IGN-3530

Global Affairs Canada

Division for Non-Proliferation, Disarmament and Space

Space Regulatory Section

REMOTE SENSING SPACE SYSTEMS ACT

Application Guide

Version 2.1

October 16, 2023

Disclaimer: This guide is intended to provide Licensees and System Participants an understanding of the licensing process and facilitate the submission of a complete licence applications. This guide is not intended to replace the *Remote Sensing Space Systems Act* and its Regulations, which supersede the guide in the event of any conflict.

Global Affairs Canada Affaires mondiales Canada

Version	Changes / Affected Sections	Date
1.0	All / Initial Version	26 October 2020
1.1	Sections 2, 3, 5, 6, and 9; Appendices B, C, and E; Editorial amendments	08 March 2021
2.0	Section 2.1; naming change from Appendices to Annexes; updates to Annex C; placeholder for Annex D; and general editorial amendments throughout.	17 July 2023
2.1	General editorial amendments throughout.	16 October 2023

EXECUTIVE SUMMARY

Space has become increasingly accessible, having transitioned from a desirable resource to an essential resource. There is more demand than ever for Earth observation images, obtained through the operation of remote sensing space systems.

Such systems are regulated in Canada pursuant to the *Remote Sensing Space Systems Act* (S.C. 2005, c. 45) ("the *Act"*) and the *Remote Sensing Space Systems Regulations* (SOR 2007-66) ("the *Regulations"*).

It is recommended that the Applicant read the *Act* and the *Regulations* before consulting this guide. The latter is intended to provide the Applicant with a complete understanding of the licensing process and facilitate the application for an operating licence under the *Act*.

In this guide, information can be found on the following:

- Application for a licence: Requirements
- The Remote Sensing Space System: Space Segment, Ground Segment, and Data
- Required documentation
- Appendices containing further details.

Global Affairs Canada (Division for Non-Proliferation, Disarmament and Space) is the author of this document. Questions or comments can be sent to the following e-mail address:

RSSSA-LSTS@international.gc.ca

TABLE OF CONTENTS

1 INTRODUCTION

The application process for a licence to operate a Remote Sensing Space System can appear daunting given the complexity and information required, pursuant to the *Remote Sensing Space Systems Act*[1] (S.C. 2005, c. 45) ("the *Act*"). This document is intended to facilitate the application process by outlining guidelines on the licensing procedure. A separate document will address other aspects of the *Act* and the *Regulations*.

The Division for Non-Proliferation, Disarmament and Space at Global Affairs Canada (GAC) administers the *Act* on behalf of the Minister of Foreign Affairs (hereinafter the Minister). Additionally, GAC is the regulatory body of the *Act* and the *Regulations*.

GAC encourages potential Applicants to engage in preliminary consultations before submitting a licence application, by contacting **RSSSA-LSTS@international.gc.ca**. GAC will review initial application information and advise if modifications are required. Such consultations provide an early opportunity to identify any potential issues associated with the development of a proposed system and the licence application.

Benefits of preliminary consultations with GAC prior to submitting an application:

- GAC is familiarized at an early stage with the Applicant's mission
- Applicant obtains clarity on whether a license is required and information expected for the application
- GAC can advise if modifications are required to the application
- The development of a proposed system and the license application provide an opportunity for both sides to identify potential issues

Who is Required to Apply for a RSSSA Licence?

In Canada, no person may operate a remote sensing space system, except under authority of a licence. Any Canadian who owns and/or operates remote sensing-capable space system(s) anywhere and foreign owners and/or operators operating such systems in Canada are required to apply for a licence under the *Act*.

As per Section 2 of the *Act*, a "person" includes partnerships, a government, a government agency and an unincorporated organization.

1.1 ACRONYMS

EULA	End-User Licence Agreement
GAC	Global Affairs Canada
IT	Information Technology
Minister	the Minister of Foreign Affairs
RCMP	Royal Canadian Mounted Police
RSSSA Remote Sensing Space Systems Act	the *Act*
RSSSR Remote Sensing Space Systems Regulations	the *Regulations*
SPA	System Participant Agreement

[1] Government of Canada, *Remote Sensing Space Systems Act (S.C. 2005, c. 45),* 2005, https://laws-lois.justice.gc.ca/PDF/R-5.4.pdf.

2 APPLYING FOR A LICENCE

Sections 2 through 7 of the *Remote Sensing Space Systems Regulations*[2] (SOR/2007-66) ("the *Regulations*") outline the documentation required to support a license application, amendment, or renewal. The written application must be dated, signed, and attested to by an authorized representative in order to affirm that the information contained in the application is true, complete and correct. A copy of the application must be submitted electronically. Copies of any proposed agreements with System Participants and the final versions of such agreements are to be included. Upon submission by the Applicant of all required information and documents, the Minister has 180 days to respond to an initial application and 90 days to respond to any amendment.[3]

The *Regulations* include *Schedule 1 Information and Documents to Support an Application*[4]. Sections 1 to 8 outline the business information and documents required in an application. If an affiliated entity is involved in the operations of the system, it must be identified and its business information provided, as indicated in Section 31. Information is also required regarding the satellite and its operation.

The application must include the following: a System Disposal Plan, Command Protection Plan, and Data Protection Plan (or a combined Command and Data Protection Plan).

The application must include:

- System Disposal Plan
- Command Protection Plan
- Data Protection Plan

The Applicant and System Participant(s) must acknowledge the obligation to maintain records and allow inspectors access to their facilities.

If seeking designation of a System Participant, the application must provide detailed business information of the proposed System Participant(s), along with a copy of an agreement between the Applicant and the System Participant (see Section 4 of this guide). Depending on its role, the System Participant(s) must also provide a System Disposal Plan, Command Protection Plan and a Data Protection Plan. The System Participant Agreement must include conditions that oblige the System Participant(s) to comply with the *Act*, its *Regulations*, and all licence conditions.

Once an application has been submitted or a licence granted, the Applicant is required to notify the Minister (via GAC's Space Regulatory Section) of any subsequent changes to the design affecting the system's operational capabilities. GAC will coordinate the review process within the Government of Canada.

As the regulator, GAC has the obligation to treat proprietary information submitted by the Applicant and subsequent Licensee[5] as confidential.

The licence application review process is illustrated in Figure 2-1 below.

[2] Government of Canada, *Remote Sensing Space Systems Regulations (SOR/2007-66),* 2007, https://laws-lois.justice.gc.ca/PDF/SOR-2007-66.pdf.
[3] RSSS *Regulations*, Section 7.
[4] RSSS *Regulations*, Section 2(1)(a), Section 2(2)(a), Section 3(2)(b), Section 6, Section 10(b) and Schedule 1.
[5] For instance, government records of an application could be subject to a request under the *Access to Information Act*. The *Act* states that a head of government shall not disclose any record requested that contains financial, commercial, scientific, or technical information supplied to the government institution by a third party that is treated consistently in a confidential manner by the third party. Note that the non-disclosure requirement is not absolute if the third party consents, or if disclosure would be deemed in the public interest on certain grounds.

Figure 2-1: Licence Application Review Process

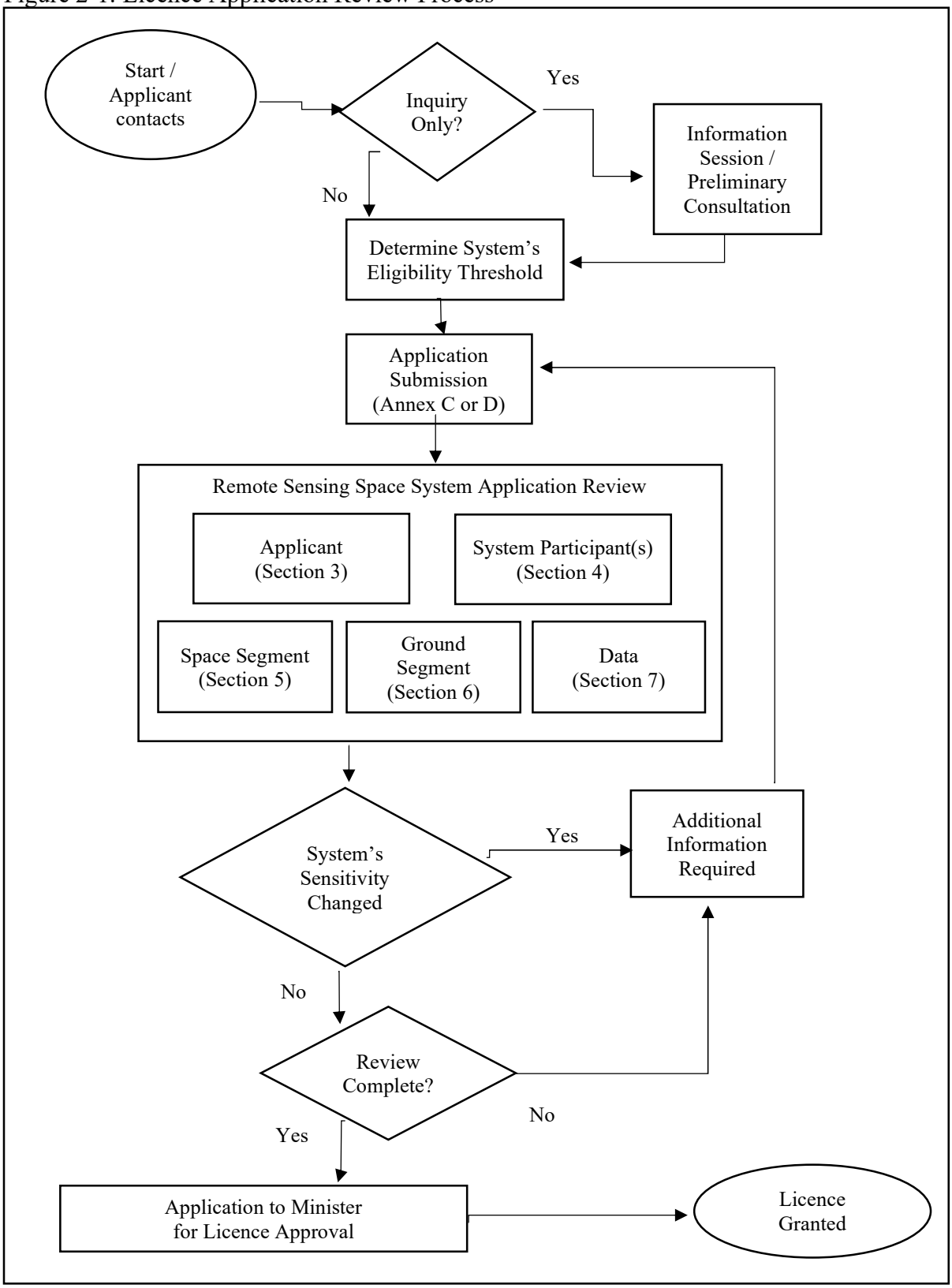

FIGURE 2-2: LICENCE APPLICATION REVIEW PROCESS

2.1 LICENCE APPLICATION PROCESS

Wherever possible, GAC encourages a potential Applicant to initiate preliminary consultations to help determine whether proposed operations of a remote sensing space system require a licence under the *Act*.

If an application for a required license is incomplete or becomes inaccurate due to an operational change or other situation prior to the license being issued, the Applicant must promptly submit the updated or corrected information to GAC as soon as possible.[6]

A complete application contains detailed information related to all elements covered in the *Regulations'* Schedule 1.

Applications and related documents should be submitted to:

Global Affairs Canada
Division for Non-Proliferation, Disarmament & Space (IGN)
Space Regulatory Section
125 Sussex Drive
Ottawa, Ontario K1A 0G2

Or emailed to:

RSSSA-LSTS@international.gc.ca

Schedule 1 of the *Regulations* outlines the requisite documentation to be included in the application. This is also detailed in Annex C and Annex D of this guide. These annexes are laid out in such a way that they can be used as a basis for an application. If any of the information required is not applicable, the Applicant must indicate "N/A" and provide a rationale. The completed application should be dated and signed by an authorized principal executive officer attesting that the information contained therein is complete and correct. Thereafter, a copy of the application should be sent by electronic mail.[7] Copies of any proposed agreements (including final versions) with System Participants should also be included.

Did You Know?

In an effort to streamline the process, GAC has developed two application streams based on the system's Eligibility Threshold to determine if the applicant can complete the Multi-Stage Application Process.

A system capable of producing high-grade remote sensing data will require the application, as per Annex C.

A system that is eligible can follow the **Multi-Stage Application** approach, starting with the completion of Stage-1. During GAC's review, additional information may be requested, possibly prompting the completion of Stage-2. Refer to Annex D for full details.

[6] RSSS *Regulations*, Section 5(2).
[7] RSSS *Regulations*, Section 5(1)(b).

3 THE APPLICANT

The Applicant is the person who submits the application for a licence under the *Act*. This may be an individual or an entity, including: a government or government agency, a corporation, or an unincorporated organization. A designated "contact person" acts as the primary contact for all future communications with GAC, which can the Applicant or another individual.

All required documentation for the Applicant should be complete and in order. Subsequently, GAC consults lists of prohibited entities to ensure that the Applicant, the contact person, and proposed System Participant(s) are not on United Nations and Canadian sanction lists or any specific prohibition lists (for example, the *United Nations Act*[8] and the *Special Economic Measures Act*[9]). Regarding the data and remote sensing products, some provisions of the *Export and Import Permits Act*[10] may apply. Additionally, GAC cross-checks other lists, such as the following:

1. Entities identified and listed from time to time under Canada's *Anti-Terrorism Act*[11] and the *Criminal Code*[12], and listed on the Public Safety Canada[13] website.

2. Other entities and persons identified and listed on the "Foreign Policy, Economic Issues and Canadian Economic Sanctions" listings, which are located at the following links:

    a. Current sanctions imposed by Canada[14] ; and
    b. Listed Persons[15].

3.1 THE APPLICANT – KEY INFORMATION AND DOCUMENTS

Data on the Applicant's proposed remote sensing space system must be sufficiently detailed to enable GAC to determine whether it meets the requirements of the *Act* and the *Regulations*. A list of all key documents is found in Annex A of this guide.

1. Identification and contact information of the Applicant.
2. Identification and contact information of the "contact person" for the Applicant.
3. Security documents for the contact person, as per Schedule 1, Section 3 of the *Regulations*:
    a. Personnel screening form; Security screening certificate; Security clearance form; and

[8] Government of Canada, *United Nations Act (R.S.C., 1985, c. U-2)*, 2019, https://laws-lois.justice.gc.ca/eng/acts/u-2/.
[9] Government of Canada, *Special Economic Measures Act (S.C. 1992, c. 17)*, 2017, https://laws-lois.justice.gc.ca/eng/acts/s-14.5/index.html.
[10] Government of Canada, *Export and Import Permits Act (R.S.C., 1985, c. E-19)*, 2019, https://laws-lois.justice.gc.ca/eng/acts/e-19/.
[11] Government of Canada, *Anti-terrorist Act (S.C. 2001, c. 41)*, 2003, https://laws-lois.justice.gc.ca/eng/acts/a-11.7/.
[12] Government of Canada, *Criminal Code Act (R.S.C., 1985, c. C-46)*, 2019, https://laws-lois.justice.gc.ca/eng/acts/c-46/.
[13] Public Safety Canada's webpage: www.publicsafety.gc.ca;
Public Safety Canada's listed entities: http://www.publicsafety.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/crrnt-lstd-ntts-eng.aspx.
[14] Government of Canada sanctions: https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/current-actuelles.aspx?lang=eng.
[15] Government of Canada listed persons: https://www.international.gc.ca/world-monde/international_relations-relations_internationales/sanctions/listed_persons-personnes_inscrites.aspx?lang=eng.

b. Royal Canadian Mounted Police (RCMP) fingerprint form.

Please note that GAC is not responsible for administering these forms. They can be obtained directly from the Treasury Board Secretariat (for forms under 3(a) above) and the RCMP (for the form under 3(b) above). The Applicant's security officer should contact relevant government departments, such as Public Services and Procurement Canada,[16] for information on obtaining the required security clearance.
The minimum required security clearance is "reliability," but this can be higher depending on the complexity and sensitivity of the remote sensing space system.

4. If the Applicant is an entity other than a government or government agency, as per Schedule 1, Section 4 of the *Regulation*, the following financial information is required:
   a. a certified copy of its instrument of incorporation or continuance or its business registration in its jurisdiction of operation, as the case may be;
   b. the name, identifying information and contact information of the chief executive officer and each of the Applicant's directors, if any;
   c. the name, identifying information and contact information of each of the Applicant's officers who will be responsible for the operation of the remote sensing space system;
   d. the name, identifying information and contact information of each owner with an interest equal to or greater than 10% in the Applicant entity, and the interest held by that owner; and
   e. the name, identifying information and contact information of each person who exercises control over the Applicant.
5. The name, identifying information and contact information of each of the Applicant's secured creditors, as per Schedule 1, Section 5 of the *Regulations*.
6. The name, identifying information, contact information and amount of indebtedness for every person to whom the Applicant is indebted for more than 5% of the Applicant's total indebtedness, as per Schedule 1, Section 6 of the *Regulations*.
7. The name, identifying information and contact information of each affiliate that will be involved in the operation of the system are also required, as per Schedule 1, Section 31 of the *Regulations*.

[16] Public Services and Procurement Canada website: https:/0823585375 /www.tpsgc-pwgsc.gc.ca/esc-src/personnel/information-eng.html.

4 THE SYSTEM PARTICIPANT

A System Participant is an individual or entity participating in the operation of the licensed remote sensing space system, through the performance of Controlled Activities. The Minister may designate any person or entity as a System Participant and authorize the Licensee to permit that person to carry out any specified Controlled Activity in the operation of the system. A System Participant Agreement is negotiated between the Applicant/Licensee and the System Participant(s), and must be approved by GAC.

Controlled Activities (*The Act, Section 2):*

(a) formulating or giving a command

(b) receiving raw data

(c) storing, processing or distributing raw data

(d) establishing or using

(i) cryptography in communications

(ii) information assurance measures

It is essential to include all information outlined in Section 32 of the *Regulations'* Schedule 1 in a System Participant Agreement. For the purpose of the licence application, a final draft of the System Participant Agreement agreed to by both parties and approved by GAC is acceptable. The final signed copy can be provided after the licence is issued.

4.1 THE SYSTEM PARTICIPANTS – KEY INFORMATION AND DOCUMENTS

Data on the System Participant should be sufficiently detailed to enable GAC to determine whether the proposal meets the requirements of the *Act* and the *Regulations*. A list of all key documents is found in Annex A of this guide.

1. Identification and contact information for each System Participant (as per the Applicant's requirements listed in Section 3.1 above).
2. Description of the Remote Sensing Space System, identifying the individual roles played by the Applicant and System Participant(s), particularly relating to the performance of Controlled Activities with regard to the Remote Sensing Space System.
3. Security documents for the contact person for each System Participant (as per the Applicant's requirements listed in Section 3.1 above).
4. Names and security information for persons performing Controlled Activities.
5. Final draft or signed copy of the System Participant Agreement, attaching other required documents such as: (i) General Site Description; (ii) Individual or consolidated Data and Command Protection Plans; and (iii) System Disposal Plans, as they relate to the operations of the System Participant, where the same information has not been presented elsewhere by the Applicant.
6. Any related documentation under the three components of a remote sensing space system (see Sections 5, 6 and 7 of this guide) for which the System Participant contributes.

5 THE SPACE SEGMENT

All satellites capable of remotely sensing the Earth through the use of electromagnetic waves fall within the jurisdiction of the *Act*. Satellites may be considered as private, public, scientific or dual-use.[17] The supporting documents submitted with the application will be reviewed and analyzed by GAC together with other departments or agencies.[18] Once a decision is reached on whether the satellite is acceptable for use in Canada or by Canadians abroad, GAC will verify that the satellite is approved for use under the *Radiocommunication Act.*[19]

A Remote Sensing System consists of three parts:

- **Space Segment** (satellite(s) and sensors)
- **Ground Segment** (ground stations, networks, mission control centre and other facilities used to operate the system, as well as related facilities)
- **Data** (the facilities used to receive, store, process and/or distribute raw data from the satellites)

Preliminary design and critical design review reports for "each type of remote sensing sensor" and "each type of satellite platform of each type of remote sensing satellite" are required by the Minister.[20] These reports are to be provided within 45 days following completion of the design reviews. As well, identifying information details for the satellite are required for registration of the satellite with the United Nations.[21]

For any satellite, four operational tasks may be considered:

1. Launch and Early Operational Phase
2. Ongoing Telemetry, Tracking and Control
3. Data download that is "bent-piped"[22] to a location outside of Canada
4. Data download and/or archiving and/or processing and/or distribution from within Canada

In addition to a general description of the satellite, as described in the *Regulations*, each proposed satellite operation comes with its unique documentation requirements. The information required is outlined in the documents referred to in the following section.

[17] "Dual Use" implies that the satellite can support a military mission and a non-military mission, typically commercial, but could also be scientific.
[18] Other government departments or agencies may be consulted on account of the various considerations taken by the Minister of Foreign Affairs when issuing a provisional approval of a license application, issuing a license, or amending or renewing a license. See Section 8(1) of the *Act*.
[19] Government of Canada, *Radiocommunication Act (R.S.C., 1985, c. R-2)*, 2017, https://laws-lois.justice.gc.ca/eng/acts/r-2/.
[20] RSSS Regulations, Section 20(1).
[21] As per the United Nations Office for Outer Space Affairs, *Convention on Registration of Objects Launched into Outer Space*, 1976, http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introregistration-convention.html.
[22] Bent-Pipe is the direct transfer of a satellite's raw data to a foreign installation without modifying or manipulating the data.

Satellite Registration Reminder

The Government of Canada is required to register all Canadian space objects with the United Nations, including those from industry and academia. Please contact the Canadian Space Agency about registering your satellite as soon as possible to begin the process:

asc.enregistrementobjetsspatiaux-spaceobjectsregistration.csa@canada.ca

5.1 SPACE SEGMENT – KEY INFORMATION AND DOCUMENTS

Data on the remote sensing space system's space segment must be sufficiently detailed to enable GAC to determine whether the proposal meets the requirements of the *Act* and the *Regulations*. A list of all key documents is found in Annex A of this guide.

1. Identification and contact information for the satellite owner/operator (if different from the Applicant)
2. Identification and contact information on the contact person for the satellite owner and/or operator (if different from the Applicant)
3. Preliminary design review and critical design review reports
4. General description of the satellite
5. Satellite technical details
6. Data and Command Protection Plans
7. Encryption Methodology
8. System Disposal Plan (disposal of satellites(s))
9. End-User Licence Agreement, if applicable
10. Copy of the International Communication Union Registration and Radiocommunication Licence

6 THE GROUND SEGMENT FACILITIES

The *Act* governs the ground stations or facilities, from the planning stage to its final disposal. The Applicant is required to submit reports on the preliminary and critical design review for the ground stations and/or facilities "*including its reception, storage, processing, delivery and information assurance subsystems*"[23] for a ground station/facility under construction. GAC further requires:

- A copy of all permits and authorisations obtained from the various authorities (e.g., the Municipal Building Permit and environmental approval);
- Structural design drawings of the facilities; and
- Engineering drawings showing the location of the ground station, the complete perimeter of the lot and the location of external security devices.

[23] RSSS Regulations, Section 20(1)(e).

6.1 PROTECTION PLANS

Two protection plans are required to accompany an application: A Command Protection Plan and a Data Protection Plan. These two plans may be combined into a single document as long as it addresses all the requirements (see Annex B of this guide).

6.1.1 COMMAND PROTECTION PLAN

The detailed components of a Command Protection Plan are listed in the *Regulations*.[24] Items to be reviewed by GAC in respect of a ground station/facility include, but are not limited to: encryption and other protective measures in place that fall under Information Technology, and physical and personnel security for satellite commands.

6.1.2 DATA PROTECTION PLAN

The detailed components of the Data Protection Plan are listed in the *Regulations*.[25] Items to be reviewed by GAC in respect of a ground station/facility include, but are not limited to: encryption and other protective measures in place that fall under Information Technology, physical and personnel security for satellite data reception, and Information Technology infrastructure for data transmission, distribution, processing and archiving.

6.1.3 PHYSICAL SECURITY

Physical security is part of the GAC review of documentation regarding the ground station and/or facility. Physical security describes security measures that are designed to deny unauthorized access to facilities, equipment and resources and to protect personnel and property from damage or harm (such as espionage, theft, or attacks). A list of possible considerations include:

- What is the material used for fencing around the facilities?
- Is there fencing around antennas as required by the *Radiocommunication Act*?[26]
- Do first responders have access to buildings in an emergency?
- Is there an Access Log in place and sign in requirement at the site?

6.1.4 INFORMATION TECHNOLOGY (IT) SECURITY

IT security is a set of cybersecurity strategies that prevents unauthorized access to assets such as computers, networks and data. It maintains the integrity and confidentiality of sensitive information by blocking the access of sophisticated hackers. Types of IT security include network, internet, endpoint, cloud and application securities.[27]

GAC requires that all satellite commands be encrypted to ensure positive control of the satellite(s).[28] The level of encryption is determined by the sensitivity and capability of the remote sensing space systems.

[24] RSSS Regulations, Schedule 1 Sections 14 to 21.
[25] RSSS Regulations, Schedule 1 sections 22 to 29.
[26] Government of Canada, *Radiocommunication Act (R.S.C., 1985, c. R-2)*, 2017, https://laws-lois.justice.gc.ca/eng/acts/r-2/.
[27] CISCO, https://www.cisco.com/c/en_ca/products/security/what-is-it-security.html#~types-of-it-security.
[28] RSSS *Act*, Section 8(5), and RSSS *Regulations*, Section 17(4) of Schedule 1.

6.2 SYSTEM DISPOSAL PLAN

Article I of the *United Nations Liability Convention* defines the term "*launching State*" as:

> "*a State which launches or procures the launching of a space object*" or "*a State from whose territory or facility a space object is launched.*"[29]

The Government of Canada **is liable** for space activities conducted **by Canadian persons** that are involved in launching satellites, whether the activities are conducted **in Canada or involving Canadians abroad**.

Article II of the Convention further states:

> "*A launching State shall be absolutely liable to pay compensation for damage caused by its space object on the surface of the earth or to aircraft flight*."[30]

This means that the Government of Canada is liable for damage on the surface of the earth caused by space activities conducted by Canadians involved in launching satellites, whether the activities are conducted in Canada or involving Canadians abroad.

RSSSA Section 9 (1):

The Minister may not issue a licence without having approved

(a) a system disposal plan for the licensed system satisfactory to the Minister that, among other things, provides for the protection of the environment, public health and the safety of persons and property; and

(b) arrangements satisfactory to the Minister relating to the guarantee of the performance of the licensee's obligations under the system disposal plan.

The disposal plan is a means for the Government to ensure that a Licensee meets these obligations. A System Disposal Plan required under Section 9 of the *Act* must meet the Space Debris Mitigation Guidelines of the UN Committee on the Peaceful Uses of Outer Space.[31] The plan must describe the disposal of the equipment, data, and other relevant components of the licensed system. In the event a ground station/facility ceases to be part of the licensed system, the plan will also describe the procedures to restore the physical site to a state required by environmental laws. Content related to satellite disposal is described in the *Regulations*.[32]

[29] United Nations Office for Outer Space Affairs, *Convention on International Liability for Damage Caused by Space Objects*, 1972, http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/liability-convention.html.
[30] Idem.
[31] United Nations Office for Outer Space Affairs, *Space Debris Mitigation Guidelines of the United Nations Committee on the Peaceful Uses of Outer Space*, 2010, https://www.unoosa.org/res/oosadoc/data/documents/2010/stspace/stspace49_0_html/st_space_49E.pdf.
[32] RSSS *Regulations*, Section 12.

6.3 REGULAR REVIEW BY THE LICENSEE

To ensure that information supplied to GAC is current, the Licensee and its System Participant(s) are required to regularly review[33] the information in the Command Protection Plan, the Data Protection Plan and the System Disposal Plan. Currently, GAC requires this review to be done annually. The Licensee must notify GAC *without delay* of any changes to those plans.

If any changes or amendments are needed for any of the plans (or other documentation), the licensee must inform the Minister without delay.

6.4 GROUND SEGMENT – KEY INFORMATION AND DOCUMENTS

Data on the ground segment of remote sensing space system must be sufficiently detailed to enable GAC to determine whether the proposal meets the requirements of the *Act* and the *Regulations*. A list of key documents is outlined in Annex A of this guide.

1. Ground Station Engineering Drawings
2. Ground Station Structural Drawings
3. Municipal Building Permit
4. Command Protection Plan
5. Data Protection Plan
6. Encryption Methodology
7. Network Plan
8. Equipment List
9. System Disposal Plan
10. End-User Licence Agreement
11. Environmental approval

7 THE DATA

The *Act* places importance on the data, which includes the remote sensing images and related products. As data is considered one of the three components of a remote sensing space system, particular consideration must be placed on the nature of the data, where it is processed (space or ground facility), where it is kept (archived), how it is accessed, and how the end user gains access to it.

Since data is often associated with ground facilities, the required documents and aspects of data are described in the preceding Section 6 of this guide.

7.1 THE DATA – KEY INFORMATION AND DOCUMENTS

Information on the remote sensing space system's images/data must be sufficiently detailed to enable GAC to determine whether the proposal meets the requirements of the *Act* and the *Regulations*. A list of key documents is outlined in Annex A of this guide.

[33] RSSS *Regulations*, Section 12(d).

1. General description of the data, raw data, imaging type, and/or remote sensing products
2. End-User Licence Agreement
3. Data Protection Plan (can be part of a combined Data & Command Protection Plan)
4. Data Disposal Plan (can be combined with a System Disposal Plan)

8 APPLICATION TO THE MINISTER

When the analysis of the application reaches a positive conclusion, a licence is prepared by GAC based on the template described in Annex E of this guide. If the licence contains any exemptions, it must be signed by the Minister as the *Act* stipulates that only the Minister may authorize exemptions to the requirements of the *Act*, as per Section 4(3). The submission to the Minister will provide the rationale for each exemption as recommended by the GAC review. If the licence does not contain exemptions, it may be issued by a person delegated by the Minister.

8.1 PROVISIONAL APPROVAL

While awaiting the approval of the Minister, the Applicant may be granted provisional approval of the application with necessary conditions, but without exemptions, as per Section 8(1)(a) of the *Act*. This allows the Applicant to finalize contracts and operate, provided there is no substantive change in the information previously submitted and on which approval was based, as per Sections 8(2) of the *Act*.

9 AUTHORIZATIONS TO CARRY OUT TESTING OPERATIONS

As per the *Act*, performance of any Controlled Activity requires an authorization.[34] At times, operations to test any component of a remote sensing space system may become necessary. Two examples include:

- testing of new antenna in a ground station by transmitting commands to an operational remote sensing satellite; or
- downlinking of data from an operating satellite to simulate and test.

RSSSA, Section 2

Controlled Activities:

(a) formulating or giving a command;
(b) receiving raw data;
(c) storing, processing or distributing raw data; and
(d) establishing or using
    (i) cryptography in communications
    (ii) information assurance measures

Any testing operation amounting to a Controlled Activity requires prior authorization from GAC, regardless of the limited time duration. Generally, data received and processed in such operations are not authorized for distribution.

[34] RSSS Act, Section 8(4)(b) and Section 8(5)(b).

This Page Intentionally Left Blank

ANNEX A.

SOLICITATION DOCUMENTS LIST

In addition to the **Schedule 1 Application**, as found in the *Regulations*, the following lists additional documents related to the licensing process.

With the *Act* and the *Regulations* covering different aspects of a remote sensing space system, the supporting documentation are required to cover these aspects.

Applicant:

1. Identification and contact information of the Applicant
2. Identification and contact information of the "contact person"
3. Security documents for the contact person, as per Schedule 1 Section 3 of the *Regulations*:
    a. Personnel Screening, Consent and Authorization Form (TBS/SCT 330-23) of the Treasury Board Secretariat
    b. Security Screening Certificate and Briefing Form (TBS/SCT 330-47) of the Treasury Board Secretariat
    c. Security Clearance Form (TBS/SCT 330-60) of the Treasury Board Secretariat
    d. Royal Canadian Mounted Police (RCMP) fingerprint form C216-C

    The Applicant's security officer should obtain these forms from their sources and apply for security clearance from the Public Services and Procurement Canada.
4. **If** the Applicant is an entity, other than a government or government agency:
    a. The entity's financial information is required, which includes:
        i. certified copy of its instrument of incorporation or continuance or its business registration in its jurisdiction of operation, as the case may be;
        ii. the name, identifying information and contact information of the chief executive officer and each of the Applicant's directors, if any;
        iii. the name, identifying information and contact information of each of the Applicant's officers who will be responsible for the operation of the remote sensing space system;
        iv. the name, identifying information and contact information of each owner with an interest equal to or greater than 10% in the Applicant, and the interest held by that owner; and
        v. the name, identifying information and contact information of each person who exercises control over the Applicant.
5. The name, identifying information and contact information of each of the Applicant's secured creditors.
6. The name, identifying information, contact information and amount of indebtedness for every person to whom the Applicant is indebted for more than 5% of the Applicant's total indebtedness.
7. Financial information for each affiliate that is involved in the operation of the system.

System Participants

According to Section 32 of Schedule 1 of the *Regulations*, the System Participants must provide:

1. Identification and contact information for each System Participant
2. Description of Remote Sensing Space System, identifying individual roles played by the Applicant and System Participant(s), particularly relating to the performance of Controlled Activities
3. Security documents on the contact person for each System Participant
4. Names and security information for persons performing Controlled Activities
5. Final draft and/or signed copy of the System Participant Agreement, attaching other required documents.[1]
6. Depending on the role of the System Participant(s):
    i. System Disposal Plan
    ii. Command Protection Plan
    iii. Data Protection Plan
7. Any related documentation on the three components of a remote sensing space system for which the System Participant contributes

***Space Segment* – Satellite(s):**

1. Identification and contact information on the satellite owner/operator (if different from the Applicant)
2. Identification and contact information on the contact person for the satellite owner and/or operator (if different from the Applicant)
3. Preliminary design review and critical design review reports
4. Common description of the satellite
5. Satellite & sensor technical details
6. Data and Command Protection Plan
7. Encryption Methodology
8. Satellite Disposal Plan (can be combined with a System Disposal Plan)
9. End-User Licence Agreement (if different than for the data component)
10. Copy of International Communication Union Registration and Radiocommunication Licence

***Ground Segment* – Ground Station(s)/Facility(ies):**

1. Ground Station Engineering Drawings
2. Ground Station Structural Drawings[2]
3. Municipal Building Permit

[1] Other documents that can be part of the System Participant Agreement includes such documents as: (i) General Site Description, (ii) individual or consolidated Data and Command Protection Plans, and (iii) System Disposal Plans, as they relate to the operations of the System Participant, where the same has not been presented elsewhere by the Applicant.
[2] These drawings (at 1 and 2) must show the location of the ground station, the complete perimeter of the area and the location of external security devices.

4. Command Protection Plan
5. Data Protection Plan
6. Encryption Methodology
7. Network Plan
8. Ground Station Equipment List
9. Ground Segment Disposal Plan (can be combined with a System Disposal Plan)
10. End-User Licence Agreement (if different than for the data component)
11. Environmental approval
12. Canadian Radio-Television and Telecommunications Commission Licence (if applicable)

Data:

1. Common description of the data and/or raw data and/or imaging type and/or remote sensing products
2. End-User Licence Agreement
3. Data Protection Plan
4. Data Disposal Plan (can be combined with a System Disposal Plan)

This Page Intentionally Left Blank

ANNEX B.

PROTECTION PLANS

1. OVERVIEW:

Schedule 1 of the *Regulations* lists the required information pertaining to a "Command Protection Plan" (Sections 14 through 21), and a "Data Protection Plan" (Sections 22 through 29). The information required is similar for telecommands transmitted up to the satellites via the ground stations and for the data relayed by the satellite(s) downward to the ground station for further processing and distribution. Depending on the complexity of the mission, these two plans may be combined and submitted as one single document: "Command and Data Protection Plan" (Section 30).

These plans should provide information addressing the following elements:

- Physical Security
- Personnel Security and
- Information Technology (IT) Security.

This document identifies baseline protection measures and specific measures for each security aspect that will be undertaken to mitigate the assessed risks that a Licensee or System Participant may face. Certain operations may encounter different risks because of their nature, their location and the appeal of their assets. Examples include facilities dealing with classified operations, facilities located in high-crime areas, and overseas facilities.

The Licensee and System Participant(s) are responsible for selecting, implementing, monitoring, and maintaining sustainable security controls to achieve security control objectives. Security controls may be administrative, managerial, operational, technical or procedural. If required, additional security controls may be stipulated by GAC as conditions within the licence to reflect the sensitivity of the mission.

2. GENERAL PROTECTION MEASURES:

2.1 Security awareness

The plan(s) should elaborate how a security awareness program covering all aspects of security is established, managed, delivered and maintained. Issues or questions to consider include:

- How are relevant individuals kept informed of security issues and concerns related to their security responsibilities?
- How do they comply with their security responsibilities in order not to inadvertently compromise security?

2.2 Security training

The plan(s) should elaborate how security training is covered. Issues or questions to consider:

- What type of specific training do individuals with security responsibilities receive to ensure they have the necessary knowledge and competencies to effectively perform their role and avoid inadvertently compromising security?
- How are these security based training obtained and made available to the staff?

2.3 Security incident management

The plan(s) should elaborate on the security incident management. Issues or questions to consider:

- What measures are taken to ensure preparedness and timely mitigation, response to, or recovery from security incidents and prevent or minimize effects and potential losses?
- How are incidents that affect or have the potential to affect mitigation, response or recovery from threats and vulnerabilities identified and reported to the law enforcement authorities?
- How are post-incident analysis and follow-up conducted?

2.4 Security inspections

The plan(s) should elaborate on how security inspections are conducted. Issues or questions to consider:

- How are routine inspections conducted of sites or systems where sensitive information and assets are processed or stored to ensure compliance with security requirements and regulatory frameworks (e.g., monitoring office areas during limited-access hours)?
- Are security inspections conducted by assigned persons with adequate training to do the job? How are such inspections made known to employees in advance of being performed?
- How would suspected violations or breaches of security be reported without delay and investigated to inform remedial action or reporting to the responsible authorities, as appropriate?

2.5 Security in emergency and increased threat situations

The plan(s) should elaborate on the management of security in emergency and increased risk scenarios. Issues or questions to consider:

- What plans and procedures are in place to move to heightened security levels in case of emergency and increased risk?
- What coordination exists with other emergency prevention and response plans (e.g., fire, bomb threats, hazardous materials, power failures, evacuations or civil emergencies) in the event of an emergency or increased risk?

2.6 Emergency and business continuity planning

The plan(s) should elaborate on the emergency and business continuity planning. Issues or questions to consider:

- What plans for business continuity and contingencies exist to support the recovery and restoration of critical business services and functions and their associated assets and resources for uninterrupted minimum service delivery?

- How are services and assets analyzed, identified and prioritized in terms of criticality?
- How are business continuity plans tested and readiness exercises conducted to ensure efficient and effective response and recovery?

3. SPECIFIC PROTECTION MEASURES:

3.1 Physical Security:

The plan(s) must elaborate on how the following aspects are managed within an operational environment.

- How are information, assets and facilities protected from unauthorized access, disclosure, modification, or destruction, in accordance with their level of sensitivity, criticality and value?
- How is access to licensed assets and facilities limited to authorized individuals who have been security-screened at the appropriate level and who have a legitimate need for access?
- How are custodian-tenant relationships defined to ensure that shared and individual responsibilities are clearly addressed to achieve optimum security outcomes?
- How are security considerations fully integrated into the process of planning, selecting, designing, modifying, building, implementing, operating and maintaining all the facilities and equipment that form part of the Remote Sensing Space System for which a licence is sought?
- How are external and internal environments of each facility managed to create conditions that, together with specific physical security controls: reduce the risk of security-related incidents, protect against unauthorized access, detect attempted or actual unauthorized access and activate an effective response?
- What processes and procedures are implemented for the transport, transmittal or destruction of information and assets?

The following is a list of physical security features that can be elaborated, as appropriate, in the document:

- Identity authentication
- Guards and patrols
- Locksets and hardware for doors and windows – e.g., mechanical locksets for doors and windows in buildings and management of security keys
- Closed-circuit television suite
- Intruder alarm systems suite, which includes:
    - Design, installation, commissioning and maintenance
    - Monitoring centres
    - Detection devices for internal use
    - Alarm transmission systems
- Chain-link fabric security fencing and gates
- Electrical installations (e.g., electric security fences)
- Safes and strongrooms
- Building elements, such as testing and rating for intruder resistance – e.g., intruder-resistant panels
- Mailroom security

- Secure storage units (e.g., requirements, classifications and methods of testing for resistance to burglary)
- Fences (e.g., specifications of steel palisade fences)
- Building hardware such as controlled door closing devices and requirements and test methods (e.g., thickness of materials and resistance to hammers, fire and firearms)

3.2 Personnel Security

Adequate personnel security measures facilitate the effective utilization of resources and are an essential mitigation tool to address a potential insider threat. Possession of the appropriate level of security clearance issued by Public Services and Procurement Canada[1] is required for the key person within the Applicant organization in whose name the licence will be issued, and all other personnel (employees and contractors) who will have access to the licensed facilities. In specific cases, equivalencies may be considered for representatives from foreign organizations, based on the rigour of the process adopted by such organizations at the time of recruitment and selection of their employees.

To achieve desired personnel security outcomes, three personnel security core methods are usually implemented to ensure employees and contractors are authorized to access the licensed facilities throughout all stages of their engagement with the licensed entity. These methods ensure personnel demonstrate integrity and honesty, specifically by, for instance:

- conducting relevant checks before gaining access to resources (e.g., verification of identity, confirmation of security clearance status, background check, reference checks, digital footprint check, police records check, financial history check, security interview and psychological assessment);
- managing their ongoing suitability to access resources throughout their engagement; and
- having processes in place to ensure continued protection of resources after personnel leave the licensed entity.

Some of the aspects that should be addressed in detail are as follows:

- How do personnel requiring access to information, assets or facilities undergo an examination of their trustworthiness, loyalty and reliability prior to being granted access to such information, assets or sites?
- What is the protocol through which individuals are formally briefed on access privileges and prohibitions attached to their screening level before the commencement of their duties?
- What is the process for periodic updates of existing clearances and whenever a change occurs in their screening level?
- Are such individuals required to sign appropriate briefing forms?
- How are security screenings conducted in a manner that meets Government of Canada standards?[2] For example, consider the following criteria:
    - review of documentation
    - verification of identity
    - verification of antecedents

[1] Public Services and Procurement Canada website: https://www.tpsgc-pwgsc.gc.ca/esc-src/personnel/information-eng.html.
[2] Additional information on Public Services and Procurement Canada website: https://www.tpsgc-pwgsc.gc.ca/esc-src/personnel/information-eng.html.

- verification of educational and professional credentials
- personal and professional reference check
- credit and financial check
- law enforcement and criminal background check through fingerprinting
- open source check in respect of personnel or company profile
- suitability interview

3.3 Information Assurance

The plan(s) should elaborate on the approach and techniques used to guarantee information assurance. Issues or questions to consider include:

- How is sensitive information protected from unauthorized access, use, disclosure, modification, disposal, transmission, or destruction?
- What is the protocol for identifying and categorizing information based on the degree of injury that could be expected to result from the compromise of its confidentiality, availability, or integrity?
- How is access to classified and protected information limited to authorized individuals who have been security-screened at the appropriate level and who have an express need for access?
- How are modification and destruction of information limited to authorized individuals?
- How are the appropriate security measures for accessing, storing, transmitting and disposing of information conducted?
- How is the security of information addressed through all phases of its life cycle or the life cycle of the information system to ensure security requirements are identified early, security controls are reviewed, management authorization is provided before operation and authorization is maintained through continuous monitoring of the security status?

3.4 Information Technology (IT) Security

This section of the Protection Plan describes how the Applicant can safeguard IT systems to support the secure and continuous conduct of business. Secure IT systems protect the integrity and facilitate the availability of the information that entities process, store and communicate.

Detailed answers to the following questions will help develop this portion of the document.

- How are IT security considerations fully integrated to meet business objectives at each stage of the IT system's life cycle, including definition, design, development, operations, maintenance and decommissioning?
- What is the procedure for identifying and authenticating users before granting access to IT systems?
- How is access to electronic information and IT systems limited to authorized users, including the types of transactions and functions that authorized users are permitted to exercise, based on business and security requirements?
- What procedures are implemented to continuously assure confidence in the security of IT systems, such as the following:
    - assessment of security controls;
    - reduction or elimination of deficiencies;

  - authorization before operation; and
  - maintenance of authorization.
- What procedures are implemented to continuously maintain the IT security posture, such as monitoring threats and vulnerabilities; detecting malicious activity and unauthorized access; and taking both pre-emptive and response actions to minimize effects?
- How are IT system audit logs and records created, protected, and retained to enable monitoring, analysis and investigation so that users are held accountable for their actions?
- How is data on all portable electronic media and devices protected and sanitized or destroyed before disposal or reuse of the equipment?
- What steps are in place to protect electronic communications such as network security zones and perimeter defence at network boundaries?
- How are computer systems and networks protected from theft or damage to their hardware, software or electronic data, as well as from the disruption or misdirection of the services they provide?

While endeavouring to answer these IT security questions, the following aspects may also be addressed in the Plan, as appropriate.

Security issue	Matters for consideration
Information security documentation	Preparing relevant documentation supports implementation of planned security measures.
Information security monitoring	Vulnerability management includes monitoring and managing vulnerabilities in, and changes to, a system that can provide valuable information about exposure to threats. Change management includes implementing routine and urgent changes to software or systems to maintain security (including if the change triggers the need for re-accreditation).
Communications security	Infrastructure security includes good cable management and emanations security regimes that help entities maintain the integrity and availability of communications infrastructure, in addition to the confidentially of information: a. Cable management practices can protect information from deliberate or inadvertent access. b. Countermeasures reduce the risk of information being intercepted and systems compromised. Systems and devices security includes measures that minimise data spills or unauthorised disclosure of information as data flows in and out of digital gateways.
Product security	Entities need assurance that products with a security function perform as claimed by the vendor and provide the necessary security to mitigate security threats. Assurance is achieved through formal and impartial evaluation.
Media security	Implementing sound security practices when connecting, storing, transferring, sanitising, destroying or disposing of media plays a major role in preventing classified or sensitive data spills and avoiding malicious attacks. Media security is critical when decommissioning an IT system.

Security issue	Matters for consideration
Software security	It is important to implement and maintain measures to protect against software vulnerabilities that may be used to undermine the integrity or availability of systems or information.
Access control	Well-structured and robust IT systems allow necessary access for personnel to undertake their work, while protecting information, technology and intellectual property.
Administrator rights	Restricting administrative privileges is one of the most effective ways to safeguard IT systems.
Network security	Network management practices and procedures assist in identifying and addressing network structure or configuration vulnerabilities.
Cryptography	Cryptography is primarily used to restrict access to information to authorised users. It provides confidentiality, integrity, authentication and non-repudiation of information. Encryption protects the confidentiality of data by making it unreadable to unauthorised users.
Cross-domain security	Mitigating risks by securely managing data flows between different domains includes: a. deploying and configuring gateways to manage information flow paths (ingress and egress of traffic) across approved systems on entity networks; b. implementing gateway firewalls to protect against intrusions, particularly for sensitive networks; c. using diodes to protect against data spills and malicious actors seeking to use information flow paths to intrude or attack information; d. allowing web access while protecting against the execution and spread of malicious software; and e. prohibiting the sharing of peripherals between IT components and ensuring unauthorised information does not pass between security domains.
Data transfers and content filtering	These pertain to implementation of procedures to ensure that content leaves a security domain in a secure manner. It also includes application of content-filtering techniques to reduce the risk of unauthorised or malicious content crossing a security boundary.
Cyber threat mitigation	Usual measures include: application control, patching applications, restricting administrative privileges, patching operating systems, user application hardening, multi-factor authentication and daily backups.

3.5 Security in Contracting

The plan(s) should elaborate on the security implemented for the contracted support utilised for the remote sensing space system. Issues or questions to consider:

- How are security requirements identified, addressed, formally documented, implemented, and monitored in all phases of the procurement and throughout the life cycle of the contract?
- How do information, assets, systems and facilities meet the industrial security requirements (where applicable) and integrate an appropriate level of protection throughout their life cycle?

This Page Intentionally Left Blank

ANNEX C.

GUIDELINES ON THE APPLICATION

This annex provides guidelines and clarifications on the information and documents required under the *Regulations'* Schedule – 1 to support an Application form.

This form is intended for system capable of producing high-grade remote sensing data.

All sections of the application form need to be completed (when it is applicable to your system) that is, if the system is capable of producing high grade remote sensing data according to the Eligibility Threshold Table (refer to Annex D for more details).

Schedule-1 Overview: The table below lists the main topics with their associated sections.

Clarifications on the Schedule 1 application: The table below provides clarifications on the information required under Schedule-1 for a submission under the Application Process.[1]

SECTION	PROVISIONS	RECOMMENDATIONS
BUSINESS INFORMATION AND DOCUMENTS		
1	The Applicant's name, identifying information and contact information.	Applicant: RSSSA Project Sponsor: Project Leader: **Name, Position, Organization, Address, email, contact number(s)**
2	The name, identifying information and contact information of the individual proposed to be the contact person for the Applicant.	Point of Contact: **Name, Position, Organization, Address, email, contact number(s)** Emergency contact (should the regular contact person be unavailable): **Name, Position, Organization, Address, email, contact number(s)**
3	The following completed forms for the individual proposed to be the Applicant's contact person.	Note: For all remote sensing space systems, at minimum, a security clearance of "Reliability Status," or equivalentis required. Some highly sensitive systems may require a higher security clearance, such as "secret" or other. The security clearance is required for the application's PoC, and the organisation's staff members that have access to controlled areas. Global Affairs Canada (GAC) recognizes security clearances under the Canada's Control Goods Program (CGP). In lieu of submitting the documents at Section 3(a) through (d), applicants can submit their CGP documentation. Applicant's contact person: **Name, Position, Organization, Address, email, contact number(s)**

[1] A Word version of this annex (and the application) can be requested at: RSSSA-LSTS@international.gc.ca.

SECTION	PROVISIONS	RECOMMENDATIONS
		***Documentation covering the listed security clearance(s) needs to be provided as part of the application information** List of clearances: Personnel ID: NATO Secret – Expiry date Secret –Expiry date Top Secret –Expiry date Please note that GAC is not responsible for the forms listed in Section 3(a) through 3(d). The Applicant's security officer should contact relevant government entities for these forms (see below), or even contact Public Services and Procurement Canada[2] for information on obtaining required security clearance.
a)	Personnel Screening, Consent and Authorization Form (TBS/SCT 330-23) of the Treasury Board Secretariat, as amended from time to time;	Form (TBS/SCT 330-23) can be found at : http://www.tbs-sct.gc.ca/tbsf-fsct/330-23-nf-eng.pdf If the security clearance of Reliability is processed through GAC, only the form in Section 3(a) is required, with two (2) copies of a picture ID.
b)	Security Screening Certificate and Briefing Form (TBS/SCT 330-47) of the Treasury Board Secretariat, as amended from time to time;	Form (TBS/SCT 330-47) can be found at: http://www.tbs-sct.gc.ca/tbsf-fsct/330-47-nf.pdf
c)	Security Clearance Form (TBS/SCT 330-60) of the Treasury Board Secretariat, as amended from time to time; and	Form (TBS/SCT 330-60) can be found at: http://www.tbs-sct.gc.ca/tbsf-fsct/330-60-nf-eng.pdf
d)	Royal Canadian Mounted Police fingerprint form C216-C, as amended from time to time.	Form can be downloaded at: https://www.fingerscan.ca/download/ This may be required if a security clearance is processed by GAC Corporate Security.

[2] Public Services and Procurement Canada website: https://www.tpsgc-pwgsc.gc.ca/esc-src/personnel/information-eng.html.

SECTION	PROVISIONS	RECOMMENDATIONS
4	If the Applicant is an entity, other than a government or government agency,	
a)	a certified copy of its instrument of incorporation or continuance or its business registration in its jurisdiction of operation, as the case may be;	Organization incorporation documents need to be provided
b)	the name, identifying information and contact information of the chief executive officer and each of the Applicant's directors, if any;	CEO/other positions: **Name, email, contact number(s)** Applicant's Board of Directors: **Names, positions and their organizations**
c)	the name, identifying information, and contact information of each of the Applicant's officers who will be responsible for the operation of the remote sensing space system;	Names, positions, email, and contact number(s) of each. Note: Applicant's officers may require a Reliability Status if they have access to Controlled Areas.
d)	the name, identifying information and contact information of each owner of an interest equal to or greater than 10% in the Applicant, and the interest held by that owner; and	List of each owner who has an interest equal to or greater than 10% in the APPLICANT (NOT the remote sensing space system), the interest held by that owner and the owner's full contact information.
e)	the name, identifying information and contact information of each person who exercises control over the Applicant.	
5	The name, identifying information, and contact information of each of the Applicant's secured creditors.	List of full contact information of each of the APPLICANT's (NOT the remote sensing space system) secured creditors.
6	The name, identifying information, contact information and amount of indebtedness for every person to whom the Applicant is indebted for more than 5% of the Applicant's total indebtedness.	Names, positions, email, and contact number(s) of each. Note: Each of these persons may require a Reliability Status if they have access to Controlled Areas.
7	The Applicant's plans for communicating raw data or providing remote sensing products, including:	

SECTION	PROVISIONS	RECOMMENDATIONS
a)	making the data or products available to governments whose territories have been sensed by the remote sensing space system; and	This section seeks confirmation that the data can be made available (sold or given) to a sensed State requesting access to the data. The *Act* implements Canada's adoption of the principle explained below: Principles Relating to Remote Sensing of the Earth from Outer Space – PRINCIPLE XII:[3] As soon as the primary data and the processed data concerning the territory under its jurisdiction are produced, the sensed State shall have access to them on a non-discriminatory basis and on reasonable cost terms. The sensed State shall also have access to the available analyzed information concerning the territory under its jurisdiction in the possession of any State participating in remote sensing activities. This access shall be on the same basis and terms, taking particularly into account the needs and interests of the developing countries. Applicants under the *Act* are required to provide information on how it plans to fulfill Principle XII.[4] For the purposes of the UN remote sensing principle XII, the term "remote sensing" only refers to remote sensing for the purpose of improving natural resources management, land use and the protection of the environment. (*Principal 1(a)*)
b)	providing preferred or exclusive access to the data or products.	If "yes", provide a list of preferred or exclusive customers. Otherwise, describe the general type of clients given access to the data or products.
8	The address where the Applicant's records will be maintained.	Name of organization, address, email and contact number(s) of the Applicant's contact person

[3] United Nations Office for Outer Space Affairs: Resolution Adopted by the General Assembly 41/65. Principles Relating to Remote Sensing of the Earth from Outer Space, https://www.unoosa.org/oosa/en/ourwork/spacelaw/principles/remote-sensing-principles.html.
[4] United Nations Office for Outer Space Affairs: Resolution Adopted by the General Assembly 41/65. Principles Relating to Remote Sensing of the Earth from Outer Space, https://www.unoosa.org/oosa/en/ourwork/spacelaw/principles/remote-sensing-principles.html.

SECTION	PROVISIONS	RECOMMENDATIONS
GENERAL SYSTEM INFORMATION		The *Act* defines a ***remote sensing space system*** as **(a)** one or more remote sensing satellites and the mission control centre and other facilities used to operate the satellites; and **(b)** the facilities used to receive, store, process or distribute raw data from the satellites, even after the satellites themselves are no longer in operation. Information provided under this section should include all components of a system: space segment, ground segment, and data.
9	The name and a short description of the remote sensing space system, including the number of remote sensing satellites of the system, the planned date that each satellite will become operational and the anticipated mission life of each satellite.	Name of the system/mission(s): Name as notified to the International Communication Union (ITU): ITU identifier: Description: Type of satellite(s): Purpose: Type of instrument(s): Launch date(s): Operated by (if different from the Applicant): Semi-Major Axis: Eccentricity: Downlink of Imagery:
10	The proposed launch date, vehicle and site.	As launch date(s) often change throughout the application process, this section needs to be updated whenever there are changes to date(s).
ORBIT INFORMATION		
11	The nominal orbit and tolerances of each remote sensing satellite of the remote sensing space system, including:	
a)	the semi-major axis, eccentricity, inclination, longitude of right ascension, argument of periapsis, argument of mean anomaly and epoch;	**Name of the satellite(s):** Orbit height: Semi-Major Axis:

SECTION	PROVISIONS	RECOMMENDATIONS
b)	the period, repeat cycle and any sub-cycle; and	Eccentricity: Inclination: Longitude of Right Ascension: Argument of Perigee: True Anomaly: Perigee with Mean EER: Apogee with Mean EER: Period: Epoch:
c)	the equator crossing time of the ascending node of any sun-synchronous orbit.	
REMOTE SENSING SATELLITE DISPOSAL		Estimated duration of the satellite disposal operation: Nominal orbital height: Local Time Ascending Node (LTAN): Spacecraft mass: Drag Area: m2 Solar Pressure Area: m2 Solar Flux: Period: Time for orbit perigee to reach 100km: Notes: GAC will also require a Ground Segment disposal plan and a Data disposal plan. At a minimum, the Applicant must describe the long-term plans of the Ground Segment and the Data. Refer to Sections 17 and 18 of the *Regulations* for specifics on data disposal.
12	The potential hazard from space debris and the strategy to mitigate that hazard for each remote sensing satellite of the remote sensing space system, including:	GAC recommends using NASA's Debris Assessment Software (DAS) in order to obtain information required in Section 12.
a)	the method of disposal that is proposed for each satellite and the reliability of that method;	For example: propulsion, natural decay, other.
b)	the estimated duration of the satellite disposal operation;	

SECTION	PROVISIONS	RECOMMENDATIONS
c)	the probability of loss of human life and how it was calculated;	
d)	the amount of debris expected to reach the surface of the Earth, the size of the impact area expressed in square metres, and how they were calculated;	
e)	the geographic boundaries of the likely debris re-entry impact area, the confidence level of the determination of the boundaries and how the boundaries and confidence level were calculated;	
f)	the identity and quantity of hazardous material and dangerous goods contained in each satellite at the end of its mission life, the quantity expected to reach the surface of the Earth on re-entry and how the quantities were calculated;	
g)	the orbital elements and epochs of the proposed disposal orbits for each satellite; and	
h)	an assessment of space debris expected to be released from each satellite during normal operations by explosions, by intentional break-ups and by on-orbit collisions, and the measures proposed to mitigate the production of space debris.	
REMOTE SENSING SATELLITE INFORMATION AND DOCUMENTS		
13	A technical description of each remote sensing satellite of the remote sensing space system, including:	
a)	a drawing of the satellite in its on-orbit configuration;	
b)	its command and data handling subsystem capabilities, including its data storage technology and capacity, data transfer rate, method of access to	For Commands and Data: • Telemetry, Tracking and Control (TT&C) Uplink: GHz, variable from kbps to Mbps

SECTION	PROVISIONS	RECOMMENDATIONS
	stored data and directionality of its command, telemetry and downlink antennas;	• TT&C Downlink: GHz, variable from kbps to Mbps • TT&C Footprint: Minimum elevation angle, which corresponds to a coverage footprint radius of km around the sub-satellite point • Inter-satellite crosslinks planned for the satellites referenced in the application. On-board storage capacity: xxx MBytes or GBytes
c)	its navigation, guidance and control capabilities, including the accuracy of position, velocity, acceleration and time, and the type of technology used for those capabilities;	
d)	its attitude control subsystem capabilities, including the jerk and jitter, and the type of technology used for those capabilities;	
e)	its propulsion subsystem capabilities, including the amount of propellant allocated for the disposal of the satellite;	Indicate the type of propulsion engine, the volume of propellant, the amount of propulsion allocated for station keeping and disposal, and an estimated value of total ΔV.
f)	its sensor technology for each sensor, including:	Provide technical details on the sensor(s).
i)	the sensor modes,	
(ii)	the spatial resolution capability of each sensor mode, and how it was calculated,	List of spatial resolution for each sensor mode at azimuth and the calculation of the spatial resolution.
(iii)	the centre frequency or wavelength, bandwidth and sweep, if any, of the transmitted and received spectral bands used in each sensor mode indicating which sensor modes are co-registered by common sensor elements and which sensor modes are independent,	List for each mode.
(iv)	the polarization of transmitted and received signals with respect to each sensor mode,	
(v)	the fields of view or beam widths for each sensor mode,	

SECTION	PROVISIONS	RECOMMENDATIONS
(vi)	for each sensor mode, the range of viewing angles or angles of incidence, and their increments of change,	This is a Synthetic Aperture Radar(SAR) Mission-specific requirement.
(vii)	for each sensor mode, the slew and squint angles and their rates of change, and a description of the scan mechanisms employed,	List for each mode. This is a SAR Mission-specific requirement.
(viii)	the ground distance from nadir and the instantaneous swath width and potential swath width for each sensor mode,	
(ix)	the image motion compensation parameters, including those for linear motion and drift,	This is a SAR Mission-specific requirement.
(x)	if applicable, the characteristics of the time-delayed integration mode used within the sensor focal plane,	
(xi)	spatial, spectral and temporal oversampling, aggregation and resampling capabilities,	This is a SAR Mission-specific requirement.
(xii)	sensitivity, including noise-equivalent-spectral-radiance for electro-optic sensors, noise-equivalent-sigmas for synthetic aperture radar sensors and noise-equivalent-temperature-differences for thermal infrared sensors,	This is a SAR Mission-specific requirement.
(xiii)	for each sensor mode, the signal-to-noise ratio, dynamic range and quantization,	This is a SAR Mission-specific requirement.
(xiv)	if applicable, the range of solar illumination angles on the surface of the Earth over which the sensor can operate,	
(xv)	the absolute and relative geolocation accuracy of the raw data and remote sensing products and how they were calculated, and	This is a SAR Mission-specific requirement.
(xvi)	calibration methods, including absolute calibration accuracy; and	

SECTION	PROVISIONS	RECOMMENDATIONS
g)	the minimum time in hours between the acquisition of raw data by the satellite and the communication of the data, or the provision of remote sensing products to a recipient.	
COMMAND PROTECTION PLAN		Additional clarifications are presented in **Annex B** of this Guide, which covers requirements on physical security, personnel security, and Information Technology (IT) security (includes cybersecurity). Note regarding Sales Orders: Information regarding the Sales Orders within this section (section 14 through 21) are only required if they drive or serve as the basis for the Commands to a satellite.
14	The general strategy with respect to command protection.	
15	The location and function of all facilities, including mobile facilities, to be used to process sales orders or to give commands in the operation of the remote sensing space system.	
16	A general description and block diagram of all facilities to be used to process sales orders or to give commands, including the longitude and latitude and station mask of each telemetry, tracking and command station.	
17 1	A general description and block diagram of the communication architecture that includes descriptions of:	Provide as much detail as possible on the IT, physical, and personnel security measures in place for every component of a system: space segment, ground segment and data.
a)	each system supporting the facilities that are to be used to process sales orders or to give commands to the remote sensing satellite;	

SECTION	PROVISIONS	RECOMMENDATIONS
b)	links between the facilities and the satellite;	
c)	links for relaying sales orders or satellite commands between facilities on the ground; and	
d)	crosslinks between satellites.	
2	The radio-frequency link information for command uplinks, including the characterization of each link and the type of information carried by each communication channel.	
3	The protocols to be used in the communication architecture.	
4	A description of the encryption to be used on all communication channels, including keying and rekeying schemes.	
5	Management plans for the keys to be used in satellite uplinks, in command relays and in facilities for command generation and the processing of sales orders.	
18	A general description of:	
a)	the content and format of the proposed sales orders and the commands to be given in the operation of the remote sensing space system; and	
b)	the process used to determine the commands given to the remote sensing satellite that sets out the priority of conflicting sales orders requiring the same resources of the satellite.	Also known as the deconflicting process.
19	A diagram that:	
a)	shows each step to be taken by the Applicant or proposed System Participant from the placement of a sales order for raw data or a remote sensing product to the communication of the raw data to a	

SECTION	PROVISIONS	RECOMMENDATIONS
	recipient or the provision of the remote sensing product to a recipient; and	
b)	indicates the command protection measures proposed for each step.	
20	A description of the command protection measures proposed for each step of the business process, including:	
a)	the measures proposed for each facility to be used to process sales orders or to give commands to the remote sensing satellite, including measures relating to:	
(i)	the security screening of personnel,	
(ii)	the physical security of the facility, and	The facilities mean all Applicant facilities involved in the operation of the system, and not the facilities of System Participant(s). Information on System Participant(s)' facilities is required in the System Participant section below under Section 32. If the Applicant has a document providing general physical security description/requirements for its facilities, such a document could be considered sufficient after GAC reviews it.
(iii)	the information assurance, within the facility, of sales orders and satellite commands;	
b)	the measures proposed for the communication of sales orders and satellite commands between the facilities of the remote sensing space system, including measures relating to physical and electronic protection and information assurance; and	
c)	the measures proposed for the communication of commands to remote sensing satellites, including measures relating to electronic protection and information assurance.	

SECTION	PROVISIONS	RECOMMENDATIONS
21	Proposed measures to comply with:	
a)	the conditions in paragraphs 8(4)(a) to (f) of the Act;	Description on how the Licensee maintains control over their segment of the remote sensing space system at all times, does not permit another person to conduct a controlled activity except in accordance with the license, that raw data and remote sensing products be made available to the government of that country, that control is kept over raw data and remote sensing products until disposal, that raw data only be communicated to the sensed country, or system participant(s).
b)	an order that may be made under section 14 or 15 of the Act; and	Priority Access Order does not only apply to the satellites of the system; it applies to any or all parts of the system, and it is not subject to any contractual agreements. An order made under this section may take effect immediately on notice to the Licensee, but the minister making the order shall give to the Licensee an opportunity — during a period of 15 days after the notice or any longer period that the minister specifies — to make representations regarding it Sections 14 and 15 of the *Act* are reproduced below:
		Interruptions of Service **Minister's order** **14 (1)** The Minister may make an order requiring a Licensee to interrupt or restrict, for the period specified in the order, any operation, including the provision of any service, of the licensed system if the Minister believes on reasonable grounds that the continuation of that operation would be injurious to Canada's conduct of international relations or inconsistent with Canada's international obligations. **Order of Minister of National Defence** **(2)** The Minister of National Defence may make an order requiring a Licensee to interrupt or restrict, for the period specified in the order, any operation, including the provision of any service, of the licensed system if the Minister of National Defence believes on reasonable grounds that the continuation of that operation would be injurious to the defence of Canada or the safety of Canadian Armed Forces.

SECTION	PROVISIONS	RECOMMENDATIONS
		Non-application of *Statutory Instruments Act* **(3)** The *Statutory Instruments Act*[5] does not apply to an order made under this section. **Non-disclosure direction** **(4)** If the minister making an order under subsection (1) or (2) is satisfied that the substance of the order ought not to be disclosed for the same reasons as those on which the order is founded, that minister may include in the order a direction that no person shall disclose its substance to any other person except as required by law or as necessary to give it effect. **Notice and opportunity to make representations** **(5)** An order made under this section may take effect immediately on notice to the Licensee, but the minister making the order shall give to the Licensee an opportunity — during a period of 15 days after the notice or any longer period that the minister specifies — to make representations regarding it.
		Priority Access **Minister's order for priority access** **15 (1)** The Minister may make an order requiring a Licensee to provide to Her Majesty in right of Canada any service through the licensed system that the Minister believes on reasonable grounds is desirable for the conduct of international relations or the performance of Canada's international obligations. **Order of Minister of National Defence** **(2)** The Minister of National Defence may make an order requiring a Licensee to provide to Her Majesty in right of Canada any service through the licensed system that that minister believes on reasonable grounds is desirable for the defence of Canada or the safety of Canadian Armed Forces. **Order of Minister of Public Safety and Emergency Preparedness** **(3)** The Minister of Public Safety and Emergency Preparedness may make an order requiring a Licensee to provide any service through the licensed system **(a)** to the Royal Canadian Mounted Police that that minister believes on reasonable grounds is desirable for the fulfilment of its members' responsibilities under subsection 6(1) of the *Security Offences Act*;[6]

[5] Statutory Instrument Act, https://laws-lois.justice.gc.ca/eng/acts/S-22/.
[6] Security Offences Act, https://laws-lois.justice.gc.ca/eng/acts/S-7/.

SECTION	PROVISIONS	RECOMMENDATIONS
		(b) to the Canadian Security Intelligence Service that that minister believes on reasonable grounds is desirable for the fulfilment of its duties and functions under the *Canadian Security Intelligence Service Act*;[7] or **(c)** to Her Majesty in right of Canada that that minister believes on reasonable grounds is desirable for critical infrastructure protection or emergency preparedness. **Details of orders** **(4)** An order made under this section must specify the period during which the service is to be provided and may specify how and with what priority it is to be provided. **Non-application of *Statutory Instruments Act*** **(5)** The *Statutory Instruments Act*[8] does not apply to an order made under this section. **Non-disclosure direction** **(6)** If the minister making an order is satisfied that the substance of the order ought not to be disclosed for the same reasons as those on which the order is founded, that minister may include in the order a direction that no person shall disclose its substance to any other person except as required by law or as necessary to give it effect. **Notice and opportunity to make representations** **(7)** An order made under this section may take effect immediately on notice to the Licensee, but the minister making the order shall give to the Licensee an opportunity — during a period of 15 days after the notice or any longer period that the minister specifies — to make representations regarding it.
c)	section 16 of the Act	Section 16 of the *Act* is reproduced below: **TRANSFER OF REMOTE SENSING SATELLITES** **Prohibition on transfer of control** **16 (1)** No Licensee or former Licensee shall permit a command to a remote sensing satellite of the remote sensing space system for which the licence was

[7] Canadian Security Intelligence Service Act, https://laws-lois.justice.gc.ca/eng/acts/C-23/.
[8] Statutory Instrument Act, https://laws-lois.justice.gc.ca/eng/acts/S-22/.

SECTION	PROVISIONS	RECOMMENDATIONS
		issued to be given from outside Canada or by any other person unless the Licensee or former Licensee **(a)** can override the command from Canada; or **(b)** has obtained the approval of the Minister. **Factors for approval** **(2)** In deciding whether to give an approval, the Minister shall have regard to national security, the defence of Canada, the safety of Canadian Armed Forces, Canada's conduct of international relations, Canada's international obligations, and any prescribed factors.
DATA PROTECTION PLAN		Additional clarifications are presented in **Annex B** of this Guide, which covers requirements on physical security, personnel security, and IT security (includes cybersecurity).
22	The general strategy with respect to data protection.	
23	The location and function of all facilities, including mobile facilities, to be used to handle raw data and remote sensing products in the operation of the remote sensing space system.	To include all facilities supporting the remote sensing space system conducting data reception, data processing, and/or data archiving. Facility Name: Owner/Operator: Function: Address: Country: Geographic coordinates (latitude & longitude): (Repeat details for all facilities used in the system.)
24	A general description and block diagram of all facilities to be used to handle raw data and remote sensing products, including the longitude and latitude and station mask of each ground station	

SECTION	PROVISIONS	RECOMMENDATIONS
25 1	A general description and block diagram of the proposed communication architecture that includes descriptions of:	
a)	each system supporting the facilities that are to be used to handle raw data and remote sensing products;	
b)	links between the facilities and the remote sensing satellite;	
c)	links for the relaying of raw data and remote sensing products between facilities on the ground; and	
d)	crosslinks between remote sensing satellites.	
2	The radio-frequency downlink information, including the characterization of each link and the type of information carried by each communication channel.	
3	The protocols to be used in the communication architecture.	
4	A description of the encryption to be used on all communication channels including keying and rekeying schemes.	
5	Management plans for the keys to be used in satellite downlinks and relays and in facilities used to handle raw data and remote sensing products.	
26	A general description of:	
a)	the content and format of raw data and remote sensing products; and	
b)	the processes to be employed to alter image quality and information content at each step from the acquisition of raw data to the provision of a remote sensing product, including such processes as spatial or spectral pixel aggregation — discarding low	

SECTION	PROVISIONS	RECOMMENDATIONS
	order analog-to-digital bits — and data compression.	
27	A diagram that:	
a)	shows each step to be taken by the Applicant or proposed system participant from the placement of a sales order for raw data or a remote sensing product to the communication of raw data to a recipient or the provision of the remote sensing product to a recipient; and	
b)	indicates the data protection measures proposed for each step.	
28	A description of the data protection measures proposed for each step of the business process, including:	
a)	the measures proposed for each facility to be used to handle raw data and remote sensing products, including measures relating to	
i)	the security screening of personnel,	
ii)	the physical security of the facility, and	
iii)	the information assurance, within the facility, in respect of raw data and remote sensing products;	
b)	the measures proposed for the transfer of raw data and remote sensing products between the facilities of the remote sensing space system, including measures relating to physical and electronic protection and information assurance; and	
c)	the measures proposed for the communication of raw data and the provision of remote sensing products to recipients, including measures relating to physical and electronic protection and information assurance.	*Bent-pipe data outside of Canada is considered communicating raw data – a Controlled Activity.

SECTION	PROVISIONS	RECOMMENDATIONS
29	Proposed measures to comply with any conditions of the licence that restrict the communication of raw data or the provision of remote sensing products related to:	Include any foreign remote sensing laws that the system may fall under in this section.
a)	recipients or classes of recipients of raw data or remote sensing products;	
b)	sensor modes;	
c)	types of raw data or remote sensing products;	
d)	the time between the acquisition of raw data by the remote sensing satellite and the communication of the raw data or the provision of a remote sensing product to a recipient;	
e)	the sensed territory;	
f)	the location of the recipients; and	
g)	any agreements entered into under paragraph 8(6)(b) or (7)(b) of the Act.	Sections 8(6)(b) and 8(7)(b) are reproduced below: **Issuance, amendment or renewal of licences** **Conditions specified by Minister — raw data** **8 (6)** In a licence, the Minister may authorize the communication of raw data or classes of raw data from the licensed system to any persons or classes of persons other than the Licensee or system participants on any conditions that the Minister considers appropriate. The conditions may include requirements that, in specified cases or circumstances, the communication of the raw data **(b)** be done only under a legally enforceable agreement, entered into in good faith, that includes measures respecting their security or their further communication. The receipt, communication, processing or storage of raw data by such persons is not a controlled activity. **Conditions specified by Minister — remote sensing products** **(7)** In a licence, the Minister may restrict the provision of remote sensing products or classes of such products from the licensed system to persons or classes of persons other than the Licensee or system participants on any conditions that the Minister considers appropriate. The conditions may include

SECTION	PROVISIONS	RECOMMENDATIONS
		requirements that, in specified cases or circumstances, the provision of the remote sensing products **(b)** be done only under a legally enforceable agreement, entered into in good faith, that includes measures respecting their security or their further provision.
COMMAND AND DATA PROTECTION PLAN		This section is not required if sections 14 (Command Protection Plan) & 22 (Data Protection Plan) are individually completed.
30	In lieu of a separate command protection plan and data protection plan, a combined command and data protection plan that contains the information and documents set out in sections 14 to 29 of this Schedule.	
AFFILIATED ENTITIES		
31	The name, identifying information and contact information of each entity affiliated with the Applicant that will be involved in the operation of the licensed system, a description of their involvement and the name, identifying information and contact information of each person who exercises control over the affiliated entity.	To further add to the *Regulations'* definition of Affiliation, GAC considers the following: One entity is affiliated with another entity if one of them is controlled by the other or both are controlled by the same person.
SYSTEM PARTICIPANT INFORMATION		
32	If the application includes a request to designate a person to be a system participant,	Ensure all information provided under this section is included in draft system participant agreement(s), typically attached as an annex to the draft agreement.
a)	the proposed system participant's name, identifying information and contact information;	List all system participant's information. Name(s) (please specify which department/division/section) Email address(es) Contact number(s)

SECTION	PROVISIONS	RECOMMENDATIONS
b)	the address of each facility to be used by the proposed system participant for carrying on controlled activities, including the location and station mask of each ground station and telemetry, tracking and command station; and	Please clearly identify and list the information of each facility to be used by each proposed system participant for carrying on Controlled Activities. The list of Controlled Activities is reproduced below as reference (*Act*, Section 2): Controlled Activity, subject to subsection 8(6), means any of the following activities in the operation of a remote sensing space system: (a) formulating or giving a command to a remote sensing satellite of the system; (b) receiving raw data from a remote sensing satellite of the system; (c) storing, processing or distributing raw data from the system; (d) establishing or using (i) cryptography in communications with a remote sensing satellite of the system, or (ii) information assurance measures for the system.
c)	a copy of an agreement or proposed agreement between the Applicant and the proposed system participant that specifies;	Provide all <u>draft</u> System Participant Agreements (SPAs) with all proposed system participants that clearly demonstrate that obligations of the Applicant under the *Act*, the *Regulations* and the operating licence flow down to proposed system participants through the SPAs. GAC review and approval of the drafts would help ensure that the SPA is complete before it is signed by both parties; otherwise, the SPAs may need to be amended and re-signed. *Remark*: A final draft SPA is sufficient for the purpose of the application. A signed copy of the SPA can be provided to GAC after the licence is issued.
(i)	the territory from which the proposed system participant will communicate raw data and provide remote sensing products or will give commands to the remote sensing satellite,	
(ii)	the proposed system participant's data protection plan that contains the information and documents	Provide a command and data protection plan for each of the proposed system participant(s)' facilities.

SECTION	PROVISIONS	RECOMMENDATIONS
	referred to in sections 22 to 29 of this Schedule as modified to relate to the proposed system participant's operations, and, if the Applicant intends to permit the proposed system participant to formulate or give a command to a remote sensing satellite of the system, its command protection plan that contains the information and documents referred to in sections 14 to 21 of this Schedule as modified to relate to the proposed system participant's operations,	*List all foreign remote sensing laws to which any of the proposed system participant(s) are subject.
(iii)	how the proposed system participant will make raw data and remote sensing products available to the governments of countries whose territories have been sensed by the system	Refer to Section 7(a) of Schedule 1. While the Applicant describes how it will adhere to *Principle XII of the Principles Relating to Remote Sensing of the Earth from Outer Space*,[9] the Applicant and System Participants need to describe and demonstrate in the SPA how its proposed system participants will meet the same Principle as part of the system. For the purposes of the UN remote sensing principle XII, the term "remote sensing" only refers to operations for the purpose of improving natural resources management, land use and the protection of the environment. (*Principal 1(a)*)
(iv)	how the proposed system participant will make raw data available to the Applicant before the data is disposed of,	
(v)	how the proposed system participant will assist the Applicant to provide service pursuant to an order under section 15 of the Act,	Refer to Section 21(b) of Schedule 1. While the Applicant describes how it will comply to an order under Section 15 of the *Act* (Priority Access), the Applicant needs to describe and demonstrate in the SPA how its proposed system participants will comply with Section 15 of the *Act* as part of the system.

[9] United Nations Office for Outer Space Affairs: Resolution Adopted by the General Assembly 41/65. Principles Relating to Remote Sensing of the Earth from Outer Space, https://www.unoosa.org/oosa/en/ourwork/spacelaw/principles/remote-sensing-principles.html.

SECTION	PROVISIONS	RECOMMENDATIONS
		Remark: Section 15 will only be applicable to any Canadian persons operating worldwide and foreign persons operating in Canada.
(vi)	the proposed system participant's obligation to maintain records, the address where the records will be maintained and the proposed system participant's obligation to allow the Applicant access to them,	
(vii)	the proposed system participant's obligation to make periodic or other reports to the Applicant,	
(viii)	the proposed system participant's obligation to allow the Applicant or an inspector access to their facilities in order to monitor compliance with the proposed system participant's data protection plan and the proposed system participant's command protection plan, if any, and	
(ix)	the obligation of the proposed system participant to allow the Applicant or an inspector access to their facilities in order to monitor compliance on the part of the Applicant with the Applicant's command protection plan and data protection plan and the Applicant's requirements under the Act, these Regulations and the conditions of the licence.	

NOTE:
The Applicant must include a list all documents provided as part of the application.

ANNEX D.

MULTI-STAGE APPLICATION PROCESS

Note: Annex D is currently under review and will be published once completed.

The intent of this annex is to provide guidance and clarification on required information and documents under the Regulations' Schedule 1 to support an Application.

For the purpose of the application, please refer to the Eligibility Threshold Table to determine if your system is eligible for the multi-stage application process.

Applicants who are not eligible for the multi-stage application process shall complete the Application (see Annex C).

Applicants who are eligible for the multi-stage application process start with the completion of Stage-1 (see Annex D Appendix 1). As GAC regulators review the Stage-1 application, additional information may be required; in which case, the completion of Stage-2 may be required (see Annex D Appendix 2).

Appendices to Annex D:

Annex D Appendix D1: Multi-Stage Application, Stage-1 (*to be promulgated*)
Annex D Appendix D2: Multi-Stage Application, Stage-2 (*to be promulgated*)

This Page Intentionally Left Blank

ANNEX E.

RSSSA OPERATING LICENCE OUTLINE

This section provides a high-level description of what to expect upon receipt of a Remote Sensing Space Systems Operating Licence, along with its annexes and schedules. The intent of this document is to describe each section that forms part of a licence. Please be advised that licences are tailored from this generic model based on the specifics of the system, and, as a result, will not look the same.

RSSSA Licence Overview:

- Official Letter signed by the Minister
- Annex A: Exemption Orders
- Annex B: Licence Conditions
  - Eight main schedules
  - Other schedules, if applicable
- Other Annexes, if applicable

OFFICIAL LETTER SIGNED BY THE MINISTER OF FOREIGN AFFAIRS OR AT THE APPROPRIATE AUTHORITY LEVEL

- Identifies under what Law/Statute this licence is granted;
- Refers to documents of the Licensee that have been approved by Global Affairs Canada (GAC) (e.g., System Disposal Plan);
- Identifies any exemption(s) granted within Annex A;
- Establishes the term of the licence (usually the designed mission life); and
- Contains the Minister of Foreign Affairs' official signature or signature at the appropriate level within GAC (depending on whether there are exemption orders or not).

ANNEX A: EXEMPTION ORDERS

- Identifies the part of the *Act* that deals with Exemptions, Section 4(3); and
- Provides a set of exemptions to the operation of specific provisions of the *Act* or *Regulations*, while subjecting them to fulfilment of conditions, if required.
- Following are examples of requirements that an Applicant may be exempted from meeting:
  1. Providing contract details about the launch[1]
  2. Providing a report on the delivery of the flight sensors[2]
  3. Specific value-added products that *should not* be considered as Raw Data or remote sensing Products and should be exempted from the *Act* and *Regulations* (interferometric product with interval not smaller than 24 days (1cycle))
  4. Maintaining certain records as well as when deemed non-applicable
  5. Providing certain reports as well as when deemed non-applicable

[1] RSSS Regulation, Section 21(a).
[2] RSSS Regulation, Section 21(b).

6. Archiving raw data or other information as well as when deemed non-applicable

ANNEX B: LICENCE CONDITIONS

As per Interpretation section of the *Regulations*

- A listing of definitions
    1. Administrative Control and Operation Control of the System
    2. System Disposal Plan and Guarantee
    3. General Operating Conditions
    4. Command and Data Protection Plan
    5. Authorized System Participants
    6. Recipient Authorizations under Section 8(6) and Restrictions under Section 8(7) of the *Act*
    7. Authorized Ground Stations
    8. Records
    9. Reports

ANNEX B: SCHEDULE 1: COMMAND AND DATA PROTECTION PLANS

- Applicant's key security documents detailing physical, personnel and Information Technology security for the entire Remote Sensing Space System.

Note: This schedule is not to be confused with the Regulations' Schedule 1 – the Application.

ANNEX B: SCHEDULE 2: SENSORS AND SENSOR MODES

- An overview of the system's remote sensing capabilities.

ANNEX B: SCHEDULE 3: SYSTEM PARTICIPANT DESIGNATIONS AND AGREEMENTS

- Listing all authorised System Participants, their contact information, as well as which Controlled Activities they are authorised to perform.

ANNEX B: SCHEDULE 4: AUTHORIZATIONS AND RESTRICTIONS

- Legend and terminology
- Access for specific entities
- General access
- Special Cases: areas subject to specific restrictions, with maps and geographical coordinates, disputed territories and agglomerations of areas

ANNEX B: SCHEDULE 5: END USER LICENCE AGREEMENTS (EULAs)

- Applicable when data is distributed from Canada.
- This annex has the authorised example(s) of an end user licence agreement to all recipients of the remote sensing data.

ANNEX B: SCHEDULE 6: PROHIBITED ENTITIES

- This schedule references prohibited countries and entities under Canada's *Anti-Terrorism Act*, the *Criminal Code, United Nations Act*, the *Special Economic Measures Act* and relevant provisions of the *Export and Import Permits Act*.

ANNEX B: SCHEDULE 7: SATELLITE and SYSTEM DISPOSAL PLAN

- An overview of the approved system disposal plan, which covers the Space Segment, the Ground Segment and the Data.

ANNEX B SCHEDULE 8: SATELLITES OF THE SYSTEM

- An overview of the approved satellites operating under the licence.

ANNEX B SCHEDULE 9: RESOURCE SHARING (for ground station-centric licence)

- This schedule covers the approvals for use of other ground station components, where appropriate.

This Page Intentionally Left Blank

ANNEX F.

FREQUENTLY ASKED QUESTIONS

1. Why do I need a licence?

Remote Sensing Space Systems are regulated in Canada pursuant to the *Remote Sensing Space Systems Act* (S.C. 2005, c. 45) (the *Act*) and the *Remote Sensing Space Systems Regulations* (SOR 2007-66) (the *Regulations*).

The *Act* is the national implementation of international obligations derived from various treaties and agreements that Canada has ratified in the past. The *Act*, as per its name, is focused on the regulation and licensing of Remote Sensing Space Systems.

The *Act* also takes into account the implications of national security, the defence of Canada, the safety of Canadian Armed Forces, Canada's conduct of international relations and Canada's international obligations. The *Regulations* also contains prescribed factors related to the ability of the Applicant to comply with the *Act* and the *Regulations*, as well as the enhancement of the competitiveness, at the national and international levels, of the Canadian remote sensing industry.

2. What is considered part of a *Remote Sensing Space System*?

Any satellite system that has the capability, directly or indirectly, of observing the Earth through the use of electromagnetic waves is considered a Remote Sensing Space System, as per the *Act*. A Remote Sensing Space System consists of three parts:

- Space Segment (satellite(s) and sensor(s));
- Ground Segment (ground stations, mission control centre and other facilities used to operate the system, networks and related facilities); and
- Data (the facilities used to receive, store, process and/or distribute raw data from the satellites, even after the satellites themselves are no longer in operation).

3. When should I first contact Global Affairs Canada (GAC)?

It is beneficial to contact GAC as early as possible in the process (ideally during the stage of planning a Remote Sensing Space System), so that the Department can assign an Officer to your project. GAC may then advise more precisely on the documentation requirements and identify elements requiring special attention. Applicants are also encourages to contact GAC at all phases of the process of developing a remote sensing system.

4. How do I make contact with GAC to discuss a possible application?

You can contact GAC by e-mail at: *RSSSA-LSTS@international.gc.ca*

5. What types of satellites are regulated by the *RSSSA*?

A satellite that is capable of sensing the surface of the Earth through the use of electromagnetic waves requires to be licensed under the *Act*.

6. I am a Canadian working as an employee of a foreign organization operating a remote sensing space system. Do I need to obtain a licence?

As an employee of a foreign organization operating a remote sensing space system, you do not need to obtain a licence.

A Canadian organization performing Controlled Activities for a foreign organization must obtain a licence under the *Act*.

If in doubt, please contact RSSSA-LSTS@international.gc.ca

7. How do I determine if a contractor needs a System Participant Agreement?

An affirmative answer to the question, "is my contractor performing any Controlled Activity", as defined under Section 2 of the *Act*, is the litmus test to determine if a contractor needs a System Participant Agreement or not.

Controlled Activities - *Summary*:

(a) formulating or giving a command;
(b) receiving raw data;
(c) storing, processing or distributing raw data; and
(d) establishing or using
    (i) cryptography in communications
    (ii) information assurance measures

RSSSA, Section 2

8. What if the contractor refuses to sign a System Participant Agreement?

If a contractor is to perform any Controlled Activity, the application for a licence must include a request to have such contractor designated as a System Participant along with a copy or a proposed copy of the System Participant Agreement and other information required as contemplated under Section 2 of the *Regulations*. Please note that it is a punishable offence to operate a remote sensing space system in any manner, directly or indirectly, except under the authority of a licence.

9. What is the significance of the 180 days of processing time to obtain a licence?

Once a complete licence application is received by GAC, 180 days is the maximum time allotted to approve or refuse a licence application, as per the *Regulations*, Section 7. This period enables GAC as the regulator to review or make any changes to official documents provided by the Applicant, and provides the necessary internal time for approval.

When the licensing team is involved early in the process, depending on the complexity of the project, this processing time may be shorter. Additionally, if the Applicant does not require exemptions, the approval may be more expedient.

10. Is there a list of all the documents I need for an application?

A list of all required documentation for the remote sensing application can be found in Annex A of this document.

11. Is a licence from the United States or another foreign country sufficient?

If you seek to conduct remote sensing activities in Canada, including such activities as storage and processing remote sensing data, a RSSSA licence is required. GAC has regular exchanges with its international regulatory counterparts to ensure a degree of harmonization. Providing information about the foreign licence will be helpful in the review of your application.

12. What other approvals are required for operations in Canada?

Innovation, Science and Economic Development Canada is responsible for radio communications and has the mandate for licensing satellite radio frequency communications for all satellites, national or foreign for use in Canada, as per the *Radiocommunication Act* (R.S.C., 1985, c. R-2).

13. Do companies that provide telecommunications services need a System Participant Agreement (SPA)?

Telecommunications services are only required to have a SPA if they contribute to the remote sensing space system in any of the Controlled Activities. Otherwise, their involvement can be detailed (typically within the Data and Command Protection Plan) without the need of a SPA.

Controlled Activities - *Summary*:

(a) formulating or giving a command;
(b) receiving raw data;
(c) storing, processing or distributing raw data; and
(d) establishing or using
    (i) cryptography in communications
    (ii) information assurance measures

RSSSA, Section 2

14. What if I sell a satellite prior to launch? What if I sell it sometime after launch?

The key consideration is if the satellite in question, and the remote sensing space system to which it belongs, was licensed under the *Act* at the time of the sale. Transfer of control of a satellite is regulated under Section 16 (1) of the *Act* by prohibiting transmission of a command to a remote sensing satellite for which the licence was issued, from outside Canada or by any other person, unless the Licensee or former Licensee:

(a) can override the command from Canada; or

(b) has obtained the approval of the Minister.

15. What if my satellite is part of a foreign constellation?

Please ensure that the application reflects how the Applicant will exercise control over the operations of the remote sensing space system as a whole, for which the licence is sought. Such information is required to demonstrate how orders passed under Sections 14 and 15 of the *Act* (relate to Interruptions of Service and Priority Access, respectively) will be implemented.

16. What efforts are made to ensure that the Canadian space industry is competitive?

Global Affairs Canada engages regularly with other regulators to ensure that Canadian regulations are on par with those of partner countries and to ensure a regulatory environment conducive to space operators. Our space regulatory team at Global Affairs Canada is available for discussions about your project at an early stage. We also conduct activities, such as outreach and presentations on the *Act*, and provide status updates at major space and remote sensing conferences.

17. Do systems with more than one ground station have different licensing arrangements than a system with only one ground station?

No, such systems are treated in a similar manner. Each ground station needs to be analyzed and will be listed in the licence and/or in System Participant Agreement(s).

18. What about a constellation comprising different foreign satellites? Will it have a different licensing arrangement than a system controlled by one "owner" / operator?

A constellation is typically covered by one licence. The licence has provisions for multiple operators conducting Controlled Activities, as required. They are normally called System Participants (refer to Section 32 of the Regulations' Schedule 1).

19. Can an Applicant appeal a denied licence application?

We encourage engaging with GAC's Space Regulatory Section. If an Applicant disagrees with the outcome of a decision on its licence application, the Applicant may request to the Minister a review of the decision. Alternatively, the Applicant has the right to seek judicial review with the Federal Court within 30 days of receiving the decision, pursuant to Section 18.1 of the *Federal Courts Act*.[1]

20. Is a foreign entity subject to Canadian regulations when performing remote sensing activities outside Canada?

Canadian regulations have jurisdiction and control over any Control Activities occurring in Canada.

The *Act* applies to all activities taking place in Canada that are part of the system. For example, building an antenna station is not a Controlled Activity, but it is covered under the law.

21. Is there a need for a foreign entity to have a Canadian subsidiary to operate in Canada?

Presently, it is not mandatory for a foreign entity to have a Canadian subsidiary in order to operate in Canada. As each situation is unique, we recommend that you contact RSSSA-LSTS@international.gc.ca.

[1] Government of Canada, *Federal Courts Act (R.S.C., 1985, c. F-7)*, https://laws-lois.justice.gc.ca/eng/acts/f-7/.

This Page Intentionally Left Blank