# Joint Statement of Requirements for Enabling Scalable Assured Drone Electronic Conspicuity, through Cellular Networks, Cellular Technologies, and Network APIs

***Published: 10 June 2026***

**A call to action for mobile network operators to support the next phase of drone aviation.**

**Introduction**

The global drone ecosystem is entering a new phase of scale, complexity and commercial relevance.

Commercial drones are increasingly being deployed across infrastructure inspection, emergency response, logistics, agriculture, security, public safety and industrial operations. As these use cases scale, the ability for drones to be electronically visible, identifiable and trusted within shared airspace becomes increasingly important.

Assured Electronic Conspicuity, i.e. electronic conspicuity that can be securely verified, will be a foundational enabler of this future.

However, current approaches to drone visibility and low and mid altitude airspace awareness remain fragmented, inconsistent and in many cases insufficient to support the scale, safety and interoperability required for routine operations.

This Joint Statement of Requirements reflects a growing alignment across the drone ecosystem that mobile networks and network APIs must now play a central role in enabling the next generation of safe, scalable and globally interoperable Electronic Conspicuity solutions.

This is not simply a future technical consideration; it is a near term requirement for the safe integration of drones into shared airspace at scale.

**The Market Reality**

The rapid growth of the drone ecosystem is fundamentally changing how low and mid altitude airspace must be managed.

Industry forecasts highlight the scale of the opportunity and the urgency of the challenge:

- The global drone market was valued at USD 73 billion in 2024 and is expected to reach USD 163 billion by 2030
- The commercial drone market alone is projected to grow from USD 30 billion in 2024 to more than USD 54 billion by 2030

- Annual drone shipments are expected to increase from approximately 1.5 million units in 2024 to over 3.3 million units by 2030

These figures make clear that drones are no longer a niche or experimental category. They are becoming a meaningful part of the future mobility, infrastructure and enterprise landscape.

As this market scales, regulators, operators, manufacturers and aviation stakeholders face a common challenge:

How do we safely integrate millions of aircraft into low and mid altitude airspace while maintaining visibility, trust, resilience and operational safety?

At this scale, millions of aircraft will require:

- persistent connectivity
- trusted identity frameworks
- reliable positioning and awareness
- and interoperable airspace services delivered consistently across markets and networks

**The Core Challenge**

Traditional aviation surveillance and visibility mechanisms were not designed for the density, diversity and operational profile of future drone ecosystems.

Several critical barriers are currently slowing the large-scale deployment of Beyond Visual Line of Sight (BVLoS) and advanced drone operations.

**Airspace awareness**

Aircraft must be able to electronically detect, identify and understand other users within shared airspace.

**Identity and trust**

Regulators, authorities and operators require mechanisms to verify the identity and legitimacy of drones operating in the airspace, while allowing anonymity for public safety and military aircraft.

**Security vulnerabilities**

Many current drone communication and visibility models remain vulnerable to spoofing, interference and weak authentication, while also failing to provide secure anonymity where appropriate.

**Connectivity limitations**

Drone operations require reliable communication across urban, rural and remote environments, and across multiple networks. Solutions are needed to ensure dependable connectivity in all settings, with resilient fallback options where traditional cellular coverage alone may not suffice.

**Fragmented global solutions**

Airspace monitoring and control systems must operate across borders. Isolated national technologies will limit scalability and introduce safety risks, making cross operator interoperability essential for seamless drone operations across networks and geographies.

These barriers are already constraining the deployment of scalable drone operations and limiting the economic potential of the wider ecosystem.

To address this, Electronic Conspicuity must increasingly be supported by the capabilities of the mobile network and exposed through standardised APIs. This approach must be globally aligned to ensure consistency across markets, give regulators and aviation authorities confidence and enable industry to scale with clarity.

**Why Telecommunications Networks Are Vital**

Telecommunications networks already possess many of the foundational capabilities required to support scalable drone Electronic Conspicuity.

These include:

- secure device and subscriber identity frameworks
- global connectivity infrastructure
- network based location intelligence
- programmable network performance
- and the ability to expose capabilities through standardised APIs

The emergence of 5G Standalone, Non-Terrestrial Networks (NTN), and A2X technologies defined by 3GPP further strengthens this opportunity by enabling hybrid architectures that combine terrestrial connectivity with satellite resilience.

Together, these capabilities provide a strong foundation for:

- Assured global connectivity coverage
- Assured secure identity and trust
- A secure backup and complement to GPS / GNSS
- scalable connectivity for millions of devices
- resilient communications in remote and underserved environments
- and programmable support for aviation grade use cases

This positions telecommunications networks not simply as connectivity providers, but as a potential digital infrastructure layer for the future of low altitude airspace.

**What Industry Requires**

To enable scalable Electronic Conspicuity for drone operations, the drone and aviation ecosystem requires mobile network operators to expose a set of capabilities that can support trust, visibility, resilience and interoperability at scale.

At a minimum, industry requires support for the following:

**Reliable command and control connectivity**

Drone operations require dependable communication between aircraft, pilots, operators, aviation services, and ground systems, including support for mission critical traffic.

**Trusted identity and authentication**

The ecosystem requires stronger mechanisms for verifying the legitimacy of drones, operators and connected systems interacting within the airspace, while enabling anonymity where required.

**Network assisted positioning and awareness**

Mobile networks can provide additional confidence layers for location, positioning and contextual awareness, complementing GNSS and other systems.

**Connectivity intelligence**

Operators should be able to expose meaningful information about coverage, performance and network suitability across planned flight routes and operational zones.

**Resilient hybrid connectivity**

Future drone operations will increasingly require support for architectures combining terrestrial cellular networks with satellite resilience layers.

These capabilities must be exposed in a way that is:

- standardised
- commercially consumable
- interoperable across operators
- and aligned to global industry and regulatory needs

**Priority Network APIs**

The following API categories are of particular relevance to this requirement:

- **Quality on Demand API** to support prioritised connectivity for mission critical drone command and control traffic
- **Location Verification API** to support trusted location checks and contribute to resilience against spoofing or false positional claims
- **Number Verification API** to support trusted authentication of drones, operators and associated systems
- **Population Density Data API** to support regulatory compliance, operational planning and ground risk modelling
- **Connectivity Insights APIs** to support visibility of network performance, route suitability and operational readiness – including QoS Estimation API and QoS Degradation Warning API
- **SIM Swap API** to support fraud detection and trust assurance by identifying recent SIM changes associated with operator or system-linked mobile numbers. In drone operations, this can help reduce the risk of compromised accounts, unauthorised mission access or malicious control attempts by flagging identity anomalies before a mission is approved or activated.

Together, these APIs represent the foundation of a programmable, scalable and interoperable Electronic Conspicuity model for the next phase of drone operations.

**Assured Outcomes Enabled by Network Capabilities**

Beyond individual APIs and technical functions, the wider opportunity is the delivery of assured outcomes required for scaled and trusted drone operations. This includes assured connectivity for priority command, control and payload data when it matters most, assured identity to strengthen trust in operators and devices, and assured awareness through reliable location, route and situational data.

Together, these capabilities move mobile networks beyond basic connectivity and toward becoming a trusted operational layer for future aviation services.

**The What, Where and When**

**What**

The drone industry requires mobile network operators to commercially expose and scale the network capabilities needed to support Electronic Conspicuity and trusted drone operations.

This includes, as a priority:

- **Quality on Demand**
- **Identity Verification**
- **Location Verification**
- **Population Density**
- **Connectivity Intelligence**
- **SIM Swap**
- and support for **hybrid terrestrial and NTN architectures**

The requirement is not simply for technical availability, but for standardised, interoperable and commercially consumable deployment.

**Where**

Initial deployment and engagement is sought in:

- the United States
- the United Kingdom
- and across the European Union

These markets are of immediate relevance because they are where:

- regulators are actively progressing BVLoS and low and mid altitude airspace frameworks
- public safety and enterprise drone demand is increasing
- and the opportunity exists for operators to establish early leadership in a new enterprise category

While early deployment is expected in these regions, the long-term objective is a globally interoperable framework that allows Electronic Conspicuity services to operate seamlessly across borders and networks.

**When**

The requirement is immediate.

Industry engagement, standards alignment and technical collaboration should begin now, with active deployment, testing and operational exposure progressing through 2026 to 2028 as drone operations move from pilots and early trials into routine operational use.

The market is forming now.

Across Europe, U-space regulation is already in force and certified service models are emerging, while in the United States the FAA is progressing BVLoS rulemaking and the market is scaling rapidly, with the US drone market expected to grow beyond $50 billion by 2030 and enterprise adoption accelerating across sectors such as energy, logistics and public safety.

**Statement of Requirements**

Based on the above, the participants in the GSMA Fusion Aviation roundtable call upon mobile network operators to work with the drone and aviation ecosystem to support scalable, secure and globally interoperable Electronic Conspicuity.

Specifically, mobile network operators are asked to:

- **Expose relevant network capabilities through standardised Network APIs** aligned with the GSMA Open Gateway and CAMARA frameworks
- **Prioritise the deployment of Quality on Demand and related APIs** to support mission critical drone command and control and operational resilience
- **Support aviation grade connectivity requirements** for drone operations, including reliability, consistency and route level suitability
- **Enable cross operator interoperability** to ensure drone services can operate seamlessly across national boundaries and multiple in-country networks
- **Support hybrid terrestrial and NTN based connectivity architectures** to enable broader operational coverage and resilience
- **Participate in collaborative testing, validation and standards development activities** with the GSMA, aviation stakeholders and regulators to help establish trusted deployment and certification pathways

This is not a request for isolated or experimental capability.

It is a call for operators to help establish the foundational infrastructure layer for the future of safe, connected and scalable low altitude aviation.

**Why This Matters Commercially for Mobile Network Operators**

The emergence of large-scale drone operations represents a clear and growing enterprise opportunity for mobile network operators.

Drone fleets operating across logistics, infrastructure, public safety, industrial inspection, utilities, security and emergency response will require more than basic connectivity. They will increasingly require:

- trusted identity services
- prioritised and assured connectivity
- route and coverage intelligence
- location and contextual awareness
- and resilient hybrid network architectures

These requirements map directly to the capabilities operators are already developing through 5G Standalone, Open Gateway and programmable network exposure.

This creates a meaningful commercial opportunity for operators to move beyond commoditised connectivity and instead provide aviation grade, enterprise grade digital infrastructure services to a rapidly growing ecosystem.

A globally standardised approach is what makes this commercially viable at scale.

Standardisation allows:

- drone manufacturers
- drone operators
- UTM (Unmanned Traffic Operators) providers
- public safety agencies
- regulators
- and enterprise users

…to build once and deploy consistently across multiple markets and networks.

That is what turns Electronic Conspicuity from a niche aviation problem into a scalable enterprise revenue opportunity.

Done correctly, this can create:

- new API monetisation opportunities
- new enterprise connectivity and assurance services
- stronger operator relevance in future mobility ecosystems
- and a strategic role for MNOs as foundational enablers of digital airspace infrastructure

In short:

This is not simply about supporting drones. It is about securing a role in the next generation of connected mobility and airspace services.

**Why Standardisation Matters**

Electronic Conspicuity will only achieve scale if it is built on globally aligned, interoperable and operator consumable foundations.

Without standardisation:

- enterprises and aviation stakeholders will face fragmented integrations
- trust models will vary by market and network
- regulators will struggle to support confidence at scale
- and commercial deployment will become slower, more costly and less interoperable

By contrast, a globally standardised model enables:

- consistency across borders
- repeatability across operators
- stronger confidence for regulators and authorities
- and a far more scalable commercial environment for industry and telecom alike

This is particularly important because drones, unlike many terrestrial connected devices, are inherently mobile across:

- geographies
- network domains
- operational environments
- and increasingly, regulatory jurisdictions

That makes standardisation not just beneficial, but essential.

**Regulatory Confidence**

Mobile networks do not only support drone operations, they can also provide greater confidence to regulators, Air Navigation Service Providers (ANSP) and public authorities through trusted, standardised and auditable data that supports safe, scalable and accountable airspace integration.

**Expected Outcome**

By enabling programmable network capabilities through standardised APIs, telecommunications networks can play a central role in the safe integration of drones into shared airspace.

This collaboration can support:

- scalable Electronic Conspicuity for millions of aircraft
- stronger identity and trust frameworks for airspace users

- resilient and interoperable connectivity for drone operations
- and a globally aligned foundation for future low altitude aviation services

Initial deployments are expected to emerge across the United States, the United Kingdom and European markets, where regulatory frameworks and operational demand are advancing most quickly.

Over time, this approach can support the development of a globally interoperable Electronic Conspicuity framework, allowing drones and aviation systems to operate more safely, consistently and commercially across borders and networks.

**Conclusion**

The drone industry is scaling quickly. The need for trusted, resilient and interoperable Electronic Conspicuity is no longer theoretical. It is now a practical requirement for safe, scalable and commercially viable drone operations.

The mobile network already contains many of the capabilities required to support this next phase.

This Joint Statement of Requirements therefore calls on mobile network operators to work with the drone and aviation ecosystem to expose the network capabilities, APIs and interoperable frameworks needed to support the future of connected airspace.

Those who engage early will not simply support the market. They will help shape it.