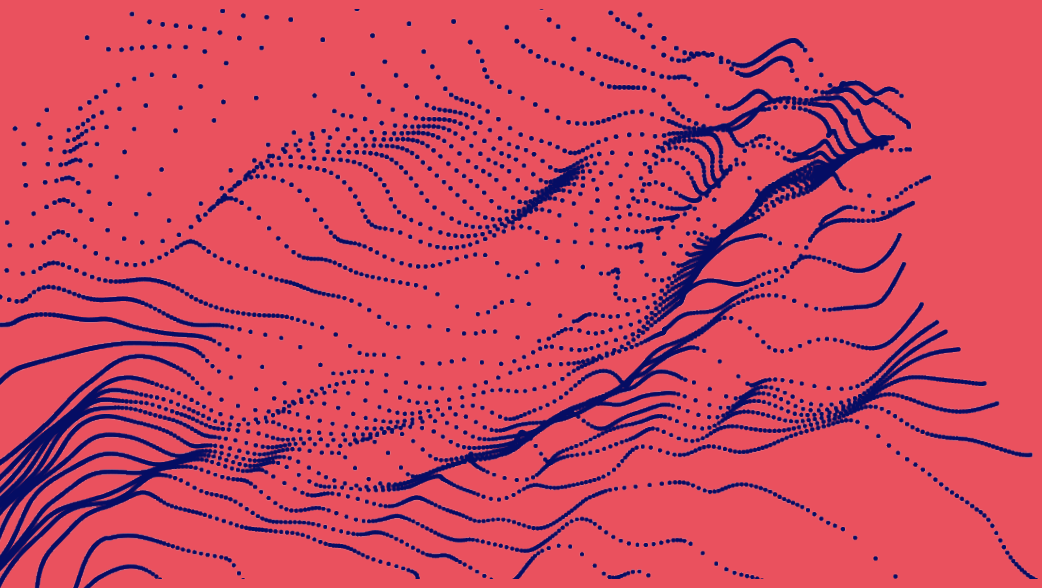
eutelsat

WHITEPAPER



PRIVATE NETWORK

LEO SATELLITE CONNECTIVITY FOR SECURE, CRITICAL, OPERATIONAL DATA

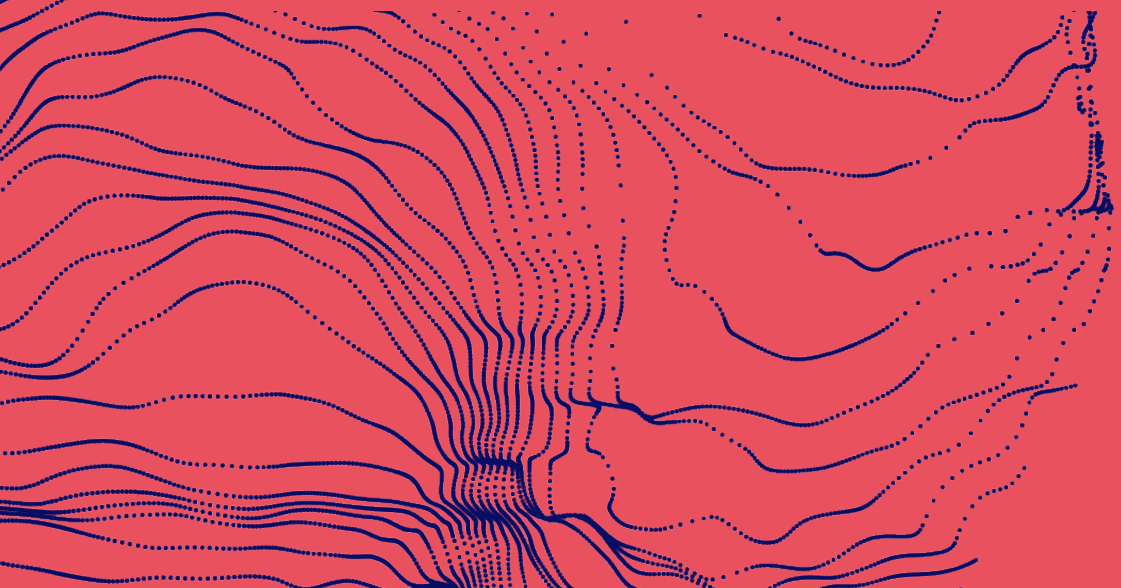
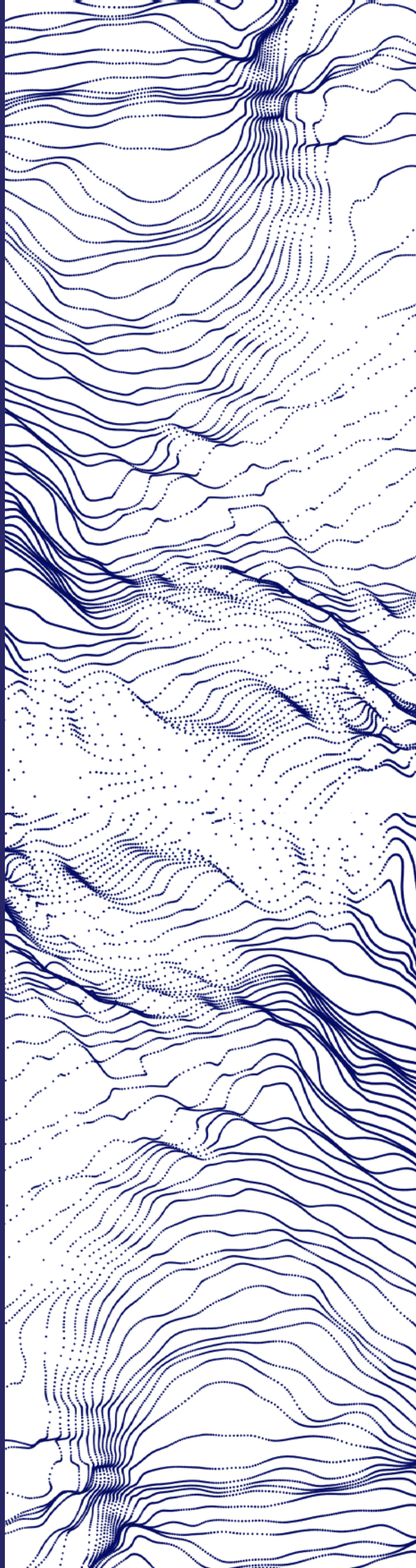


TABLE OF CONTENTS



EXECUTIVE SUMMARY

Critical Government and Enterprise operations– defence, emergency response, energy utilities, transport networks, and mining to name a few - are digitising their operations and generating higher volumes of commercially sensitive or highly regulated data in the process.

Part of this transformation requires new applications and technologies that rely on robust, reliable network solutions to serve and protect their customers. Without securing their networks, organisations place that data at risk.

Private network solutions can offer them greater guarantees and controls over security, data assurance, and locality to keep that information safe. This can be game-changing in times of severe disruption or congestion on the public network.

At a policy level, new regulatory and spectrum policies are in direct support of private networks as a service. India, for example, is evaluating direct allocation of 5G spectrum to enterprises, which will enable on-premise private networks. The European Union's Digital Decade strategy and associated compliance frameworks encourage secure, sovereign connectivity models for critical sectors. In the United States, the CBRS shared-spectrum regime at 3.5 GHz has opened a practical path for enterprises to deploy private LTE/5G, expanding areas where unencumbered private service can operate.

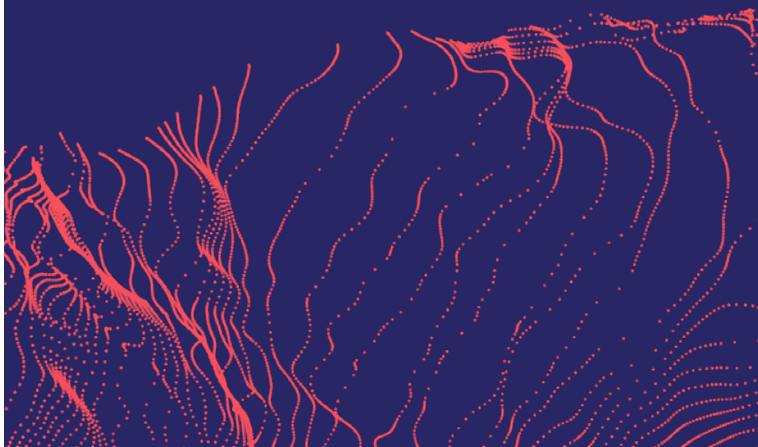
Satellite communications systems and their supporting ground infrastructure have a significant role to play. Low Earth orbit (LEO) communications in particular are taking high-speed, low-latency network access to the edge, along with the features and plans needed that enable private, secure connectivity for enterprise and government operations.

With LEO's global reach and performance, more customers can access the benefits of a private network service, even in the most remote locations, and across distributed environments.

HOW NEW POLICIES AND STANDARDS ARE CHANGING THE WAY ORGANISATIONS CONNECT

Guidance (e.g., agencies such as CISA's Cross-Sector Cybersecurity Performance Goals in the US) now frames a baseline of controls for critical infrastructure that organisations must translate into network design and operations.

Decision-makers should assess spectrum options, run focused pilots, design for zero-trust and resilience, and plan phased migrations that integrate with legacy systems to unlock safer operations and greater strategic control of private data.

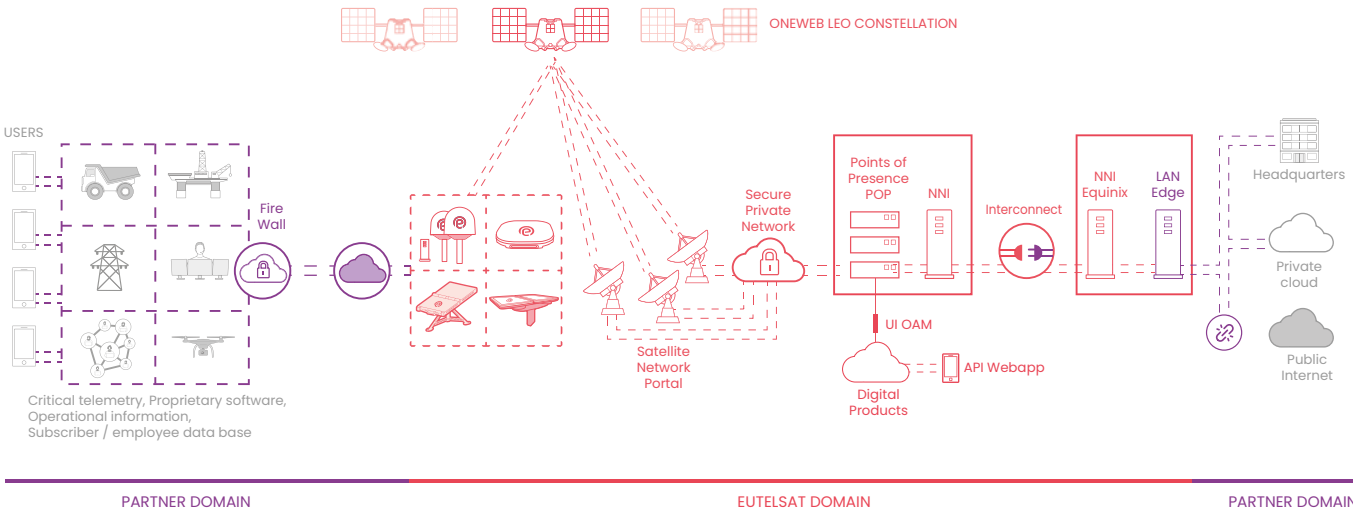


INTRODUCTION

MANAGING SENSITIVE DATA IN CRITICAL OPERATIONS

Industries that specialise in critical services increasingly rely on high-bandwidth, low-latency connectivity to run their operations. They may use new tools and applications for supply chain logistics, situational awareness, smart-grid controls, or autonomous operations. These workloads generate private data and safety-critical telemetry that require protection to mitigate risk as well as meet compliance standards (examples: EU's GDPR, Singapore's PDPA, Brazil's LGPD) through strict auditability and local processing.

Simultaneous advances in satellite communications technology mean that they can also benefit from satellite systems that orbit much closer to Earth than ever before. Unlike traditional geostationary (GEO) satellites, low Earth orbit (LEO) systems deliver the low-latency, high-bandwidth connectivity needed for handling critical workloads, either as the primary private network or as a resilient backup to existing fibre, microwave, or cellular infrastructure, ensuring continuity of operations when primary links are limited or disrupted.



Eutelsat delivers service features and plans so any data traffic through our domain can stay off the public internet. DPs who interconnect with us have the opportunity to apply additional layers of security whilst delivering that data to their customer.

HOW REGULATORS AND SERVICE PROVIDERS ARE RESPONDING

The need to better manage ever-increasing volumes of data has sent enterprise and public sector organisations in search of new standards, technologies and zero-trust policies, where traffic is kept local and restricted to dedicated cores and subscriber management.

Modern global 4G/5G standards (for e.g. 3GPP) are taking shape that explicitly support Non Public Networks (NPNs), where the compute can be isolated on premise, or data traffic is prioritised and managed securely alongside public networks.

WHY PRIVATE NETWORKS ARE GAINING ATTENTION

As AI becomes more powerful and as more critical data travels over public networks, organisations are becoming increasingly exposed, contributing to a sharp rise in data breaches worldwide. **worldwide**.

$4.44M

The global average cost (USD) of a data breach

Faster identification and containment of breaches—much of it from inhouse security service teams, with help from AI and automation— has moved the global average down. The global average would be lower were it not for the United States, where the average cost surged by 9% to USD 10.22 million, an all-time high for any region. Higher regulatory fines and higher detection and escalation costs in the United States contributed to this surge.

97%

Share of organisations that reported an AI related breach and lacked proper AI access controls

On average, 13% of organisations reported breaches that involved their AI models or applications. Among them, almost all (97%) lacked proper AI access controls. The most common of these security incidents occurred in the AI supply chain, through compromised apps, APIs, or plugins. These incidents had a ripple effect: they led to broad data compromise (60%) and operational disruption (31%). The findings suggest AI is emerging as a high-value target.

99%

Percentage of profit (before tax) for first half of 2025 that was wiped out following a cyberattack on the UK retailer Marks & Spencer

Data breaches in 2025 hit companies like 23andMe (genetic data), Samsung (customer records), TikTok (data transfers), Coinbase, Facebook, Amazon, and Meta. Sensitive data—including genetic, ID, account, and behavioral information—is especially high-risk. Regulatory penalties and public scrutiny increased significantly, with record fines imposed.

Key findings described are based on IBM analysis of research data independently compiled by Ponemon Institute. Download full report Cost of a data breach 2025 | IBM

https://www.ibm.com/reports/data-breach

LEO ADOPTION, INTEGRATION AND BENEFITS

LEO satellite communications network operators have taken a leading role, with infrastructure, plans and features that deliver private multilink solutions either as back-up or as primary. MNOs and other service providers incorporate these new LEO satellite solutions into their own portfolios, to meet a growing customer demand for what private networks offer. Whether their customer solutions are backed by Service Level Agreements and CIR for assured network performance can depend on which LEO satellite service provider they decide to use.

LEO HARDWARE AND INSTALLATIONS

As part of the LEO offering, worldclass equipment manufacturers are developing new, more portable, and easy-to-install products, designed for robust Enterprise-grade Land Fixed, Land Mobility (comms-on-the-move and comms-on-the-pause), Government, Maritime and Aviation applications.

KEY ADVANTAGES OF A PRIVATE NETWORK

OPERATIONAL

- End-to-end control with predictable outcomes
- Scalability at the edge
- Integrations with legacy systems

TECHNICAL AND SECURITY

- Data minimisation & locality
- Regulatory alignment for critical infrastructure
- Assured spectrum with CBRS

STRATEGIC

COMPETITIVE ADVANTAGE
Private networks give organisations a unique operational edge for sensitive telemetry that public networks cannot guarantee. With LEO, there are fewer latency or bandwidth constraints for valuable applications such as autonomous systems, real-time analytics, and predictive maintenance. This can result in higher productivity, lower operational costs, and improved safety metrics.

For Enterprise
Faster innovation cycles and reduced downtime improve profitability and shareholder value.

COMPLIANCE AND RISK GOVERNANCE
Critical industries operate under stringent regulatory frameworks. Private networks simplify compliance by providing segregated environments, controlled access, and audit-ready logs

For Enterprise
Reduces exposure to penalties and reputational damage while ensuring resilience against cyber threats

DATA SOVEREIGNTY AND IP PROTECTION:
Mining models, grid topologies, and emergency response strategies represent high-value intellectual property. Private networks keep this data within company-controlled infrastructure, preventing leakage through shared public networks.

For Enterprise:
Protection of algorithms and operational insights. Preservation and consolidation of long-term competitive advantage.

CUSTOMER BENEFITS

Brand trust and customer confidence
By ensuring sensitive operational telemetry remains within a controlled environment, companies can demonstrate a more robust approach to cybersecurity and compliance. This transparency builds trust with customers who depend on uninterrupted service and data integrity - critical for services where public safety is at stake.

Service reliability and continuity
Reduced dependence on a heavily congested or severely disrupted public internet service ensures continuity of communications in the event of traffic spikes or sudden crises. This translates into fewer outages, faster restoration times, consistent service quality, more reliable supply chains, and competitive pricing for the end customer.

More innovation for customer value
With localised data processing and edge computing, companies can deploy advanced analytics and automation faster. Mining firms can optimise production and safety. Utilities can accelerate smart grid rollouts. Emergency services can enhance their real-time situational awareness

Regulatory assurance
Meeting compliance standards (e.g., NERC CIP, CISA CPGs) not only avoids penalties but reassures customers that their service provider adheres to best practices for resilience and security—critical for sectors where public trust is non-negotiable .

SECTOR TRENDS AND PREDICTIONS

EMERGENCY SERVICES

Use cases

1. Disaster response bubbles
2. LMR–broadband interworking
3. UAS/robotics for SAR

Forecast
Expect widespread deployment of private 5G incident-area networks integrated with FirstNet's nationwide backbone. These networks will support mission-critical voice, video, and IoT sensors for disaster response. Communities benefit through faster, more coordinated emergency interventions, reducing casualties and property loss.

UTILITIES

Use cases

1. Smart grid Field Area Networks
2. Substation private cells
3. Storm/outage response

Forecast
Private networks will underpin distributed energy resource (DER) orchestration and real-time grid automation. This ensures faster outage detection and restoration, improving reliability for millions of households and businesses. Customers will experience fewer blackouts and better integration of renewables, supporting sustainability goals.

MINING

Use cases

1 Remote site connectivity
2 Autonomous haulage & drilling
3 Worker safety & situational awareness

Forecast
Within three years, most Tier-1 mining operations will adopt hybrid private LTE/5G networks with local cores. This will enhance autonomous haulage and predictive maintenance capabilities, reducing downtime and improving worker safety. For end customers—such as downstream manufacturers—this means more reliable supply chains and stable commodity pricing.

SUPPORTING EVIDENCE

- FCC and NTIA spectrum policy changes have expanded CBRS usability, enabling cost -effective private deployments in rural and industrial zones.
- NIST's 5G cybersecurity guidance reinforces the need for enterprise -controlled architectures, validating the trend toward private networks for critical sectors.
- FirstNet's $8 billion investment in 5G for public safety demonstrates institutional commitment to private or semi-private mission-critical connectivity

ASSUMPTIONS, GAPS AND RISKS

By addressing certain fundamental aspects below, businesses and organizations are best able to identify the private network solution most suited to their requirements.

ASSUMPTIONS:

- Licensed/shared spectrum remains available (spectrum availability and vendor ecosystems vary widely by country)
- Devices and network elements are available

GAPS:

- Operational skills gap
- Standards implementation lag

RISKS:

- Cyber & supply-chain exposure
- Geopolitical interference
- Coverage constraints
- Vendor lock-in
- Cost overrun
- Regulatory evolution

RISK MITIGATION

With better-informed implementation and strategies around data security, resilience and assurance on their networks, customers can reduce risk to a tolerable level, to restrict or eliminate setbacks.

1. System security by design
2. Spectrum planning with fallbacks
3. Role of open, standards-based architecture for interoperability, accessibility, and collaboration
4. Pilot-then-scale approach
5. Regulatory watch & governance
   Pilot-then-scale
6. Service management and support

ACTION LIST FOR DECISION-MAKERS

- **Feasibility study**
  Review local regulatory and infrastructure conditions.
- **Zero-trust reference architecture**
  Implement identity-centric access controls, device posture checks, and micro-segmentation across the private network. Ensure that every user and device is continuously verified, reducing the risk of lateral attacks.
- **Pilot in a high-value area**
  Pilot private network services to validate ROI and refine processes before scaling. Measure KPIs like latency, uptime, and safety improvements.
- **Set-up an operating model**
  Establish governance for lifecycle management of SIMs, devices, patches, and certificates. Define SLAs for performance and security monitoring and train staff for incident response.

WHAT EUTELSAT CAN OFFER

Eutelsat has a global LEO footprint and works with a network of trusted Distribution Partners (DPs) around the world that are expert in delivering private LEO satellite communications network solutions as part of their primary or backup service portfolio. We excel at partnership, flexibility and delivery, offering unique SLAs and CIR plans that provide Government and Enterprise operators with unique or complimentary LEO services depending on what they need.

NEXT STEPS

Speak to your Eutelsat account manager to find out more about private networks for your organisation.

CITATIONS

FCC – 3.5 GHz Band Overview:
https://www.fcc.gov/wireless/bureau-divisions/mobility-division/35-ghz-band/35-ghz-band-overview

NTIA Press Release:
https://www.ntia.gov/press-release/2024/ntia-fcc-navy-work-expand-innovative-35-ghz-spectrum-sharing-framework

FCC News Release:
https://www.fcc.gov/document/fcc-looks-modernize-35-ghz-citizens-broadband-radio-service-rules

NIST SP 1800-33A:
https://www.nccoe.nist.gov/sites/default/files/2025-03/nist-sp-1800-33a-ipd.pdf

CISA CPGs:
https://www.cisa.gov/cross-sector-cybersecurity-performance-goals

NERC US Reliability Standards:
https://www.nerc.com/pa/Stand/Pages/USRelStand.aspx

3GPP NPN:
https://www.3gpp.org/technologies/npn

FirstNet Authority:
https://about.att.com/story/2024/firstnet-investment.html

GLOSSARY

CBRS - Citizens Broadband Radio Service

CIP - Critical Infrastructure Protection

CISA - Cybersecurity & Infrastructure Security Agency

CPGs - Cross-sector cybersecurity performance goals

DER - Distributed energy resource

DPA - Dynamic Protection Areas

EU - European Union

FCC - Federal Communications Commission

GDPR - General Data Protection Regulation

LGPD - Lei Geral de Proteção de Dados (General Personal Data Protection Law)

LMR - Land mobile radio

NERC - North American Electric Reliability Corporation

NIST - National Institute of Standards and Technology

NTIA - National Telecommunications and Information Administration

NPN - Non-Public Network

OEM - Original equipment manufacturer

PDPA - Personal Data Protection Act

3GPP - Third Generation Partnership Project

QoS - Quality of service

SAR - Search and rescue

UAS - Unmanned aerial systems

32 BOULEVARD GALLIENI,
92130 ISSY-LES-MOULINEAUX. FRANCE
WWW.EUTELSAT.COM
+33 1 53 98 47 47

What can we do for you? Please visit
www.eutelsat.com/enquiries

CONNECTIVITY_ETL_WP_PRIVATE NETWORKS_12P_EN_1125