Agency



Communications Security Establishment Canada

Canadian Centre for Cyber Security

Centre de la sécurité des télécommunications Canada

Centre canadien pour la cybersécurité



National Cyber Security Centre

NEW ZEALAND



Table of contents

Introduction 4

Intended audience 4

Background 5

Emerging trends in LEO SATCOM technologies 6

- Advanced communication technologies 6
- Multi-orbit hybrid constellations 6
- Edge and cloud integration 6
- Synergy with terrestrial networks and 5G/6G 6
- Integrated, intelligent satellite ecosystems 6

LEO SATCOM cyber security risks and mitigation strategies 7

- Space segment 8
- Ground segment 9
- User segment 10
- Communication links 11
- Supply chain 12
- Secure data management in LEO SATCOM networks 13
- Data sovereignty and control across borders 14
- Cyber security questions to ask LEO SATCOM service providers 15

Further information 17

- Satellite communications and space systems 17
- Cyber security for satellite operations 17
- Threat modelling 17

Introduction

The rapid expansion and increasing reliance on Low Earth Orbit (LEO) satellite communication (SATCOM) systems have introduced significant cyber security challenges. As LEO satellite constellations grow, the attack surface for adversaries increases. This growth puts critical networks that depend on these satellite services at greater risk. Securing this infrastructure is essential to ensuring the resilience of commercial communications, national security systems and emergency response capabilities.

Example use cases for LEO SATCOM services include:

- delivering low-latency and high-bandwidth internet to remote areas for consumers and businesses
- enabling direct-to-device communication
- supporting mobile backhaul
- facilitating Internet of Things (IoT) connectivity.

LEO SATCOM systems improve network resilience and enable emergency communications across both government and private sectors. They are used in sectors such as telecommunications, mining, agriculture, healthcare, and maritime operations.

A successful cyber attack could lead to service disruptions, exposure of sensitive data, and even physical harm to individuals and assets. This reinforces the urgent need for robust cyber security measures.

Intended audience

The Australian Signals Directorate's Australian Cyber Security Centre (ASD's ACSC) authored this publication in collaboration with the Australian Space Agency, the Canadian Centre for Cyber Security (Cyber Centre), the National Security Agency (NSA), and the New Zealand National Cyber Security Centre (NCSC-NZ). Throughout this publication, these organisations are referred to as the 'authoring agencies'.

This publication is intended for users of LEO SATCOM services. It highlights key cyber security risks and corresponding mitigation strategies to support informed decision-making. When procuring LEO SATCOM services, users should have a clear understanding of their roles and responsibilities for securing their equities as well as the responsibilities of the service provider.

This publication also provides a set of critical questions that organisations can ask when discussing security with LEO SATCOM providers. These questions help ensure that security and resilience are considered alongside performance and capability requirements in the context of evolving threats in the space domain.

The authoring agencies acknowledge that many of the cyber security risks and mitigation strategies outlined in this publication may be broadly relevant to satellite communications, beyond just LEO SATCOM services.

Background

In LEO SATCOM networks, the CIA triad – Confidentiality, Integrity, and Availability – is critical to maintaining secure and reliable operations (Figure 1). LEO SATCOM systems face unique challenges due to their distributed architecture and limited physical access to space-based assets. They also rely on radio frequency links that are susceptible to jamming, spoofing and interception.

The constant movement of LEO satellites and frequent handovers make it harder to keep connections secure. These factors demand specialised security approaches that go beyond conventional terrestrial models. These approaches must protect against space-specific threats such as spoofing, signal degradation and compromised ground stations.

Organisations should define security expectations and requirements with their SATCOM service providers. These discussions ensure risk profiles are understood, and appropriate protections are in place. Users and organisations should consider regular testing and updating of incident response and continuity plans, to include scenarios for satellite service loss or compromise.

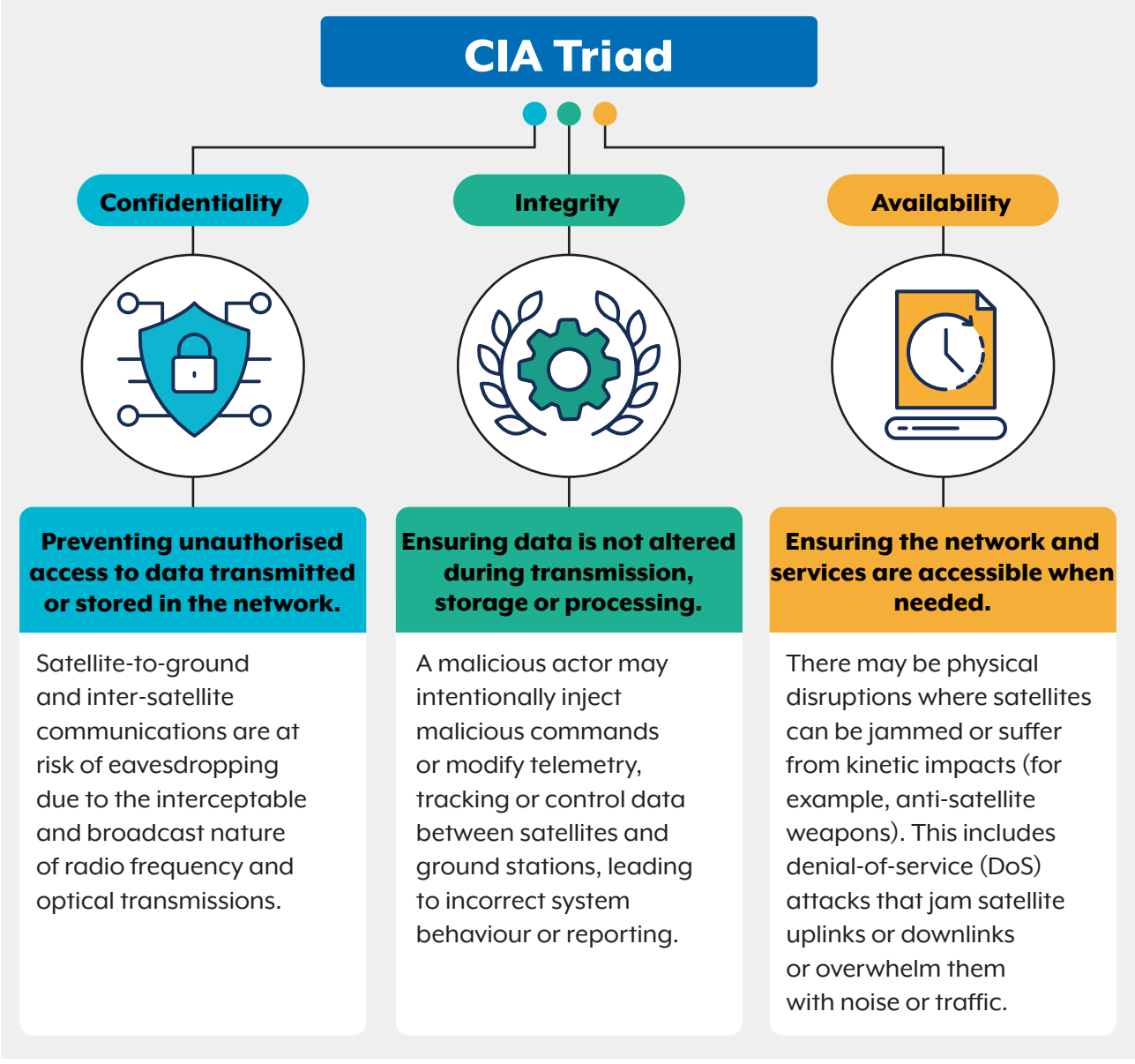


Figure 1. The CIA triad: Confidentiality, Integrity, Availability

Emerging trends in LEO SATCOM technologies

As the LEO SATCOM industry evolves, emerging technologies are introducing new cyber security complexities. The following are examples that SATCOM service users need to consider when managing risks.

Advanced communication technologies

Technologies such as optical inter-satellite links (ISL) enable high-speed, direct satellite-to-satellite communication without relying on ground infrastructure. While this enhances performance and autonomy, it also introduces new attack surfaces for adversarial interference and potential environmental disruptions in the optical domain, requiring encryption and authentication methods tailored to free-space optics.

Multi-orbit hybrid constellations

This layered architecture increases system complexity and interdependence. It requires coordinated cyber security strategies across orbital layers to prevent cascading failures or cross-segment vulnerabilities.

Edge and cloud integration

Advances in edge and cloud integration is transforming LEO satellites into orbiting computing nodes. While complete integration may be years away, this shift raises concerns around secure data processing and remote software updates. Addressing these requires robust endpoint protection and secure orchestration frameworks.

Synergy with terrestrial networks and 5G/6G

The integration of terrestrial networks with 5G and potentially 6G in the future introduces a unified connectivity paradigm, blending terrestrial and non-terrestrial networks. While this promises ubiquitous access, it also expands the attack surface, requiring harmonised security protocols and cross-domain threat detection capabilities.

Integrated, intelligent satellite ecosystems

These ecosystems may combine multi-orbit architectures, on board compute, ultra-fast optical links, and AI-enhanced traffic management. However, their complexity demands a holistic cyber security approach that spans hardware and software, with emphasis on resilience, trust and real-time threat response.

Integration and use of commercial off-the-shelf components

Unlike bespoke space-grade solutions, commercial off-the-shelf products often inherit vulnerabilities from terrestrial environments, introducing new cyber security challenges such as exposure to common exploits, unpatched firmware, and supply chain risks. When integrated into LEO platforms, these vulnerabilities can propagate across space and ground segments, complicating threat modelling and incident response.

LEO SATCOM cyber security risks and mitigation strategies

The following section outlines high-level cyber security risks and mitigation strategies for LEO SATCOM systems, viewed through the lenses of the space segment, ground infrastructure, user segment, communication links, and the broader supply chain. Figure 2 illustrates the key components of a typical LEO network architecture, including the space, ground, and user segments and the communication links between them.

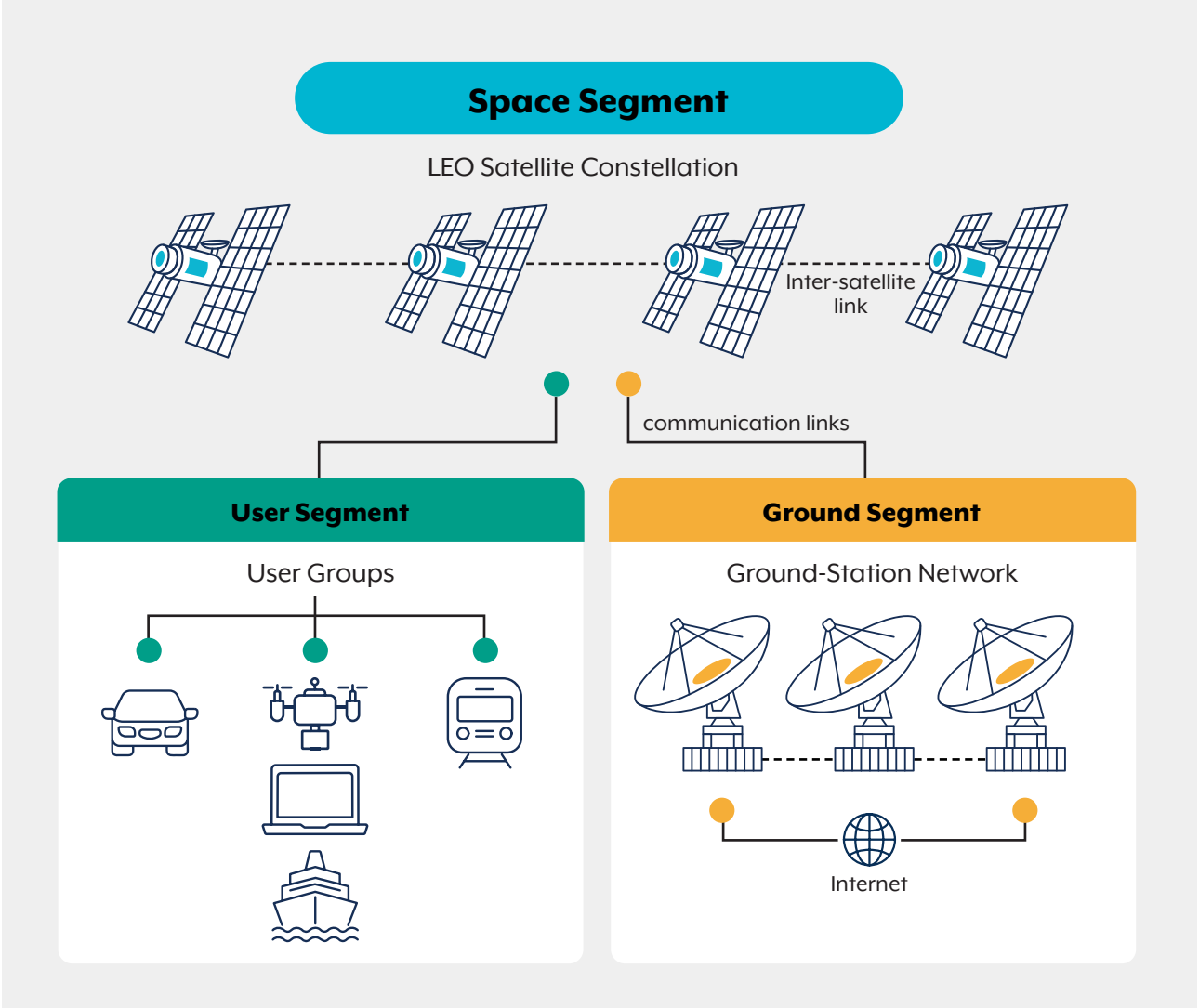


Figure 2. Typical LEO network architecture

LEO SATCOM users also need to consider secure data management and data sovereignty risks, which is further discussed below. For more information, refer to ASD's ACSC *Information security manual* and *Ten things to know about data security*.

Space segment

The space segment, comprising the satellites themselves, faces unique cyber threats due to its critical role in satellite communications.

Risks

Cyber threats such as jamming, unauthorised command injection, payload or platform hijacking, and firmware tampering target the space segment. Attackers may exploit vulnerabilities in command and control channels when encryption and authentication are not enforced consistently throughout the satellite's operational life. They may also impose additional risks including signal spoofing, malware injection, and memory corruption caused by deliberate fault injection.

Legacy space equipment faces acute challenges because designers built it before modern cyber security standards existed. Older satellites often lack secure-by-design architectures, making them more vulnerable to exploitation. Limited on-board processing capabilities and outdated software can hinder the implementation of security patches or advanced threat detection. Legacy systems also rely on unencrypted communication protocols or hardcoded credentials, increasing the risk of unauthorised access and control.

Mitigation strategies

To mitigate these threats, where possible, LEO SATCOM service providers may:

- implement bespoke security measures tailored to the specific satellite communications asset
- use frequency-hopping and spread signals over a wider frequency band to counter jamming
- implement redundant communication paths and diverse frequency bands
- employ anti-jam antennas, utilising cognitive radio technologies to detect the best available channels, geographically dispersing communication nodes, and deploying jamming detection and alert systems
- use dedicated management hosts and applications to access control interfaces, and separate out-of-band administration from data plane traffic flows
- ensure authentication and encryption of command links, general system hardening, and redundant system architectures to enhance resilience against both malicious and non-malicious threats.

For legacy systems still in operation, SATCOM providers should consider secure lifecycle management practices for the remaining operational life of these assets. This includes:

- retrofitting security controls where feasible
- restricting access through network segmentation
- monitoring telemetry for anomalies that may indicate compromise.

Ground segment

The ground segment encompasses satellite control centres, ground stations, gateways, and user terminals. This makes it a highly interconnected part of the space system and a critical target for malicious actors.

Risks

The ground segment is highly exposed to cyber threats due to its extensive connectivity with terrestrial networks. Ground segments are typically the most interconnected and vulnerable points in a space system.

Many of the cyber security threats associated with ground segments mirror those with terrestrial counterparts, and many of the mitigation measures are the same. Risks include malware injection, social engineering, and weak cyber security practices by users.

Ground segment systems are also susceptible to DoS attacks and unauthorised access through compromised credentials or software vulnerabilities.

Mitigation strategies

Continuous monitoring and anomaly detection in the ground segment of LEO SATCOM networks is essential for identifying cyber threats, system misconfigurations, and operational deviations in real time. Users may also request the following provider-managed capabilities:

- tenant isolation at gateways
- multi-factor authentication (MFA)
- network segmentation and isolation of critical systems and assets
- customer-specific logging and near real-time data export capabilities
- immutable audit trails
- resilience testing to validate gateway failover capabilities.

Mitigations provided by LEO SATCOM providers may also include enforcing strict access controls and regular software patching. Physical security of ground facilities also plays a critical role in maintaining security and operational continuity.



User segment

The user segment encompasses end-user devices, applications, and associated interfaces that connect to LEO SATCOM services. This segment is often the most distributed and least controlled environment, making it highly susceptible to cyber threats.

Risks

Risks include compromised user terminals, weak endpoint security, unpatched software, and insecure configurations. Attackers may exploit these vulnerabilities to gain unauthorised access, intercept sensitive data, or pivot into the broader SATCOM ecosystem.

Additional threats include credential theft, phishing, and exploitation of insecure application programming interfaces (API) or mobile applications used for SATCOM service management.

Inadequate user awareness and poor cyber hygiene further amplify these risks, as misconfigured devices or weak authentication practices can undermine even robust network-level protections.

Mitigations strategies

Mitigation strategies for the user segment should focus on strengthening endpoint security and enforcing secure access practices. Users should implement MFA, strong password policies, and device hardening measures such as disabling unused services and enforcing least-privilege principles.

Regular patching and updates for user terminals and associated applications are critical to address known vulnerabilities. Deploy endpoint detection and response (EDR) solutions where feasible to monitor for anomalous behaviour and potential compromise. Encryption of data at rest and in transit – preferably using end-to-end encryption – adds an additional layer of protection beyond provider-level safeguards.

Adopt secure configuration baselines for terminals, validate firmware integrity, and enable tamper-evident features where available. It is essential to provide comprehensive training for users on phishing awareness, credential management, and secure device handling to reduce human-factor risks. Service providers can support these efforts by offering hardened terminal configurations, security advisories, and managed security services tailored to user environments where possible.



Communication links

Communication links form an important part of LEO SATCOM systems. They enable data transfer between satellites and ground infrastructure but introduce unique security challenges.

Risks

Wireless communication links expose LEO SATCOM systems to threats such as jamming, spoofing, replay attacks, and eavesdropping. These threats can disrupt service availability, or compromise data confidentiality and integrity. Continuous monitoring and anomaly detection of LEO SATCOM communication links are vital for promptly identifying signal disruptions, spoofing attempts, or unauthorised access. Users may also request SATCOM providers to disclose cyber security considerations on:

- anti-jamming measures
- uplink/downlink power control mechanisms
- beamforming or nulling capabilities for dealing with interference
- the ability to quickly shift operational frequencies (frequency agility)
- the ability to select US Federal Information Processing Standards (FIPS)-validated link encryption suites
- replay attack protection
- time-limited cryptographic session keys.

Mitigation strategies

To counter these risks, LEO SATCOM service providers may adopt encryption protocols, anti-jamming techniques, frequency hopping solutions, and authentication mechanisms. Additionally, frequency diversity, beamforming (for dealing with interference), and adaptive modulation (changing the modulation scheme dynamically with the channel conditions) can help mitigate the impact of interference and improve link resilience.

Due to these risks, users of LEO SATCOM services are strongly encouraged to adopt strong encryption for all communications. This adds an additional layer of protection beyond what the LEO SATCOM provider may offer. Adopting strong encryption means using approved cryptographic algorithms or encryption mechanisms – including user controlled end-to-end encryption if possible – and secure data management practices as discussed in subsequent sections of this publication.

Preparing for post-quantum cryptography (PQC) is also essential. Users and providers of LEO SATCOM services should:

- establish key management strategies aligned with PQC standards
- define minimum encryption requirements for inter-satellite links
- define minimum encryption requirements for user access links.

For more information, refer to:

- *Information security manual*
- *Planning for post-quantum cryptography*
- Space systems and services – Cybersecurity and Infrastructure Security Agency (CISA)
- *Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) Cybersecurity Advisory* - NSA
- Cybersecurity for the space domain – National Cybersecurity Center of Excellence
- Space systems cyber-resiliency – Lincoln Laboratory, Massachusetts Institute of Technology

Supply chain

The supply chain for LEO SATCOM systems is a critical foundation for delivering secure and reliable connectivity, yet its complexity introduces unique challenges that demand careful oversight.

Risks

The supply chain for LEO SATCOM systems usually spans multiple vendors and subcontractors. It introduces risks such as hardware and software backdoors, tampering during manufacturing, and insertion of counterfeit components. The complexity and global nature of the supply chain make it difficult to ensure consistent security practices. Such complexity should not prevent users from requesting supplier attestation to secure-by-design and tamper-evident manufacturing, component provenance, transparency, and traceability.

Mitigation strategies

Mitigation strategies by LEO SATCOM service providers may include implementing supply chain risk management frameworks, conducting security audits, and enforcing component traceability. The adoption of common criteria security standards, along with testing and validation in controlled environments, may also help to detect vulnerabilities before deployment.

Sovereignty and trust in suppliers are also key considerations for critical components. As such, users are encouraged to request a Software Bill of Materials (SBOM) for satellite and ground software. Such Bills of Materials may provide insight into software components onboard satellites and ground systems. This enables vulnerability detection, compliance auditing, and secure lifecycle management in a highly sensitive and distributed communications environment. For best practices and SBOM consumption, visit NSA's *Securing the Software Supply Chain: Recommended Practices for Software Bill of Materials Consumption*.

Users of LEO SATCOM services should also request their service providers to implement secure-by-design and secure-development-lifecycle practices, ensuring satellite systems and ground infrastructure are architected with security from inception, and that that all software and hardware components undergo rigorous development, testing, and validation to proactively mitigate vulnerabilities before deployment.

For more information, refer to guidance on managing cyber supply chains and CISA's *A Shared Vision of Software Bill of Materials (SBOM) for Cybersecurity*.

Organisations may also consider minimising reliance on a single provider or platform by adopting modular and interoperable architectures where appropriate. This ensures the ability to switch to alternative SATCOM solutions when needed to strengthen resilience.

Secure data management in LEO SATCOM networks

Ensuring robust data management is essential to maintaining mission integrity and trust across highly distributed satellite ecosystems.

Risks

Effective data management in LEO SATCOM networks requires securing sensitive information across all states: at rest, in motion, and in use. These networks face a range of risks, including:

- unauthorised access to data transmitted between satellites and ground stations or between satellites
- manipulation of telemetry, mission data, or logs
- data theft from compromised ground station storage systems.

Mitigation strategies

To address these risks, LEO SATCOM service providers should implement a variety of mitigation strategies that embody Zero Trust principles.

Data loss prevention and network monitoring

Implementing a data loss prevention (DLP) strategy, alongside comprehensive network monitoring solutions, is critical for safeguarding sensitive information in LEO SATCOM environments. DLP strategies should include encryption of data at rest and in transit, strict access controls, and automated policies to prevent unauthorised data exfiltration.

Encryption of stored data

Apply approved quantum-safe cryptographic standards to secure onboard satellite storage, ground station data storage, and cloud environments. Full-disk encryption may further ensure that all data stored on spacecraft and ground systems remains secure.

Role-based access control

Role-based access control (RBAC) is a critical measure for limiting access to sensitive data. By assigning permissions based on job roles, providers can prevent unauthorised personnel from accessing restricted datasets. Enforce RBAC consistently across the satellite systems, ground stations, and API interfaces.

Continuous monitoring and audit log trails

Comprehensive event logging enables traceability and supports forensic analysis in the event of a breach. It also helps maintain the integrity of satellite operations. Additionally, data deletion policies should be in place to ensure secure handling of data during satellite decommissioning or end-of-life procedures.

Segmentation and trusted data zones

Isolate sensitive information within secure enclave environments on satellites or ground networks. Govern access to these zones with explicit, policy-based controls. Support these controls with cross-domain solutions to manage data flows securely between different security domains. Ensure only authorised users can interact with the data.

For more guidance on Zero Trust principles, refer to *Foundations for modern defensible architecture* and NSA's *Embracing a Zero Trust Security Model*

Data sovereignty and control across borders

Ensuring sovereignty over data becomes increasingly complex when information traverses global satellite infrastructures with fixed geographic boundaries.

Risks

Deploying and using LEO satellites introduces a range of sovereignty-related challenges that organisations should address. Users of LEO SATCOM services should engage with providers to obtain clear security assurances tailored to their specific operational and regulatory requirements.

A primary concern is the ownership and jurisdiction of data transmitted via LEO satellites. These systems often relay data across multiple national borders without passing through local infrastructure, so countries other than the origin may process or store the data. This cross-border transmission creates ambiguity around which national laws govern the data, complicating compliance with privacy and data protection regulations.

In many jurisdictions, national laws require telecom or internet service providers to obtain licenses and operate physical infrastructure within the country. However, LEO SATCOM operators may deliver connectivity without establishing a local presence or securing domestic licenses. This lack of physical infrastructure can exempt them from local oversight, making enforcement of national data regulations difficult.

Moreover, private satellite operators – due to their global infrastructure and operational autonomy – can exert significant control over data flows and access. This influence may exceed the regulatory capacity of individual nations, raising concerns about sovereignty and the protection of national interests.

Mitigation strategies

To address these risks, LEO SATCOM service providers may offer several mitigation strategies.

Geofenced data routing

Service providers can configure satellites to downlink data exclusively to ground stations within permitted jurisdictions. Providers should also document lawful access exposure by jurisdiction to ensure transparency about where and how local laws allow data access.

Multi-tenant segregation

Customer data is isolated at the satellite operating system, network and storage levels. Enforcing this segregation enables governments and organisations to align with national and regional regulations. It also enables them to better monitor activities, perform audits, and meet jurisdiction-specific data protection and strict data separation, confidentiality and privacy requirements.

Sovereign data zones

In-country edge computing and storage infrastructure ensures sensitive data remains under national legal control. In-country key management with customer-held keys may also help maintain cryptographic sovereignty and prevent unauthorised cross-border access.

Data localisation policies

Telemetry and other satellite-generated data should be stored only in designated or compliant cloud regions, aligned with national or regional regulations. Users may also request contractual terms that define data localisation and incident notification obligations.

Space traffic agreements

Providers should work with national regulators to predefine how satellite-generated data is handled across jurisdictions. These agreements help ensure that providers meet both technical compliance requirements (for example, encryption, storage location) and legal obligations related to data sovereignty.

Cyber security questions to ask LEO SATCOM service providers

The following section provides examples of cyber security questions to ask a LEO SATCOM services provider. Organisations should adapt these questions to their unique security needs and comply with any regulatory requirements.

Users and organisations should also consider strategies to reduce vendor lock-in and promote vendor diversification, especially for critical networks and services to improve resiliency and redundancy.

Encryption and data protection

- Do your SATCOM services support encryption?
- How does the system encrypt data in transit across uplinks, downlinks, and inter-satellite links?
- Do you cryptographically authenticate command and control traffic?
- What encryption algorithms and key management practices are used and are they quantum resistant?
- What is the post quantum cryptography migration plan and cutover triggers?
- How do you encrypt customer data at rest within your ground infrastructure and cloud systems?
- Can customers bring their own cryptographic keys with in-country hardware security modules?

Ground segment security

- How is access to ground control systems secured and monitored?
- What physical security controls are in place at your ground stations?
- Do you keep customer ground network traffic separate from your core operations infrastructure?
- What logging and audit capabilities do you provide for ground-based operations?
- Do you provide per-tenant security telemetry and APIs?

Communications network security

- How do you segment your satellite network to isolate tenants, missions or geographic zones?
- Do you support sovereign routing and in-region data residency?
- Can customers configure or request dedicated VPNs, VLANs, or isolated logical circuits?
- What protections do you have in place against jamming, spoofing, and replay attacks?

Threat detection, response and monitoring

- What telemetry or alerts can customers receive about potential cyber incidents?
- Do you have continuous monitoring for anomalies across your satellite and ground infrastructure?
- How quickly can you isolate or shut down a compromised node?
- What steps do you take to respond if you suspect a cyber attack in space or on the ground (for example, telemetry triage, node isolation, safe-mode fall back, key revocation, technical advisory publication, post-incident security attestations)?
- How often do you test and update this incident response process for scenarios of service loss and compromise?
- Are satellites capable of autonomous recovery from cyber or software failures (for example, safe modes)?
- How do you plan to evolve threat detection and response capabilities to address emerging threats and technologies (for example, artificial intelligence, 5G/6G integration)?

Supply chain assurance

- What measures are in place to protect the integrity of your hardware and software supply chain?
- Where is your equipment made, including internal components, and are they rebranded from another vendor?
- Do you maintain a Hardware Bill of Materials (HBOM) and can you share them?
- Do you maintain SBOMs for satellite and ground systems and can you share them?
- How are third-party software libraries or hardware components security vetted?
- Do you implement secure development environments for satellite software if you have in-house capabilities?

Security compliance, certifications and standards

- Do you align your systems with internationally recognised cyber security standards, and which standards do you follow?
- Have your systems been assessed under recognised cyber threat frameworks or a similar space-specific threat model?
- Do you support security assessments or certifications for satellite components and networks?
- How do you conduct compliance checks?
- What customer responsibilities exist in a shared-responsibility model (for example, user or ground network security)?
- Do you undertake red teaming or cyber security exercises, and are there any reports that you can share?

Contracts, service level agreements and security guarantees

- What are your service level agreements for data security, confidentiality, availability, and integrity?
- Do you provide service-level security guarantees (for example, encryption always-on or link tampering alerts)?
- What are your liabilities in the case of a cyber security breach?
- What does a shared responsibility model look like between SATCOM users and service providers?
- Can you provide an independent cyber security risk assessment for your satellite architecture?

Further information

Satellite communications and space systems

- 9.0 Communications - NASA
- Satellites and space systems - Australian Communications and Media Authority (ACMA)
- *Analysis of Low Earth Orbit Satellites: Implications for Australia's agriculture and mining sectors* - Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts
- *Low Earth Orbit (LEO) SATCOM Cybersecurity Assessment* - European Union Agency for Cybersecurity
- Space Information Sharing and Analysis Center (ISAC) - Space ISAC
- Space technology - Department of Home Affairs

Cyber security for satellite operations

- *Introduction to Cybersecurity for Commercial Satellite Operations* - National Institute of Standards and Technology (NIST)
- *Satellite Ground Segment* - NIST
- *Strengthening cybersecurity of SATCOM network providers and customers* - CISA

Threat modelling

- ATT&CK - MITRE
- SPARTA framework - Aerospace Corporation

Disclaimer

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Copyright

© Commonwealth of Australia 2026

With the exception of the Coat of Arms and where otherwise stated, all material presented in this publication is provided under a Creative Commons Attribution 4.0 International license https://creativecommons.org/licenses/by/4.0/

For the avoidance of doubt, this means this license only applies to material as set out in this document.



The details of the relevant license conditions are available on the Creative Commons website as is the full legal code for the CC BY 4.0 license https://creativecommons.org/licenses/by/4.0/legalcode.en

Use of the Coat of Arms

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website
https://www.pmc.gov.au/resources/commonwealth-coat-arms-information-and-guidelines

For more information, or to report a cyber security incident, contact us:

cyber.gov.au | 1300 CYBER1 (1300 292 371)

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian **Cyber Security** Centre