Ministry of Electronics and Information Technology
Government of India

FEBRUARY 2026

CYBER SECURITY FRAMEWORK AND GUIDELINES FOR SPACE INCLUDING SATELLITE COMMUNICATION

ISSUED BY

Indian Computer Emergency Response Team
(CERT-In)
in collaboration with SIA-India

certin
Enhancing Cyber Security in India

SIA INDIA
An association for space industry

Table of Contents

Executive Summary

Space cyber security including Satellite Communication (SatCom) systems are crucial and play a key role in India's communication infrastructure, enabling connectivity across remote and tactical regions, supporting national security operations, disaster management, navigation services, broadcast, and economic activities. With the rapid expansion of commercial satellite services, ground stations, and user terminals, the space cyber security ecosystem has grown significantly in complexity and exposure to cyber risks.

Recognizing this, the Indian Computer Emergency Response Team (CERT-In), under the Ministry of Electronics and Information Technology (MeitY), Government of India in collaboration with SatCoM Industry Association (SIA-India) has developed a comprehensive framework and guidelines for Space Cyber Security for securing space communication assets and contributing towards the resilience of India's space ecosystem.

The framework and guidelines are designed to support stakeholders of space ecosystem including government agencies, satellite service providers, ground station operators, terminal equipment vendors, and private space entities by laying out essential cybersecurity principles, controls, and responsibilities.

The framework and guidelines provide:

- A detailed cyber threat landscape assessment specific to space systems, including risks such as signal jamming, spoofing, unauthorized command uplink, ground station compromise, and firmware manipulation.
- Segment-wise security controls across the space segment, ground infrastructure, communication links, and user terminals, covering authentication, encryption, access control, intrusion detection, and secure firmware practices.
- Mandates and best practices for incident detection, response, and reporting, in alignment with CERT-In Directions and sectoral coordination mechanisms.
- Provisions for risk assessment, supply chain security, equipment certification, and compliance with national and international cybersecurity standards.
- Emphasis on training, awareness, and the appointment of a Chief Information Security Officer (CISO) to enforce governance within organizations operating SatCom systems.
- A roadmap for periodic review, threat intelligence sharing, and alignment with global cybersecurity frameworks, such as those from the ITU (International Telecommunication

Union), CCSDS (Consultative Committee for Space Data Systems), NIST (National Institute of Standards and Technology), SPACE-Shield (Space Attacks and Countermeasures Engineering Shield), TREKS (Targeting, Reconnaissance, & Exploitation Kill Chain for Space) and SPARTA (Space Attack Research and Tactic Analysis)

By issuing this framework and guidelines, CERT-In aims to strengthen India's space-cybersecurity posture, promote secure deployment of satellite technologies, and enable trusted connectivity in both civilian and strategic domains. The document can be used as a baseline guiding document for assessing and auditing the cyber security posture of the space ecosystem.

1. Introduction

India's increasing reliance on Satellite Communication (SatCom) systems for strategic, commercial, and societal functions underscores the critical importance of ensuring their cyber resilience and operational integrity. SatCom networks play a pivotal role in national security, disaster management, navigation, broadcasting, e-governance, and remote connectivity. The growing convergence of satellite and terrestrial networks coupled with the integration of cloud-based services, software-defined payloads, and Commercial-Off-The-Shelf (COTS) components has expanded the cyberattack surface across the space cyber security ecosystem.

In recent years, the global space sector has witnessed a rise in cyber incidents targeting space assets, including unauthorized command uplinks, signal interference, ground station intrusions, and supply chain exploitation. These evolving threats can have cascading effects on communication reliability, data integrity, and mission continuity posing serious implications for both civilian and defense operations. Geographic Information Systems (GIS) are targeted for disruption, manipulation and exploitation of spatial data.

Space systems differ fundamentally from terrestrial digital systems in ways that are directly relevant to cybersecurity, and these differences are not marginal but instead shape threat exposure, response options, and consequence pathways. Space missions typically operate over long lifecycles with limited or no ability to patch systems once deployed, rely on intermittent connectivity, constrained bandwidth, and RF links, and make extensive use of bespoke protocols and mission-specific software rather than standardized stacks. They also increasingly depend on on-board autonomy and fault-management logic, meaning cyber events can directly influence system behaviour without immediate human intervention. As a result, cyber incidents in space may manifest as mission loss, orbital safety hazards, or physical damage, rather than purely informational compromise. These characteristics challenge core assumptions embedded in conventional enterprise and industrial cybersecurity models, making it inappropriate to treat space cybersecurity as a simple extension of IT or OT security. Instead, it must be understood as a cyber-physical mission-assurance problem

in which design choices, operational concepts, and consequence management are tightly coupled. The key threats are provided in Annexure A.

Recognizing these challenges, the Indian Computer Emergency Response Team (CERT-In), under the Ministry of Electronics and Information Technology (MeitY), has formulated the framework and guidelines for Space cyber security. The objective is to provide a comprehensive, risk-based cybersecurity framework for securing the end-to-end SatCom infrastructure spanning the space, ground, and user segments.

This framework and guidelines establish minimum security requirements, recommended best practices, and governance mechanisms for all entities engaged in satellite communication activities, including government agencies, public sector undertakings, satellite operators, service providers, equipment manufacturers, and private space enterprises.

Furthermore, CERT-In advocates a "security-by-design and defense-in-depth" approach, integrating cybersecurity considerations into every phase of the SatCom lifecycle from system design and launch operations to in-orbit management and decommissioning. By promoting continuous risk assessment, certification, monitoring, and incident response preparedness, this framework aims to build a resilient, trusted, and secure SatCom environment for India's growing digital and strategic ecosystem.

2. Definitions and Acronyms

This section defines key terms, technical expressions, and abbreviations used throughout the cyber security framework and guidelines for Satellite Communication (SatCom). The definitions aim to ensure a common understanding among all stakeholders, including government agencies, satellite operators, service providers, equipment manufacturers, and other entities involved in SatCom operations.

2. 1 Definitions

Term	Definition
Satellite Communication (SatCom)	The use of artificial satellites to provide communication links between points on Earth, enabling data, voice, video, and broadcast services through space-based systems.
Space Segment	The part of the SatCom system comprising satellites and their onboard subsystems, including the payload, bus, communication transponders, antennas, and onboard software.
Ground Segment	The terrestrial infrastructure supporting satellite operations, including ground control stations, mission operation centers, teleport facilities, network gateways, and associated ICT systems.
User Segment	The set of user terminals, modems, antennas, mobile or fixed devices, and related hardware/software that interface with satellite networks to access communication services.
Command and Control (C2) Link	The uplink and downlink communication channel used to transmit commands to and receive telemetry data from the satellite, ensuring operational control and monitoring.
Telemetry, Tracking, and Command (TT&C)	The system used to monitor and control a satellite, including communication for command uploads, tracking, and health status monitoring.
Payload	The mission-specific portion of a satellite responsible for performing its primary function, such as communication relay, imaging, or data transmission.

Encryption	The process of encoding data using cryptographic algorithms to ensure confidentiality and prevent unauthorized access.
Authentication	A process of verifying the identity of a user, device, or system component before granting access or executing a command.
Integrity	The assurance that data and system configurations are protected against unauthorized modification or corruption.
Availability	The assurance that systems and services are accessible and operational when required.
Cybersecurity Incident	Any event that compromises or has the potential to compromise the confidentiality, integrity, or availability of SatCom systems or services.
Vulnerability	A weakness in software, hardware, or process that could be exploited by a threat actor to gain unauthorized access or disrupt operations.
Threat Actor	An individual or group of individuals with the capability and intent to exploit vulnerabilities in SatCom systems. Examples include nation-states, cybercriminals, hacktivists, and insiders.
Security by Design	An approach where cybersecurity is integrated into system architecture and design from the earliest stages of the lifecycle.
Defense-in-Depth	A layered approach to security that employs multiple protective mechanisms across physical, logical, and operational domains.
Incident Response (IR)	A structured approach to detecting, analyzing, containing, and recovering from cybersecurity incidents affecting SatCom systems.
Supply Chain Security	Assurance mechanisms that prevent tampering, counterfeit components, or malicious code insertion across vendors, integrators, and manufacturers.
Chief Satellite Security Officer (CSSO)/ Chief Information Security Officer (CISO)	A designated officer responsible for the governance, compliance, and enforcement of cybersecurity policies as well as cyber security operations & process within space entities / space ecosystem.

Security Certification	A formal validation that a system, component, or process meets defined cybersecurity requirements, as per recognized standards (e.g., the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001, Federal Information Processing Standards (FIPS) 140-3, European Cooperation for Space Standardization (ECSS)).
Anomaly Detection	Continuous monitoring process to identify deviations from normal operational or network behavior that may indicate a security breach or system failure.
Cryptographic Module	A hardware or software component that performs encryption, decryption, key management, and authentication functions in SatCom systems.
Zero-Trust Architecture (ZTA)	A cybersecurity framework that assumes no implicit trust between network components and enforces verification of every access attempt.
Space Situational Awareness (SSA)	The ability to monitor, track, and analyze objects in orbit to ensure operational safety and threat detection in the space domain.
Space Domain Awareness (SDA)	The ability to detect, track, identify, and understand objects and activities in the space domain.
Data and Communication network	Collection of interconnected nodes and links that enables the transmission and exchange of data

2.2 Acronyms

Acronym	Full Form
AIS	Automatic Identification System
API	Application Programming Interface
CERT-In	Indian Computer Emergency Response Team
CSSO	Chief Satellite Security Officer
COTS	Commercial Off-The-Shelf
C2	Command and Control

ECSS	European Cooperation for Space Standardization
ENISA	European Union Agency for Cybersecurity
FIPS	Federal Information Processing Standards
GNSS	Global Navigation Satellite System
HSM	Hardware Security Module
ICT	Information and Communication Technology
IR	Incident Response
ITU	International Telecommunication Union
ISR	Intelligence, Surveillance, and Reconnaissance
LEO/MEO/GEO	Low, Medium, and Geostationary Earth Orbit
MeitY	Ministry of Electronics and Information Technology
NIST	National Institute of Standards and Technology
PNT	Positioning, Navigation, and Timing
QoS	Quality of Service
RF	Radio Frequency
SatCom	Satellite Communication
SOC	Security Operations Centre
TT&C	Telemetry, Tracking, and Command
VPN	Virtual Private Network
ZTA	Zero-Trust Architecture

2.3 International Cyber security Frameworks

Framework / Standard	Organization / Origin	Primary Focus	Space-Specific Emphasis	Mission Phase	Applicability
SPARTA (Space Attack Research and Tactic Analysis)	The Aerospace Corporation	Threat modelling / TTP taxonomy	Space-system attack techniques across ground, link, and space segments	Design, Operations	Threat-focused

SPARTA2	The Aerospace Corporation	Mission-centric threat modelling	Cyber-physical mission impacts, autonomy, lifecycle constraints	Design, Operations	Threat-focused (mission-driven)
SPACE-SHIELD	ESA-aligned research	ATT&CK-style threat framework	Space-specific attack and defense mapping	Design, Operations	Threat-focused
TREKS (Targeting, Reconnaissance, & Exploitation Kill Chain for Space)	Academic / industry research	Kill-chain modelling	Space vehicle–specific attack progression	Design, Operations	Threat-focused
SpaDoCs (Space Domain Cybersecurity Framework)	Research community	Layered cybersecurity framework	Enterprise-to-mission-to-system integration	Design, Launch, Operations	Assurance-focused
EMB3D (Embedded Device Threat Model)	MITRE	Embedded systems threat modelling	Spacecraft avionics and embedded flight hardware	Design	Threat-focused
NASA Space Security Best Practices Guide (BPG)	NASA	Mission assurance guidance	End-to-end space mission cybersecurity practices	Design, Launch, Operations	Assurance-focused
NIST IR 8401	NIST	Risk management adaptation	Satellite command and control cybersecurity	Design, Operations	Assurance-focused
NIST Cybersecurity Framework (CSF)	NIST	Cyber risk management	Tailored for space ground and ops segments	Design, Operations	Assurance-focused
NIST SP 800-53 (with Space Overlays)	NIST / DoD	Security control baselines	Space platform-specific control tailoring	Design, Operations	Assurance-focused

ISO/IEC 27001	ISO	Information security management	Organizational and ground infrastructure security	Design, Operations	Assurance-focused
CCSDS Security Recommendations	CCSDS	Secure communications standards	Cryptography and authentication for space links	Design, Operations	Assurance-focused
Space ISAC Guidance	Space ISAC	Threat intelligence & best practices	Sector-specific threat sharing and resilience	Operations	Threat-focused (operational)

3.Regulatory and Policy Framework

The Cybersecurity of Satellite Communication (SatCom) systems is a matter of national importance, given their critical role in supporting governance, defence, navigation, disaster response, and economic growth. To safeguard these assets, a robust regulatory and policy framework is essential, one that ensures accountability, standardization, and alignment with both national cybersecurity directives and global best practices. The Indian Space Policy 2023 (ISP-2023) and the subsequent Norms, Guidelines, and Procedures (NGP) by IN-SPACe provide a comprehensive regulatory framework for authorizing private sector (Non-Government Entity - NGE) space activities in India, detailing which activities need permission (like satellite operations, launches, ground systems), the criteria for approval, application processes, and conditions (like FDI limits, registration, incident reporting) to foster a robust, transparent, and responsible Indian space ecosystem..

This section outlines the regulatory mandates, governance structures, and compliance expectations that SatCom stakeholders must adhere to for maintaining a secure, resilient, and trusted communication infrastructure.

3.2 Regulatory Obligations for space entities

3.2.1 Incident Reporting and Response

- All SatCom operators and service providers must report cybersecurity incidents, breaches, or anomalies within 6 hours of noticing the incident to CERT-In. Detailed information can be found at www.cert-in.org.in.

- Maintain incident logs for a minimum rolling period of 180 days, accessible to authorities for audit or forensic investigation.
- Participate in coordinated response and recovery efforts during national-level cyber events.
- The details of the Point of Contact of the organizations must be shared with CERT-In and should be updated regularly as per CERT-In Directions, 2022.

3.2.2 Security Baseline and Certification

- All mission systems, ground infrastructure, and communication networks must comply with Catalogue of Indian Standards for Space Industry, Norms, Guidelines and Procedures (NGP) released by the Department of Space.
- Hardware, firmware, and cryptographic modules must be certified as per recognized standards (e.g., FIPS 140-3**,** Common Criteria**,** ISO/IEC 27001**,** ECSS-E-ST-80C).

3.2.3 Supply Chain Assurance

- Entities shall ensure procurement only from trusted sources, following the Government of India's Trusted Telecom Directive and National Security Directive on Telecommunication Sector (NSDTS).
- Supply chain risk assessments and third-party audits shall be mandatory before integration or deployment.

3.2.4 Data Protection and Privacy

- All SatCom operations must comply with the Digital Personal Data Protection Act, 2023 for handling user or customer information.
- Implement data minimization, encryption, and secure retention measures for telemetry and operational data.

3.2.5 Ubiquitous Communication Security

- International collaboration and data exchange including data localization within India, lawful interception capabilities, restrictions on routing data through foreign gateways, and requirements to indigenize ground infrastructure must be in compliance with the Indian Space Policy, 2023 and rules enforced by the Department of Telecommunications (DoT). Operators

must conduct periodic security reviews for international gateways and ground stations located abroad.

3.2.6 Periodic Auditing and Compliance Verification

- Entities shall undergo cyber security audits through CERT-In empanelled auditing organizations at least once in a year. Comprehensive Cyber Security Audit Policy Guidelines may be referred for a holistic cyber security audit. Findings and remediation actions shall be submitted to CERT-In for review

4. Situational Awareness/Threat Landscape in Space ecosystem

Situational awareness in the context of space ecosystem refers to the continuous understanding of the operational environment, potential threats, vulnerabilities, and ongoing incidents affecting the satellite ecosystem. Given that SatCom systems are of national importance supporting defense, navigation, disaster management, commercial communications, and scientific missions, maintaining a comprehensive view of the threat landscape is essential for risk mitigation and resilience.

4.1 Key Aspects of Situational Awareness in SatCom:

1. Asset Visibility:
    - Identification of all satellite assets, ground stations, control networks, and user terminals.
    - Awareness of satellite payloads, orbital parameters, communication frequencies, and interconnections.
2. Threat Monitoring:
    - Active monitoring of cyber and physical threats targeting satellites, ground stations, data links and including debris.
    - Tracking known vulnerabilities in satellite communication protocols (e.g., Digital Video Broadcasting - Satellite - Second Generation (DVB-S2), Consultative Committee for Space Data Systems (CCSDS), Transmission Control Protocol/Internet Protocol (TCP/IP) over SatCom).
    - Observing anomalous activities such as signal jamming, spoofing, or unauthorized access attempts.
3. Intelligence Gathering:

- Leveraging threat intelligence from CERT-In, regulatory authorities, other relevant & responsible agencies and industry partners.
- Monitoring global reports of cyber-attacks on commercial and government satellites for proactive defense.

4.2 Common Threats and Attack Vectors:

Communication Link	Common Cyber Attacks	Attack Vectors
Space to Ground (Downlink)	• Eavesdropping / interception • Data tampering • Signal spoofing • Replay attacks • Cyber-enabled jamming • Malicious data injection	• RF signals • Data links • Telemetry channels • Communication protocols
Ground to Space (Uplink)	• Command injection • Uplink spoofing • Unauthorized TT&C access • Denial of Service (DoS) • Credential theft • Firmware/software manipulation	• Control channels • Ground station networks • Command uplinks • Authentication/credentials
Ground to Ground (Terrestrial)	• Malware & ransomware • Phishing & social engineering • DDoS attacks • Insider threats • Database breaches • Supply-chain attacks	• IT networks • Email/social platforms • Server and database systems • Software/hardware components

4.3 Emerging Concerns:

- Increasing adoption of small satellites and mega-constellations increases attack surface.
- Integration of SatCom with terrestrial networks (5G, IoT) creates hybrid vulnerabilities.
- Use of AI-driven satellite operations introduces new threat vectors including adversarial attacks on decision algorithms.

4. 4 Situational Awareness Practices:

- Continuous monitoring of satellite telemetry and operational data for anomalies.
- Maintaining updated threat intelligence feeds from both domestic and international sources.
- Incident logging and trend analysis to identify patterns or recurring attack vectors.
- Collaboration with other space-faring nations and commercial operators for shared threat intelligence.
- Periodic cybersecurity assessments and penetration testing for both satellite and ground networks.
- Hazard and Damage Mitigation (HDM) planning to proactively identify, assess, and mitigate risks to satellite and ground systems.

5. Cybersecurity Principles for space ecosystem

Space ecosystems operate as part of a nation's strategic infrastructure, providing essential communication, navigation, and broadcast services across national, defence, and commercial domains. Given the strategic importance and high interdependence of SatCom networks, cybersecurity must be embedded as a core design and operational principle and not as an afterthought.

These cybersecurity principles serve as foundational pillars for ensuring the confidentiality, integrity, availability, and resilience of SatCom assets across all segments i.e space, ground, and user. They guide stakeholders in establishing governance, implementing controls, and maintaining trust in the end-to-end SatCom ecosystem.

5.1. Security-by-Design and by-Default

- Integrate security considerations from the earliest stages of system design, development, and integration.
- Implement secure coding, cryptographic safeguards, and vulnerability assessments throughout the satellite and ground system lifecycle.
- Default configurations should favour secure states (e.g., encrypted links, multi-factor authentication enabled).
- Developers can refer the principles outlined in the Guidelines for Secure Application Design, Development, Implementation & Operations published by CERT-In for more detailed Secure by design approach across the entire development life cycle.

5.2. Defense-in-Depth

- Employ multiple layers of protection across all network, hardware, and software interfaces: space, ground, and user.
- Combine physical, logical, and procedural controls to prevent single points of failure.
- Reinforce link security with redundant command authentication, secure telemetry handling, and protected data paths.

5.3. Least Privilege and Access Control

- Restrict system and data access strictly to authorized personnel and processes.
- Use role-based access control (RBAC) and just-in-time authorization for mission-critical functions.
- Implement multi-factor authentication (MFA) for all operator, vendor, and remote access interfaces.

5.4. Zero-Trust Architecture (ZTA)

- Assume no implicit trust between network components or users, even within secured boundaries.
- Continuously verify identities, validate communications, and monitor behavior across the ecosystem.
- Apply micro-segmentation and continuous verification for both ground control networks and user terminals.

5.5. Secure Communication and Encryption

- Enforce end-to-end encryption for telemetry, tracking, command (TT&C), and data payload links.
- Adopt standardized and validated cryptographic protocols (e.g., FIPS 140-3, Consultative Committee for Space Data Systems Space Data Link Security (CCSDS SDLS), Advanced Encryption Standard (AES)-256).
- Ensure key management systems are isolated, auditable, and resilient to compromise.

5.6. System Integrity and Assurance

- Establish mechanisms for verifying firmware, software, and configuration integrity through digital signatures or checksums.
- Enable secure boot and cryptographic validation of all mission-critical components.
- Implement change management procedures to track, test, and validate all updates.

5.7. Continuous Monitoring and Anomaly Detection

- Deploy real-time monitoring tools for telemetry, network activity, and payload performance.
- Detect anomalies, unauthorized commands, or unusual data flows through AI/ML-assisted analytics.
- Integrate monitoring data with CERT-In reporting systems.
- Subscribe and integrate machine readable alerts/feeds received from CERT-In and other stakeholder organization for proactive monitoring of threats.

5.8. Supply Chain Security

- Vet vendors, contractors, and component suppliers through security due diligence and certification.
- Verify hardware provenance, test for firmware tampering, and mandate secure update channels.
- Maintain traceability and auditability throughout manufacturing and logistics processes.
- Maintain Bill of Materials as per the technical guidelines on SBOM, QBOM & CBOM, AIBOM, HBOM issued by CERT-In.

5.9. Incident Preparedness and Resilience

- Develop and maintain a crisis management plan with a detailed Incident Response Procedure (IRP) and Business Continuity Plans (BCP) specific to SatCom operations.
- Conduct regular cyber drills, tabletop exercises, and red-team simulations involving all operational segments along with CERT-In.
- Participate in the technical drills and exercises organized by CERT-In
- Establish mechanisms for failover operations and rapid restoration of affected services.
- Prepare a Cyber Crisis Management Plan (CCMP) in line with the CCMP developed by CERT-In.

5.10. Governance, Accountability, and Compliance

- Appoint a Chief Satellite Security Officer (CSSO) to oversee cybersecurity governance within the organization.
- Deploy a dedicated team under the CSSO to develop policies and oversee the operations.
- Define clear accountability for compliance with CERT-In directions and other applicable guidelines issued by Department of Space and other relevant central agencies.
- Periodically assess and audit compliance to strengthen institutional security posture.
- Conduct internal cyber security audits at least once in six months and external cyber security audit through CERT-In empanelled auditing organization at least once in a year.

5.11. Awareness and Capacity Building

- Conduct regular cybersecurity training for mission operators, engineers, and vendor personnel.
- The CSSO must be trained with space sector related specific trainings in addition to cyber security related domains.
- Promote awareness of evolving cyber security threats and cyber security best practices.
- Encourage active participation in cyber security trainings organized by CERT-In, Department of Space and other relevant agencies.
- Cyber security awareness session should be made part of all induction training programmes for all employees.
- Cyber security awareness sessions must be conducted for all employees at least once in six months.
- Phishing/Awareness drills may also be conducted to regularly promote awareness against latest social engineering techniques.
- Promote professional certification programs in cybersecurity, networking, and space systems security.
- Encourage personnel to stay updated with the latest threat intelligence, vulnerability disclosures, and regulatory developments

6. Security Guidelines by Segment

The Satellite Communication (SatCom) ecosystem is composed of three interdependent segments Space Segment, Ground Segment, and User Segment. Each has unique assets, interfaces, and vulnerabilities that require layered defenses and a zero-trust

approach, enforcing strict access and continuous verification. The Network Operations Center (NOC) monitors network performance, traffic, and telemetry, while the Security Operations Center (SOC) detects threats, analyzes incidents, and coordinates responses. Having dedicated NoC and SoC capabilities is critical to maintain situational awareness, quickly identify anomalies or attacks, and ensure coordinated, timely action to protect operations. Together, they provide real-time oversight and protection, safeguarding the confidentiality, integrity, availability, and resilience of SatCom systems.

6.1 Space Segment

The Space Segment includes satellites and their subsystems such as the communication payload, telemetry, tracking and command (TT&C) module, onboard software, power systems, and cryptographic modules.

Domain	Guideline / Control	Space Cybersecurity Frameworks / Standards
Access Control & Authentication	Implement strong cryptographic authentication for all uplink commands using unique credentials per satellite	i. Consultative Committee for Space Data Systems Space Data Link Security (CCSDS SDLS) ii. NIST SP 800-53 – Security and Privacy Controls (IA-7, IA-5) iii. NIST CSF– Protect: Access Control (PR.AC) iv. ECSS – Software Product Assurance (ECSS-Q-ST-80) v. ISO/IEC 27001 – Information Security Management (ISO/IEC 27001 A.9)
	Enforce multi-factor authentication for command authorization at ground control	i. NIST SP 800-63 – Digital Identity Guidelines ii. NIST Cybersecurity Framework – Protect iii. Access Control (PR.AC-7) iv. ISO/IEC 27001 – Access Control (A.9) v. MITRE Adversarial Tactics, Techniques, and Common Knowledge for Space Systems (MITRE ATT&CK for Space – Initial Access)

Command and Data Link Protection	Use end-to-end encryption for telemetry, tracking, and command (TT&C) and payload data links	i. CCSDS SDLS ii. ECSS – Communications Engineering (ECSS-E-ST-70) iii. NIST Special Publication 800-53 – System and Communications Protection (SC-12) iv. ISO/IEC 27001 – Cryptographic Controls (A.10)
	Employ anti-jamming and anti-spoofing techniques for radio frequency (RF) communication	i. CCSDS Space Communications Security Standards ii. NIST Cybersecurity Framework – Protect: Protective Technology (PR.PT) iii. ECSS Software and System Security Standards (ECSS-Q-ST-80) iv. MITRE ATT&CK for Space – Communications Disruption
	Periodically rotate encryption keys and enforce key expiry policies	i. CCSDS Space Data Link Security (SDLS) ii. NIST Special Publication 800-57 – Key Management Guidelines iii. ISO/IEC 27001 – Cryptographic Key Management (A.10) iv. NIST Cybersecurity Framework – Protect: Data Security (PR.DS)
Software and Firmware Security	Use secure boot mechanisms and digitally signed firmware	i. NIST Special Publication 800-193 – Platform Firmware Resiliency Guidelines ii. ECSS Software Product Assurance and Safety Standards (ECSS-Q-ST-80) iii. ISO/IEC 27001 – System Acquisition, Development and Maintenance (A.14) iv. MITRE ATT&CK for Space – Persistence Techniques
	Disable or sandbox untrusted code or payload software	i. NIST Special Publication 800-53 – Configuration Management: Least Functionality (CM-7) ii. NIST Cybersecurity Framework – Protect: Information Protection Processes (PR.IP)

		iii. ECSS Software Security Standards (ECSS-Q-ST-80) iv. NIST Special Publication 800-207 – Zero Trust Architecture
	Maintain audit trails for software changes and version control	i. NIST Special Publication 800-53 – Audit and Accountability (AU-2) ii. ISO/IEC 27001 – Logging and Monitoring (A.12) iii. NIST Cybersecurity Framework – Protect: Information Protection Processes (PR.IP-3)
Configuration Management	Maintain a secure baseline configuration and restrict remote modifications	i. NIST Special Publication 800-53 – Baseline Configuration (CM-2) ii. ISO/IEC 27001 – Operational Security (A.12) iii. ECSS Software and System Security Standards (ECSS-Q-ST-80)
	Apply formal change control procedures before operational updates	i. NIST Special Publication 800-53 – Configuration Change Control (CM-3) ii. ISO/IEC 27001 – Change Management (A.12) iii. NIST Cybersecurity Framework – Protect: Information Protection Processes (PR.IP)
Anomaly Detection and Telemetry Monitoring	Continuously monitor telemetry for abnormal spacecraft behavior	i. NIST Special Publication 800-53 – System Monitoring (SI-4) ii. NIST Cybersecurity Framework – Detect: Anomalies and Events (DE.AE) iii. MITRE ATT&CK for Space – Detection Coverage iv. ECSS Communications and Operations Engineering Standards (ECSS-E-ST-70)
	Integrate anomaly detection alerts with ground-based Security Operations Centres (SOCs)	i. NIST Cybersecurity Framework – Detect: Security Continuous Monitoring (DE.CM) ii. ISO/IEC 27035 – Information Security Incident Management iii. NIST Special Publication 800-61 – Computer Security Incident Handling Guide

Redundancy and Fault Tolerance	Implement failover mechanisms for command links and subsystems	i. NIST Special Publication 800-53 – Contingency Planning: Alternate Communications (CP-7) ii. ECSS Dependability and Safety Standards (ECSS-Q-ST-80) iii. ISO/IEC 27001 – Information Security Continuity (A.17)
	Backup cryptographic modules and communication channels for resilience	i. NIST Special Publication 800-53 – Information System Backup (CP-9) ii. Consultative Committee for Space Data Systems – Space Data Link Security (CCSDS SDLS) iii. NIST Cybersecurity Framework – Protect: Protective Technology (PR.PT) iv. ISO/IEC 27001 – Information Security Continuity (A.17)

6.2 Ground Segment

The Ground Segment comprises mission control centres, ground stations, network gateways, data processing facilities, teleport sites, launch control systems, and associated ICT infrastructure.

Domain	Guidelines / Controls	Cybersecurity Frameworks and Standards
Physical and Environmental Security	Secure all control facilities with layered physical access controls (biometric, surveillance, guards)	i. ISO/IEC 27001 – Physical and Environmental Security (ISO/IEC 27001 A.11) ii. NIST SP 800-53 – Physical and Environmental Protection (NIST SP 800-53 PE family) iii. NIST Cybersecurity Framework – Protect: Access Control (NIST CSF PR.AC)
	Protect against environmental hazards through redundant power and heating, ventilation, and air conditioning (HVAC) systems	i. NIST SP 800-53 – Contingency Planning and Environmental Controls (CP, PE) ii. ISO/IEC 27001 – Business Continuity (A.17)

		iii. European Cooperation for Space Standardization – Dependability and Safety (ECSS-Q-ST-80)
	Implement tamper detection for communication racks and cryptographic hardware	i. NIST SP 800-53 – Physical Access Control and Monitoring (PE-6) ii. Federal Information Processing Standards 140-3 – Cryptographic Module Security (FIPS 140-3) iii. ISO/IEC 27001 – Physical Security Monitoring (A.11)
Network Security	Segregate mission-critical networks from enterprise IT and public internet using firewalls and virtual local area networks (VLANs)	i. NIST SP 800-53 – System and Communications Protection (SC-7) ii. NIST Cybersecurity Framework – Protect: Protective Technology (PR.PT) iii. ISO/IEC 27001 – Network Security Controls (A.13)
	Implement network intrusion detection and prevention systems (NIDS/NIPS)	i. NIST SP 800-53 – System Monitoring (SI-4) ii. NIST Cybersecurity Framework – Detect: Security Continuous Monitoring (DE.CM) iii. ISO/IEC 27001 – Logging and Monitoring (A.12)
	Employ virtual private networks (VPNs) with strong encryption (Internet Protocol Security or Transport Layer Security version 1.3) for remote access	i. NIST SP 800-52 – Guidelines for Transport Layer Security ii. NIST SP 800-77 – Guide to Internet Protocol Security (IPSec) VPNs iii. ISO/IEC 27001 – Cryptographic Controls (A.10)
Endpoint and System Hardening	Harden operating systems, disable unused ports/services, and enforce regular patch management	i. NIST SP 800-53 – Configuration Management and Vulnerability Remediation (CM, SI) ii. NIST Cybersecurity Framework – Protect: Information Protection Processes (PR.IP) iii. ISO/IEC 27001 – Secure Configuration and Patch Management (A.12)

	Use application whitelisting and restrict universal serial bus (USB) or removable media	i. NIST SP 800-53 – Least Functionality and Media Protection (CM-7, MP-7) ii. ISO/IEC 27001 – Media Handling (A.8) iii. NIST SP 800-207 – Zero Trust Architecture
Identity and Access Management	Implement Role-Based Access Control (RBAC) for operators, engineers, and contractors	i. NIST SP 800-53 – Access Control (AC-2, AC-6) ii. NIST Cybersecurity Framework – Protect: Access Control (PR.AC) iii. ISO/IEC 27001 – Access Management (A.9)
	Maintain logs of all operator activities and privileged access	i. NIST SP 800-53 – Audit and Accountability (AU family) ii. ISO/IEC 27001 – Logging and Monitoring (A.12) iii. NIST Cybersecurity Framework – Detect (DE.CM)
	Revoke credentials immediately upon role change or termination	i. NIST SP 800-53 – Account Management (AC-2) ii. ISO/IEC 27001 – User Access Removal (A.9) iii. NIST Cybersecurity Framework – Protect: Identity Management (PR.AC)
Supply Chain and Vendor Security	Validate all hardware and software through integrity checks and vendor certification	i. NIST SP 800-161 – Cybersecurity Supply Chain Risk Management ii. ISO/IEC 27036 – Information Security for Supplier Relationships iii. ECSS-Q-ST-80 – Software Assurance
	Ensure secure shipping and installation of ground equipment	i. NIST SP 800-53 – Supply Chain Protection (SR family) ii. ISO/IEC 27001 – Supplier Service Delivery (A.15)
	Conduct periodic third-party security audits	i. ISO/IEC 27001 – Information Security Reviews (A.18) ii. NIST Cybersecurity Framework – Identify: Risk Management (ID.RM)

Monitoring and Incident Response	Establish a dedicated Satellite Security Operations Centre (Sat-SOC) and integrate with Indian Computer Emergency Response Team (CERT-In)	i. NIST SP 800-61 – Computer Security Incident Handling Guide ii. ISO/IEC 27035 – Information Security Incident Management iii. NIST Cybersecurity Framework – Respond (RS)
	Enable centralized log collection, correlation, and real-time alerting	i. NIST SP 800-53 – Security Information and Event Management (SIEM) Controls (AU, SI) ii. ISO/IEC 27001 – Logging and Monitoring (A.12)
	Develop an incident response plan aligned with CERT-In procedures	i. NIST SP 800-61 – Incident Response Lifecycle ii. ISO/IEC 27035 – Incident Management Framework
Data Protection and Storage Security	Encrypt mission data at rest and in transit	i. NIST SP 800-53 – Cryptographic Protection (SC-12) ii. ISO/IEC 27001 – Cryptography (ISO/IEC 27001 A.10) iii. CCSDS SDLS
	Store cryptographic keys in Hardware Security Modules (HSMs) with audit logging	i. FIPS 140-3 – Security Requirements for Cryptographic Modules (FIPS 140-3) ii. NIST SP 800-53 – Key Management and Audit Controls (KM, AU families) iii. ISO/IEC 27001 – Key Management (A.10)
	Implement data retention and secure deletion policies	i. NIST SP 800-53 – Media Sanitization (MP-6) ii. ISO/IEC 27001 – Information Lifecycle Management (A.8) iii. NIST Cybersecurity Framework – Protect: Data Security (PR.DS)
	Implement post-quantum secure cryptographic algorithms in a phased rollout as suggested by Indian Computer Emergency Response Team (CERT-In)	i. National Institute of Standards and Technology Post-Quantum Cryptography Standardization Program (NIST PQC) ii. NIST SP 800-208 – Recommendation for Stateful Hash-Based Signature Schemes

		iii. ISO/IEC 23837 – Information security — Security requirements, test and evaluation methods for quantum key distribution

6.3 Communication Links

The Communication Link segment i.e the RF and transport pathways that connect space, ground, and user segments is a critical, distinct layer of the SatCom architecture. It carries telemetry, telecommands, payload data, and service traffic, and therefore requires dedicated controls beyond those for Space, Ground and User assets. The logical and physical communication links include:

- RF links (uplink/downlink, inter-satellite links),
- Ground-to-ground backhaul (satellite gateway→core network),
- Satellite payload links (bus↔payload),
- Cross-domain transports (SLE/SDL/Space Link Extension),
- Multiplexed terrestrial links used for telemetry or operator access.

The security objective of these links is focussed on

- Availability: Links must remain usable under normal and degraded conditions (resilience to jamming and DoS).
- Confidentiality: Prevent unauthorized access to link content (telemetry, payload, user traffic).
- Integrity & Authenticity: Ensure commands/data are from authorised sources and unmodified in transit.
- Non-repudiation & Auditability: Maintain tamper-evident logs for link events and key operations.
- Timeliness & Continuity: Preserve required timing and QoS for command/telemetry exchanges.

6.3.1 Primary threats to communication links

- Jamming / Denial of Service (DoS):
    - Intentional RF interference that degrades or blocks link availability.

- Spoofing / Replay / Injection:
    - False signals, replayed telemetry, or crafted uplink commands to mislead systems.
- Eavesdropping / Interception:
    - Passive or active capture of link content (telemetry, payload data).
- Man-in-the-Middle (MitM):
    - Tampering with link relays, gateways, or protocol endpoints to alter or reroute traffic.
- Signal Hijacking through weak authentication/keys:
    - Use of stolen/weak keys to authenticate malicious uplinks.
- Timing and Synchronisation Attacks:
    - Manipulation of timing protocols causing misordering or misinterpretation of telemetry/commands.
- Configuration Abuse / Misrouting:
    - Misconfiguration at gateways, routers or SLE endpoints causing data leakage.
- Supply-chain compromise (firmware in modems/ground modems/antenna controllers).

6.3.2 Technical controls

(a) Cryptography & Authentication

- End-to-end encryption for TT&C and payload data (use standardized, peer-reviewed ciphers crypto modules validated to FIPS 140-3 or equivalent).
- Cryptographic message authentication (MACs, digital signatures) on telecommands and critical telemetry.
- Mutual authentication for link endpoints (satellite and ground) using certificates or strong symmetric key mechanisms.
- Replay protection (sequence numbers / nonces / anti-replay windows).

(b) Key Management

- Use Hardware Security Modules (HSMs) for key storage at ground centers and secure elements/crypto modules onboard where possible.
- Strong key lifecycle management: generation, distribution, rotation, revocation, emergency recovery, with audit trails.
- Multi-party key approval for sensitive operations (threshold signing / multi-signature command authorization).

(c) RF Resilience & Anti-Jamming

- Spectrum planning and real-time spectrum monitoring to detect interference.
- Spread-spectrum / frequency hopping where operationally feasible.
- Adaptive power & link margin management and dynamic modulation schemes to tolerate interference.
- Use of directional antennas and nulling/beamforming techniques where available.
- Pre-arranged fallback frequencies / alternate gateways and link redundancy.

(d) Anti-Spoofing & Signal Validation

- Validate signal source by combining cryptographic authentication with RF-level checks (expected Doppler, time-of-flight, signal signature).
- Enforce command syntax whitelisting and context-aware checks on commands (e.g., do not accept high-impact commands outside scheduled windows or without multi-party approval).
- Implement process ID / command whitelisting aboard the satellite for allowed message types.

(e) Network-level Protections

- Segregate link-control traffic (TT&C) from payload/user traffic; use separate networks or strong virtual segmentation.
- Use IPsec/TLS for ground-backhaul transport where IP-based links are used.
- Enforce strict ACLs, firewall rules and next-gen NIDS at gateway boundaries.

(f) Operational Controls

- Time-bounded vendor maintenance windows with recorded, audited remote sessions (jump hosts, session recording).
- Out-of-band verification for high-risk actions (phone/email confirmation to independent contacts; out-of-band channels for emergency command authorization).
- Strict change management and signed/verified firmware update processes for modems, modems' controllers and baseband equipment.

6.4 User Segment (Terminals)

The User Segment includes end-user terminals, VSATs, modems, satellite phones, IoT gateways, and related equipment that connect to satellite networks for communication or data services.

Domain	Guidelines / Controls	Cybersecurity Frameworks and Standards
Device and Terminal Security	Ensure all user terminals (Very Small Aperture Terminals, satellite modems) use unique credentials and are not left at factory defaults	i. NIST SP 800-53 – Identification and Authentication (IA-5, IA-7) ii. ISO/IEC 27001 – Access Control (ISO/IEC 27001 A.9) iii. NIST CSF – Protect: Identity Management and Access Control (PR.AC)
	Enforce firmware signing and secure firmware updates from trusted sources	i. NIST SP 800-193 – Platform Firmware Resiliency Guidelines ii. ISO/IEC 27001 – Secure System Development and Maintenance (A.14) iii. ECSS – Software Product Assurance (ECSS-Q-ST-80)
	Disable open ports, debugging interfaces, and insecure protocols such as Telnet and File Transfer Protocol	i. NIST SP 800-53 – Least Functionality and Secure Configuration (CM-7) ii. ISO/IEC 27001 – Secure Configuration (A.12); NIST CSF – Protect: Protective Technology (PR.PT)
Encryption and Communication Security	Mandate quantum-resistant cryptographic algorithms for user data transmission	iii. NIST PQC iv. ISO/IEC 23837
	Prevent unencrypted backhaul connections from user terminals to ground gateways	i. NIST SP 800-52 – Guidelines for Transport Layer Security ii. NIST SP 800-77 – Guide to Internet Protocol Security Virtual Private Networks iii. ISO/IEC 27001 – Cryptographic Controls (A.10)

	Use authenticated key exchange protocols such as Internet Key Exchange version 2 and Transport Layer Security	i. NIST SP 800-56 – Recommendation for Pair-Wise Key Establishment ii. NIST SP 800-52 – Transport Layer Security Guidelines iii. ISO/IEC 27001 – Secure Communications (A.13)
Network and Access Control	Segment user networks from satellite control channels and critical infrastructure	i. NIST SP 800-53 – Boundary Protection and Network Segmentation (SC-7) ii. NIST Cybersecurity Framework – Protect: Protective Technology (PR.PT) iii. ISO/IEC 27001 – Network Security Management (A.13)
	Use firewalls or access control lists to limit external exposure	i. NIST SP 800-53 – Boundary Defense (SC-7) ii. ISO/IEC 27001 – Network Access Control (A.13)
	Continuously monitor terminal connectivity and access attempts	i. NIST SP 800-53 – System Monitoring (SI-4) ii. NIST Cybersecurity Framework – Detect: Security Continuous Monitoring (DE.CM) iii. ISO/IEC 27001 – Logging and Monitoring (A.12)
User Authentication and Policy Enforcement	Implement identity management for user devices accessing satellite networks	i. NIST SP 800-63 – Digital Identity Guidelines ii. ISO/IEC 27001 – Identity and Access Management (A.9) iii. NIST Cybersecurity Framework – Protect: Identity Management (PR.AC)
	Enforce strong password policies and account lockouts after repeated failures	i. NIST SP 800-63 – Authentication Assurance Levels

		ii. NIST SP 800-53 – Authenticator Management (IA-5) iii. ISO/IEC 27001 – Access Control Policy (A.9)
	Prohibit anonymous or guest access	i. NIST SP 800-53 – Account Management (AC-2) ii. ISO/IEC 27001 – User Access Restrictions (A.9)
Awareness and Training	Conduct regular awareness programs on social engineering, phishing, and device hygiene	i. NIST SP 800-53 – Security Awareness and Training (AT family) ii. ISO/IEC 27001 – Information Security Awareness (A.7) iii. NIST Cybersecurity Framework – Protect: Awareness and Training (PR.AT)
	Provide security advisories for configuration changes and software updates	i. ISO/IEC 27001 – Communications Security (A.13) ii. NIST Cybersecurity Framework – Protect: Information Protection Processes (PR.IP)
Remote Management and Logging	Secure remote management interfaces using multi-factor authentication and virtual private networks	i. NIST SP 800-63 – Multi-Factor Authentication ii. NIST SP 800-77 – Guide to Internet Protocol Security Virtual Private Networks iii. ISO/IEC 27001 – Secure Remote Access (A.13)
	Log all administrative actions on user terminals for traceability	i. NIST SP 800-53 – Audit and Accountability (AU family) ii. ISO/IEC 27001 – Logging and Monitoring (A.12)
	Restrict remote diagnostics to authorized personnel only	i. NIST SP 800-53 – Least Privilege (AC-6)

		ii. ISO/IEC 27001 – Privileged Access Management (A.9)

6.5 Cross-Segment Security Coordination

Since SatCom operations rely on seamless integration between space, ground, and user segments, the following cross-domain measures should be enforced:

- **End-to-End Risk Management:** Conduct joint vulnerability assessments involving all segments.
- **Unified Incident Response:** Ensure coordinated procedures among operators, ground stations, and service providers.
- **Shared Threat Intelligence:** Establish mechanisms for sharing alerts and advisories via CERT-In or sectoral CERTs.
- **Testing and Certification:** Mandate security testing (penetration, RF resilience, cryptographic validation) and certification for all critical assets before deployment.
- **Lifecycle Security:** Apply cybersecurity controls throughout the mission lifecycle from design and launch to operation and decommissioning.

7. Incident Detection, Response & Recovery

Given the strategic importance of satellite communication (SATCOM) infrastructure to India's national security, economic stability, and strategic information flow, robust mechanisms must be established for timely detection, coordinated response, and effective recovery from cyber incidents.

7.1. Incident Detection

- Monitoring & Logging: All ground, space, and user segment systems shall implement continuous monitoring of network traffic, system logs, and security events through Security Information and Event Management (SIEM) tools or equivalent frameworks.
- Anomaly Detection: Advanced analytics, threat intelligence feeds, and behavior-based anomaly detection shall be deployed to identify deviations in system performance, communication patterns, or command telemetry that may indicate malicious activity.

- All confirmed or suspected cybersecurity incidents affecting satellite networks, ground control systems, or user data shall be reported to CERT-In within 6 hours of noticing such incidents or being brought to notice about such incidents as per the cybersecurity directions of CERT-In.
- Sector-specific Security Operations Centers (SOCs) shall maintain an incident repository and coordinate with CERT-In/NCCC for threat intelligence correlation and policy refinement.
- The incidents can be reported to CERT-In via email (incident@cert-in.org.in), Phone (1800-11-4949) and Fax (1800-11-6969). The details regarding methods and formats of reporting cyber security incidents are also published on the website of CERT-In www.cert-in.org.in and will be updated from time to time. Incident reporting form is provided in Annexure E and contact details are provided in Annexure F.

7.2. Incident Response

- Incident Response Plan (IRP) - Each organization operating in the SATCOM and space ecosystem must maintain a documented and periodically tested Incident Response Plan detailing roles, escalation hierarchies, and communication channels. Organizations can also develop playbooks to handle cyber security incidents.
- Containment & Eradication - Upon detection, containment measures (such as isolation of affected network segments, disabling compromised accounts, or restricting command uplinks) shall be executed immediately to prevent propagation.
- Forensic Analysis - A structured digital forensic process shall be initiated to preserve evidence, identify the root cause, and assess the extent of compromise without disrupting mission operations.
- Stakeholder Coordination - Rapid coordination among the mission control, ground station operators, network administrators, and national cybersecurity agencies shall be ensured for unified response actions.

7.3. Recovery & Continuity

- System Restoration - Affected systems shall be restored to a verified secure state through re-imaging, patching, and validation of integrity before resumption of full operations.
- Backup & Redundancy - Regular, secure, and offline backups of mission-critical data and configurations shall be maintained, ensuring swift recovery from ransomware or data corruption events.

- Post-Incident Review - A post-incident analysis report shall be prepared to identify lessons learned, improve resilience, and update preventive controls.
- Resilience Drills - Space-sector entities shall conduct periodic cyber resilience exercises simulating communication jamming, data manipulation, or satellite control compromise scenarios to test and enhance response readiness in collaboration with CERT-In.

8. Risk Management and Assessment

Risk management and assessment in the space domain aim to identify, evaluate, and mitigate risks to the confidentiality, integrity, and availability (CIA) of assets across the Ground, Space, and User segments. Given the high-value, long-lifecycle, and remote nature of space assets, risk assessment must be continuous, dynamic, and integrated across all mission phases from design to decommissioning. Five-step approach to space cyber risk management:

Step	Description
a) Asset Identification	Map mission-critical assets (hardware, software, data, people) across all segments. Implement Bill of Materials based on CERT-In's Technical Guidelines on SBOM, QBOM, CBOM, AIBOM and HBOM.
b) Threat & Vulnerability Analysis	Identify internal/external threats from cyberattacks to environmental and supply chain risks. Evaluate vulnerabilities from outdated software, weak encryption, misconfigurations, or human error.
c) Risk Evaluation	Assess risks and Prioritize high-risk assets and systems essential to mission operations. .
d) Mitigation & Control Implementation	Apply controls (e.g., encryption, segmentation, authentication, patch management). Include physical security for ground systems and cryptographic security for command links.
e) Monitoring & Continuous Assessment	Continuously monitor mission health, security telemetry, and anomaly detection. Reassess after system updates, incidents, or environmental changes.

9. Security Governance and Compliance

Effective cybersecurity in the Satellite Communication (SatCom) domain requires more than technical controls as it demands structured governance, clear accountability, and measurable compliance. Security governance ensures that cybersecurity decisions, resource allocations, and incident responses are aligned with the mission objectives, national policies, and organizational risk appetite. This section provides guidance on establishing a governance framework for SatCom cybersecurity and ensuring ongoing compliance with regulatory and operational requirements as set forth by CERT-In, MeitY, DoS and IN-SPACe.

9. 1 Governance Framework Objectives

The governance framework aims to:

- Embed cybersecurity into strategic and operational decision-making within SatCom organizations.
- Establish roles, responsibilities, and accountability for cybersecurity across all segments.
- Ensure compliance with national and international standards through transparent processes and audits.
- Promote risk-informed, evidence-based security management across the SatCom lifecycle.
- Facilitate coordination and information sharing among stakeholders.

9.2 Governance Mechanisms

(a) Policy and Strategic Planning

- Each organization shall maintain a Cybersecurity Policy for SatCom Operations approved by top management and aligned with the guidelines of CERT-In, Department of Space and other relevant agencies.
- The policy must define objectives, scope, roles, data classification levels, and reporting structure.
- Cybersecurity considerations shall be integrated into mission design, procurement, and operations planning ("security by design" principle).

(b) Risk Oversight and Reporting

- The CISO and his team shall be responsible for conducting cyber security audits and compliance. CISO shall share the reports to senior management and CERT-In.
- Cyber threats must be escalated to CERT-In and IN-SPACe within defined timelines.
- A cyber risk register shall be maintained, with periodic reviews and tracking of mitigation progress.

(c) Coordination

- All SatCom entities must maintain communication channels with CERT-In and other relevant agencies & stakeholders for threat intelligence, advisories, and incident coordination.
- Maintain the list of Point of Contacts and update them regularly for effective coordination with all relevant agencies & stakeholders.

9.3 Compliance

(a) Standards and Baselines

- Compliance shall be based on a combination of:
    - National Standards: CERT-In Directions, MeitY security policy and DoS/IN-SPACe cybersecurity requirements.
    - International Standards: ISO/IEC 27001 (ISMS), ISO/IEC 27019 (Industrial Control Systems), CCSDS 355.0-B-2 (Space Link Security), NIST IR 8270 (Satellite Operations Security Framework), NIST SP 800-53 (Security and Privacy Controls for Information Systems and Organizations) ECSS-E-ST-80C.
- Entities shall map controls to these frameworks and maintain an evidence repository demonstrating compliance.

(b) Continuous Monitoring and Improvement

- Establish a Security Operations Centre (SOC) integrated with mission monitoring systems for continuous surveillance.
- Adopt a Plan–Do–Check–Act (PDCA) model for continuous improvement.
- Review security controls after each major satellite launch, ground network expansion, or vendor onboarding.

- Perform self-assessment using checklist in Annexure- B to assess progress from baseline compliance to advanced resilience

(c) Third party Outsourcing

- Information security audit report of the vendor to be made available to Procuring entity on periodic basis or when required.
- External party personnel should comply with the information security policies, processes and procedures of the organisation.The following information security requirements should be documented as part of the contract:
    - General policy on information security.
    - Procedures to protect organisational assets.
    - Restrictions on copying / disclosure.
    - Controls to ensure return of information/assets in their possession at the end of the contract.
    - The right to monitor and the right to terminate services in the event of a security
    - incident or a security breach.
    - Right to audit contractual responsibilities or to have the audits carried out by third parties.
    - Arrangements for reporting, notification and investigation of security incidents and breaches.
    - Background verification of all officials.

10. Security Testing and Certification

Security testing and certification are integral to ensuring that Satellite Communication (SATCOM) systems meet defined cybersecurity and reliability standards throughout their lifecycle. Given the mission-critical, high-cost, and long-duration nature of satellite operations, testing and certification help verify that the design, software, communication protocols, and operational processes are resilient to cyber threats, tampering, and data manipulation. The goal is to establish trust in both the spaceborne and ground-based components before and during operational deployment. The objectives include

- Validate that SATCOM systems comply with cybersecurity requirements defined in applicable standards and frameworks.
- Detect vulnerabilities and configuration weaknesses before deployment.

- Ensure the integrity, authenticity, and confidentiality of data, control commands, and telemetry.
- Provide an evidence-based assurance of security posture to regulators, operators, and end users.
- Enable continuous improvement and re-certification across lifecycle phases (design → launch → operations → decommissioning).

10.1. Security Testing Phases

Phase	Description	Focus Areas
a. Design Validation	Early security testing integrated in design reviews.	Threat modeling, secure coding, architecture validation, and encryption design verification.
b. Component & Integration Testing	Conducted during assembly and integration (AIT) of satellite subsystems.	Hardware/firmware integrity, interface testing, cryptographic key management, supply chain verification.
c. Pre-Launch Security Testing	Before launch, simulate communication and control operations.	Penetration testing of ground stations, command authentication, radio frequency (RF) link robustness, and access control.
d. In-Orbit & Operational Testing	Continuous and periodic validation during mission operations.	Vulnerability scanning, anomaly detection, intrusion simulation, update/patch validation.
e. End-of-Life Verification	Conducted before decommissioning or disposal.	Secure data erasure, command link disablement, and system isolation assurance.

10.2. Testing Techniques

- Penetration Testing (Red Team Assessments): Simulated attacks on ground stations, TT&C (Telemetry, Tracking, and Command) systems, and network infrastructure to reveal exploitable flaws.
- Vulnerability Scanning: Automated tools assess onboard software, ground infrastructure, and communication protocols for known vulnerabilities.
- Cryptographic Validation: Verification of encryption algorithms, key lengths, and management systems against standards such as FIPS 140-3 and CCSDS SDLS.
- RF and Signal Integrity Testing: Assessing susceptibility to jamming, spoofing, or signal interference.
- Software Assurance Testing: Static and dynamic analysis of onboard software and firmware.
- Supply Chain Testing: Tamper detection, hardware provenance verification, and third-party component validation.

10.3. Certification Frameworks & Standards

Security certification validates that a system conforms to agreed cybersecurity baselines and can safely interoperate with other systems. Recommended frameworks include:

Standard / Body	Focus
European Union Agency for Cybersecurity – Space Cybersecurity Controls Framework (ENISA, 2025)	Defines structured cybersecurity control families across space, ground, communication link, and user segments; aligned with European space and critical infrastructure protection objectives.
European Cooperation for Space Standardization – Security in Space Systems Lifecycle (ECSS-E-ST-80C)	Specifies security engineering requirements across the space system lifecycle, including design, verification, validation, testing, and certification activities.
Consultative Committee for Space Data Systems – Space Data Link Security (CCSDS 355.0-B-2)	Defines standardized link-level security mechanisms for telemetry, tracking, and command, including encryption, authentication, key management, and anti-replay protections.
National Institute of Standards and Technology Interagency Report 8270 – Cybersecurity Assurance for Satellite Operations (NIST IR 8270)	Provides cybersecurity assurance principles, threat models, and control guidance tailored to commercial and civil satellite operations.

Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408)	Enables independent third-party security evaluation and certification of satellite components such as operating systems, cryptographic modules, firmware, and secure elements.
Federal Information Processing Standards 140-3 – Security Requirements for Cryptographic Modules (FIPS 140-3)	Specifies validation requirements for cryptographic modules and hardware security modules used in satellite, ground, and communication systems.
International Organization for Standardization / International Electrotechnical Commission 27001 – Information Security Management Systems (ISO/IEC 27001)	Establishes a risk-based Information Security Management System applicable to satellite operators, ground stations, service providers, and vendors.
ISO/IEC 27002 – Information Security Controls	Provides detailed implementation guidance for organizational, technical, and operational security controls supporting ISO/IEC 27001 compliance.
ISO/IEC 27019 – Information Security for Industrial Control Systems	Extends ISO/IEC 27001/27002 controls for operational technology environments such as satellite control systems and ground station infrastructure.
National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)	High-level framework for managing cybersecurity risk across Identify, Protect, Detect, Respond, and Recover functions; widely used for governance and compliance mapping.
NIST Special Publication 800-53 – Security and Privacy Controls for Information Systems	Comprehensive catalog of security controls used for high-assurance and regulated systems, including satellite ground and control environments.
NIST Special Publication 800-193 – Platform Firmware Resiliency Guidelines	Defines protection, detection, and recovery requirements for firmware in satellite, ground, and user equipment.
NIST Post-Quantum Cryptography Standardization Program (NIST PQC)	Defines quantum-resistant cryptographic algorithms and transition guidance for long-lived satellite and ground systems.
MITRE Adversarial Tactics, Techniques, and Common Knowledge for Space Systems (MITRE ATT&CK® for Space)	Provides a threat-based adversary model for space systems, supporting threat modeling, detection, and resilience planning.
International Telecommunication Union – Radio Regulations and Security-Relevant Recommendations (ITU-R)	Governs spectrum use, interference mitigation, and radio communication integrity for satellite systems.
ISO/IEC 27035 – Information Security Incident Management	Defines incident detection, response, and coordination processes applicable to satellite and ground operations.

ISO/IEC 22301 – Business Continuity Management Systems	Supports resilience and continuity planning for satellite operations, ground stations, and communication links.
ISO/IEC 27036 – Information Security for Supplier Relationships	Addresses supply-chain and vendor security risks in satellite manufacturing, launch services, and ground infrastructure.
EN 303 645 – Cybersecurity for Consumer and IoT Devices	Relevant for user terminals and satellite-connected devices, particularly in mass-market SatCom and IoT services.
Zero Trust Architecture – NIST Special Publication 800-207	Provides a modern security architecture model applicable to satellite ground networks, user access, and control plane protection.

References

1. CERT-In Guidelines on Information Security Practices for Government Entities
2. CERT-In's 15 Elemental Cyber Defense Controls for Micro, Small, and Medium Enterprises (MSMEs)
3. CERT-In's Technical Guidelines on |SBOM | QBOM & CBOM | AIBOM | HBOM
4. CERT-In's Comprehensive Cyber Security Audit Policy Guidelines
5. ENISA Space Threat Landscape 2025
6. CISA Recommendations to Space system Operators for Improving Cybersecurity 2025
7. CERT-In Advisory on Cybersecurity Threats and Best Practices for Satellite Communications
8. NIST: Cybersecurity Framework Profile for Hybrid Satellite Networks (HSN)
9. NIST: Introduction to Cybersecurity for Commercial Satellite Operations
10. NIST: Foundational PNT Profile: Applying the Cybersecurity Framework for the Responsible Use of Positioning, Navigation, and Timing (PNT) Services
11. MITRE: Cyber Best Practices for Small Satellites
12. BSI TR-03184 Information Security for Space System

Annexures

A. Key threats and mitigation mechanisms

B. Self-Assessment Maturity assessment

C. CERT-In's Incident Reporting Format

D. CERT-In contacts

Annexure A

Key threats and Mitigations

I. Radio Frequency (RF) and Link Segment Threats (Availability & Integrity)

These threats specifically target the wireless communication links between the ground and space segments.

Threat / Tactic	Target Segment	Adversary Goal	Potential Impact	Key Mitigation Strategies
Jamming	Link (Uplink/Downlink)	Overpower legitimate signals with high-power interference.	Denial of Service (DoS): Total loss of data transfer, Telemetry, Tracking, and Command (TT&C) link disruption, service outages.	Frequency Hopping Spread Spectrum (FHSS), Anti-Jamming (AJ) techniques, High-gain/Directional antennas, Signal Monitoring (RF/Spectrum).
Spoofing	Link/User Terminal	Send false or deceptive signals (e.g., false GPS signals or malicious commands) to deceive receivers.	Integrity/Control Loss: Satellite disorientation, false navigation data, misrouting of communications, unauthorized command injection.	Robust Authentication (PKI/Digital Signatures for commands), independent timing sources, Cryptographic integrity checks (MACs).
Interception / Eavesdropping	Link (Downlink)	Passive listening to capture transmitted data and telemetry.	Confidentiality Loss: Disclosure of sensitive command data, intelligence, user communications, or proprietary system telemetry.	End-to-End Encryption (Strong, modern algorithms), Secure Key Management (PKI), Low Probability of Intercept/Detection (LPI/LPD) waveforms.
Signal Replay Attack	Link (Uplink)	Re-broadcasting a legitimate, captured command or signal to achieve	Integrity/Control Loss: Re-execution of old, valid commands (e.g., turning on/off a component).	Time-Varying Encryption Keys, Sequence Numbers, or Time-Sensitive Challenge-Response

		unauthorized access or disrupt operations.		Authentication protocols.

II. Ground Segment Threats (Access & System Compromise)

These threats target the IT and Operational Technology (OT) infrastructure that controls the satellite fleet.

Threat / Tactic	Target Segment	Adversary Goal	Potential Impact	Key Mitigation Strategies
Ground Network Compromise	Network Operations Center (NOC) / Gateways	Exploit IT vulnerabilities (phishing, malware, unpatched servers) on the corporate network.	Lateral Movement: Pivot from IT to the specialized TT&C Network or payload networks.	Network Segmentation/Isolation (Zero Trust between IT/OT/TT&C), Intrusion Detection Systems (IDS), strong EDR.
Command Injection	Mission Control / TT&C Systems	Gain unauthorized access to inject malicious code or commands into the satellite's operating system or firmware.	System Damage/Loss: Manipulate orbital mechanics, disable safety protocols, exfiltrate or wipe mission data, *Kinetic attack enablement*.	Multi-Factor Authentication (MFA) for all control systems, Command Validation (redundant checks, sanity limits), Secure Boot.
Insider Threat	All Systems (Ground Personnel)	Malicious or unintentional misuse of authorized access by an employee or contractor.	Data Compromise (Theft of intellectual property), System Sabotage (TT&C system failure).	Principle of Least Privilege (PoLP), strict Privileged Access Management (PAM), mandatory separation of duties, comprehensive logging and auditing.
Supply Chain Attack	Ground Station Equipment / Flight Software	Compromise hardware or software components before	Integrity Loss: Backdoors in ground terminal modems or satellite flight	Rigorous Vetting of vendors, component manifest and integrity checks, Hardware Root of Trust.

		deployment (e.g., malware in vendor firmware).	software, long-term espionage.	

III. Space Segment Threats (On-Orbit Persistence)

These threats target the satellite platform itself, often facilitated by a successful attack on the Ground or Link Segment.

Threat / Tactic	Target Segment	Adversary Goal	Potential Impact	Key Mitigation Strategies
Firmware/Software Tampering	Flight Software / Onboard Computers	Modify the satellite's operating instructions or payload software.	Degraded Function: Altering sensor calibration, corrupting data processing, enabling covert C2 channels.	Write Protection on memory, Cryptographically Signed Firmware Updates, integrity checking of sensitive files.
Side-Channel/Bus Snooping	Internal Satellite Bus (Spacecraft Wiring)	Exploiting physical access (via a ground compromise) or inherent system access to listen to internal data exchange.	Confidentiality Loss: Stealing cryptographic keys, command history, or payload data from internal memory.	Internal Network Segmentation, physical isolation of cryptographic modules (Hardware Security Modules - HSMs).
Resource Exhaustion	Onboard Processor / Battery	Overwhelm the satellite's processor or power systems with continuous, unnecessary tasks.	Temporary Denial of Service: Reduction in mission capability, rapid battery drain, premature hardware failure.	Rate Limiting on command inputs, dynamic Power Management policies, resource monitoring and alerting.

Annexure B

Self-Assessment Maturity Checklist

I. Identify (Asset Management, Risk Assessment, Governance)

Parameter	Description	SATCOM Specific Focus	Status
1.1 Asset Inventory	Maintain a complete, accurate inventory of all hardware, software, and systems	**Space & Ground:** Include satellites, ground stations (antennas, control centers), user terminals, network devices, and specialized OT/ICS systems.	☐ Full ☐ Partial ☐ No
1.2 Regulatory Mapping	Identify and map applicable laws, regulations, and standards	**Regulatory:** Identify requirements for data sovereignty, infrastructure protection, and incident reporting	☐ Full ☐ Partial ☐ No
1.3 Risk Assessment	Conduct a continuous, documented risk assessment process that considers threats and vulnerabilities.	**Threats:** Include signal jamming/spoofing, unauthorized satellite access, supply chain compromise, and attacks on command and control links.	☐ Full ☐ Partial ☐ No
1.4 Supply Chain Risk Management (SCRM)	Assess and manage cybersecurity risks associated with third-party vendors, suppliers, and service providers (e.g., launch services, component manufacturers).	**Vendor Due Diligence:** Require vendors to provide proof of security controls, especially for hardware/software components and managed services.	☐ Full ☐ Partial ☐ No
1.5 Bill of Materials	Bill of Materials as per CERT-In Guidelines	SBoM, QBoM, CBoM, AIBoM, HBoM	☐ Full ☐ Partial ☐ No
1.6 Security Policy & Governance	Document, approve, and communicate cybersecurity policies, roles, and responsibilities organization-wide.	**Policy:** Establish a formal policy for physical and logical security across all segments (space, ground, network).	☐ Full ☐ Partial ☐ No

II. Protect (Access Control, Data Security, System Hardening)

Parameter	Description	SATCOM Specific Focus	Status

2.1 Access Control	Implement the principle of least privilege.	**Authentication:** Enforce Multi-Factor Authentication (MFA) for all accounts, especially for remote access and privileged accounts on ground and network control systems.	☐ Full ☐ Partial ☐ No
2.2 Encryption	Encrypt data at rest and in transit.	**Secure Communications:** Implement independent encryption across all satellite communication links (uplink, downlink, crosslink) to protect against interception and eavesdropping.	☐ Full ☐ Partial ☐ No
2.3 Network Segmentation	Divide the network into secure zones to limit the blast radius of an attack.	**Isolation:** Isolate Operational Technology (OT) and satellite control systems from corporate IT networks.	☐ Full ☐ Partial ☐ No
2.4 Vulnerability Management	Implement a continuous process for identifying, prioritizing, and patching vulnerabilities in all systems.	**Patching/Configuration:** Ensure a rigorous Configuration Management and Secure Software/Firmware Update process for satellite and ground station systems (considering limited remote access and unique testing requirements).	☐ Full ☐ Partial ☐ No
2.5 Physical Security	Protect ground station equipment, control centers, and data centers from unauthorized physical access.	**Facilities:** Implement access controls, surveillance, and environmental controls for antennas, server rooms, and control centers.	☐ Full ☐ Partial ☐ No

III. Detect (Continuous Monitoring, Anomalies)

Parameter	Description	SATCOM Specific Focus	Status
3.1 Security Monitoring	Continuously monitor network traffic, system logs, and security events.	**Log Ingestion:** Ingest logs from specialized SATCOM systems, firewalls, and EDR/SIEM tools to detect suspicious activity.	☐ Full ☐ Partial ☐ No
3.2 Anomaly Detection	Establish baseline network and system behavior and monitor for deviations.	**Traffic Baselines:** Monitor SATCOM traffic for anomalies like large spikes in volume, unusual command patterns, or unexpected connection attempts (which could indicate jamming or spoofing).	☐ Full ☐ Partial ☐ No

3.3 Intrusion Detection/Prevention	Deploy systems to monitor and block malicious network activity.	**Network Protection:** Use specialized systems to detect and potentially mitigate signal interference, spoofing, or unauthorized radio frequency (RF) access.	☐ Full ☐ Partial ☐ No

IV. Respond (Incident Response Planning, Communications)

Parameter	Description	SATCOM Specific Focus	Status
4.1 Incident Response Plan (IRP)	Maintain a documented, tested, and regularly exercised Incident Response Plan.	**Scenario Testing:** Conduct tabletop exercises for SATCOM-specific scenarios, such as a loss of satellite control or a sustained jamming event.	☐ Full ☐ Partial ☐ No
4.2 Communications	Define internal and external communication plans for a cybersecurity incident.	**Stakeholders:** Establish procedures for notifying critical infrastructure partners, regulatory bodies, and customers, especially when service disruption occurs.	☐ Full ☐ Partial ☐ No
4.3 Analysis	Perform root cause analysis and forensic investigations to understand the incident.	**Data Preservation:** Ensure secure logging and data preservation mechanisms are in place for post-incident analysis of both IT and OT/space systems.	☐ Full ☐ Partial ☐ No

V. Recover (Backup & Recovery, Resilience)

Parameter	Description	SATCOM Specific Focus	Status
5.1 Backup and Restoration	Maintain isolated, tested backups of critical data, system configurations, and software.	**Critical Data:** Backup flight software, command sequences, network configurations, and all ground system data. Test restoration procedures regularly.	☐ Full ☐ Partial ☐ No
5.2 Business Continuity/Disaster Recovery (BC/DR)	Develop and test plans to maintain or quickly restore mission-critical functions with defined maximum tolerable	**Resilience:** Include contingency plans for switching to redundant systems, alternate ground stations, or alternative	☐ Full ☐ Partial ☐ No

	downtime and normalization time for critical systems.	communication methods (e.g., terrestrial links) during a SATCOM disruption.	
5.3 Continuous Improvement	Incorporate lessons learned from incident response and recovery activities into the overall risk management strategy.	**Post-Incident Review:** Conduct a thorough review after any major incident or exercise to update security policies, controls, and technical architecture.	☐ Full ☐ Partial ☐ No

Self Assessment Matrix (Full- **5**, Partial-**2.5**, No-**0**)

Process	Max. Score	Score Obtained
Identity	30	
Protect	25	
Detect	15	
Respond	15	
Recover	15	
	Total	

Maturity level

Score	Security Posture
<50	Weak
50-80	Moderate
>80	Good

Annexure C

CERT-In Incident Reporting format

Incident Reporting Form

I am: ☐ the effected entity ☐ reporting incident affecting other entity			
Contact Information of the Reporter			
Name & Role/Title	☐ Individual ☐ Organization		
Organization name (if any)			
Contact No.		Email:	
Address:			
Basic Incident Details			
Affected entity (if not same as reporting entity above)			
Incident Type			
☐ Targeted scanning/probing of critical networks/systems ☐ Compromise of critical systems/information ☐ Unauthorised access of IT systems/data ☐ Defacement or intrusion into the website ☐ Malicious code attacks ☐ Attack on servers such as Database, Mail and DNS and network devices such as Routers ☐ Identity Theft, spoofing and phishing attacks ☐ DoS/DDoS attacks ☐ Attacks on Critical infrastructure, SCADA and operational technology systems and Wireless networks ☐ Attacks on Application such as E-Governance, E-Commerce etc.	☐ Data Breach ☐ Data Leak ☐ Attacks on Internet of Things (IoT) devices and associated systems, networks, software, servers ☐ Attacks or incident affecting Digital Payment systems ☐ Attacks through Malicious mobile Apps ☐ Fake mobile Apps ☐ Unauthorised access to social media accounts ☐ Attacks or malicious/ suspicious activities affecting Cloud computing systems/servers/software/applications	☐ Attacks or malicious/suspicious activities affecting systems/ servers/ networks/ software/ applications related to Big Data, Block chain, virtual assets, virtual asset exchanges, custodian wallets, Robotics, 3D and 4D Printing, additive manufacturing, Drones ☐ Attacks or malicious/ suspicious activities affecting systems/ servers/software/ applications related to Artificial Intelligence and Machine Learning ☐ Other (Please Specify) --- ---	
Is the affected system/network critical to the organization's mission? (Yes / No). (Brief details.)			
Basic Information of Affected System (Provide information that is readily available.)	Domain/URL: IP Address: Operating System: Make/ Model/Cloud details: Affected Application details (If any): Location of affected system (including City, Region & Country): Network and name of ISP:		
Brief description of Incident:	Occurrence date & time (dd/mm/yyyy hh:mm): Detection date & time (dd/mm/yyyy hh:mm):		
Note: (i) This form provides general guidance in terms of information which could be relevant to the incident. (ii) It is not mandatory to fill and/or sign this form. Incidents may also be reported by providing relevant information in the communication itself or in any other readable form. (iii) Reporting entity may, if desired, also provide relevant information other than mentioned in this form.			
Mail/Fax incident reports to: CERT-In, Electronics Niketan, CGO Complex, New Delhi 110003 Fax:+91-11-24368546 or email at: incident@cert-in.org.in			

Annexure D

CERT-In Contacts

For reporting Cyber Security Incidents to CERT-In

Visit website: https://www.cert-in.org.in

Email: incident@cert-in.org.in

Toll Free Phone: +91-1800-11-4949

Toll Free Fax: +91-1800-11-6969

Information Desk Phone: +91-11-22902657

For Collaboration with CERT-In

Visit website: https://www.cert-in.org.in

Email: collaboration@cert-in.org.in

Phone: +91-11-22902600 Ext: 1012, +91-11-24368572

For Trainings/ Awareness programmes:

Email: training@cert-in.org.in

For receiving Cyber security threat feeds

CSK feeds on botnet infections and vulnerable services: csk@cert-in.org.in

Threat intelligence: cmtx.certin@meity.gov.in

Empanelment: empanelment@cert-in.org.in

Drills/exercises: exercises@cert-in.org.in

Alerts, advisories and Vulnerability notes: subscribe@cert-in.org.in

Official social media handles of @IndianCERT

- Facebook: https://www.facebook.com/IndianCERT/
- X (formerly Twitter): https://twitter.com/IndianCERT
- Instagram: https://www.instagram.com/cert_india/
- LinkedIn:https://www.linkedin.com/company/indiancert-cert-in/
- YouTube: https://youtube.com/@indiancert