
## Introduction

The Indian Computer Emergency Response Team (CERT-In), under the Ministry of Electronics and Information Technology (MeitY), in collaboration with SatCoM Industry Association (SIA-India) released the Cyber Security Framework and Guidelines for Space including Satellite Communication (Framework) on 26 February 2026.

Given the critical role played by satellite communication (SatCom) in supporting governance, defence, navigation, disaster response, and considering the impact of potential safety and physical hazards, CERT-In recognises cybersecurity of SatCom systems as a matter of national importance and security. Accordingly, CERT-In has released the Framework establishing baseline cybersecurity obligations across the space, ground, communication link, and user terminal segments of satellite systems. It is designed for stakeholders in the space ecosystem such as government agencies, satellite service providers, ground station operators, terminal equipment vendors, and private space entities.

## Key Compliance Obligations

- *Incident reporting to CERT-In and log retention*: The Framework reiterates obligations specified in the the CERT-In Directions issued in 2022 (2022 Directions), expressly extending them to space infrastructure and requiring SatCom operators and service providers to: (a) report all confirmed or suspected cybersecurity incidents within 6 (six) hours of noticing such incident; (b) maintain incident logs for a minimum rolling period of 180 (one hundred eighty) days; (c) share point of contact details with CERT-In, and provide regular updates. Additionally, organisations in the SatCom / space ecosystem must maintain a documented and periodically tested incident response plan (IRP), execute containment measures immediately upon detection, undertake forensic analysis etc.

- *Security Certification*: The Framework requires all mission systems, ground infrastructure, and communication networks to comply with the Catalogue of Indian Standards for Space Industry, Norms, Guidelines and Procedures released by the Department of Space. Hardware, firmware and cryptographic module must undergo certification in accordance with recognised standards, such as ISO/IEC 27001, FIPS 140-3 etc.

- *Supply Chain Assurance*: SatCom entities must procure hardware and software only from trusted sources in accordance with Trusted Telecom Directive and the National Security Directive on Telecommunication Sector. Entities must also conduct supply-chain risk assessments and third-party audits before integration or deployment of components. In addition, such entities are required to maintain traceability of software and hardware components through mechanisms such as Bills of Materials as per the technical guidelines by CERT-In on SBOM, QBOM & CBOM, AIBOM, HBOM.

- *Auditing*: SatCom entities are required to undertake annual cybersecurity audits through CERT-In empanelled auditors and submit their findings and remediation actions to CERT-In. In addition to external audits, the entities are also required to implement an internal governance mechanism and conduct internal cybersecurity audit at least bi-annually.

- *Governance*: The Framework requires satellite operating entities to designate officers to oversee cybersecurity governance inside the organisation and maintain cybersecurity policies and crisis management plans for SatCom operations. Entities are also required to conduct resilience exercises to ensure preparedness for large-scale cyber incidents affecting satellite infrastructure.

- *Security by design and defense in depth*: SatCom entities are required to adopt "security-by-design" and "defense-in-depth" principles when developing and operating satellite communication systems. This means that cybersecurity considerations must be incorporated from the earliest stages of system design and development, rather than being added after integration or deployment, and that multiple layers of security controls should be implemented across the space, ground, and user segments to prevent single points of failure.

- *Incident Detection and Monitoring*: There are several provisions which address monitoring at different levels of the SatCom ecosystem. Entities are required to deploy continuous monitoring and anomaly detection mechanisms for telemetry, network activity, and system behaviour, and integrate monitoring data with CERT-In reporting systems. While the precise mechanism for reporting the monitoring data to CERT-In is not specified, it appears that entities are required to actively submit the monitoring data to CERT-In. Monitoring requirements are also specified for different segments i.e. space, ground and user, which can be achieved through dedicated Network Operations Center (NOCs) and Security Operations Center (SOCs).

## Conclusion

Recognizing space and satellite communication systems as critical infrastructure, the Framework provides a comprehensive and structured approach directly aimed at strengthening cybersecurity across India's space ecosystem. Although the Framework is presented as a '*baseline guiding document*', it uses expressions (such as 'must' and 'shall') which are articulated as mandatory and largely aligns with 2022 Directions. While there is no penalty provision, the Framework mandates SatCom entities to comply with applicable data protection, space and telecom laws and accordingly, any enforcement consequences may arise under such applicable laws.

In effect, the Framework establishes a common baseline of cybersecurity practices for stakeholders and serves as a de facto benchmark for cybersecurity practices in the space and SatCom ecosystem.

- *Harsh Walia (Partner); Sanjuktha A. Yermal (Senior Associate) and Aadarsh Prakash (Associate)*

## About Khaitan & Co

Khaitan & Co is a top tier and full-service law firm with over 1300+ legal professionals, including 300+ leaders and presence in India and Singapore. With more than a century of experience in practicing law, we offer end-to-end legal solutions in diverse practice areas to our clients across the world. We have a team of highly motivated and dynamic professionals delivering outstanding client service and expert legal advice across a wide gamut of sectors and industries.

To know more, visit **www.khaitanco.com**