



**Norms, Guidelines and Procedures
for Implementation of
Indian Space Policy-2023
in respect of
Authorisation for Undertaking
Space Situational Awareness (SSA)
related Activities**

*[To be read in conjunction with the “Norms, Guidelines and Procedures in respect of
Authorisation of Space Activities” (NGP), IN:ISP2023:NGP2024/V1.0, May 2024]*



**Indian National Space Promotion and Authorization Centre
Department of Space
Government of India**

June 2026

Left Blank Intentionally

DOCUMENT AND VERSION CONTROL SHEET

Title	Norms, Guidelines and Procedures for implementation of the Indian Space Policy 2023 in respect of Authorisation for undertaking Space Situational Awareness (SSA) related Activities. <i>[To be read in conjunction with the "Norms, Guidelines and Procedures in respect of Authorisation of Space Activities" (NGP), IN:ISP2023:NGP2024/V1.0, May 2024]</i>		
Abstract	This document describes the Norms, Guidelines, And Procedures for implementation of Indian Space Policy 2023 in respect of Authorisation for undertaking Space Situational Awareness (SSA) related Activities.		
Originating Agency	Indian National Space Promotion and Authorization Centre (IN-SPACE), Department of Space, Government of India, Ahmedabad		
Prepared by	Program Management and Authorization (PMA) Directorate, IN-SPACE, Ahmedabad  (P. K. Jain) Director, PMA		
Release Date	June 25, 2026		
Approved by	IN-SPACE Board  (Pawan Goenka) Chairman, IN-SPACE		
Contact	Director (PMA), IN-SPACE, Ahmedabad (director-pmad@inspace.gov.in)		
No. of Pages	51	No. of Annexures	5
Security & distribution status		Unrestricted	
Document Number	IN:PMA:SSA:2026/V1.0	Version No.	1.0

Left Blank Intentionally

Index

Section	Description	Page no.
A.	Definitions	1
B.	General Terms & Conditions	3
C.	Authorisation Guidelines for specific SSA activities	13
	I. Establishment and/or operations of space-based SSA Sensors	13
	II. Establishment and/or operations of ground-based SSA Sensors	19
	III. Providing SSA Services	25
	Annexure-1 Guidelines for the Remote Access (RA) of the Ground Stations in India from a location outside India	29
	Annexure-2 - Part A - Reporting Mechanism - Part B - Prior Intimation/Approval Mechanism - Part C - Audit & Monitoring Mechanism	32
	Annexure-3 End-Use Cum End-User Certificate (EUC) For Disseminating SSA Raw Data Or Providing SSA Services	47
	Annexure-4 Intimation by Academic Entities for ground based SSA sensor installations	49
	Annexure-5 Application Templates for Different Categories of Authorization	51

Left Blank Intentionally

AUTHORIZATION GUIDELINES FOR UNDERTAKING SSA RELATED ACTIVITIES

[To be read in conjunction with the “Norms, Guidelines and Procedures in respect of Authorisation of Space Activities” (NGP), IN:ISP2023:NGP2024/V1.0, May 2024]

A. DEFINITIONS:

- i. **“Academic Entity”** shall mean any School, College, University, or other educational institution established or incorporated by law, engaged in imparting formal education. Such entity must be recognised by a competent statutory authority or affiliated with a University or Education Board established by the Government of India or any State/Union Territory Government.
- ii. **“Astronomy”** shall mean the observations and scientific study of celestial bodies and phenomena in outer space.
- iii. **“Basic SSA Services”** shall mean SSA Services needed by a satellite operator/owner or launch operator, purely for ensuring the safe and sustainable operations of the satellite or launch vehicle such as LEOP support, collision avoidance analysis, re-entry analysis, fragmentation analysis, real-time orbital position updates/ephemeris, end-of-life disposal support, etc.
- iv. **“Resident Space Object (RSO)”** is an operational or inactive trackable Space Object, including operational satellites, defunct satellites, spent rocket stages, Space Debris, etc., orbiting the Earth or is beyond Earth orbit.
- v. **“Space Debris”** shall mean any non-functional human-made Space Object, including fragments and elements of it, in Space or entering Earth's atmosphere.
- vi. **“SSA Data Dissemination”** shall mean supply, sale or distribution of the SSA Data to a user for further usage, processing, developing data products, applications or application interface for the purpose of commercial or free of cost. User for this purpose can be an individual, NGE, Government entity or a non-Indian Entity;
- vii. **“SSA Data”** shall mean information or data, regardless of the format or delivery mechanism, pertaining to SSA obtained through real-time observations or SSA Processed Data. For example, physical parameters of space objects including Resident Space Objects acquired by SSA Sensors or orbital parameters of Resident Space Objects derived from SSA Sensor observations, etc., shall be treated as SSA Data. For clarity, both SSA Raw Data and SSA Processed Data fall under the definition of the SSA Data.

- viii. **“Space Object”**, as defined in the Indian Space Policy 2023, shall mean: (i) any object launched or intended to be launched into an orbital or sub-orbital trajectory around the earth or to a destination beyond earth orbit; (ii) any constituent element of an object referred to in sub-clause (i), or (iii) any other object as may be notified from time to time;
- ix. **“SSA Processed Data”** is data that has undergone one or more operations such as filtering, calibration, enhancement, aggregation, anonymization, or analysis, transforming it into a product suitable for further decision-making or dissemination. This typically involves tasks like removing noise, applying algorithms for object detection, generating event reports, or creating visualisations and summaries.
- x. **“SSA Raw Data”** refers to original, unaltered observations and measurements collected directly from SSA sensors or instruments. This includes unprocessed files, recordings, images, telemetry, and associated contextual metadata (timestamps, instrument settings, operator details) that capture the initial state of the measurement before any analytical, calibration, or enhancement steps have occurred.
- xi. **“Space Situational Awareness (SSA)”** shall mean activities towards acquiring the comprehensive knowledge, understanding and continual awareness of the current status and future evolution of Space Objects and space environment, and the hazards posed by them to operational space objects and terrestrial safety.
- xii. **“SSA Sensors”** shall mean a device or combination of devices such as ground-based sensors (including radars, laser ranging stations, optical telescopes, RF sensors) and space-based sensors (including laser ranging sensors/ LiDAR, optical sensors, and RF sensors) which are capable of, among others, surveying and tracking space objects, and measuring the physical parameters such as size, location, velocity, etc., of the space objects.
- xiii. **“SSA Services”** shall mean services related to SSA including cataloguing, collision avoidance support, conjunction analysis, covariance analysis, manoeuvre detection, modelling of Space Debris environment, space weather monitoring, orbit determination, orbit propagation, predictions on atmospheric re-entry of space objects, cis-lunar SSA, dissemination of SSA Data to the end-users/customers, etc. For the purpose of the IN-SPACE Authorisation, it is clarified that the term “SSA Services” shall only include the delivery of such services to the customer/end-users and exclude any decisions taken by such customer/end-users on the basis thereof.

.....

B. GENERAL TERMS & CONDITIONS

1. Any Indian Entity intending to establish and/or operate Space Situational Awareness (SSA) facilities or provide SSA Services shall require Authorisation from IN-SPACE. More specifically, the following activities related to SSA shall need Authorisation with IN-SPACE, as applicable, except for the exemptions provided in certain cases and described in this document:

- a) Establishment and/or operations of Space-based Sensors for SSA related observations
- b) Establishment and operations of Ground-based Sensors for SSA related observations
- c) Providing SSA Services

- i. Each of these SSA activities shall require a separate Authorisation. To further clarify, if an Applicant intends to establish and operate both Space-based and Ground-based SSA Sensors, then they shall seek two separate Authorisations.
- ii. Similarly, an Applicant seeking the Authorisation for Space or Ground-based SSA sensor and intends to provide SSA Services as well, shall obtain separate Authorisation for providing SSA Services to its customers/end-users.

However, Applicants shall not require a separate authorisation for providing SSA Services, if they intend to disseminate only the SSA Raw Data pertaining to their authorised/under-authorisation SSA sensor to their customers/end-users and not providing any other type of SSA Services.

- iii. If a satellite carrying space-based SSA Sensor downlinks the SSA Data after onboard processing (filtering, enhancement, etc) using edge computing, AI/ML or any other technology, then the IN-SPACE Authorization Certificate shall also include the dissemination of such onboard SSA Processed Data along with appropriate terms & conditions.

Application Templates for different categories of Authorisation are provided in [Annexure-5](#).

2. Astronomy does not fall under the ambit of IN-SPACE Authorisation. Hence, entities undertaking any ground-based Astronomy activity do not require IN-SPACE Authorisation.
3. Applicants undertaking the SSA activities described above may establish either a separate or integrated SSA Data control, storage/archival or processing facility, as applicable. No separate IN-SPACE Authorisation is needed for such auxiliary facility/facilities. However, Applicants shall provide the basic information such as broad configuration, flow/block diagram, geo-coordinates,

SSA data handling security mechanism, mechanism for transfer of the SSA Data from the source, etc. envisaged in such facilities, at the time of submitting the Application to IN-SPACE.

4. (a) Non-Indian entities intending to undertake any SSA activity in India shall seek IN-SPACE Authorisation only through Indian incorporated entities (such as Indian subsidiary, joint venture, partnership or collaboration with Indian entities), which shall be responsible for compliance with Indian laws, regulations, and national security requirements.

However, sharing/supplying/disseminating the SSA Raw Data, or certain SSA Data/SSA Services can be undertaken by the Non-Indian entities directly or through an Indian Entity without requiring IN-SPACE Authorisation, as explained in the subsequent sections/sub-sections of this document.

(b) In case of a collaboration with non-Indian Entity, the consent from both Applicant and such Non-Indian Entity is to be furnished to IN-SPACE affirming that the complete control over the concerned SSA activity including SSA Data/Services dissemination rights shall reside with the Applicant and the jurisdiction being under Indian government and law. The Applicant shall also provide an undertaking to this effect at the time of submitting the Application to IN-SPACE.

(c) In such case when the Applicant is a subsidiary, joint venture, or partnership with a Non-Indian Entity, the applicant shall disclose the extent of control exercised by the Indian Entity. Where control resides wholly or partly with the Non-Indian Entity, a risk assessment to determine whether such control poses any risk to India's national security, strategic interests, or policy objectives will be undertaken by the Government of India while processing the Authorisation application. However, the lack of controlling interest by the Indian Entity shall not, by itself, constitute a ground for denial of authorisation. In any case, the consent from both Applicant and the Non-Indian Entity is to be furnished to IN-SPACE affirming that the complete control over the concerned SSA activity including SSA Data/SSA Services dissemination rights shall reside with the Applicant and the jurisdiction being under Indian government and law.

5. Any entity in India can source the SSA Raw Data for their self-use from any Indian or Non-Indian entity. However, an Indian entity intending to supply/sell/disseminate the SSA Raw Data to any Indian or non-Indian entity shall seek IN-SPACE Authorisation for providing SSA Services, as applicable.
6. **Exemption from IN-SPACE Authorisation:**

Authorisation requirement as mandated in B(1) is exempted for:

a) Individual hobbyists, amateurs or formal/informal groups of people engaging in watching, collecting/exchange of the SSA Data or information on the space objects for recreation, general awareness, interest or research, provided that such activities meet all of the following criteria:

- i. **Non-Commerciality:** The activity is conducted without remuneration, contractual obligation to a commercial or government entity within or outside India, or the sale of data or derived products.
- ii. **Technical Thresholds:** The ground based SSA sensor's hardware and software systems employed and observations made are limited to:
 - Angular slew rate ≤ 1 deg./sec (automated close-loop tracking)
 - Timing precision ≥ 10 ms
 - Aperture Diameter ≤ 0.5 m
 - No real time data dissemination (latency of at least 2 (two) hours from acquisition to distribution)

To clarify, the exemption is conditional to meeting all of the above thresholds together.

iii. **Public/Academic Awareness Intent:** SSA Data dissemination is limited to general interest, hobbyist forums, or public/academic education/research. Therefore, the dissemination shall not be done for the purpose of supporting space operations such as operational flight safety or conjunction assessment (CA) services.

b) Academic Entities satisfying the criteria as stated above in a(i), a(ii), a(iii). While such Academic Entities are exempted from IN-SPACe Authorisation, they shall intimate IN-SPACe about their ground based SSA sensor installations (existing or planned), as per the proforma provided in [Annexure-4](#).

In addition, there are other exemptions/relaxations provided in the subsequent sections for certain cases.

7. SSA Activities pertaining to certain RSOs:

(a) Prior to IN-SPACe Authorisation or any time during the Authorisation Period, Government of India reserves the right to designate certain Resident Space Object(s), which shall not be identified, associated, attributed or catalogued while providing SSA Services by the Applicants, for the national security and strategic requirements. Applicants seeking authorisation for establishment and operations of the space-based or ground-based SSA sensors may also be

directed to adhere to the above guideline before disseminating the SSA Raw Data from these sensors to end-users/customers.

(b) Applicants shall, however, be permitted to internally track and analyse such designated Resident Space Object(s) for the purpose of safety of other Resident Space Objects, provided the SSA Data specific to the designated Resident Space Object(s) is not disseminated externally.

(c) Government of India reserves the right to grant exemptions or impose additional conditions on a case-by-case basis in this regard, or implement an appropriate mechanism aligned with international best practices for protecting sensitive information and strategic assets of the country.

(d) On site verification to monitor the operations and use of filters/appropriate mechanism to restrict dissemination of such SSA Data shall be part of the 'Audit & Monitoring Mechanism' conducted by IN-SPACE or any other authorised agency of Government of India.

8. Government of India reserves the right to direct an Applicant, as applicable, to not to disseminate the SSA Data pertaining to the authorised space-based or ground-based SSA Sensors or provide specific SSA Service(s) to certain users/customers, for the national security and strategic requirements.

9. Obligation to Share Data with Government

- a. Authorised entities shall share SSA Data and information with the Government of India, upon request, on a non-discriminatory basis strictly for purposes of national security, ensuring the safety of space operations and fulfilling India's international commitments.
- b. Such sharing shall be subject to fair market value compensation, determined in accordance with procurement guidelines and valuation mechanisms notified by Government from time to time.
- c. All data sharing shall be subject to applicable confidentiality, security, and data-handling requirements prescribed by the Government.

10. Access and control by the Government:

- a. The Government of India reserves the right, in circumstances of national emergency, armed conflict, war, or other crisis affecting national security, to take over, assume control of, or direct the operation of any authorised SSA infrastructure, assets, or services, whether operated by a governmental or non-governmental entity.

- b. Any such takeover or assumption of control shall be subject to the payment of reasonable compensation, determined in accordance with principles of fair market value and in case of foreign companies or foreign satellites consistent with applicable rules of international law governing lawful expropriation.
 - c. In exercising the rights under this clause, the Government of India shall not compel any entity — particularly those with foreign ownership, participation, or footprint — to undertake actions that would place them in violation of:
 - i. applicable foreign export control laws; or
 - ii. binding international sanctions recognised by India.
 - d. Government of India shall notify, in advance where practicable, the scope, duration, and conditions of such takeover, and shall ensure that the takeover is limited to what is necessary to address the emergency and is terminated once the exigency ceases.
- 11.** The Applicants are advised to make adequate arrangements for maintaining continuity of services including redundancies, backup systems and contingency planning to minimise interruptions and to ensure operational functionality of SSA capabilities especially in the events of cyber, high-energy or kinetic (physical) attacks.
- 12.** The Applicants are also advised to put in place the requisite protocols to ensure the quality of SSA Data being disseminated/supplied such as accuracy, reliability, integrity, etc., including validation methods and error correction mechanisms.
- Applicants should also define/specify the deliverable SSA Data quality parameters such as accuracy, latency, periodicity, etc.
- 13. End-Use cum End-User Certificate (EUC):** Applicants shall obtain and maintain the End-User Certificate (EUC) from their customers/recipients while disseminating the SSA Data or providing the SSA Services. The contract with their customers shall also include a clause requiring the customers/recipients to obtain and maintain such EUC in turn from their subsequent customer(s), if the same SSA Data or SSA Services are to be disseminated further by them (even if they fall under the authorisation-exemption cases, which are brought out in the subsequent section on “Providing SSA Services” of this document). These EUCs shall be maintained for 3 years by the Applicants and their customers, as applicable. The format of the EUC is included in [Annexure-3](#).

14. Procurement from the Trusted Sources:

- a. Entities shall ensure that any procurement(s) needed for establishing their facilities/systems is done only from the trusted sources, following the Government of India's Trusted Telecom Directive and National Security Directive on Telecommunication Sector (NSDTS), wherever applicable, till separate framework/guidelines for space systems are brought out and implemented.
- b. In any case, Applicants shall carry out due diligence at their end while procuring the components, systems & subsystems, hardware & software, ensuring that only Trusted Sources are used. Records of the procurement of the critical hardware and software shall be maintained by the Applicants. Government of India reserves the right to ask for these details for the purpose of ensuring that the national security is not compromised in any way. Government of India shall also reserve the right to direct the replacement of certain components/subsystems/systems, if found to be compromising with the national security.

15. Development of Standards:

- a) IN-SPACe may in future, in consultation with SSA businesses, industry associations, academia, and other stakeholders, develop standards, protocols, and benchmarks for SSA services, hardware and data, aligning with the recognised industry standards worldwide and best practices.
- b) Such standards may be issued as binding or non-binding instruments, depending upon the nature of the requirement and the stage of industry development.
- c) IN-SPACe may review and update such standards periodically to reflect technological progress, international developments, and India's strategic interests.

16. Publication and Dissemination of SSA Data:

a) Publication of SSA Data

- i) Government of India may, in consultation with Authorised SSA Service Providers & the Authorised satellite operators and in accordance with license agreements, publish and disseminate SSA Data and products for the purposes of enhancing safety and sustainability of space operations.

- ii) The dissemination of SSA Data, in such cases, shall be carried out through designated Government or IN-SPACe identified platform(s).
- iii) The scope, type, format, resolution, and access conditions for such published SSA Data shall be determined by the Government, taking into account:
 - a. the need to promote safe and sustainable space operations;
 - b. obligations under international treaties and cooperation agreements;
 - c. protection of sensitive data with national security implications
 - d. the intellectual property rights and legitimate business interests of SSA Service Providers.
- iv) Government of India shall ensure that such publication (a) shall respect the intellectual property and commercial rights of the authorised SSA Service Providers/operators, (b) is done only within the scope defined in the license agreements, and (c) provides due credit/visibility to contributing providers.

b) Global Space Traffic Management Efforts

- i) With a view to supporting global Space Traffic Management (STM) and cooperative safety initiatives, Government of India may, as far as practicable and subject to the consent of the person(s) owning such data or information, publish methodologies, protocols, or standards developed in India for:
 - a. Collision avoidance assessments;
 - b. Conjunction analysis;
 - c. Re-entry prediction
 - d. Other SSA-related risk mitigation measures.
- ii) Publication of such methodologies shall be at the discretion of the Government, and subject to:
 - a. Consideration of national security interests
 - b. Protection of intellectual property rights and proprietary information belonging to stakeholders.

c) License Conditions

- i) SSA Service Providers whose SSA Data is selected for publication under this section and who have consented for the same, shall enter into license agreements with the Government, which shall define the scope of data use, attribution, confidentiality obligations, and compensation (where applicable).
- ii) No publication under this Chapter shall abrogate or diminish the proprietary rights of SSA Service Providers in their SSA Data, except to the extent expressly provided for in such license agreements.

17. Authorisation Tiers

- a) Recognizing that SSA activities vary in their risk profiles, national security implications, and operational complexity, and to promote innovation and avoid overburdening smaller actors while ensuring appropriate control, a two-tiered regulatory approach shall be adopted that scales obligations proportionate to risk and sensitivity levels.

- i) **Restricted Tier:** SSA Activities of sensitive nature or high security relevance shall go through additional layer of approval and shall require enhanced authorisation terms & conditions, reporting and audit & monitoring mechanism.

Applicant with non-Indian Management & Control OR intending to provide SSA Data/Service to a non-Indian government OR intending to provide SSA Data/Service to a non-Indian Entity for defence/security purpose OR establishing ground-based SSA sensor outside India shall fall under the Restricted Tier.

- ii) **Controlled Tier:** SSA Activities which are other than those falling under Restricted Tier shall be dealt with standard and simplified regulations with a view to providing ease of doing business, without compromising the security aspects and national interest.

SSA Activities of non-critical nature and general-purpose usage such as academia, research, hobby etc. shall either be exempted from Authorisation or will be dealt with soft-touch regulations without compromising the security aspects and with a view to encourage the innovation and research in SSA domain.

- b) Based on the applicability criteria provided in the subsequent section, the Applicant requiring Authorisation shall self-assess and declare the applicable tier in the application to IN-SPACE. However, IN-SPACE shall reserve the right to treat an application under the tier which could be different than the declared tier by the Applicant based on the evaluation and overall assessment of the application. The decision of IN-SPACE in this regard shall be binding on the Applicant.
- c) Once Authorised by IN-SPACE under a tier, the Applicant shall inform IN-SPACE if the concerned authorised SSA activity or the Applicant anytime qualifies for another tier, and shall take prior approval of IN-SPACE before undertaking such SSA activity under the new tier. IN-SPACE shall reserve the right to grant a fresh Authorisation or amend the existing one.

18. Applicants seeking IN-SPACE authorisation shall employ appropriate measures for safety and security in respect of the SSA activities being carried out by them:

- a. The measures shall include, among others, physical security, cyber security resilience measures including safeguards against cyber intrusions, cloud security mechanism, API security mechanism adequacy to prevent data leakage/pilferage, encryption mechanism (onboard and/or ground systems, as applicable), prevention of unauthorised use/access to the hardware and/or software, secured transfer/ storage/ handling/ processing/ dissemination of SSA Data, disaster recovery systems, maintaining the immutable log of activities, etc., as applicable. The Applicant shall also comply with the safety and security guidelines as and when brought out by IN-SPACE.
- b. Applicants shall comply with the relevant guidelines, as applicable, pertaining to information security and management including the 'Cyber Security Framework and Guidelines for Space including Satellite Communication (presently dated Feb 26, 2026)', as and when issued/revised by CERT-In, MeitY, as the baseline framework for data security until separate safety and security guidelines are brought out by IN-SPACE.
- c. The information on such reasonable security measures proposed to be adopted shall be provided at the time of applying to IN-SPACE.
- d. The Applicants are also mandated to carry out the periodic cyber security audits of these facilities through designated government agencies or MeitY empanelled security auditors to ensure the effectiveness of information security controls and help identify and mitigate potential vulnerabilities, if any.
- e. The Applicants shall inform IN-SPACE regarding detection of any security or data breach and the corresponding details and measures taken/planned to address the breach and avoiding any further occurrence, within 1 (one) week of the breach detection.

Guidelines in para 18-b. & 18-d. shall not be mandatory for the Academic Entities carrying out research activities, except for the following cases, which shall require adherence to these guidelines:

- i. Collaboration with a non-Indian entity, OR
- ii. The concerned SSA activity is not for the own-use, OR
- iii. The SSA Data is disseminated to a non-Indian Entity

However, such exempted entities are encouraged/advised to adopt the guidelines in para 18-b. & 18-d. for ensuring the information and data security.

- 19.** Applicants shall make appropriate provision for Lawful Interception Management System (LIM) for lawful interception by Law Enforcement

Agencies (LEAs). Such LIM could be provisioned preferably at the SSA Data control, storage /archival and/or processing facility of the Applicants.

Provision for RF signal monitoring and providing feed to DoT and other government departments/ministries shall also be made, wherever applicable (such as Data reception stations).

- 20.** Applicants shall inform IN-SPACE in writing as well as email about the commencement of the operations of the Authorised SSA Sensors/Services within 7 (seven) working days.

21. Logging, Reporting and Audit & Monitoring mechanism:

- a) Applicants shall maintain a complete and immutable log of activities including metadata of the operations of the Authorised SSA Sensors or the SSA Services, for a period up to 3 (three) years.

The Applicant shall make available the requisite information including the log of the activities to IN-SPACE/audit team, if demanded.

- b) Applicants shall periodically report the respective SSA activities being carried out by them to IN-SPACE on the IDP or by email, as prescribed by IN-SPACE. Information to be provided to IN-SPACE would be captured in the Authorisation Certificate issued by IN-SPACE.

- c) IN-SPACE or any other authorised agency of Government of India reserves the right to carry out periodic or random audit/inspection (on-site or off-site) for confirming information provided by the Applicant during the process of its application and compliance to the terms & conditions of the Authorisation Certificate issued by IN-SPACE including the security mechanism. IN-SPACE also reserves the right to suspend and/or terminate the Authorisation in the event of detection of violation of any of the terms & conditions of the Authorisation Certificate or in case of any discrepancy found during the Audit. Further, in case of any violation noticed in the authorised or exempted cases, Government of India reserves the right to take appropriate penal action.

However, a show-cause notice shall be issued and, if necessary, the violator shall be advised to take the corrective actions within a defined period, before taking such penal action.

- d) Sample reporting and audit & monitoring mechanism for all types of Authorisation based on the applicable tiers of the Applications is included in the [Annexure-2](#).

- 22.** Export of any SSA Data or SSA Services shall be undertaken subject to applicable Indian export control laws overseen by concerned regulatory authorities such as DGFT, DDP, etc., as applicable).

C. AUTHORISATION GUIDELINES FOR SPECIFIC SSA ACTIVITIES

The authorisation guidelines specific for each type of SSA activities, along with the associated tiers, are provided in the following subsections.

I. Establishment and/or operations of space-based SSA Sensors

- a) Establishment and/or operations of any space-based SSA Sensor owned and/or operated by an Indian Entity requires one-time IN-SPACE Authorisation.
- b) Separate IN-SPACE authorisation shall be required, if the Applicant intends to own, establish and operate the associated Ground Systems, viz., data reception station and TT&C stations. No separate IN-SPACE authorisation is required for the MCC and this would be an integral part of the Authorisation for space-based SSA sensor itself. However, the tier-wise applicable guidelines shall be adhered to in respect of the MCC operations.

Data reception stations for acquisition of the Space-based SSA sensor data and the TT&C ground station can be located within or outside Indian Territory. IN-SPACE may seek the details of such stations along with arrangements made with foreign data reception station operator, if necessary, to assess whether operations of such stations do not pose a threat to the national security, foreign relations, intelligence and security operations in the interests of the Republic of India.

- c) In case, the Applicant owning the satellite as well as the onboard Space-based SSA Sensor, an integrated single IN-SPACE Authorisation shall be granted for establishment and operation of the satellite.
- d) The Space-based SSA Sensor(s) could be carried on a satellite/space-based-platform owned by the Applicant or could be hosted on any Indian or non-Indian satellite/space-based-platform.
- e) MCC could be self-owned & operated or could be a third-party MCC within or outside Indian territory depending upon the applicable tier. Captive network or commercial cloud based MCC operations (with secured access through API) are also permitted with servers being within or outside Indian territory depending upon the applicable tier.

In all such above cases, the Applicant must have the absolute decision-making powers (full operational authority) with regard to the operations and control of the SSA Sensor, and the Applicant should be able to cease the operations of the SSA Sensor without any delay, as and when directed by IN-SPACE for national security and geopolitical considerations.

- f) Remote Access (RA) to MCC shall not be permitted from outside Indian Territory.

- g) The Applicant shall ensure that the authorised space-based SSA Sensor(s) are not tasked to collect data pertaining to any ground establishments/activities, and the authorisation granted for such SSA Sensor shall not be deemed to include acquisition of the data pertaining to any ground establishment/activities. The Applicant shall seek a separate Authorisation for the establishment and/or operations of Remote Sensing satellite/hosted-payload and/or Authorisation/Registration as a Data Disseminator, as applicable, if the proposed SSA Sensor is also meant for Remote Sensing applications.
- h) Any Indian Entity can seek Authorisation for establishment and/or operation of the space-based SSA Sensor, which if applicable, may use ITU Filing under Indian or non-Indian Administration.
- i) If applicable, the Applicant shall provide details regarding the ITU Filing status, if it intends to use the existing ITU Filing.

The Applicant may also make a new ITU Filing to ITU, or may make use of the under-process Indian ITU Filings or coordinated/allotted orbit resource through a pre-defined framework. The framework and guidelines for making a new ITU Filing and to provide access to the available orbital resources to the interested Indian Entity are provided in the Chapter-VI [of the IN-SPACE NGP]. In case of a new ITU Filing, the Applicant shall apply to IN-SPACE and seek an advisory-note. With the IN-SPACE advisory-note, the Applicant may submit the ITU Filing to ITU through WPC. "Guidelines and procedures for submission of satellite network filings to ITU by Indian Entities", brought out by DoT, shall be followed by the Applicant for further processing of the ITU Filing.

While WPC shall carry out the detailed evaluation of the proposed ITU Filing including conformance to the ITU process, the application shall be preliminary investigated by IN-SPACE on factors including the compliances to national and international (ITU) regulatory provisions and protection of the services of the incumbent Indian satellites and the Indian ITU Filings with overlapping frequencies which are under consideration by IN-SPACE as potential candidates for the planned satellites by Indian Entities. A detailed interference analysis shall be carried out by the Applicant to this effect along with additional measures and strategy to coexist with other satellite systems serving India to provide services without any harmful interference. No analysis would be required to be submitted, if a coordination/coexistence agreement with the relevant satellite system(s) already exists, although reference to such agreement(s) shall be brought out in the application.

IN-SPACE may consider granting the Authorisation to the Applicant on non-protection non-interference basis, if it is satisfied that the operation of the new

entrant Space-based SSA sensor would not interfere with the incumbent services.

- j) If applicable, the Applicant can also use Non-Indian Orbital Resources. The Applicant shall provide details of arrangements made for obtaining the rights for using Non-Indian Orbital Resource for the operations of the Space-based SSA sensor for which the IN-SPACe Authorisation is being sought along with the concurrence/approval or a copy of the corresponding Authorisation or similar documentation granted by the concerned non-Indian Administration. In such cases, the Applicant shall still retain exclusive control over payload operations, encryption keys, and access to raw data under Indian jurisdiction. The information provided by the Applicant shall be treated with due diligence, if declared as commercial confidential information by the Applicant.

Other provisions and process in respect of the protection of the services of the incumbent Indian satellites and ITU Filings under consideration by IN-SPACe, and interference analysis, etc. shall be same as described above in the previous para i).

- k) The Space-based SSA sensor shall have the provision to cease the emission (if applicable)/operation immediately, through an appropriate telecommand, as and when needed.
- l) Applicants shall employ onboard encryption on the data being transmitted from the space-based SSA Sensor to Earth for downloading by the data receive station, as per prevailing industry standards, to prevent unauthorised access.
- m) Applicants are also permitted to procure/acquire an already operational in-orbit Space-based SSA sensor from Indian or non-Indian Entities or transfer the ownership to Indian or non-Indian Entities, after obtaining Authorisation/approval of IN-SPACe.
- n) As applicable, the details of the satellite/space-based-platform carrying space-based SSA sensor, launch vehicle and the launch service agreements, agreement to host the Space-based SSA sensor on the satellite/space-based-platform shall be provided by the Applicant, while seeking IN-SPACe authorisation.
- o) The Applicant will be required to coordinate with the existing Indian satellite/launch operators to manage the data reception from the satellite passes that clash with other Indian satellites/launches over the same area of data reception station. The new-entrant and the incumbent operators shall collaborate, negotiate, coordinate and enter into an operational/coexistence arrangement in good faith for interference-free data reception and TT&C

operations over India. If found necessary, IN-SPACe may facilitate discussions among the operators or make appropriate enforceable interventions.

Notwithstanding above, IN-SPACe, in coordination with WPC, WMO and NOCC, shall reserve the right to direct an operator to cease the emission in case the harmful interference from its satellite/ Space-based SSA sensor to other networks is not removed or resolved within the notice period provided by IN-SPACe.

- p) Relevant guidelines for Establishment and/or Operation of Remote Sensing and Amateur Satellite Systems, Establishment and/or Operation of Hosted Payloads and Establishment and/or Operation of the Ground Systems included in the extant NGP shall, mutatis mutandis apply:
- i. When Space-based SSA sensor is part of the Satellite to be owned and operated by the Applicant itself;
 - ii. When Space-based SSA sensor is to be hosted on an Indian or Non-Indian satellite;
 - iii. When the Applicant intends to own, establish and operate the associated ground systems.

In case of a contradiction on any of the above guidelines, the guidelines provided in this chapter/document shall be applicable.

- q) Applicant, during the design, operational and end-of-life phases of the space-based SSA Sensor/associated satellite, shall adhere to the relevant guidelines included in Chapter-XI (Registration of the Space Objects) of the extant NGP, and the framework for safe and sustainable space operations as and when brought out by DoS.
- r) The Authorisation granted shall be applicable to the specific space-based SSA Sensor(s) and any material change in the major specifications/configuration of the sensor shall be intimated to IN-SPACe and may require amendment or a fresh Authorisation from IN-SPACe.
- s) Tier-wise specific guidelines are provided below:

1) Restricted Tier

- i. Applicants with non-Indian Management & Control OR intending to provide SSA Raw Data to non-Indian government OR intending to provide SSA Raw Data to a non-Indian Entity for defence/security purpose, shall fall under this tier.

- ii. The authorisation applications shall go through the additional scrutiny by other relevant departments. The entire authorisation process shall be coordinated by IN-SPACE.
- iii. Applicants intending to disseminate SSA Raw Data to a non-Indian government OR to a non-Indian Entity for defence/security purpose shall declare so in the Application at time of seeking IN-SPACE Authorisation, and the following shall be applicable:
 - a) Applicants shall provide intimation to IN-SPACE, minimum 15 working days in advance, before disseminating/selling the SSA Raw Data.
 - b) Applicants shall seek one-time prior approval of IN-SPACE before disseminating/selling the SSA Raw Data, if such data pertains to a targeted 'Indian Space Object' or an 'unidentified Space Object' (Space Object which is not identified or assigned any 'satellite catalogue identification number, by the global sources for free/open SSA Data for space safety, such as USSPACECOM/Space-track.org, Celestrak, EU SST, ESA DISCOS, ISON, etc).
- iv. SSA Data (downlinked by the satellite/SSA sensor) being received using data-reception ground station outside Indian territory shall be routed through India before dissemination to customers/end-users. In case of the captive network/commercial cloud based (with secured access through API) dissemination, the commercial cloud/network should be hosted on server(s) in India.
- v. **MCC Operations:** (a) Use of a third-party MCC or the MCC located outside Indian territory shall not be permitted.
 - (b) Captive network/ commercial cloud based (secured access through API) MCC operations are permitted provided it is hosted on Indian server(s).
 - (c) Remote access from outside the Indian Territory shall not be permitted.
- vi. In case of the captive network/commercial cloud based (with secured access through API) dissemination of the SSA Raw Data, the commercial cloud/network shall be hosted on server(s) in India.
- vii. Enhanced logging, reporting and audit & monitoring mechanism shall be employed. The mechanism is included in [Annexure-2](#). The major points are given as under:
 - a) Applicants shall maintain a complete and immutable log of activities including metadata of the operations of the Authorised SSA Sensors for minimum three years.

- b) Reporting of the dissemination of the SSA Raw Data by the Applicants, only if the recipient is a non-Indian Entity.
- c) Reporting only on the targeted RSO (when SSA Sensor is tasked to focus on a specific RSO), if any, shall be included in the periodic report to IN-SPACE. Details of the customer/recipient of such SSA Raw Data, other than the owner/operator of the RSO, shall also be included in the periodic report.

2) **Controlled Tier**

- i. Applications not falling under the Restricted Tier shall come under the ambit of the Controlled Tier.
- ii. MCC locations and operations shall be permitted as given under:
 - a) **If the SSA Sensor is hosted on an Indian or non-Indian satellite:** Use of any third-party MCC within or outside Indian territory shall be permitted.
 - b) **If the SSA Sensor is carried on a satellite/space-based platform owned by the Applicant:** No third-party MCC shall be permitted.
 - c) Any captive network or commercial cloud with secured access through API, hosted on Indian or non-Indian servers, can also be used for the MCC operations.
- iii. Logging, reporting and audit & monitoring mechanism shall be eased out. The mechanism is included in [Annexure-2](#). The major points are given as under:
 - a) Applicants shall maintain a complete and immutable log of activities including metadata of the operations of the Authorised SSA Sensors for three years. However, this limit shall be relaxed to one year for the Academic Entities, except for the following cases, which require maintaining the logs for minimum 3 years like any other entity:
 - i. Collaboration with a non-Indian entity, OR
 - ii. The concerned SSA activity is not for the own-use, OR
 - iii. The SSA Raw Data is disseminated to a non-Indian Entity
 - b) Reporting of the dissemination of the SSA Raw Data by the Applicants, only if the recipient is a non-Indian Entity.
 - c) Reporting only on the targeted RSO (when SSA Sensor is tasked to focus on a specific RSO), if any, shall be included in the periodic report to IN-SPACE. Details of the customer/recipient of such SSA Raw Data, other than the owner/operator of the RSO, shall also be included in the periodic report.

II. Establishment and operations of ground-based SSA Sensors

- a) Establishment and operations of the ground-based SSA Sensor within or outside Indian Territory by Indian Entities shall require one-time IN-SPACE Authorisation which shall normally have a validity of 10 years. An Indian entity is permitted to carry out the operations of only IN-SPACE authorised ground-based SSA Sensors (such as optical, radar, RF, laser, etc.) in India or outside India (as the case may be).

- b) Applicants shall require the requisite clearance/approval for identified geographical site/location before establishment of ground-based SSA sensors.

There may be some prohibited zones/areas where SSA Ground Sensor deployment shall not be permitted such as areas near international border, proximity to Defence/Nuclear/Strategic installations, etc.

In addition, there may be some temporarily declared time-bound prohibited zones during missile tests, defence exercises, satellite launches, etc.

These prohibited zones may be subject to review and changes by the Government of India, solely on the national security grounds, and shall be adhered to by the Applicants and the already Authorised Entities.

- c) If any station is already set up in such Prohibited Zones notified by the Government of India, IN-SPACE, may direct, the shifting of such station to another location, provided, however, that such direction is found to be necessary in the national interest, security or in conformance to the prevailing regulations by the Government of India.
- d) Government of India reserves the right through its authorised representative(s) to carry out inspection of the site, the ground-based SSA Sensors, security mechanism and confirming other information provided by the Applicant during the process of Authorisation as well as before operationalisation of the Authorised ground-based SSA Sensors.
- e) Indian Entities are permitted to procure an already operational ground-based SSA Sensor from Indian or non-Indian Entities, within or outside Indian Territory, or to transfer the ownership of their established station to other Indian or non-Indian Entities, after obtaining Authorisation/approval of IN-SPACE.

Applicants, wherever applicable, shall ensure that the appropriate data wiping/deletion procedures are followed before transferring ownership of Indian-owned Ground-based SSA Sensor to a Non-Indian Entity. Similarly, the Applicants, wherever applicable, shall employ proper data sanitization procedures before acquiring a ground-based SSA Sensor from non-Indian Entities to remove any threat that might have been left behind.

- f) The ground-based SSA Sensor can be established on the land owned by the Applicant or on the leased/rented land. In case of the lease/rent, the Applicant is encouraged to go for a long-term lease/rent. The validity of the Authorisation shall co-terminate with the lease/rent period or ten (10) years from the date of issue of the Authorisation Certificate, whichever is earlier.
- g) The ground-based SSA Sensor shall have the provision to cease the emission/operations immediately, as and when needed.
- h) Any change in the location of the authorised ground-based SSA Sensors, whether within or outside Indian Territory, shall require approval of IN-SPACE.
- i) The Applicant shall ensure that the Authorised ground-based SSA Sensors collect data pertaining to SSA activities only and not pertaining to ground establishments/activities. The Applicant shall provide an undertaking to this effect while submitting the application to IN-SPACE.

The Applicant shall declare in the application seeking IN-SPACE Authorisation the intended minimum elevation angle of the ground-based SSA Sensor at which the observations would be made. However, IN-SPACE shall specify, in the Authorisation Certificate, an elevation angle below which the ground-based SSA sensors cannot be operated, depending on the proposed location of the ground-based SSA sensors. The tentative and indicative minimum elevation angles for different geographical areas are as follows:

- a) Remote Areas (plains, deserts, plateaus, and non-sensitive regions): 5°
 - b) Urban/Populated Areas (metros, industrial zones, civilian airports): 10°
 - c) Border Belt (LAC/LOC/IB): 20°
 - d) Coastal & Naval Defence Zones (East/West naval corridors): 15°
 - e) Astronomical / Dark Sky Sites: 10°
- j) Applicants shall provide the detailed technical specifications and parameters of the ground based SSA sensors being established, while applying for the Authorisation. Test results of Factory Acceptance Tests (FAT) and post-installation Verification Tests at the Site shall also be provided at the time of seeking Authorisation or post-Authorisation, as applicable.
 - k) Any existing ground-based SSA sensors which are already operational within or outside Indian Territory by an Indian Entity shall also need to be regularised through IN-SPACE Authorisation. Such IN-SPACE Authorisation shall be obtained by May 31, 2027. With effect from June 01, 2027 only IN-SPACE authorised ground-based SSA sensors shall be permitted to operate by an Indian Entity within or outside Indian Territory.
 - l) In case of establishment and operations of sensors employing RF frequencies, the Applicants shall obtain the requisite clearance/approval/license from the

relevant Government department(s)/ministries, including the frequency assignment/authorisation from WPC wing of DoT, as applicable, before operationalization of such ground-based SSA sensors.

- m) Wherever applicable, Applicants shall ensure and carry out due diligence to the effect that the operation of the authorised ground-based SSA Sensor at any time does not cause harmful interference to other satellites or terrestrial networks or launch vehicle operations.

IN-SPACE, in coordination with WPC, WMO and NOCC, shall reserve the right to direct the Applicant to cease the emission, if applicable and in case the harmful interference from its authorised ground-based SSA Sensor to other satellite/ terrestrial networks is not removed or resolved after a notice period.

- n) Wherever necessary Applicants shall collaborate, negotiate, coordinate and enter into an operational arrangement in good faith with other operators of relevant satellite/terrestrial networks/systems in India, for interference free operations.
- o) Applicants may seek an integrated IN-SPACE Authorisation for multiple ground-based SSA Sensors provided all these sensors are located at the same site. Further, the IN-SPACE Authorisation shall be applicable to a specific ground-based SSA sensor(s) and any material change/upgradation in the critical parameters or specifications that affect the SSA capability shall be intimated to IN-SPACE, which shall reserve the right to ask the Applicants to obtain a fresh or amendment to the Authorisation.
- p) **Remote Access (RA) from outside India:** (i) Remote access, if any, to control and operate the Authorised ground-based SSA Sensors from outside the Indian Territory shall be governed by the “Guidelines for the Remote Access (RA) of the ground stations at India from the locations outside India” included in [Annexure-1](#).
- (ii) Approval of the regulatory authority of the country hosting the RA system of the Authorised ground-based SSA Sensor shall be obtained by the Applicant before commencing the operations.
- q) Applicants wishing to decommission an Authorised ground-based SSA Sensor shall provide prior intimation to IN-SPACE 3 (three) months before the intended decommissioning.
- r) Academic Entities operating a ground based SSA Sensor or planning to establish and operate ground-based SSA Sensor and satisfying the authorisation-exempt conditions given in para B-6-a(i), a(ii), a(iii) of section B of General Terms & Conditions, shall intimate IN-SPACE as per proforma given in [Annexure-4](#).

s) Tier-wise specific guidelines are provided below:

1) Restricted Tier

- i. Applicants under non-Indian Management & Control OR intending to provide SSA Raw Data to non-Indian government OR intending to provide SSA Raw Data to a non-Indian Entity for defence/security purpose OR owning or operating the ground-based SSA Sensor outside Indian territory, shall fall under this tier.
- ii. The authorisation applications shall go through the additional scrutiny by other relevant departments. The entire authorisation process shall be coordinated by IN-SPACE.
- iii. In case of establishment of the ground-based SSA Sensors outside the Indian Territory:
 - a) Applicants shall obtain the necessary approvals/authorisation/ license from the concerned non-Indian regulatory authorities, in addition to authorisation from IN-SPACE.
 - b) Applicants shall provide information on the data transfer mechanism and remote access setup if any, to manage the ground-based SSA Sensors located outside Indian territory, at the time of submission of the Application to IN-SPACE. IN-SPACE may assess the security provisions and take a decision accordingly. IN-SPACE, may require the Applicants to discontinue operations at such foreign-based station and relocate the SSA Sensor to another site, if such action is found necessary in the national interest, security or in conformance to the prevailing regulations by the Government of India. The relocation may be either within India or in another foreign jurisdiction, subject to the applicable local laws and permissions.
 - c) Applicants are encouraged to have remote access from India for the ground-based SSA Sensors located outside Indian territory.

Applicants shall furnish approvals of the regulatory authority of the respective country for undertaking the RA operations of the ground-based SSA sensor, before commencing such operations.
 - d) SSA Data captured from the ground-based SSA Sensor located outside Indian territory shall be routed through India before dissemination to customers/end-users. Further, in case of the captive network/commercial cloud based (with secured access through API)

dissemination, the commercial cloud/network shall be hosted on server(s) in India.

- iv. Applicants intending to disseminate SSA Raw Data to a non-Indian government OR to a non-Indian Entity for defence/security purpose shall declare so in the Application at time of seeking IN-SPACE Authorisation, and the following shall be applicable:
 - a) Applicants shall provide intimation to IN-SPACE, minimum 15 working days in advance, before disseminating/selling the SSA Raw Data.
 - b) Applicants shall seek one-time prior approval of IN-SPACE before disseminating/selling the SSA Raw Data, if such data pertains to a targeted 'Indian Space Object' or an 'unidentified Space Object' (Space Object which is not identified or assigned any 'satellite catalogue identification number, by the global sources for free/open SSA Data for space safety, such as USSPACECOM/Space-track.org, CelesTrak, EU SST, ESA DISCOS, ISON, etc).
- v. In case of the captive network/commercial cloud based (with secured access through API) dissemination of the SSA Raw Data to customers/end-users, the commercial cloud/network shall be hosted on server(s) in India.
- vi. Enhanced logging, reporting and audit & monitoring mechanism shall be employed. The mechanism is included in [Annexure-2](#). The major points are given as under:
 - a) Applicants shall maintain a complete and immutable log of activities including metadata of the operations of the Authorised SSA Sensors for minimum three years.
 - b) Reporting of the dissemination of the SSA Raw Data by the Applicants, only if the recipient is a non-Indian Entity.
 - c) Reporting only on the targeted RSO (when SSA Sensor is tasked to focus on a specific RSO), if any, shall be included in the periodic report to IN-SPACE. Details of the customer/recipient of such SSA Raw Data, other than the owner/operator of the RSO, shall also be included in the periodic report.

2) Controlled Tier

- i. Applications not falling under the Restricted Tier shall come under the ambit of the Controlled Tier.

- ii. Academic Entities shall require one-time Authorisation from IN-SPACE before undertaking the SSA activity. Authorisation of these entities shall be processed on fast-track basis except for the following cases, which shall go through the standard Authorisation process:
 - a) Collaboration with a non-Indian entity, OR
 - b) The concerned SSA activity is not for the own-use, OR
 - c) The SSA Raw Data is disseminated to a non-Indian Entity
- iii. Logging, reporting and audit & monitoring mechanism shall be eased out. The mechanism is included in [Annexure-2](#). The major points are given as under:
 - a) Applicants shall maintain a complete and immutable log of activities including metadata of the operations of the Authorised SSA Sensors for minimum three years. However, this limit shall be relaxed to one year for the Academic Entities carrying out research work except for the cases ii.-a), b) and c) identified above.
 - b) Reporting of the dissemination of the SSA Raw Data by the Applicants, only if the recipient is a non-Indian Entity.
 - c) Reporting only on the targeted RSO (when SSA Sensor is tasked to focus on a specific RSO), if any, shall be included in the periodic report to IN-SPACE. Details of the customer/recipient of such SSA Raw Data, other than the owner/operator of the RSO, shall also be included in the periodic report.

III. Providing SSA Services

- a) An Indian Entity, intending to provide the SSA Services, whether on commercial or non-commercial basis, shall obtain one-time Authorisation from IN-SPACe valid for a period of 5 (five) years. However, certain usage/entities are exempted from this requirement as explained subsequently.
- b) Such IN-SPACe authorised SSA Service Providers can provide SSA Services to individuals, NGEs, government entities or non-Indian entities. Customers/end-users of such SSA Services do not require any authorisation from IN-SPACe. However, barring a few exceptions/exemptions as explained subsequently, the end-users in India shall avail the SSA Services or SSA Data only from the IN-SPACe authorised SSA Service Providers recognised under this framework. Any deviation from this shall be deemed as non-compliance to the Indian Space Policy-2023.
- c) **Exemptions:**

Following cases are exempted from IN-SPACe Authorisation:

- i. IN-SPACe Authorised satellite owners/operators and launch operators shall be free to avail only the Basic SSA Services (such as LEOP support, collision avoidance analysis, re-entry analysis, fragmentation analysis, real-time orbital position updates/ephemeris, end-of-life disposal support, etc.) or sharing the SSA Data (such as onboard ephemeris, etc), pertaining to their IN-SPACe authorised satellites/payloads, from/with any Indian or non-Indian SSA Service Provider, purely for ensuring the safe and sustainable operations of these Indian satellites/payloads/launch vehicles, irrespective of whether such Service Provider is IN-SPACe-authorised or not.

This also means that Indian or non-Indian SSA Service Providers (directly or through an Indian entity) are permitted to provide the above Basic SSA Services to the Indian satellite owners/operators and launch operators without requiring any Authorisation from IN-SPACe, subject to the following:

- i) Only Basic SSA Services, as mentioned above, pertaining to the concerned IN-SPACe authorised satellite only shall be provided; and
- ii) The recipient of such SSA Services shall be only the concerned satellite owner/operator and launch operator, who shall use these services purely for the purpose of ensuring the safe and sustainable operations of the satellite/launch vehicle.

The contract/agreement signed between the recipient and the SSA Service Provider shall include these undertakings by the recipient and

the SSA Service Provider. The SSA Service Provider shall also verify and confirm that the concerned satellite/launch vehicle is IN-SPACe-Authorised and is owned/operated by the recipient, before providing the SSA Services or entering into the contract/agreement. Further, the End-Use cum End-User Certificate (EUC) requirement shall be applicable for such cases as well.

- ii. Academic Entities shall be free to avail the SSA Services or exchanging the SSA Data (except for the dissemination of the SSA Raw Data which shall be governed by the respective guidelines for the space-based or ground-based SSA Sensors), from/with any Indian or non-Indian SSA Service Provider, for their own-use or purely for the research & development purpose, irrespective of whether such Service Provider is IN-SPACe-authorized or not.

This also means that Indian or non-Indian SSA Service Providers (directly or through an Indian entity) are permitted to provide the SSA Services to these entities without requiring any Authorisation from IN-SPACe, subject to the following:

- i) The recipient of the SSA Services shall be only the Academic Entities; and
- ii) The recipient shall use these services for its own use/self-consumption, not for any commercial gain and purely for the purpose of academic interest, research and development.

The contract/agreement signed between the recipient and the SSA Service Provider shall include such undertaking by the recipient, with the recipient certifying that it is an Academic Entity. The SSA Service Provider shall also carry out due diligence in verifying the status of such Academic Entity recipient by seeking and verifying the copy of recognition with the Government of India/education authorities of State or Union Territory, before providing the SSA Services or signing the contract/agreement. Further, the End-use cum End-User Certificate (EUC) requirement shall be applicable for such cases as well.

- iii. SSA Data and SSA Services for space safety such as orbital element sets, conjunction notices and related information published/made available by the recognised international or academic sources such as USSPACECOM/Space-track.org, CelesTrak, EU SST, ESA DISCOS, ISON, etc are exempted from IN-SPACe Authorisation.
- d) Applicants shall provide details of the mechanism for transfer of the input SSA Data from the source, SSA Data storage and processing facility if any, security

mechanism, geo-coordinates of the facility, etc., as applicable, at the time of submitting the application to IN-SPACE.

- e) Applicants processing the SSA Raw Data shall maintain links to its original raw data source, uphold integrity, and support reconstruction and verification of findings or conclusions, for a minimum period of six (6) months.
- f) The Authorised SSA Service Providers shall indemnify Government of India for any claim, whatsoever made by the customer/end-user or any third-party for a damage or loss arising due to the services provided by them.
- g) **Logging, reporting and audit & monitoring mechanism:** The mechanism is included in [Annexure-2](#). The major points are given as under:
 - (a) Applicants shall maintain a complete and immutable log of activities including metadata for minimum three years.
 - (b) Reporting of the dissemination of the SSA Raw Data by the Applicants, only if the recipient is a non-Indian Entity.
 - (c) Reporting of the dissemination of the SSA Data or SSA Services by the Applicants, only if the recipient is a non-Indian Entity.
 - (d) Reporting only on the SSA Data or SSA Services pertaining to the targeted RSO (when SSA Data is produced focussing on a specific RSO), if any, shall be included in the periodic report to IN-SPACE. Details of the customer/recipient of such SSA Data/SSA Services, other than the owner/operator of the RSO, shall also be included in the periodic report.
- h) Tier-wise specific guidelines are provided below:

1) Restricted Tier

- i. Applicants under non-Indian Management & Control OR intending to provide SSA Data or SSA Services to non-Indian government OR intending to provide SSA Data or SSA Services to a non-Indian Entity for defence/security purpose, shall fall under this tier.
- ii. The authorisation applications shall go through the additional scrutiny by other relevant departments. The entire authorisation process shall be coordinated by IN-SPACE.
- iii. Applicants intending to disseminate SSA Data or SSA Services to a non-Indian government OR to a non-Indian Entity for defence/security purpose shall declare so in the Application at time of seeking IN-SPACE Authorisation, and the following shall be applicable:

- i) Applicants shall provide intimation to IN-SPACE, minimum 15 working days in advance, before disseminating the SSA Data or SSA Services.
- ii) Applicants shall seek one-time prior approval of IN-SPACE before disseminating/selling the SSA Raw Data, if such data pertains to a targeted 'Indian Space Object' or an 'unidentified Space Object' (Space Object which is not identified or assigned any 'satellite catalogue identification number, by the global sources for free/open SSA Data for space safety, such as USSPACECOM/Space-track.org, CelesTrak, EU SST, ESA DISCOS, ISON, etc).
- iv. In case of the captive network/commercial cloud based (with secured access through API) dissemination of the SSA Data or SSA Services to customers/end-users, the commercial cloud/network shall be hosted on server(s) in India.
- v. Enhanced logging, reporting and audit & monitoring mechanism shall be employed.

2) Controlled Tier

- i. Applications not falling under the Restricted Tier shall come under the ambit of the Controlled Tier.
- ii. Logging, reporting and audit & monitoring mechanism shall be eased out.

.....

Guidelines for the Remote Access (RA) of the Ground Stations in India from a location outside India

1. The Ground Stations for purpose of these guidelines shall mean the IN-SPACe-Authorised ground-based SSA Sensors, located within Indian territory and being controlled from outside India through RA.

Remote Access (RA) to IN-SPACe authorised Ground Station is permitted from location within or outside India. However, such RA from outside India is permitted subject to provisioning of equivalent Local Access or Remote Access from within the Indian Territory by the Applicant, hence ensuring that the RA from outside the Indian Territory does not lead to non-provisioning of any Local Access or RA from Indian Territory of the authorised Ground Station.

2. The Applicant shall ensure that there is no unauthorised Remote Access (RA) to any of the equipment installed in the authorised ground stations. Only the Applicant, by itself or through its authorised representative, shall operate the Authorised ground stations through such RA, if any. The customer furnished equipment installed in the authorised ground station premises exclusively for customer's use could be given the authorised Remote Access by the Applicant to the concerned customer.
3. Applicant shall provide the list of locations from which the RA of the ground station is proposed (Foreign locations along with IP address. All RA control points must use static IP address). IN-SPACe approval is mandatory for each of such remote access control points.
4. The Applicant shall comply with the following after receiving IN-SPACe Authorisation/approval for the RA of the authorised ground stations:

- i. Suitable technical device shall be made available at Indian end to the designated security agency/IN-SPACe in which the mirror image of the RA information is available online for monitoring purpose.

Mirror image of RA information pertaining to all ground stations in India may be made available at one of the ground stations (if more than one ground station requiring RA from abroad).

- ii. The hardware and software type, configuration & network flow diagram of implementing the RA mechanism shall be provided at time of seeking IN-SPACe approval/Authorisation.
- iii. Complete audit trail of the RA activities pertaining to the ground station should be maintained in immutable form for a period of six months and provided on request to IN-SPACe or any other agency authorised by IN-SPACe. After six months, the RA logs should be stored offline (in external memories) for a further period of one year.

Applicant shall also ensure that a provision exists to search for specific commands or key words from the available audit trail by IN-SPACE or any other agency authorised by IN-SPACE.

- iv. The applicant shall ensure the capability to restrict remote access to the authorised ground station as and when directed by IN-SPACE.
- v. Applicant shall capture RA command logs from approved locations and store it directly on its local RA storage server. The applicant shall notify IN-SPACE of any hardware/software changes to the RA storage server.
- vi. RA logs should be in simple text format when exported for analysis.
- vii. RA of the GUI based console of an equipment shall be permitted only wherever essential and unavoidable and shall be subject to ensuring that appropriate logging of all user interaction events (keystrokes, mouse clicks etc.) takes place and the logs thus generated can be analysed and searched for keywords/commands. It is to make clear that the video logs cannot be the substitute of the above desired logging mechanism.
- viii. Remote access to ground station should be automatically stopped when RA logs storage is down or becomes non-functional.
- ix. Authentication system for RA and RA log storage should be separate in hardware with adequate facility for storage of tamper proof audit trail.
- x. The connectivity from RA location to the authorised ground station should be through secured connection to ward off any attempt to intrude into the ground station from undesirable and unauthorised IP locations.
- xi. Relevant authentication protocols including multifactor authentication mechanism and position agents should be considered for secure remote access. Furthermore, it is suggested to adopt an industry level mechanism for monitoring for data breaches. If a breach is detected, the same must be intimated to IN-SPACE along with the corresponding details and measures taken/planned to address the breach and avoiding any further occurrence, within 1 (one) week of the breach detection. A standard SOP should be prepared and followed to deal with such incidences of security/data breach.
- xii. Any change in the IP address of the approved foreign locations shall be notified immediately and latest within a week by the applicant to IN-SPACE.
- xiii. The uptime of RA storage server should not be less than 99.99%. This should be ensured while setting up the server through its hardware/software design. Record of any maintenance / shut down of the RA storage server, shall be maintained by the applicant and will be provided to IN-SPACE as and when demanded.

- xiv. The Applicant shall submit the list of all the commands and their functions related to RA so as to make IN-SPACE aware about each and every command and its function at the time of seeking IN-SPACE approval/Authorisation.
- xv. The applicant shall inform IN-SPACE, within one week of operationalization of the RA mechanism (hardware/software) at the respective approved location(s).

IN-SPACE or any other agency authorised by IN-SPACE shall have the right to audit periodically or as and when required, on RA setup or RA logs.

.....

Reporting, Prior Intimation/Approval and Audit & Monitoring Mechanism

Part-A (Reporting Mechanism)

'Establishment and/or operations of Space-based Sensors for SSA related observations'	
Reporting as and when become applicable: Below information needs to be submitted to IN-SPACE on IN-SPACE Digital Platform (IDP) <i>with a copy to director-pmad@inspace.gov.in</i> as and when the event occurs or requires to be reported as per the guidelines.	
1.	Report upon detection of any security or data breach and the corresponding details and measures taken/planned to address the breach and avoid any further occurrence, within 1 (one) week of the breach detection.
2.	Report about the date of commencement of the operations of the Authorised SSA Sensors within 7 (seven) working days.
3.	One (1) month prior reporting, if any material change in the major specifications/configuration of the sensor is planned.
4.	<i>For Restricted Tier applications:</i> a) Submit information for prior intimation [as per format of Part-B] in case Applicant intends to disseminate/sell SSA Raw Data to non-Indian govt. or non-Indian entity for defence/security purpose at least 15 working days in advance. b) <i>Applicants shall seek one-time prior approval of IN-SPACE before disseminating/selling the SSA Raw Data, if such data pertains to a targeted 'Indian Space Object' or an 'unidentified Space Object'.</i>
Periodic Reporting	
Below information needs to be submitted to IN-SPACE on IN-SPACE Digital Platform (IDP) <i>with a copy to director-pmad@inspace.gov.in</i> periodically every 6 months of the calendar year, latest by one month after the end of six months period (e.g., the record of the first half from Jan – June shall be submitted to IN-SPACE before 31st July of that calendar year).	
I.	General Section (applicable for all Tiers)
A.	Details of the non-Indian entity (End-user/customer) to whom the SSA Raw Data is provided
i)	Type (Govt./Pvt. etc.)
ii)	Legal Name of the Entity
iii)	Registered Address
iv)	Purpose/end-use of the SSA Raw Data provided
v)	Service Period
II.	Additional Section applicable for the Controlled Tier
A.	If SSA Raw Data provided pertains to a targeted RSO (when SSA Sensor is tasked to focus on a specific RSO), then provide the details: such as,
i)	Name of RSO
ii)	Identification of RSO available in public domain such as NORAD ID, UN Registration number, etc.
iii)	Owner/Operator details (name & address) of the RSO/satellites

iv)	If the customer/end-user (whether Indian or non-Indian) is other than the owner/operator of the RSO, then provide such customer/end-user details (similar to mentioned above in I.-A.)
III.	Additional Section applicable for the Restricted Tier
A.	If SSA Raw Data provided pertains to a targeted RSO (when SSA Sensor is tasked to focus on a specific RSO), then provide the details: such as,
i)	Name of RSO
ii)	Identification of RSO available in public domain such as NORAD ID, UN Registration number etc.,
iii)	Owner/Operator details (name & address) of the RSO/satellites
iv)	If the customer/end-user (whether Indian or non-Indian) is other than the owner/operator of the RSO, then provide such customer/end-user details (similar to mentioned above in I.-A.)
B.	If the customer/end-user is a non-Indian government or a non-Indian entity having received the SSA Raw Data for defence/security purposes, then provide the prior intimation/approval (as applicable) details (date of intimation to IN-SPACE or IN-SPACE approval number/date) for providing such data.
IV.	General Declarations
i)	Confirming that RSOs which are designated by IN-SPACE / GoI for the national security and strategic requirements are not identified, associated, attributed or catalogued while providing SSA Raw Data by the Applicant.

'Establishment and operations of Ground-based Sensors for SSA related observations'	
Reporting as and when become applicable: Below information needs to be submitted to IN-SPACE on IN-SPACE Digital Platform (IDP) <i>with a copy to director-pmad@inspace.gov.in</i> as and when the event occurs or requires to be reported as per the guidelines.	
1.	Report upon detection of any security or data breach and the corresponding details and measures taken/planned to address the breach and avoid any further occurrence, within 1 (one) week of the breach detection.
2.	Report about the date of commencement of the operations of the Authorised SSA Sensors within 7 (seven) working days.
3.	One (1) month prior reporting, if any material change in the major specifications/configuration of the sensor is planned.
4.	Report if any replacement of the SSA sensor is planned
5.	<i>For Restricted Tier applications:</i> a) Submit information for prior intimation [as per format of Part-B] in case Applicant intends to disseminate/sell SSA Raw Data to non-Indian govt. or non-Indian entity for defence/security purpose at least 15 working days in advance. b) <i>Applicants shall seek one-time prior approval of IN-SPACE before disseminating/selling the SSA Raw Data, if such data pertains to a targeted 'Indian Space Object' or an 'unidentified Space Object'.</i>
Periodic Reporting	
Below information needs to be submitted to IN-SPACE on IN-SPACE Digital Platform (IDP) <i>with a copy to director-pmad@inspace.gov.in</i> periodically every 6 months of the calendar year, latest by one month after the end of six months period (e.g., the record of the first half from Jan – June shall be submitted to IN-SPACE before 31st July of that calendar year).	
I.	General Section (applicable for all tiers)
A.	Details of the non-Indian entity (End-user/customer) to whom the SSA Raw Data is provided
i)	Type (Govt./Pvt. Etc.)
ii)	Legal Name of the Entity
iii)	Registered Address
iv)	Purpose/end-use of the SSA Raw Data provided
v)	Service Period
II.	Additional Section applicable for the Controlled Tier
A.	If SSA Raw Data provided pertains to a targeted RSO (when SSA Sensor is tasked to focus on a specific RSO), then provide the details:
i)	Name of RSO
ii)	Identification of RSO available in public domain such as NORAD ID, UN Registration number etc.,
iii)	Owner/Operator details (name & address) of the RSO/satellites
iv)	If the customer/end-user (whether Indian or non-Indian) is other than the owner/operator of the RSO, then provide such customer/end-user details (similar to mentioned above in I.-A.)

III.	Additional Section applicable for the Restricted Tier
A.	If SSA Raw Data provided pertains to a targeted RSO (when SSA Sensor is tasked to focus on a specific RSO), then provide the details:
i)	Name of RSO
ii)	Identification of RSO available in public domain such as NORAD ID, UN Registration number etc.,
iii)	Owner/Operator details (name & address) of the RSO/satellites
iv)	If the customer/end-user (whether Indian or non-Indian) is other than the owner/operator of the RSO, then provide such customer/end-user details (similar to mentioned above in I.-A.)
B.	If the customer/end-user is a non-Indian government or a non-Indian entity having received the SSA Raw Data provide the prior intimation/approval (as applicable) details (date of intimation to IN-SPACe or IN-SPACe approval number/date) for providing such data.
IV.	General Declarations
i)	Confirming that RSOs which are designated by IN-SPACe / GoI for the national security and strategic requirements are not identified, associated, attributed or catalogued while providing SSA Raw Data by the Applicant.

‘Providing SSA Services’ (applicable for all tiers)	
Reporting as and when become applicable: Below information needs to be submitted to IN-SPACE on IN-SPACE Digital Platform (IDP) with a copy to director-pmad@inspace.gov.in as and when the event occurs or requires to be reported as per the guidelines.	
1.	Report upon detection of any security or data breach and the corresponding details and measures taken/planned to address the breach and avoid any further occurrence, within 1 (one) week of the breach detection.
2.	Report about the date of commencement of the services of the Authorised SSA Sensors within 7 (seven) working days.
3.	For Restricted Tier applications: a) Submit information for prior intimation [as per format of Part-B] in case Applicant intends to disseminate/sell SSA Data or provide SSA Service to non-Indian govt. or non-Indian entity for defence/security purpose at least 15 working days in advance. b) Applicants shall seek one-time prior approval of IN-SPACE before disseminating/selling the SSA Data or providing SSA Service, if such data or service pertains to a targeted ‘Indian Space Object’ or an ‘unidentified Space Object’.
Periodic Reporting	
Below information needs to be submitted to IN-SPACE on IN-SPACE Digital Platform (IDP) with a copy to director-pmad@inspace.gov.in periodically every 6 months of the calendar year, latest by one month after the end of six months period (e.g., the record of the first half from Jan – June shall be submitted to IN-SPACE before 31st July of that calendar year).	
I.	General Section (applicable for Controlled and Restricted Tiers)
A.	Source(s) from which the Applicant has procured/obtained the SSA Data in order to provide the service(s)
i)	Name & address of the supplier of SSA Data
ii)	Type of SSA Sensor (space-based and/or ground-based along with the Sensor type such as optical, RADAR, LiDAR, RF, LASER etc.)
B.	Details of the non-Indian entity (End-user/customer) to whom the SSA Data or Service is provided
i)	Type (Govt./ Pvt. etc.)
ii)	Legal Name of the Entity
iii)	Registered Address
iv)	Purpose/end-use of the SSA Data or Service provided
v)	Service Period
vi)	Type of SSA Data (whether raw or processed) or SSA Service provided (cataloguing, collision avoidance support, conjunction analysis, covariance analysis, manoeuvre detection, modelling of Space Debris environment, orbit determination, orbit propagation, predictions on atmospheric re-entry of space objects, sharing of SSA Data etc., or any other type of service, please specify.)
C.	If SSA Data or Service provided pertains to a targeted RSO (when SSA Sensor is tasked to focus on a specific RSO), then provide the details:
i)	Name of RSO

ii)	Identification of RSO available in public domain such as NORAD ID, UN Registration number etc.,
iii)	Owner/Operator details (name & address) of the RSO/satellites
iv)	If the customer/end-user (whether Indian or non-Indian) is other than the owner/operator of the RSO, then provide such customer/end-user details (similar to mentioned above in I.-B.)
II.	Additional Section applicable for the Restricted Tier
A.	If the customer/end-user is a non-Indian government or a non-Indian entity having received the SSA Data or Service for defence/security purposes, then provide the prior intimation/approval (as applicable) details (date of intimation to IN-SPACe or IN-SPACe approval number/date) for providing such data or service.
III.	General Declarations
i)	Confirming that RSOs which are designated by IN-SPACe / GoI for the national security and strategic requirements are not identified, associated, attributed or catalogued while providing SSA Data or service by the Applicant.

Part-B (Prior Intimation/Approval Mechanism)

Information to be provided on IN-SPACE Digital Platform (www.inspace.gov.in) with a copy to director-pmad@inspace.gov.in as part of the “prior-intimation” (at least 15 working days in advance) or “prior-approval”, as applicable, in case Applicant intends to disseminate/sell SSA Raw Data or provide SSA Service to a non-Indian govt. or a non-Indian entity for defence/security purpose.	
	Purpose (prior intimation or prior approval)?
A.	Details of the non-Indian entity (End-user/customer) to whom the SSA Raw Data or SSA Service is to be provided
i)	Type (Govt./Pvt. etc.)
ii)	Legal Name of the Entity
iii)	Registered Address
iv)	Purpose/end-use of the SSA Raw Data/Service to be provided
v)	Service Period
vi)	Type of SSA Raw Data (Source-Sensor name/identification and type, targeted area/direction of the FOV of the sensor, if applicable, etc) or SSA Service to be provided (sharing of SSA Raw Data, sharing of SSA Data, cataloguing, collision avoidance support, conjunction analysis, covariance analysis, manoeuvre detection, modelling of Space Debris environment, orbit determination, orbit propagation, predictions on atmospheric re-entry of space objects, etc., or any other type of service, please specify.)
B.	If SSA Raw Data or SSA Service provided pertains to a targeted RSO(s), then provide the details:
i)	Name of RSO(s)
ii)	Identification of RSO(s) available in public domain such as NORAD ID, UN Registration number etc.,
iii)	Owner/Operator details (name & address) of the RSO/satellites
C.	General Declarations
i)	Confirming that RSOs which are designated by IN-SPACE / GoI for the national security and strategic requirements shall not be identified, associated, attributed or catalogued while providing SSA Raw Data or SSA service to the proposed customer/end-user.

Part-C (Audit & Monitoring Mechanism)

Establishment and/or operations of <u>space-based SSA Sensors</u> An indicative list of the information/aspects which could be subject to the audit is provided below.			
Typical Sample Size (could be varied on case by case basis): (i) 10% of the transactions pertaining to 20% of the randomly selected customers/end-users; (ii) 100% for non-Indian govt. /end-users or non-Indian entity/end-users for defence/strategic purpose			
Sl. No.	Details	Information/aspects to be verified	Remarks
1	Compliance to Reporting mechanism	- Verification of the reporting requirements as per the reporting mechanism. - Verification of prior approval/intimation, if any. (applicable for Restricted tier)	Based on declaration by the Applicant
2	Tier Applicability	Verify the scope of activities authorised to check if the tier declared in the Authorisation Certificate issued by IN-SPACE is applicable or not.	
3	Company credentials	Verify Management and Control Credentials vis-à-vis declared in the application - Shareholding pattern of Authorised entity; - Management & Control of the Authorised Entity - Change in KMPs.	
4	SSA Satellite/sensor Mission	Verification of launch and Orbital parameters achieved	Based on declaration by the Applicant
		Date of operationalisation of the SSA satellite/sensor (intimation within 7 days)	
		Verification of the major sensor specifications as per the details declared in the Application.	
		Health of the SSA satellite/sensor (balance operational life) as applicable	Based on declaration by the Applicant
		Verification of necessary approvals/licenses from the relevant Govt. department(s)/ ministries, as applicable and necessary for operationalization of the sensor	
		Verification of log of observations carried out from Authorised SSA Sensor. Logging period: 3 years (1 year for Academic Entities except if they are collaborating with non-Indian entity OR SSA Activity is not for own-use OR SSA Raw Data disseminated to non-Indian entity)	On-Site verification

5	General Compliances	Verify the mechanism by which RSOs, as designated by IN-SPACE / GoI for the national security and strategic requirements, are not being identified, associated, attributed or catalogued while Applicant is providing SSA Raw Data. Verify to monitor the operations and use of filters/appropriate mechanism to restrict dissemination of such SSA Data	On-Site verification
6	Space Object Registration Compliance	Periodical ephemeris data being uploaded on IDP, if applicable	
		Verification of regular Conjunction assessment and mitigation measures being carried out by the Authorised Entity, if applicable	
		Compliance to framework for safe and sustainable space operations as and when brought out by DoS, if applicable	
7	Operations, Control, storage & Data Acquisition	Verification of operating mechanism of data reception/ TTC earth station/ SSA Data control, storage /archival and/or processing facility / MCC, including arrangement with foreign data reception station operator(s) in case of data reception station being outside Indian territory vis-a-vis as declared in the application.	On-site audit
		Confirmation on the location of MCC in India or cloud-based MCC is hosted on Indian server (Exercise of control & decision making from Indian territory) (applicable for Restricted Tier)	
		Verification of provision for LIM	
		Verification of SSA Data Routing through India, (applicable for Restricted Tier)	
8	Security & Safety Measures for the entire system/network	Verification of the End-use cum End-User Certificates (EUC) from Applicant's customers/recipients.	On-site audit
		Compliance to safety and security guidelines as and when brought out by IN-SPACE.	
		Verify the provision to cease the emission/operation as and when needed.	
		Verification of adoption of measures as declared in application including - Physical security - Cyber resilience against potential threats	Check report of MeitY empanelled security auditors if available.

		• Access control mechanism to prevent unauthorised use • Confirmation on onboard encryption, (applicable for Controlled and Restricted Tier) • Verify the aspects related to procurement from Trusted Sources. • Compliance with Information Security and Management guidelines and Cyber Security Framework and Guidelines for Space including Satellite communication issued by CERT-In, MeitY <i>(not applicable for Academic Entities except if they are collaborating with non-Indian entity OR SSA Activity is not for own-use OR SSA Data disseminated to non-Indian entity)</i> • Any other applicable security aspects brought out in the NGP/SSA Authorisation Guidelines.	
9	ITU Filings & Interference	Verification with application parameters, milestone/due diligence procedures and reported interference & resolution. (To be carried out in coordination with WPC)	
10	Audit of terms & conditions specific to the Authorisation Certificate As per T&C		
Note:	(1) In addition, audit & monitoring mechanism for establishment and operations of remote sensing, amateur satellite, hosted payload and ground systems authorisations shall be considered, if applicable. (2) Both the Auditor/IN-SPACe and the Applicant shall sign the Audit Report along with an undertaking from the Applicant to the effect that the information provided by the Applicant during the audit is true to the best of its knowledge.		

Establishment and operations of ground-based SSA Sensors

An indicative list of the information/aspects which could be subject to the audit is provided below.

Typical Sample Size (could be varied on case by case basis):

- (i) 10% of the transactions pertaining to 20% of the randomly selected customers/end-users;
- (ii) 100% for non-Indian govt. /end-users or non-Indian entity/end-users for defence/strategic purpose

Sl. No.	Details	Information/aspects to be verified	Remarks
1	Compliance to Reporting mechanism	- Verification of the reporting requirements as per the reporting mechanism. - Verification of prior approval/intimation, if any. (applicable for Restricted Tier)	Based on declaration by the Applicant
2	Tier Applicability	Verify the scope of activities authorised to check if the Tier declared in the Authorisation Certificate issued by IN-SPACE is applicable or not.	
3	Company credentials	Verify Management and Control Credentials vis-à-vis declared in the application - Shareholding pattern of Authorised entity; - Management & Control of the Authorised Entity - Change in KMPs.	
4	SSA Ground-based sensor/ Mission	Date of operationalisation of the SSA sensor (intimation within 7 days)	Based on declaration by the Applicant
		Verify any change/replacement of ground-based SSA sensor.	On-site verification
		Verify any major change in specification of sensor.	
		Verify operational constraints such as the range of elevation angle, location, scope of activity etc.	
		Verification of log of observations carried out from Authorised SSA Sensor.	
		Logging period: 3 years (1 year for Academic Entities except if they are collaborating with non-Indian entity OR SSA Activity is not for own-use OR SSA Raw Data disseminated to non-Indian entity)	
		Verification of validity of leased/rented land vis-à-vis validity of Authorisation granted for each sensor	Based on declaration by the Applicant
		Verification of necessary approvals/ licenses from the relevant Govt. department(s)/ ministries, as applicable and necessary for establishment and operationalization of the sensor within and outside India	

5	General Compliances	Verify the mechanism by which RSOs, as designated by IN-SPACe / GoI for the national security and strategic requirements, are not being identified, associated, attributed or catalogued while Applicant is providing SSA Raw Data. Verify to monitor the operations and use of filters/appropriate mechanism to restrict dissemination of such SSA Data	On-site verification
6	Control, Storage & Processing system	Verification on location of control and processing facility/system as declared in the application Confirmation on the operational control of the ground sensor from India Verification of compliance to RA guidelines for the ground-based Sensor as included in Annexure-1 Confirmation if cloud-based dissemination of SSA Raw Data is hosted on Indian server (applicable for Restricted Tier) Verification of provision for LIM Verification of SSA Data Routing through India, (applicable for Restricted Tier) Verification of the End-use cum End-User Certificates (EUC) from Applicant's customers/recipients.	Onsite audit
7	Security & Safety Measures of the entire system/network	Compliance to safety and security guidelines as and when brought out by IN-SPACe. Verify the provision to cease the emission/ operation as and when needed. Verification of adoption of measures as declared in the application including - Physical security - Cyber resilience against potential threats - Access control mechanism to prevent unauthorised use - Confirmation on secured data transfer mechanism for SSA Raw Data dissemination - Verify the aspects related to procurement from Trusted Sources. - Compliance with Information Security and Management guidelines and Cyber Security Framework and Guidelines for Space including Satellite communication issued by CERT-In, MeitY <i>(not applicable for Academic Entities except if they are collaborating with non-Indian entity OR SSA Activity is not for own-use OR SSA Data disseminated to non-Indian entity)</i>	Onsite audit Check report of MeitY empanelled security auditors.

		Any other applicable security aspects brought out in the NGP/SSA Authorisation Guidelines.	
8	Interference aspect	In case of reported interferences being caused by the ground sensor, if applicable: Confirmation of the cause of interference and suitable remedial measures (To be carried out in coordination with WPC)	As & when interference is reported
9	Audit of terms & conditions specific to the Authorisation Certificate issued to the Authorised Entity, as applicable.		As per T&C
Note:	Both the Auditor/IN-SPACE and the Applicant shall sign the Audit Report along with an undertaking from the Applicant to the effect that the information provided by the Applicant during the audit is true to the best of its knowledge.		

Providing SSA Services

An indicative list of the information/aspects which could be subject to the audit is provided below.

	Typical Sample Size (could be varied on case by case basis): (i) 10% of the transactions pertaining to 20% of the randomly selected customers/end-users; (ii) 100% for non-Indian govt. /end-users or non-Indian entity/end-users for defence/strategic purpose		
Sl. No.	Details	Information/Aspects to be verified	Remarks
1	Compliance to Reporting mechanism	• Verification of the reporting requirements as per the reporting mechanism. • Verification of prior approval/intimation, if any. (applicable for Restricted tier)	Based on declaration by the Applicant
2	Tier Applicability	Verify the scope of activities authorised to check if the Tier declared in the Authorisation Certificate is applicable or not.	
3	Company credentials	Verify Management and Control Credentials vis-à-vis declared in the application • Shareholding pattern of Authorised entity; • Management & Control of the Authorised Entity • Change in KMPs.	
4	Security & Safety Measures of the entire system/network	Verification of adoption of measures as declared in the Application including • Cyber resilience against potential threats • Access control mechanism to prevent unauthorised use • Provision for securing the SSA data transfer • Verify the aspects related to procurement from Trusted Sources. • Compliance with Information Security and Management guidelines and Cyber Security Framework and Guidelines for Space including Satellite communication issued by CERT-In, MeitY <i>(not applicable for Academic Entities except if they are collaborating with non-Indian entity OR SSA Activity is not for own-use OR SSA Data disseminated to non-Indian entity)</i> • Any other applicable security aspects brought out in the NGP/SSA Authorisation Guidelines.	On-site audit Report of MeitY empanelled security auditors, if available

5	SSA Data/Services Dissemination	Date of commencement of the SSA services (intimation within 7 days)	Based on declaration by the Applicant
		Verify the mechanism by which RSOs, as designated by IN-SPACe/GoI for the national security and strategic requirements, are not being identified, associated, attributed or catalogued while Applicant is providing SSA Raw Data. Verify to monitor the operations and use of filters/appropriate mechanism to restrict dissemination of such SSA Data	On-site Verification
		Verify that the mechanism of processing SSA Raw data maintaining links to its original raw data source for minimum period of 6 months.	On-site audit
		Confirmation on availability of IN-SPACe approval for SSA Data/Services for non-Indian government or for non-Indian security / defence purpose	
		Verification of the Log containing complete details of the SSA services provided including source of SSA Data and storage being maintained by the Applicant. Logging period: 3 years	
		Confirmation for case of cloud-based dissemination of SSA Data or service is hosted on Indian server. (applicable for Restricted tier)	
		Verification of provision for LIM	
		Verification of the End-use cum End-User Certificates (EUC) from Applicant's customers/recipients.	
6	Audit of terms & conditions specific to the Authorisation Certificate issued to the Authorised Entity, as applicable.		As per T&C
Note:	Both the Auditor/IN-SPACe and the Applicant shall sign the Audit Report along with an undertaking from the Applicant to the effect that the information provided by the Applicant during the audit is true to the best of its knowledge.		

END-USE CUM END-USER CERTIFICATE (EUC) FOR DISSEMINATING SSA RAW DATA OR PROVIDING SSA SERVICES

*[To be filled by customer/recipient/end-user duly signed by authorised signatory of
customer/recipient]*

1. Details of the Entities:

- a) Name of IN-SPACE Authorised Entity/Supplier/Disseminator:
- b) Name of Customer/Recipient:
- c) Customer or Recipient's Address:
- d) Name of End-user (if different than the customer/recipient):
- e) End-user's Address:

2. Details of SSA Services obtained by Customer/Recipient:

- a) I hereby declare that the following SSA Services/SSA Raw Data are obtained from IN-SPACE Authorised Entity/Supplier/Disseminator (tick everything as applicable):
 - ☐ Cataloguing
 - ☐ Collision avoidance support
 - ☐ Conjunction analysis
 - ☐ Covariance analysis
 - ☐ Manoeuvre detection
 - ☐ Modelling of Space Debris environment
 - ☐ Space weather monitoring
 - ☐ Orbit determination
 - ☐ Orbit propagation
 - ☐ Predictions on atmospheric re-entry of space objects
 - ☐ Cis-lunar SSA
 - ☐ Dissemination of SSA Raw Data to the end-users/ customers, etc.
 - ☐ Dissemination of SSA Data, other than SSA Raw Data, to the end-users/ customers, etc.
 - ☐ Others (please specify): _____
- b) I hereby declare that the SSA Services as obtained will be used exclusively for the following purpose(s) of (tick everything as applicable):
 - ☐ Dissemination of SSA Data to its subsequent customers
 - ☐ End-use in ensuring the safe and sustainable operations of the satellite
(name and ID of the satellite)
 - ☐ Operational satellite tracking
 - ☐ Conjunction assessment and Collision avoidance
 - ☐ Space object cataloguing and monitoring

- ☐ Space debris analysis and mitigation
- ☐ Research and academic study related to space situational awareness
- ☐ Identification and understanding/characterisation of RSOs (*name and ID of the RSO*)
- ☐ End-use in military/security/strategic/defence domain
- ☐ Others (please specify): _____

Declaration

I, the undersigned, acknowledge and agree to:

- a) use the SSA data and SSA services only for authorised purposes as declared herein.
- b) maintain EUC if same SSA Service/SSA Raw Data is provided to any other Customer/third party
- c) not share, disseminate, or transfer SSA Data related to prohibited space objects or sensitive data as per Government of India and IN-SPACe guidelines, as and when notified or intimated to us.
- d) maintain confidentiality and security of sensitive SSA Data in accordance with the applicable regulatory and national security norms brought out by IN-SPACe/Government of India.
- e) confirm that all information provided in this declaration is true and accurate to the best of my knowledge.

I undertake to comply with all relevant laws, regulations, and conditions pertaining to the authorised use of SSA Data and SSA Services brought out by IN-SPACe/Government of India.

Name	
Designation	
Complete office address	
Email	
Authorised Signatory of Customer/Recipient	Signature (authorised signatory): Official seal / stamp: Date of issue: Validity date (specify the period):

Intimation by Academic Entities for ground based SSA sensor installations

[To be filled by Academic Entities who are exempted from IN-SPACE Authorisation and have been operating or planning to establish & operate ground based SSA sensors and submit on IN-SPACE Digital Platform (www.inspace.gov.in) with a copy to director-pmad@inspace.gov.in]

1. Details of the Entity:

- a) Name of the Academic Entity:
- b) Complete address of the Academic Entity:
- c) Address of the ground-based SSA Sensor installation site & Lat/Long:
- d) Source of procurement of the ground-based SSA Sensor:
- e) Date of sensor operationalisation (expected date can be provided in case of planned installation):
- f) Objective of the activity:
- g) Whether any collaboration with any foreign entity is involved for this activity? If so, provide details.
- h) Salient specifications of the ground-based SSA Sensor (including hardware and software) such as:
 - i) Angular slew rate:
 - ii) Automated close-loop tracking (Yes/No):
 - iii) Timing precision:
 - iv) Aperture Diameter:
 - v) Real time data dissemination (Yes/No):
 - vi) Latency from acquisition to dissemination:
 - vii) Information on the processing of the raw data (if any):

2. Undertakings:

1. We hereby affirm that we have clearly read and understood the Authorisation guidelines for undertaking SSA related activities guidelines issued by IN-SPACE.
2. We hereby confirm and certify that the activities pertaining to establishment and operations of the ground-based SSA Sensor intimated through this proforma are non-commercial, public/academic awareness intent and within the technical

thresholds as specified for exempting the IN-SPACE authorisation requirement in the said authorisation guidelines.

3. We undertake that there will be no real time transmission of data to anyone.
4. We hereby agree to notify IN-SPACE promptly regarding any material change and seek authorisation in case the activity falls beyond the authorisation-exempt conditions as specified in the said guidelines.

Signature (authorised signatory):

Official seal / stamp:

Contact details:

Email id:

Web-site

Date:

Place:

.....

**APPLICATION TEMPLATE FORMS FOR DIFFERENT CATEGORIES OF
AUTHORIZATION**

Sl. No.	Category	Template Form (See attached file)
1.	Establishment and/or operations of space-based SSA Sensors	
2.	Establishment and/or operations of ground-based SSA Sensors	
3.	Providing SSA Services	