Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Travaux publics et Services gouvernementaux Canada
Place Bonaventure,
800 rue de la Gauchetière Ouest
Voir aux présentes - See herein
Montréal
Québec
H5A 1L6
FAX pour soumissions: (514) 496-3822

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet LOI Sat Ops	
Solicitation No. - N° de l'invitation 9F044-190565/A	**Date** 2020-02-03
Client Reference No. - N° de référence du client 9F044-190565	**GETS Ref. No. - N° de réf. de SEAG** PW-$MTB-255-15637
File No. - N° de dossier MTB-9-42283 (255)	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2020-03-10**	**Time Zone** **Fuseau horaire** Heure Normale du l'Est HNE
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☐ **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à: Desforges, Julie	**Buyer Id - Id de l'acheteur** mtb255
Telephone No. - N° de téléphone (514) 602-8307 ( )	**FAX No. - N° de FAX** (514) 496-3822
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:** AGENCE SPATIALE CANADIENNE 6767 ROUTE DE L AEROPORT ST HUBERT Québec J3Y8Y9 Canada	

Comments - Commentaires

Instructions: See Herein

Instructions: Voir aux présentes

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Delivery Required - Livraison exigée Voir doc.	**Delivery Offered - Livraison proposée**
Vendor/Firm Name and Address **Raison sociale et adresse du fournisseur/de l'entrepreneur** **Telephone No. - N°de téléphone** **Facsimile No. - N° de télécopieur**	
Name and title of person authorized to sign on behalf of Vendor/Firm (type or print) **Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)** **Signature** **Date**	

Issuing Office - Bureau de distribution
Travaux publics et Services gouvernementaux Canada
Place Bonaventure, portail Sud-Oue
800, rue de La Gauchetière Ouest
7e étage, suite 7300
Montréal
Québec
H5A 1L6

Canada

ANNEX A

SERVICE LEVEL AGREEMENT
FOR
FLIGHT OPERATIONS AND DATA MANAGEMENT SERVICES

Table of Content

Contents

Table of Tables

1 Introduction

1.1 Purpose

This document defines the Service Levels of the Satellite Operations contract required by the Canadian Space Agency (CSA) for the provision of Flight Operations and Data Management Services to be performed at the John H. Chapman Space Center (JHCSC) in Longueuil, Quebec.

The Services and activities performed under the Flight Operations and Data Management Services contracts are defined within 3 different Domains:

- Flight Operations
- Data Management
- Ground System Operations

From this perspective, and in order to capture the end-to-end service provision and apply standardized processes and performance targets, unified performance indicators have been defined for all the Domains, where possible and where processes are applicable. When requirements of a Domain service demand specific performance or process indicators, they have been also reflected.

The Quality of Service (QoS) is described in terms of Performance Indicators (PI), and service levels that are to be considered as Key Performance Indicators (KPI) are defined (Section 3.3), together with the proposed Incentive Scheme (Section 4).

1.2 Scope

The scope of this document is to stand as a complementary requirement document to the SOW for the provision of Flight Operations and Data Management Services. While the SOW describes the Mandatory Work to be performed under a Firm-Fixed Price contract, the SLA describes the QoS in terms of specific KPIs where over-performance will lead to financial incentive (bonus) to the Contract.

1.3 Conventions and Definitions

1.3.1 Language Convention

As English is the standard oral and written language for design, development, operation and utilization of space projects, the Contractor must use English for this Work, and for exchanges with CSA, along with System International (SI) units

1.3.2 Document Convention

A number of the sections in this document describe controlled requirements and specifications and therefore the following verbs are used in the specific sense indicated below:

“Must” is used to indicate a mandatory requirement,

“Should” indicates a preferred alternative but not mandatory,

“May” indicates an option,

“Will” indicates a statement of intention or fact, as does the use of present indicative active verbs.

1.3.3 Terminology

"Contractor ": team that will conduct the work, which could be a mixed team drawn from Canadian industry, universities or research institutes, including subcontractors;

"Contractor Operational Personnel": all individuals identified and assigned by the Contractor to undertake tasks described in this Service Level Agreement throughout the contract period;

“Data Management”: subset of all mission activities related to the mission payload data ordering, reception, processing, calibration, distribution and archiving, and the maintenance of its system and procedures;

“Domain”: is on area of Satellite Operation activities covering Flight Operations, Data Management and Ground Systems Operation and maintenance;

"Government Furnished Personnel (GFP)": Government employees paid by the government and lend to the Contractor, part or full-time, for an agreed period of time to accomplish work under the Contractor`s authority;

“Flight Operations”: subset of all mission activities related to spacecraft health, monitoring and control, spacecraft activity planning, flight dynamics and orbital maintenance, and the maintenance of its system and procedures;

“Ground System Operations”: subset of all activities related to satellite infrastructure, ground antennas Telemetry, Tracking & Control, communication systems, networking, and the maintenance of its system and procedures;

"Mission": the complete life cycle of a satellite and its products, from pre-launch preparation to de-commissioning;

"Operational Database": the collection of all data elements, resident in the operational system, required for its on-going operation, including operational procedures, data, and documentation;

"Operational Product": a data element, derived from the operational schedule, whose passage between elements of the operational system constitutes a portion of an operational activity;

"Operational System": the collection of all software, hardware, and operational database elements required to conduct those operational activities required to complete the mission.

"SCAN" Spacecraft Anomaly Notice: Contains the summary information of a Spacecraft anomaly event, including the anomaly occurrence time, the detection time, the recovery time and notification times

"Spacecraft Control System": The Ground-Segment components that ensure the Spacecraft Control function (e.g. Flight Dynamics System, Real-time Command and Telemetry System, Spacecraft Planning System)

"Space Segment Asset": Satellite systems (spacecraft bus and payload components) of a mission in orbit.

1.3.4 Acronyms

AD	Applicable Document
BCF	Backup Control Facility, 3701 Carling Ave, Ottawa, Ontario
CA	Contract Authority
CADMS	Configuration And Data Management System
CCB	Change Control Board
CCR	Contract Completion Review
CM	Configuration Management
CoC	Certificate of Conformance
COLA	Collision Avoidance
CRB	Change Review Board
CSA	Satellite Operations, Space Utilization, Canadian Space Agency, responsible for the overall management of this Contract
CSE	Communications Security Establishment
DFL	David Florida Laboratory, 3701 Carling Ave, Ottawa, Ontario
ESD	Electro Static Discharge
EODMS	NRCan's Earth Observation Data Management System
EOP	Extended Operations Phase
FD	Flight Dynamics System
FHD	Facility Help Desk
GFE	Government-Furnished Equipment
GFP	Government-Furnished Personel
GSS	NRCan's Gatineau Satellite Station, Cantly, Quebec
ICAN	NRCan's Inuvik Canadian Satellite Facility, Inuvik, North-West Territories
IOP	Initial Operations Phase
IQS	Image Quality System
IR	Initial Release
ITS	Information Technology System

KOM	Kick-Off Meeting
KPI	Key Performance Indicator
LCS	Life-Cycle Support
LEOP	Launch and Early Operation Phase
MA	Management Authority
MDA	MacDonald, Dettwiler and Associates
MOP	Mission Operation Plan
MPS	Mission Planning System
NA	Not Applicable
NC	Non-Conformance
NOP	Nominal Operations Phase
OA	Operational Authority
OAR	Operational Analysis Report
OHS	Order Handling System
OMRR	Operations and Maintenance Readiness Review
OSR	Operations Service Review
PA	Product Assurance Authority
PASS	NRCan's Prince-Albert Satellite Station, Prince-Albert, Saskatchewan
PCF	Primary Control Facility, 6767 route de L'Aéroport, St-Hubert, Québec
PI	Performance Indicator
PIP	Phase-In Phase
PGS	Product Generation System
PLAN	Spacecraft Activity Planning System
PM	Project Manager
POP	Phase-Out Phase
PSPC	Public Services Canada
QoS	Quality of Service
RAS	Reception & Archiving System
RCM	RADARSAT Constellation Mission
RD	Reference Document
RFP	Request for Proposals
RPT	RADARSAT Precision Transponder
SASK	Saskatoon TT&C antenna station (SASK), 18 Innovation Blvd, Saskatoon, Saskatchewan
SCAN	Spacecraft Anomaly Notice
SCS	Spacecraft Control System

SE	Systems Engineer
SLA	Service Level Agreement
S&MA	Safety and Mission Assurance
SOB	System Operation Board
SOW	Statement Of Work
SRB	System Review Board
SRR	Service Readiness Review
TA	Technical Authority (The TA will be the single point of contact with the Contractor for all work under this contract)
TT&C	Telemetry, Tracking and Command
TTCS	Telemetry, Tracking and Command System
TBC	To Be Confirmed
TBD	To Be Determined
VCM	Verification and Compliance Matrix
WOSM	Weekly Operation Scheduling Meeting

2 References

2.1 Applicable documents

The following documents of the exact issue date and revision level shown are applicable and form an integral part of this document to the extent specified herein.

ID	Number	Revision	Title
AD-01	CSA-FODMS-SOW-0001	IR	Statement of Work – Flight Operations and Data Management Services

2.2 Reference documents

The following documents provide additional information or guidelines that either may clarify the contents or are pertinent to the history of this document.

ID	Number	Revision	Title
RD-01	CSA-RC-RD-0002	H	RADARSAT Constellation : Mission Requirements Document (MRD)

3 General

Metrics are measures of quantitative assessment commonly used for assessing, comparing, and tracking performance. Performance Indicators (PI) are those metrics that will be collated to evaluate and report on the effectiveness and efficiency of CSA satellite flight operations and data management services. As per Section 3.2 of this document, Key Performance Indicators (KPI) must be well-defined and quantifiable measures, applicable to satellite operations, that are crucial to achieving Flight Operations and Data Management Services goals at the CSA.

3.1 Performance Indicators

Service level requirements must be tailored to match the required quality and performance of the Service. PIs are used to measure the performance levels and as input for defining and computing the KPIs. These requirements must constitute the basis for PIs and KPIs and the related Service Level agreement (SLA).

PIs are classified into two groups:

- *Mandatory performance indicators provided by the CSA,* characterizing the actual performance of the satellite Flight Operations and Data Management Services and intended to be used for KPI definition; and,
- *Performance indicators proposed by the Contractor,* only for monitoring purposes.

The PIs required by the CSA are introduced in Table 1 and Table 2 for Flight Operations and Data Management Services respectively. Additional PIs must be proposed by the Contractor if relevant to effectively manage the SLA and report on the Service.

For each PI, a *Performance Target* figure is provided, which characterise the nominal performance expected as from the System requirements and/or mission objectives.

3.2 Performance Indicators Requirements

In order to better formulate the PI and KPI, a set of guidelines and requirements are provided below.

[PI-REQ-01] The performance of the Service will be characterised and measured through a set of Performance Indicators (PI) with the following aspects:

1. The PIs must allow to characterise the Service level performances (e.g. availability, timeliness, completeness…);
2. The PIs must be unambiguously measurable in time;
3. The number of PIs should be limited in number (less than 25)

[PI-REQ-02] Each PI must be defined with:

1. PI ID: a unique ID to identify the service and performance indicator within the service;
2. Description: a short description of the measured indicator;
3. The detailed measurement method as required, including:
    a. The identification of any raw information used to compute the PI,
    b. The mechanism and tools for the collection of the raw information used to compute the PI,

c. The detailed description of the rationale used to derive the final PI,
d. The PI unity (e.g. % of sensing time),
e. The PI validity scope (e.g. timelines….), and
f. The PI time unit (e.g. orbit, day, month...).

4. The monitoring and reporting approach; and
5. Monitoring and Reporting Periods: specifies the time interval in which the performance indicator is collected/measured and reported, e.g.: orbit basis, daily basis, weekly basis, monthly basis.

[PI-REQ-03] The Contractor must systematically and continuously measure metrics and compute and monitor PI values according to their Monitoring Period starting from the Initial Operations Phase.

1. The collect and processing of raw metrics to derive the PI values must be automated
2. The Contractor should provide visibility to CSA at any time of the current PIs values through an interactive web based interface
3. The PI monitoring web-interface should support a machine-to-machine query interface available to CSA for content access or download.

[PI-REQ-04] A subset of Key Performance Indicators (KPI) will be derived from one or more the PIs and will be used for the cost calculation of the Incentive Scheme (Section 4).

1. The KPIs must include in their definitions
   a. The Target performance levels
   b. The Weight factor for the purpose of Incentive cost calculations (Section 4)

2. The number of KPIs should be limited in number (no more than 10).

[PI-REQ-05] The Contractor must allow the computation of KPIs on a monthly and quarterly interval for any monthly/quarterly based sliding window, with the exclusion of:

1. A total maximum planned maintenance of 12h/month, where planned maintenance is defined as a maintenance announced at least 10 days in advance;
2. A total maximum planned emergency maintenance of 6h/month, where emergency planned maintenance is defined as a maintenance announced at least 2 hours in advance.

[PI-REQ-06] The Contractor must report the status of the defined PIs and KPIs through alarm notifications, monthly/quarterly reports, and Service reviews according to their Reporting Frequency.

[PI-REQ-07] The Contractor must ensure that any instances where the required service levels have not been achieved are identified and reported, with justifications for deviations and actions for resolution.

[PI-REQ-08] The definition of the PIs and KPIs will be revised on a yearly basis and fine-tuned according to the operations experience in agreement between CSA and the Contractor.

3.3 Performance Indicator Listing

The PI are tabulated in Table 1 and Table 2 for Flight Operations and Data Management respectively where Flight Operations include also PIs pertaining to the Ground System Operations Domain. PIs are uniquely identified with a P00 identification number (ID). Whenever a PI is deemed key to the operations, it has a K00 identifier (ID) and has a weight associated to it for Incentive cost calculation (Section 4).

3.3.1 Service Performance Indicators for Flight Operations

Table 1 PERFORMANCE INDICATORS FOR FLIGHT OPERATIONS

ID	Title	Objectives	Description	Raw Metric Used	Mechanism for Metric Collection	Rational to derive PI	PI Unit	PI Validity Scope	PI Time Unit	Monitoring and Reporting Approach	Monitoring Period	Reporting Period	Target[1] per Quarter	KPI Weight
K01	Space Segment Availability - RCM	• Monitor overall Spacecraft anomaly impacts on mission performance; • Perform timely preventive maintenance and upgrades; • Improve recovery response time and efficiency.	The percentage of time the Space Segment Asset(s) is available to perform its mission requirements.	From SCAN data							Daily	Monthly	For each RCM satellite ≥TBD%	0.5
P02	Space Segment Availability – Small Missions		The percentage of time the Space Segment Asset(s) is available to perform its mission requirements.	From SCAN data							Daily	Monthly	For each Small Mission ≥TBD%	N/A
K03	Satellite Control System Availability	• Ensuring the ground system issues are detected promptly and recovered rapidly to ensure Spacecraft safety and mission throughput • Ensure routine maintenance is performed • Ensuring proper redundancy schemes are maintained throughout operations.	The percentage of time the Spacecraft Control System is available to perform its mission services.	From SCAN data or Anomaly Database system							Daily	Monthly	For RCM and Small Mission ≥TBD%	5
P04	System Anomaly Resolution Time	• Ensuring the anomalies are managed efficiently and towards final resolution • Ensuring no open work related to spacecraft safety.	The average time from initial anomaly file opening to final disposition/closure	From Anomaly Database system							Daily	Monthly	<1 mth	N/A
P05	System Anomaly Resolution Efficiency		The percentage of spacecraft anomaly files disposed and closed within 6 months from file opening.	From Anomaly Database system							Daily	Monthly	100%	N/A
P06	Space Segment Risk Assessment Time	• Minimize health and safety risk to space assets due to undetected anomalous signatures	The percentage of spacecraft anomalies where the initial anomaly notifications occurred within 24 hours from anomaly occurrence.	From SCAN data							Daily	Monthly	≥TBD%	N/A

[1] Unless otherwise specified, the PI Target applies to all missions.

		• Improve anomaly detection and diagnostic capability • Improve trending algorithms and reporting												

3.3.2 Service Performance Indicators for Data Management

Table 2 PERFORMANCE INDICATORS FOR DATA MANAGEMENT

ID	Title	Objectives	Description	Raw Metric Used	Mechanism for Metric Collection	Rational to derive PI	PI Unit	PI Validity Scope	PI Time Unit	Monitoring and Reporting Approach	Monitoring Period	Reporting Period	Target [2] per Quarter	KPI Weight
P11	SAR Downlink to Delivery Time – Canada Maritime AOI within Canadian mask	Meet the RCM Mission Requirement MRD34010	The percentage of passes where all the non-ship-detection maritime SAR data collected over Canadian Maritime Areas of Interest inside Canadian station masks was processed and delivered within 30 minutes from downlink.								Data Reception Pass	Monthly	RCM ≥TBD%	N/A
P12	SAR Downlink to Delivery Time – Canada Maritime AOIs within Canadian masks for Ship Detection		The percentage of passes where all the ship-detection maritime SAR data collected over Canadian Maritime Areas of Interest inside Canadian station masks was processed and delivered within 10 minutes from downlink.								Data Reception Pass	Monthly	RCM ≥TBD%	N/A
K13	SAR Acquisition to Delivery Time – Canada Maritime AOIs outside Canadian mask	Meet the RCM Mission Requirement MRD34030	The percentage of passes where all the maritime SAR data collected over Canadian Maritime Areas of Interest outside Canadian station masks was processed and delivered within 3 hours from acquisition.								Data Reception Pass	Monthly	RCM ≥TBD%	0.5
K14	SAR Acquisition to Downlink Time –	Meet Mission Operations Procedures Operations Latency Requirement	The percentage of SAR images over Canadian land mass that was downlinked within 2 hours from acquisition.								Data Reception Pass	Monthly	RCM ≥TBD%	0.5

[2] Unless otherwise specified, the PI Target applies to all missions.

	Canada Land													
P15	SAR Downlink to Delivery Time – Canadian Land Areas	Meet the RCM Mission Requirement MRD34040	The percentage of passes where all the SAR data collected over Canadian land mass was processed and delivered within 24 hours from downlink.								Data Reception Pass	Monthly	RCM ≥TBD%	N/A
K16	SAR Downlink to Delivery Time – Near-Real-Time Orders	Meet Mission Operations Procedures Operations Latency Requirement	The percentage of Near-Real-Time Orders processed and delivered within 10 minutes from downlink.								Daily	Monthly	RCM ≥TBD%	0.5
K17	SAR Order to Tasking Time – Fast-Tasking	Meet RCM Operations Requirements	The percentage of SAR Fast-Tasking Orders successfully planned and uploaded to a spacecraft within 4 hours from order placement.								Daily	Monthly	RCM ≥TBD%	0.5
P18	Maximum Order to Delivery Time	Meet Mission Operations Procedures Operations Latency Requirement	The percentage of Orders processed and delivered within 48 hours from order placement.								Daily	Monthly	RCM ≥TBD% Neossat ≥TBD%	N/A
P19	Small Mission Data Management Availability	Availability of Data Management Subsystems for ordering/generation/delivery of data products from small missions	The percentage of time the ground segment Data Management Subsystem assets are available for ordering/generation/delivery of data products from small missions, as needed.								Daily (TBC)	Monthly	NEOSSat ≥TBD% M3MSat ≥TBD% SCISat ≥TBD%	N/A

4 Incentive Scheme

The Quality of Service (QoS) will be measured using the KPIs indicated in the previous sections. As such, the set of criteria for categorising a specific QoS level to be provided by the Service Provider is defined in this SLA, and when applicable, by specific provisions within the SOW.

Whereas the focus within provision of Service is on the Quality, Capacity and Availability of the Service being delivered, the core principles of the proposed Service Incentive Scheme are as follows:

- Service Incentives only arise in relation to services for which the Contractor has responsibility under the terms of the Contract;
- Minimum Service Level Requirements (i.e. the performance standards below which service Incentives become payable) are applied as agreed and stated in the applicable "KPIs" tables given above, weighted according to their operational criticality;
- Service Incentives are capped yearly to a maximum of 10% of the total Service Value, aggregated for all services delivered in any given quarter;
- Incentives must not be applied to non-conformant services of less than one month's duration (temporary assignments etc);
- In the event that a KPI does not meet its Target value, the Contractor must provide a recovery plan as part of the quarterly report.
- The systematic non-fulfilment of the service generates an operational situation that is not simply managed by the application of such scheme, and will require specific management measures.

The proposed Service Incentive Scheme is as follows:

$$\text{COST} = \Sigma\ (\text{WEIGHT} \times (\text{METRIC-TARGET})/\text{TARGET}) \times \text{SERVICE VALUE}/4$$

Where:

- WEIGHT factor and TARGET taken from KPI tables
- METRIC measured as per KPI tables, systematically and continuously
- COST, Incentive computed quarterly
- COST Cap = +10% SERVICE VALUE for the year

Example:

Let's assume:

- SERVICE VALUE of $100k
- TARGET_1 = 99.5%, METRIC_1 = 100%, WEIGHT_1 = 10
- TARGET_2 = 10min, METRIC_2 = 8min, WEIGHT_2 = 0.05

COST = (10x(100% - 99.5%)/99.5% + 0.05x(8min-10min)/10min) *$100,000/4 = +$1,507 in that Quarter

5 Review Process

This SLA may be subject to periodic reviews and updated when one or more of the following events occur:

- Service requirements in the SOW have changed;
- Working processes have changed;
- Quality of Service requirements have changed;
- Better metrics, measurement tools and processes have evolved; and
- Introduction of new services requiring a different Service management approach.

Additionally, this SLA will be reviewed normally as part of the Operational Service Reviews and document any changes in the Annual Operations Performance Report. The CSA will incorporate all subsequent revisions of this SLA and obtain mutual agreements / approvals as required.

APPENDIX 1 Sample KPI Calculation Spreadsheet

Table 3 KPI Calculation Spreadsheet Simulation

CSA-FODMS-SOW-0002

CONTRACT #	
TITLE	Flight Operations and Data Management Services
DOCUMENT	Service Level Agreement (SLE) - Key Performance Indicator (KPI) Calculation Spreadsheet
ASSESSMENT PERIOD	1 Dec 2020 to 30 Nov 2021
FILE UPDATED	18-Dec-19

KPI							Q1		Q2		Q3		Q4		YEARLY TOTAL	
ID	TITLE	WEIGHT	TARGET	MAX VALUE	MAX COST	INSTANCE	METRIC	COST	METRIC	COST	METRIC	COST	METRIC	COST	METRIC	COST
K01	Space Segment Availability - RCM	0.5	95.0%	100%	+2.63%	RCM-1	93.0%	-0.26%	94.0%	-0.13%	96.0%	+0.13%	97.0%	+0.26%	95.0%	+0.00%
		0.5	95.0%	100%	+2.63%	RCM-2	96.0%	+0.13%	92.0%	-0.39%	98.0%	+0.39%	99.0%	+0.53%	96.3%	+0.66%
		0.5	95.0%	100%	+2.63%	RCM-3	90.0%	-0.66%	93.0%	-0.26%	95.0%	+0.00%	96.0%	+0.13%	93.5%	-0.79%
K03	Satellite Control System Availability	5	99.5%	100%	+2.51%	RCM	99.0%	-0.63%	99.6%	+0.13%	99.3%	-0.25%	99.8%	+0.38%	99.4%	-0.38%
		5	99.5%	100%	+2.51%	SMALL	99.5%	+0.00%	98.0%	-1.88%	99.8%	+0.38%	100.0%	+0.63%	99.3%	-0.88%
K13	SAR Acquisition to Delivery Time - Canada Maritime	0.5	95.0%	100%	+2.63%	RCM	94.0%	-0.13%	96.0%	+0.13%	98.0%	+0.39%	99.0%	+0.53%	96.8%	+0.92%
K14	SAR Acquisition to Downlink Time - Canada Land	0.5	95.0%	100%	+2.63%	RCM	99.0%	+0.53%	93.0%	-0.26%	95.0%	+0.00%	97.0%	+0.26%	96.0%	+0.53%
K16	SAR Downlink to Delivery Time – Near-Real-Time Orde	0.5	95.0%	100%	+2.63%	RCM	98.0%	+0.39%	99.0%	+0.53%	94.0%	-0.13%	94.0%	-0.13%	96.3%	+0.66%
K18	SAR Order to Tasking Time – Fast-Tasking Orders	0.5	95.0%	100%	+2.63%	RCM	97.0%	+0.26%	98.0%	+0.39%	97.0%	+0.26%	98.0%	+0.39%	97.5%	+1.32%
Total Cost Capped between 0 and +10%					**+10.00%**			**-0.36%**		**-1.76%**		**+1.18%**		**+2.98%**		**+2.03%**

YEARLY SERVICE VALUE	**$ 7,000,000**
INCENTIVE COST	**$ +142,323**

Signatures:	**CSA**		**Contrator**
Technical Authority:		Operational Authority:	
	<NAME>		<NAME>
	<PHONE>		<PHONE>
Contracting Authority:			
	<NAME>		
	<PHONE>		

ANNEX B

EVALUATION PROCEDURES AND BASIS OF SELECTION
FOR
SATELLITE FLIGHT OPERATIONS AND DATA MANAGEMENT SERVICES

ANNEX B - EVALUATION PROCEDURES AND BASIS OF SELECTION
SATELLITE FLIGHT OPERATIONS AND DATA MANAGEMENT SERVICES

Evaluation Criteria Summary

Table 1 Evaluation Criteria Summary

Item	Evaluation Criteria Title	Criteria Type: Mandatory (M) Point-Rated (P)	Maximum Score [pts]	Minimum Required Score [pts]
M1.	**Mandatory Documents**	M	N/A	N/A
P1	Corporate Profile and Experience in providing Flight Operations and Data Management Services	P	8	4
P2	Team Experience with Satellite Operations, Ground Systems, and Data Systems	P	12	6
P3	Understanding and Implementation Approach	P	12	8
P4	Performance Indicators	P	13	6
P5	Value-Added Proposal	P	15	0
	Overall		**60**	**30**

ANNEX B - EVALUATION PROCEDURES AND BASIS OF SELECTION
SATELLITE FLIGHT OPERATIONS AND DATA MANAGEMENT SERVICES

Mandatory Criteria

Each of the following Mandatory Criteria must be presented in the Proposal. Proposals not meeting the mandatory requirements will be deemed non-responsive. Only those proposals which are responsive (compliant) with all of the mandatory criteria will be further considered for evaluation in the next step: Point-Rated Criteria.

In all cases, explicit evidence must be provided and the level of detail provided must be sufficient to confirm compliance with the requirements.

For the following criteria, when a detailed substantiation is required, the Bidder must provide a detailed statement of how it complies with the requirements. Cross-references to appropriate sections of the proposal should be provided when applicable and the essence of the referenced information should be summarized in the substantiation.

Where an approach is deemed credible, it means that an evaluator, using his/her expertise, experience and the information solely provided in the Proposal, is of the opinion that the Bidder has clearly demonstrated, through clear examples and verifiable assertions that the approach can meet the objectives.

M1. Mandatory Documents

The Proposal must include all the documents required in Initial Release (IR) version at Proposal submission as per SOW. Some documents are only required in Draft (D) version at Proposal submission and are therefore not mandatory but highly recommended for the Point-Rated Criteria. Any one document for IR at Proposal submission missing from the list or found without substantive content will result in the Proposal being deemed unresponsive.

ANNEX B - EVALUATION PROCEDURES AND BASIS OF SELECTION
SATELLITE FLIGHT OPERATIONS AND DATA MANAGEMENT SERVICES

Point-Rated Criteria

For each of the following Point-Rated Criteria, Proposals must obtain the minimum points required for each rated criterion to be assessed as responsive under the point rated technical criteria section. Proposals not meeting the minimum required points will be deemed non-responsive. Proposals which are not responsive (i.e. not compliant) with all of the mandatory criteria will not have their point-rated criteria evaluated.

In all cases, the level of detail provided must be sufficient to confirm compliance with the requirements. The Bidder Self-Evaluation requested below will be used to guide the reviewer but points will be awarded only where sufficient evidence is found.

Where an approach is deemed credible, it means that an evaluator, using his/her expertise, experience and the information solely provided in the Proposal, is of the opinion that the Bidder has clearly demonstrated, through clear examples and verifiable assertions that the approach can meet the objectives.

The evaluator will only provide points for criteria where there is sufficient evidence.

Bidder Experience

Except where expressly provided otherwise, the experience described in the Proposal must be the experience of one or more of the following:

1. The Bidder itself;

2. The Bidder's affiliates;

3. The Bidder's subcontractors.

The experience of the Bidder's suppliers will not be considered.

The Proposal should include a self-evaluation which provides explicit evidence of compliance. The self-evaluation must be documented in the following format. For mandatory criteria, the Bidder must evaluate themselves as either “compliant” (C) or “non-compliant” (NC) with explicit evidence to justify the evaluation. For point-rated criteria, the Bidder must evaluate themselves by provided their score with explicit evidence to justify the evaluation.

Item	Evaluation Criteria Title	Evaluation[1]	Evidence
M1.	Mandatory Documents		
P1	Corporate Profile and Experience in providing Flight Operations and Data Management Services		
P2	Team Experience with Satellite Operations, Ground Systems, and Data Systems		
P3	Understanding and Implementation Approach		
P4	Performance Indicators		
P5	Value-Added Proposal		

[1] Compliant (C), Non-Compliant (NC)

ANNEX B - EVALUATION PROCEDURES AND BASIS OF SELECTION
SATELLITE FLIGHT OPERATIONS AND DATA MANAGEMENT SERVICES

P1. Corporate Profile and Experience in providing Flight Operations and Data Management Services

The Contract will deliver Flight Operations and Data Management Services. This criterion assess the Bidder's corporate profile and experience in providing the Services.

To demonstrate conformance with the criteria, the Bidder must provide a substantive description of experience for each of the three (3) required Domains of Service, in which the Bidder had a role within the past fifteen (15) years and a description of the business model to implement the service. The experience for a Domain must include all of the following sub-domain activities, as defined in the SOW:

1. Satellite Flight Operations
    a. Spacecraft Activity Planning and Contact Operations
    b. Satellite Health Maintenance, Monitoring and Control
    c. Orbit Maintenance, Monitoring and Control
    d. Flight System Configuration Management

2. Satellite Data Management
    a. Payload Data Order Handling and Acquisition Planning
    b. Payload Data Reception and Processing
    c. Payload Data Product Quality Control
    d. Data Reporting Support
    e. Data System Configuration Management

3. Satellite Ground Systems Operations and Maintenance
    a. Antenna Reservation System Operation
    b. Telemetry, Tracking and Commanding System Operation
    c. Network and Communication System Operation
    d. Operational System Configuration Management
    e. Life-Cycle Support

ANNEX B - EVALUATION PROCEDURES AND BASIS OF SELECTION
SATELLITE FLIGHT OPERATIONS AND DATA MANAGEMENT SERVICES

For P1 criterion, all the Elements will be evaluated together and assigned “Poor”, “Inadequate”, “Minimal”, “Adequate” or “Excellent” and receive the corresponding point value as per table below. The minimum passing score is Minimal.

ELEMENTS	Poor 0 point	Inadequate 2 points	Minimal 4 points	Adequate 6 points	Excellent 8 points
Flight Operations Services **Satellite Data Management Services** **Satellite Ground Systems Operations and Maintenance**	The Proposal does not identify relevant experience in two or more of the three (3) specified Domains of Service. OR The business models have been presented with insufficient details or are not relevant to this contract.	The Proposal identifies some experience in at least two (2) of the specified Domains of Service. The proposed example shows a limited role that the Bidder had in the development of the service; the business model is poorly described.	The Proposal identifies relevant experience in at least two (2) of the specified Domains of Service. The proposed example shows an important but not lead role that the Bidder had in the development of the service; the business model is well described and could be relevant for this contract.	The Proposal clearly identifies relevant experience in ALL three (3) specified Domains of Service. For each Domain, at least one (1) example demonstrates that the Bidder led the development of the service and reached delivery of service using a business model that could be relevant to this contract.	The proposal clearly identifies relevant experience in ALL three (3) specified Domains of Service. For each Domain, at least two (2) examples demonstrate that the Bidder led the development of the service and reached delivery of service using a business model that could be relevant to this contract.

P2. Team Experience with Satellite Operations, Ground Systems, and Data Systems

This criterion assesses the capability (education, knowledge, experience, expertise and complementarities) of the key resources, including subcontractors, identified to carry out the Mandatory Work as described in the SOW. The Bidder should demonstrate that the skills of the team include those necessary to lead teams located in different locations and through different Contract Phases. The Proposal must be in accordance with the following requirements:

1. The Bidder must identify the management team (Service Manager, delegates, supervisors…) and outline their relevant qualifications and experience. The resume of the management team must be provided in an Appendix of the Technical Proposal, and must clearly and explicitly demonstrate relevant years of experience, including project descriptions, roles, responsibilities, and dates.

2. The Bidder must identify the "Key members" of the projects' technical and management teams and state their roles, specific qualifications and experience for the Work involved. Resumes of Key members must be provided in an Appendix of the Technical Proposal, and must clearly and explicitly demonstrate relevant years of experience, including project descriptions, roles, responsibilities, and dates. The Key members must have the required experience in each of the sub-domains, listed below:

    1. Satellite Flight Operations;
        a. Spacecraft Activity Planning and Contact Operations
        b. Satellite Health Maintenance, Monitoring and Control
        c. Orbit Maintenance, Monitoring and Control
        d. Flight System Configuration Management

    2. Satellite Data Management, Data Processing and Calibration; and
        a. Payload Data Order Handling and Acquisition Planning
        b. Payload Data Reception and Processing
        c. Payload Data Product Quality Control
        d. Data Reporting Support
        e. Data System Configuration Management

    3. Satellite Ground Systems Operations and Maintenance.
        a. Antenna Reservation System Operation
        b. Telemetry, Tracking and Commanding System Operation
        c. Network and Communication System Operation
        d. Operational System Configuration Management
        e. Life-Cycle Support

For P2 criterion, Proposals will be evaluated based on the following evaluation table. Each Element will be evaluated independently and assigned "Poor", "Minimal", "Adequate" or "Excellent" and receive the corresponding point value. The minimum score for each element is "Minimal". The total score for criteria P2 is the cumulative points for all the elements and the minimum passing score for the whole criteria P2 is presented in Table 1.

ANNEX B - EVALUATION PROCEDURES AND BASIS OF SELECTION

SATELLITE FLIGHT OPERATIONS AND DATA MANAGEMENT SERVICES

ELEMENTS	**Poor** **0 point**	**Minimal** **1 points per element**	**Adequate** **2 points per element**	**Excellent** **3 points per element**
1. Management	The requirement is not addressed or fully substantiated, or otherwise does not meet the level defined for “Minimal”	At least one (1) member of the management team has a minimum of five (5) years of management experience in aerospace within last ten (10) years.	At least two (2) members of the management team have has a minimum of seven (7) years of management experience in aerospace within last ten (10) years, specifically in Satellite Operations.	At least two (2) members of the management team have a minimum of ten (10) years of management experience in aerospace within last fifteen (15) years specifically in Satellite Operations.
2. Key members: Satellite Flight Operations	The requirement is not addressed or fully substantiated, or otherwise does not meet the level defined for “Minimal”	For all four (4) sub-domain activities listed, there is at least one (1) identified Key member with leadership responsibilities, who has a minimum of five (5) years working experience on that sub-domain activity.	For all four (4) sub-domain activities listed, there is at least one (1) identified Key member with leadership responsibilities, who has a minimum of seven (7) years working experience on that sub-domain activity.	For all four (4) sub-domain activities listed, there are at least two (2) identified Key members with leadership responsibilities, who each have a minimum of ten (10) years working experience on that sub-domain activity.
3. Key members: Satellite Data Management, Processing and Calibration	The requirement is not addressed or fully substantiated, or otherwise does not meet the level defined for “Minimal”	For all five (5) sub-domain activities listed, there is at least one (1) identified Key member with leadership responsibilities, who has a minimum of five (5) years working experience on that sub-domain activity.	For all five (5) sub-domain activities listed, there is at least one (1) identified Key member with leadership responsibilities, who has a minimum of seven (7) years working experience on that sub-domain activity.	For all five (5) sub-domain activities listed, there are at least two (2) identified Key members with leadership responsibilities, who each have a minimum of ten (10) years working experience on that sub-domain activity.

4. Key members: Satellite Ground Systems Operations and Maintenance	The requirement is not addressed or fully substantiated, or otherwise does not meet the level defined for “Minimal”	For all four (4) sub-domain activities listed, there is at least one (1) identified Key member with leadership responsibilities, who has a minimum of five (5) years working experience on that sub-domain activity.	For all four (4) sub-domain activities listed, there is at least one (1) identified Key member with leadership responsibilities, who has a minimum of seven (7) years working experience on that sub-domain activity.	For all four (4) sub-domain activities listed, there are at least two (2) identified Key members with leadership responsibilities, who each have a minimum of ten (10) years working experience on that sub-domain activity.

ANNEX B - EVALUATION PROCEDURES AND BASIS OF SELECTION

SATELLITE FLIGHT OPERATIONS AND DATA MANAGEMENT SERVICES

P3. Understanding and Implementation Approach

The purpose of this criterion is to assess the Bidder's understanding of the Work as well as the implementation approach being proposed. The primary objective of this requirement is to ensure that the implementation approach covers all aspects of the work described in the SOW and that it is performed in the most effective manner.

The Bidder must provide the following Elements:

1. A credible and implementable[2] Service Management and Implementation Plan (SMIP) that demonstrates an effective strategy to deliver the scope of work;
2. An efficient organisation chart with roles and responsibilities, and level of effort; and
3. A credible Risk Management Plan and Risk Register

The Elements should be based on recognized management tools most applicable to the required Services, such as a scope planning (Work Breakdown Structure (WBS) and Work Package Description (WPD)) and schedule development charts (e.g. Gantt chart). Equivalent contractor-developed, project-tailored tools/charts are also acceptable.

For P3 criterion, each Element will be evaluated independently and assigned "Poor", "Minimal", "Adequate" or "Excellent" and receive the corresponding point value. The total score for criteria P3 is the cumulative points for all the elements.

[2] implementable means that an evaluator, using his/her expertise, experience and the information solely provided in the Proposal, is of the opinion that the Bidder has clearly demonstrated that the work can be successfully conducted by following the plan.

ANNEX B - EVALUATION PROCEDURES AND BASIS OF SELECTION
SATELLITE FLIGHT OPERATIONS AND DATA MANAGEMENT SERVICES

ELEMENTS	Poor 0 points per element	Minimal 2 points per element	Adequate 4 points per element	Excellent 6 points per element
SMIP – Management Plan Elements + Organization + Risk Plan **(Organizing the Work)**	Management elements are not provided or are provided with insufficient detail.	Management elements are provided with limited details. The elements are barely credible or implementable, generating poor confidence in the ability to manage the Work.	Management elements are provided, but some of these are not sufficiently detailed. Most elements are credible and implementable, generating reasonable confidence in the ability to manage the Work.	Management elements are provided with extensive details. Each element is both credible and implementable, generating strong confidence in the ability to manage the Work.
SMIP – Implementation Plan Elements **(Understanding the Work)**	Implementation elements are not provided or are provided with insufficient detail.	Implementation elements are provided with limited details. The elements are barely credible or implementable, demonstrating a poor understanding of the work.	Implementation elements are provided, but some aspects are not sufficiently detailed. Most implementation elements are credible and implementable, demonstrating a reasonable understanding of the Work.	Implementation elements are provided with extensive details. These elements are both credible and implementable, demonstrating an excellent understanding of the Work.

P4. Performance Indicators

The purpose of this criterion is to assess the Bidder's understanding of the mission objectives, the operational priorities and the Service Level Agreement (SLA). In order to obtain technical merit within this section, the Bidder must populate the measurable metrics for the provided Mandatory Performance Indicators (PI) defined in the SLA.

In addition, the Bidder should propose new meaningful PI formulated as per the requirements in the SLA. PIs that are too similar to the ones provided in the SLA will be disregarded.

For P4 criterion, each Element (PI) will be evaluated independently and assigned the corresponding point value. The total score for criteria P4 is the cumulative points for all the elements and the minimum passing score for the whole criteria P4 is presented in Table 1.

ELEMENTS	Poor 0 to 2 point	Minimal 2.5 to 4.5 points	Adequate 5 to 6.5 points	Excellent 7-8 points
Mandatory Performance Indicator Metrics	Half (0.5) a point for each mandatory PI metric that is, well-formulated and easy to assess/monitor. **Maximum: 8 points**			
	Poor **0 point**	**Minimal** **1 point**	**Adequate** **2-3 points**	**Excellent** **4-5 points**
New Performance Indicators	One (1) point for each new proposed PI that is unique, well-formulated, operationally relevant and easy to assess/monitor. **Maximum: 5 points**			

P5. Value-Added Proposal

The purpose of this criterion is to assess the Proposal's alignment with key government objectives for added benefits to Canadians. In order to obtain technical merit within this section, the Proposal should propose:

1. Partnership with Canadian Small & Medium Enterprise (SME) with roles in the following sub-domains activities:
    a. Satellite Flight Operations
        i. Spacecraft Activity Planning and Contact Operations
        ii. Satellite Health Maintenance, Monitoring and Control
        iii. Orbit Maintenance, Monitoring and Control
        iv. Flight System Configuration Management

    b. Satellite Data Management
        i. Payload Data Order Handling and Acquisition Planning
        ii. Payload Data Reception and Processing
        iii. Payload Data Product Quality Control
        iv. Data Reporting Support
        v. Data System Configuration Management

    c. Satellite Ground Systems Operations and Maintenance
        i. Antenna Reservation System Operation
        ii. Telemetry, Tracking and Commanding System Operation
        iii. Network and Communication System Operation
        iv. Operational System Configuration Management
        v. Life-Cycle Support

2. Implementation of specific innovative changes to automate operational systems and processes in order to reduce operational cost and/or complexity, where:
    a. any required additional level of effort for this implementation must be costed as Additional Work according to the SOW, covered within the Task Authorization portion of the Contract, and provided in the Financial Proposal (this cost is not affecting Proposal's pricing score), and
    b. any required material to be provided by CSA will be subject to CSA internal authorizations and processes. (If this required material cannot be provided by CSA, then no points will be awarded for this innovation.)

3. Leveraging the Government infrastructure to increase the benefits to Canada, at no additional cost to CSA, while
    a. maintaining fulfillment of the Mandatory Work as per SOW,
    b. maintaining the required service level as per Service Level Agreement (SLA), and
    c. complying with the Security constraints and not imposing an additional security risk to CSA Missions, subject to CSA security approval.

ANNEX B - EVALUATION PROCEDURES AND BASIS OF SELECTION
SATELLITE FLIGHT OPERATIONS AND DATA MANAGEMENT SERVICES

For P5 criterion, each Element will be evaluated independently and assigned “Poor”, “Minimal”, “Adequate” or “Excellent” and receive the corresponding point value. The total score for criteria P5 is the cumulative points for all the elements.

Key Objective	Poor 0 point per objective	Minimal 2 points per objective	Adequate 4 points per objective	Excellent 5 points per objective
Partnership with Canadian SME	The Bidder does not provide a leading role to Canadian SME.	At least one (1) Canadian SME has a leading role in one (1) or more sub-domain activities.	At least two (2) Canadian SMEs have a leading role in one (1) or more sub-domain activities each.	At least two (2) Canadian SMEs have a leading role in two (2) or more sub-domain activities each.
Implementation of specific innovative changes (The changes must be described with enough details and deemed beneficial and implementable within the timeframe of the Contract)	The Bidder does not provide innovative changes with enough details, benefits or cannot be implemented within the timeframe of the Contract or has unrealistic expectations for CSA resources.	The Bidder proposes to implement one (1) specific innovative change to automate one system or process, with little to no operational cost savings.	The Bidder proposes to implement one (1) specific innovative change to automate one system or process, with operational cost savings that are greater than the implementation cost.	The Bidder proposes to implement two (2) or more specific innovative changes to automate several systems or process, with operational cost savings that are greater than the implementation cost.
Leveraging CSA infrastructure to increase benefits to Canada	The Bidder does not provide a leveraging proposition or it is detrimental to CSA.	The Bidder’s proposition is beneficial to the Bidder while introducing only minor/acceptable security risk to the CSA.	The Bidder’s proposition is mutually beneficial.	The Bidder’s proposition is mutually beneficial, and clearly identifies additional benefits to Canadians.

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
9F044-190433 20190433

Security Classification / Classification de sécurité
UNCLASSIFIED

Revision A

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A – CONTRACT INFORMATION / PARTIE A – INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine: **Canadian Space Agency (CSA)**	2. Branch or Directorate / Direction générale ou Direction: **Space Utilization Branch**
3. a) Subcontract Number / Numéro du contrat de sous-traitance: **NOT APPLICABLE**	3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant: **TBD**

4. Brief Description of Work / Brève description du travail
Flight Operations and Data Management Services for current Canadian missions (SCISAT, NEOSSAT, M3MSAT, RCM) as well as future missions

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées ?	☐ No / Non	☒ Yes / Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques ?	☐ No / Non	☒ Yes / Oui

6. Indicate the type of access required / Indiquer le type d'accès requis

6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS ? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	☐ No / Non	☒ Yes / Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes ? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	☒ No / Non	☐ Yes / Oui
6. c) Is this a commercial courier or delivery requirement with **no** overnight storage? S'agit-il d'un contrat de messagerie ou de livraison **sans** entreposage de nuit?	☒ No / Non	☐ Yes / Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada ☒	NATO / OTAN ☐	Foreign / Étranger ☐

7. b) Release restrictions / Restrictions relatives à la diffusion

No release restrictions / Aucune restriction relative à la diffusion ☒	All NATO countries / Tous les pays de l'OTAN ☐	No release restrictions / Aucune restriction relative à la diffusion ☐
Not releasable / À ne pas diffuser ☐		
Restricted to: / Limité à : ☐	Restricted to : Limité à : ☐	Restricted to : Limité à : ☐
Specify country(ies) : / Préciser le(s) pays :	Specify country(ies) : / Préciser le(s) pays :	Specify country(ies) : / Préciser le(s) pays :

7. c) Level of information / Niveau d'information

PROTECTED A / PROTÉGÉ A ☒	NATO UNCLASSIFED / NATO NON CLASSIFIÉ ☐	PROTECTED A / PROTÉGÉ A ☐
PROTECTED B / PROTÉGÉ B ☒	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ☐	PROTECTED B / PROTÉGÉ B ☐
PROTECTED C / PROTÉGÉ C ☐	NATO CONFIDENTIAL / NATO CONFIDENTIEL ☐	PROTECTED C / PROTÉGÉ C ☐
CONFIDENTIAL / CONFIDENTIEL ☐	NATO SECRET / NATO SECRET ☐	CONFIDENTIAL / CONFIDENTIEL ☐
SECRET / SECRET ☒	COSMIC TOP SECRET / COSMIC TRÈS SECRET ☐	SECRET / SECRET ☐
TOP SECRET / TRÈS SECRET ☐		TOP SECRET / TRÈS SECRET ☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
9F044-190433
Security Classification / Classification de sécurité
UNCLASSIFIED

Revision A

PART A *(Continued)* / PARTIE A *(suite)*

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets?
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS ?
If Yes, indicate the level of sensitivity :
Dans l'affirmative, indiquer le niveau de sensibilité: **SECRET**

☒ No / Non ☐ Yes / Oui

9. Will the supplier require access to extremely sensitive INFOSEC information or assets?
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate?

☒ No / Non ☐ Yes / Oui

Short Title(s) of material / Titre(s) abrégé(s) du matériel:
Document Number / Numéro du document:

PART B – PERSONNEL (SUPPLIER) / PARTIE B – PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la Sécurité du personnel requis

☒	RELIABILITY STATUS COTE DE FIABILITÉ	☐	CONFIDENTIAL CONFIDENTIEL	☒	SECRET SECRET	☐	TOP SECRET TRÈS SECRET
☐	TOP SECRET – SIGNIT TRÈS SECRET - SIGNIT	☐	NATO CONFIDENTIAL NATO CONFIDENTIEL	☐	NATO SECRET NATO SECRET	☐	COSMIC TOP SECRET COSMIC TRÈS SECRET
☐	SITE ACCESS ACCÈS AUX EMPLACEMENTS						

Special comments:
Commentaires spéciaux: _____

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE: Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10.b) May unscreened personnel be used for portions of the work?
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail?

☒ No / Non ☐ Yes / Oui

If Yes, will unscreened personnel be escorted?
Dans l'affirmative, le personnel en question sera-t-il escorté?

☐ No / Non ☐ Yes / Oui

PART C – SAFEGUARDS (SUPLIER) / PARTIE C – MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises?
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS?

☐ No / Non ☒ Yes / Oui

11.b) Will the supplier be required to safeguard COMSEC information or assets?
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC?

☒ No / Non ☐ Yes / Oui

PRODUCTION

11.c) Will the production (manufacture, and/or repair and/or modification of PROTECTED and/or classified material or equipment occur at the supplier's site or premises?

☒ No / Non ☐ **Yes / Oui**

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11.d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data?

☐ No / Non ☒ Yes / Oui

11.e) Will there be an electronic link between the supplier's IT systems and the government department or agency?
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui ministère ou de l'agence gouvernementale?

☒ No / Non ☐ Yes / Oui

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
9F044-190433
Security Classification / Classification de sécurité
UNCLASSIFIED

Revision A

For users completing the form **manually** use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire **manuellement** doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form **online** (via the internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire **en ligne** (par internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL / NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET / COSMIC TRÈS SECRET	PROTECTED / PROTÉGÉ A	PROTECTED / PROTÉGÉ B	PROTECTED / PROTÉGÉ C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET
Information / Assets Renseignements / Biens	X	X														
Production																
IT Media / Support TI	X	X														
IT Link / Lien électronique																

12.a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

☒ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le present formulaire en indiquant le niveau de Sécurité dans la case intitulée «Classification de sécurité» au haut et au bas du formulaire.

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☒ No / Non ☐ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le present formulaire en indiquant le niveau de sécurité dans la case intitulée «Classification de sécurité» au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

PART D – AUTHORIZATION / PARTIE D - AUTORISATION

13. Organization Project Authority / Chargé de projet de l'organisme

Name (print) – Nom (en lettres moulées)	Title – Titre	Signature	
GUENNADI KROUPNIK	**RCM PROJECT MANAGER**		
Telephone No. – N° de telephone	Facsimile No. – N° de télécopieur	E-mail address – Addresse courriel	Date
450-926-4614	N/A	**guennadi.kroupnik@canada.ca**	26 NOV. 2019

14. Organization Security Authority / Responsable de la Sécurité de l'organisme

Name (print) – Nom (en lettres moulées)	Title – Titre	Signature	
ANNIE DESROCHERS	**A/ Departmental Security Officer (CSA)**		
Telephone No. – N° de telephone	Facsimile No. – N° de télécopieur	E-mail address – Addresse courriel	Date
450-926-6448	450-926-4885	**annie.desrochers@canada.ca**	2019/11/27

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached?
Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes ?
☐ No / Non ☒ Yes / Oui

16. Procurement Officer / Agent d'approvisionnement

Name (print) – Nom (en lettres moulées)	Title – Titre	Signature	
Caroline Niquette			
Telephone No. – N° de telephone	Facsimile No. – N° de télécopieur	E-mail address – Addresse courriel	Date
	N/A		

17. Contracting Security Authority / Autorité contractante en matière de sécurité

Name (print) – Nom (en lettres moulées)	Title – Titre	Signature	
Telephone		dresse courriel	Date

Paul Lepinski
Agent à la Sécurité des contrats | Contract Security Officer
Programme de la Sécurité des contrats | Contract Security Program
Téléphone : 613 957-1294 | *paul.lepinski@tpsgc-pwgsc.gc.ca*

UNCLASSIFIED

RADARSAT Constellation Mission (RCM)
and
Project Polar Epsilon 2 (PE2)

SECURITY CLASSIFICATION GUIDE

Canadian Space Agency

&

Department of National Defence

April 11, 2019

This Page Intentionally Left Blank

Table of Contents

1 INTRODUCTION

1.1 PURPOSE

The RCM and PE2 Security Classification Guide (SCG) is a working document that guides the Canadian Space Agency (CSA), the Department of National Defence (DND) as well as other agencies/organizations involved in the handling of classified information related to the RCM and PE2 capability. This SCG has been written to provide classification guidance for the RCM and PE2 projects based on information that is most likely to be encountered in the design, development, operations and maintenance phases of these projects. It is not intended to be an exhaustive document covering all aspects of security for RCM and PE2 projects and does not relieve anyone from complying with the Government of Canada (GC) directives on security. If a discrepancy exists between this document and a GC directive, the GC directive will have precedence.

1.2 DOCUMENT CONVENTIONS

This SCG is unclassified.

1.3 ACRONYMS AND ABBREVIATIONS

A	
AIS	Automatic Identification System
C	
CCD	Canadian Cryptographic Doctrine
CCI	Controlled Cryptographic Item
CDS	Cross Domain Solution
CFU	Cryptographic Flight Unit
CGU	Cryptographic Ground Unit
CICA	CSE Industrial COMSEC Account
COMSEC	Communications Security
cPE2	Classified Polar Epsilon 2 system
CSE	Communications Security Establishment
CSNI	Consolidated Secret Network Infrastructure
CSS	Common Subsystem
E	
EODMS	Earth Observation Data Management System
F	

F/W	Firewall
G	
GC	Government of Canada
H	
HTTPS	Hypertext Transfer Protocol Secure
I	
IDS	Intrusion Detection Systems
ISM	Industrial Security Manual
IT	Information Technology
ITSD	IT Security Directive
K	
KEK	Key Encryption Keys
L	
LEOP	Launch and Early Operations Phase
O	
O/S	Operating System
OHS	Order Handling Subsystem
P	
PCF	Primary Control Facility
PE2	Polar Epsilon 2
PKI	Public Key Infrastructure
R	
RCM	RADARSAT Constellation Mission
S	
SAR	Synthetic Aperture Radar
SCG	Security Classification Guide [this document]
SDAC	Science Data Access Control
STE	Secure Terminal Equipment
STM	S-Band Telemetry
T	

TC	Telecommand
TEK	Traffic Encryption Keys
U	
uPE2	Unclassified Polar Epsilon 2 system
UNTEK	Unclassified Traffic Encryption Keys
V	
VRF	Virtual Routing and Forwarding
X	
XTM	X-Band Telemetry

1.4 DEFINITIONS

Term	Definitions
Cryptographic Flight Unit (CFU)	The CSE approved cryptographic unit on-board the RCM satellite which encrypts/decrypts the TeleCommand (TC), S-Band Telemetry (STM) and X-Band Telemetry (XTM) communication links.
Cryptographic Ground Unit (CGU)	The CSE approved cryptographic unit used in a ground facility to decrypt/encrypt the TC, STM and XTM communication links.
Data	Any information that is used by personnel, ground segment equipment/systems or space segment equipment/systems for interpretation, transmission, configuration, insight, calculations or in support of activities of any kind.
Information	Value-added facts which are used to convey meaning or particulars about a specific element. Information can be electronic, physical or verbal.

Term	Definitions
LEOP	The Launch and Early Orbit Phase (LEOP) of the RCM mission is the phase during which each RCM spacecraft is launched into its initial orbit, its essential systems activated and checked-out, and a sequence of events carried out which will place the spacecraft in an orbit, attitude and configuration suitable for the commencement of activities that ready the spacecraft for routine operations. The official start of each LEOP campaign is considered to begin at Launch Readiness Review, and is considered complete when LEOP performance criteria (such as deployment of Solar panel SAR antennas and AIS Antenna, etc….) are met and a successful Go/No-Go meeting is held.
Science Data	Data included in the X-Band signals transmitted by the RCM Spacecraft. This data includes Payload Data (raw SAR, raw AIS and OBP AIS) from the Payload and Ancillary Data from the Bus which is subdivided into Bus Ancillary Data (spacecraft time, attitude and positional information), Payload Ancillary Data (payload telemetry and pass-through data derived from the Activity Requests received from the Payload) and Image Ancillary Data (time and pulse setting information with associated echo and replica data packets).
Metadata	Additional information associated with the Science Data for the purposes of creating and archiving image products which can include: geographic extents of the data, processing parameters, Downlink Segment ID, catalogue update and visibility restrictions etc.

Term	Definitions
Order data	The content of specific Order fields when considered individually are considered UNCLASSIFIED. When Classified Order contents are considered in sub-combinations these are UNCLASSIFIED if those Order contents do not contain all of the following: Order Classification, Identification of the geographical area of interest and the time period within which the Science Data must be collected. Once a classified Order is submitted the aggregate of all the information contained in that Order is considered SECRET.

1.5 DOCUMENTS CONVENTIONS

In the context of this document, the following words have the specific meaning indicated:

a) "must" is used to indicate a mandatory requirement.

b) "should" is used to indicate a preferred alternative that is not mandatory.

c) "may" is used to indicate an option.

d) "will" is used to indicate a statement of intention or fact.

2 DOCUMENTS

2.1 REFERENCE DOCUMENTS

TABLE 1: REFERENCE DOCUMENTS

RD No.	Document Title	Link
1.	Security of Information Act http://lois-laws.justice.gc.ca/eng/acts/O-5/index.html	Sec of Inf Act
2.	The Government of Canada (GC) Policy on Government Security (PGS), Date modified 2012-04-01 http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578&section=text	PGS
3.	IT Security Directive for the Application of Communications Security Using CSE-Approved Solutions (ITSD-01A) https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsd01a-eng_0.pdf	ITSD-01A

RD No.	Document Title	Link
4.	IT Security Directive for the Control of COMSEC Material in the Government of Canada (ITSD-03A), Effective date March 2014 https://cse-cst.gc.ca/en/node/1264/html/22979	ITSD-03A
5.	IT Security Directive for the Control of COMSEC Material in the Canadian Private Sector (ITSD-06A) https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsd-06a-eng_0.pdf	ITSD-06A
6.	IT Security Directive for the Ordering of Cryptographic Key (ITSD-09) Note: ITSD-09 will be released imminently.	ITSD-09
7.	RCMP G1-001 - Security Equipment Guide (Access is **restricted** to Government of Canada departments and agencies)	
8.	RCMP Guide G1-009, Standard for the Transport and Transmittal of Sensitive Information and Assets *(Access is **restricted** to Government of Canada departments and agencies)*	
9.	Industrial Security Manual http://www.tpsgc-pwgsc.gc.ca/esc-src/msi-ism/index-eng.html	ISM
10.	National Defence Security Orders and Directives (NDSOD) (available on demand through PE2)	
11.	Controlled Goods Program https://www.tpsgc-pwgsc.gc.ca/pmc-cgp/index-eng.html	CGP
12.	COMSEC Material Control Policy, Standards and Procedures (INFOSEC (2E)) http://admim-smagi.mil.ca/assets/IM_Intranet/docs/en/security/comsec/infosec-2e.pdf	(INFOSEC (2E)
13.	Operational Security Standard on Physical Security https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12329	Operational Security Standard on Physical Security
14.	Harmonized Threat and Risk Assessment Methodology (HTRA) (https://cyber.gc.ca/sites/default/files/publications/tra-emr-1-e.pdf	HTRA

3 CATEGORIZATION

The highest level of classification for the RCM system and Polar Epsilon 2 Classified System (cPE2) is SECRET. It is the Crown's responsibility to determine the criteria for the classification and declassification of information for the RCM and the Polar Epsilon 2 systems. The originator of the material (document Owner) is responsible for its classification/declassification based on this SCG. If an originator suspects that some information/data is not covered by this SCG, that originator must contact their local RCM or PE2 authority to determine if the SCG should be amended; industrial personnel must communicate via their Company Security Officer iaw the ISM while GC personnel may contact those authorities directly.

4 CLASSIFICATION

Personnel must classify information in accordance with Canadian Policies. Airbus referenced documentation will be classified according to the applicable RCM and/or PE2 contracts.

There are two (2) main types of sensitive information designations used by the Government of Canada: Classified and Designated. The access and protection of both types of information is governed by the Security of Information Act (RD-01). To access the information, a person must have the appropriate level of clearance and a need to know.

The Policy on Government Security (PGS) (RD-02) gives directions to effectively manage security activities within departments and contribute to effective government-wide security management.

5 GUIDELINES

5.1 General

The Government of Canada's RCM satellites and ground system, through the cPE2, will provide a capability to generate and use information up to SECRET level for space-based surveillance and reconnaissance purpose. The cPE2 will order, receive, process, exploit, disseminate and archive RCM Synthetic Aperture Radar (SAR) data at a classified level of up to SECRET.

Most of the RCM data will not be sensitive (i.e. it will be UNCLASSIFIED). However, there could be instances where a combination of contextual circumstances and acquisition parameters would have RCM generate orders, remote sensing data and/or metadata that would contain sufficiently sensitive information to meet the injury test leading to the classification at a SECRET level and a requirement to protect the data accordingly. In these circumstances the originators of the acquisition request(s) are responsible to ensure they are submitted using the cPE2 capability vice uPE2. For example, this may happen through:

I. DND's nominal usage plans; or
II. Exceptional and unforeseen circumstances situations where RCM could be used in a national or international security context such as in support of theater of operations of the Canadian Armed Forces or those of our close allies and partners.

RCM is a highly valuable National Security asset. As such GC stakeholders have also determined that these assets warrant tight security measures to ensure continued positive control, health and safety of the spacecraft that form part of RCM. Hence security measures have been added to protect the integrity and availability of telecommand and telemetry data to and from the spacecraft.

Unless specified in this SCG, all hardware, software, documentation and algorithm components of the RCM and PE2 systems are UNCLASSIFIED except for the CGU/CFU design[1]. Further guidance about the classified Acquisition Mask security classification is provided in section 5.6.

All unclassified hardware and software that has been exposed to classified data becomes classified to the highest level of that data. Classified hardware and software will always be classified regardless of whether it has been exposed to classified data through or not. If information (i.e. operational data) is required to be declassified to support debugging or anomaly resolution, it will be done so by the respective data owner (CSA or DND).

5.2 Handling of classified information:

SECRET information must be treated with appropriate measures approved by the GC directives.

SECRET documents are not based on the type of document (e.g. Design document, Test procedure and reports, validation reports) but rather on the nature of the information that it contains. Most of the baseline design of cPE2 is derived from unclassified PE2 and RCM documentation. Instances of cPE2 and RCM design which are classified will be delivered to Canada in a separate document, classified appendix or an equivalent, as long as the resulting combination of documents is usable by Canada for the purposes it is delivered for. If separation of classified and unclassified information would make the document unusable by Canada, it must be delivered in a combined form. In some special cases, a document initially provided to RCM will require updates that may include a small amount of classified information. In these cases, the initial document may retain the original classification but provide the classified content as a classified

[1] From CSE: The crypto will be at the classification of the highest classification of key or data on the crypto. For CGU-X, the classification of the unit is unclassified when powered off and then subsequently powered on again – until key is loaded and data processed for the first time. For testing, it will be CCI unclassified.

addendum. Consequently, the documents without the classified addendum should be marked “UNCLASSIFIED without attachment” but with the addendum, the document becomes classified to the highest security classification of the addendum included and should be marked appropriately. The addendum should also be clearly marked with its security classification.

NOTE: An unclassified document may refer to a separate classified document, so long as the fact of the existence of that classified document is UNCLASSIFIED and no classified reason for accessing that other document is given. (For example: The reason given for accessing a classified document must not state that the vulnerabilities/weaknesses are given in that classified document, as that identifies the fact that there is a classified vulnerability.)

5.3 Confidentiality

The following statements provide high-level guidance on the RCM and PE2 capability:

The fact that a classified order can be placed for classified RCM SAR data is UNCLASSIFIED.

The fact that satellites can downlink classified data is UNCLASSIFIED.

The fact of the existence of the classified portion of RCM and cPE2 is UNCLASSIFIED.

The overall design and associated documentation of the RCM and PE2 is UNCLASSIFIED, with certain exceptions that is either Protected or Classified. Classification of document is done on a document-by-document basis, for example the RCM Key Management Support Plan is classified.

The fact of the existence of contracts for the design, implementation, operation and maintenance of the classified portion of RCM and of cPE2 is UNCLASSIFIED. The contents of these contracts will be UNCLASSIFIED, unless it is necessary to include classified material in the contracts; if so, only the classified contents will be classified, though the contract documents will be properly marked to reflect the fact that the contract contains classified material.

The existence of each classified order being planned or placed is SECRET.

The list of authorized users that could request a classified order is SECRET. Format of the list is UNCLASSIFIED.

The processed products resulting from a classified order are SECRET, including images and ship detections.

Any intermediate products between decrypted classified Science Data and processed products are SECRET.

The cPE2 will provide a capability to declassify Science Data and to transfer it to the unclassified RCM archive. The fact that the Science Data has been declassified is UNCLASSIFIED.

All inter-facility connections making-up the RCM/PE2 VRF network will be protected to the level of Protected A. Inter-facility connection between cPE2 and cRCM network will be protected to the level of SECRET. Any hardware (i.e. encryptors) required to achieve SECRET level protection will be provided by the Government of Canada (i.e. DND or CSA).

5.4 Security Classification distinction beyond RCM ORR

For purpose of integration RCM GS subsystems are considered UNCLASSIFIED up to the point of the RCM Final Operational Readiness Review (ORR). Following the RCM ORR, RCM GS subsystems must assume their appropriate classification and physical security zoning will apply accordingly.

5.5 System design, testing and verification

RCM and PE2 Information kept at a high level may remain unclassified.

"High level" refers to schematics or information which show or describe the boundaries of a System or Subsystem, the inputs and outputs of the System or Subsystem, the surrounding interacting Systems or Subsystems, environment and activities, but which do not detail any of the internal structure. High level information can include relationships and interoperability with other Systems, Subsystems or groups on the understanding that explicit functional details are not included. High level also includes commercial product names and versions (if non-PE2/RCM specific) and applicable standards and guidelines when applied in accordance with industry best practices. Lower level information is unclassified except where specific criteria contained within the SCG require a SECRET classification.

"Vulnerability" is defined as "*A flaw or weakness in a system's design, implementation, or operation and management that could be exploited to violate the system's security policy*". A vulnerability is a weakness which allows an attacker to reduce an information system's confidentiality, integrity or availability.

The existence of a vulnerability that affect the classified RCM or cPE2 systems must be SECRET.

Verification, testing and integration of the RCM and PE2 development system can be conducted at the UNCLASSIFIED level. Documents, test plans, test results associated with the unclassified verification, testing and integration will also be UNCLASSIFIED.

Test results and reports with the defined purpose of discovering/disclosing potential vulnerabilities of RCM and PE2 classified or unclassified systems must be delivered in SECRET documents. Example – vulnerability assessment & penetration testing. Although portions of these reports may be UNCLAS, classification conventions of (U) and (S) will be observed within the document.

The knowledge of failures of certain items of unclassified testing of IT oriented requirements (i.e. CSS requirements) may be of serious enough importance to require classification of the test and its result. For example, a failure which can and would be fixed may be assessed a low risk of injury, however if serious concerns are identified as part of the injury assessment done in accordance with ITSG-33, Annex 2, Section 3.5.1., the procedures of the tests should be amended to provide additional controls. A mitigation to that problem could be to introduce a risk assessment activity prior to unclassified testing of IT being conducted. Test results and reports as part of the system test activities, that identify the existence of vulnerabilities in a deployed/operational instance of RCM and PE2 classified or unclassified systems must be marked as SECRET.

If during the course of a test, discussion, etc. it is believed that the relevant data is classified, then that data should be provided to the appropriate local authority who can assist in the classification. Such data may be provided in a separate classified document, appendix or addendum or an equivalent.
Example - If a test is run and the plaintext crypto key is visible. If the test is with development key, the test result/observations are NOT classified but there would be a vulnerability if Test or Operational key is used. Note that an operational key will NOT be used during a test.

Any test of or involving MPS which contains a mix of unclassified and classified software, must be conducted in an environment accredited at the SECRET level. If the classified software is not loaded, the MPS may be tested under unclassified conditions, so long as the processor(s) have not been previously used for classified processing or have previously contained classified software. Note that any medium containing the classified software is itself classified and its incorporation or use in a test or test configuration means that the test must be conducted in a location accredited to SECRET level.

The RCM Ground Segment (GS) and PE2 source code are UNCLASSIFIED.

The cPE2 network and its information systems architecture and the cross-domain solutions (CDS) design are classified SECRET and the testing of their classified elements of design is also SECRET.

Any aspect of training that include classified information, must be conducted in an appropriate secure location.

5.6 Classified Acquisition Mask

The classified Acquisition Mask is the proposed solution by the contractor to hide the existence of classified orders.

The facts that classified Acquisition Masks in general (and its function) exist are UNCLASSIFIED.

The process for the operator to build a classified Acquisition mask is UNCLASSIFIED.

The existence of classified Orders is classified SECRET. If Acquisition Masks are created to hide the classified Acquisition Orders during system operations, then specific Acquisition Masks and their associated data are SECRET.

The classified Acquisition Mask response logic, to ensure that users of the UNCLASSIFIED PE2 and RCM systems cannot be aware of existing classified Acquisition Masks and Orders when an order is placed via the uOHS within a classified Acquisition Mask, is UNCLASSIFIED. The entire response logic for the development is to be handled as UNCLASSIFED from concept, to source code, compiler, design and execution.

The design of the interfaces between the classified OHS and the classified Acquisition Mask response logic and between the classified Acquisition Mask response logic and the MPS is UNCLASSIFIED.

5.7 IT Security Architecture

All information concerning the design of the PE2 and RCM IT network is considered UNCLASSIFIED except the following:

- Design, implementation and configuration details of the RCM and PE2 Cross-Domain Solution – SECRET;
- Configuration of RCM Intrusion Detection Systems (IDS) – PROTECTED B;

- Configuration of uPE2 Intrusion Detection Systems (IDS) – PROTECTED B;
- Configuration of cPE2 Intrusion Detection Systems (IDS) – SECRET;
- Hostnames for uPE2 - UNCLASSIFIED if the naming convention obfuscates the purpose of the host. If this cannot be achieved, then the hostname should be treated as PROTECTED B. The hostname and detailed description of its purpose/function must NOT be published in an UNCLAS document
- Hostnames for cPE2 is SECRET;
- Aggregate of RCM IP addresses – PROTECTED B;
- Aggregate of uPE2 IP addresses – PROTECTED B;
- Aggregate of cPE2 IP addresses – SECRET;
- Configuration of uPE2 IP addresses – PROTECTED B;
- Configuration of cPE2 IP addresses – SECRET;
- Detailed design of RCM Out-Of-Band systems – PROTECTED B;
- Detailed configuration of RCM Operating System (O/S) hardening other than Industry best practices - PROTECTED B;
- Detailed configuration of uPE2 Operating System (O/S) hardening other than Industry best practices – PROTECTED B;
- Detailed configuration of cPE2 Operating System (O/S) hardening other than Industry best practices - SECRET;
- Configuration of RCM Firewalls (F/W) other than the Classified F/W – PROTECTED B; and,
- Configuration of PE2 Firewalls (F/W) other than the Classified F/W – PROTECTED B.
- Configuration of the RCM and PE2 Classified Firewall – SECRET;

5.8 Network security

The manufacturer and model of firewall units for the PE2 system is UNCLASSIFIED. The classification for the firewalls on the classified DND/CAF's CNET/CSNI network is SECRET.

Network Device configuration settings and Network Architecture Diagrams with IP addresses and context - SECRET for cPE2, PROTECTED B for uPE2.

6 OPERATIONAL TELEMETRY / TELECOMMAND

From just prior to the Polar Epsilon 2 classified System Verification Review where live (RED) crypto keys are loaded for classified orders and onwards, operational RCM telemetry / telecommand data are classified SECRET with the following exceptions:

a. when absolute time and/or position information is removed in accordance with the approved process. Note - The process will be captured in CSA-RC-PL-0081 RCM Process to remove sensitive data from Telemetry and

Telecommand Data (Protected B) and will include limiting the dataset to a maximum observation window defined by the Packet Classification Guide; or

b. the packets have been deemed to be UNCLASSIFIED in the Packet Classification Guide.

Irrespective of the timeframe the following telemetry/telecommand related to operational keys will need to be handled as SECRET:

- Some of the fields within the 64-bytes of the CFU Housekeeping Status Summary as listed in Section 6 of L1S0113981-ASTR - CFU Telecommand and Telemetry List (refer to Attachment 1); and
- Some of the fields within the 66-bytes of the CGU Health Status as listed in Section 9 of ICD-DG0114710-ASTR - RCM CGU Command and Monitor Interface Control.

Trending or averaging of telemetry data may be declassified in accordance with the approved process.

Simulated telemetry/telecommand data is considered unclassified.

7 O&M

Passwords, combinations, PINs and similar information are classified at the security level of the information or material that they protect but no less than PROTECTED B.

Maintenance information showing status of classified RCM and PE2 capability is UNCLASSIFIED.

O&M statistics for the cPE2 are UNCLASSIFIED.

Operations reports for the cPE2 are SECRET.

Operation reports for the uPE2 are UNCLASSIFIED.

System maintenance reports for the uPE2 and cPE2 are UNCLASSIFED unless it identifies a vulnerability as per Section 5.5.

8 DATA

The Science Data Access Control (SDAC) is considered PROTECTED B.

Science Data, metadata, order data or other data related to classified orders are SECRET.

The RCM Earth Observation Data Management System (EODMS) and all messages to and from this system are considered UNCLASSIFIED. The unclassified RCM Science Data archive and its contents are UNCLASSIFIED.

The raw Science Data resulting from a classified order is SECRET.

The classified RCM Science Data archive and its contents are SECRET. Any listing of these contents is SECRET.

AIS: The raw AIS data produced by the AIS sensor on board the spacecraft is deemed to be UNCLASSIFIED, but raw and OBP AIS data produced during the execution of a classified order must be handled as SECRET.

Classified Order data may only be entered in the classified OHS and its data is SECRET. The order template itself is UNCLASSIFED. The fields necessary to build a classified or unclassified order such as Time, Location, Beam mode, Customer reason for order are UNCLASSIFIED, however once a field is filled in with operational data for a classified order, it is SECRET. Prior to having any operational classified data flow through the cOHS, UNCLASSIFIED data can be created and entered in the classified OHS for UNCLASSIFIED testing purpose, the completed fields are UNCLASSIFIED and they must be identified as such in the order if it is possible. Note that each field does not need to be identified as UNCLASSIFIED but a predominant field to indicate the entire order is UNCLASSIFIED would meet this requirement.

Once classified operational data flow through the system, UNCLASSIFIED testing will no longer be possible as the system components (both hardware and software) have become classified to the highest level of the classified data. Software installed in the cOHS that was UNCLASSIFIED prior to the classified operational orders flow through becomes classified to the highest level of that data. UNCLASSIFIED software and/or updates can be uploaded in the cOHS but they will become classified to the same level as the software in the cOHS once installed.

Encrypted classified Science Data being transmitted in the black is to be treated as UNCLASSIFIED.

9 COMSEC

In order for the system to be designed, built and tested, the Contractor will require information about cryptographic systems, processes and test keys to integrate cryptographic systems, all up to the level of SECRET. The Contractor will not

require actual GC cryptographic keys, since those will only be kept and used under GC custody and control except for Secure Voice use in support of CPE2.

Cryptographic equipment (aka Controlled Cryptographic Item (CCI)) are controlled goods and must as a minimum be managed under the guidance of the Controlled Goods Program. Specifically, cryptographic equipment must be handled and managed iaw its associated Canadian Cryptographic Doctrine (CCD) issued by the Communication Security Establishment (CSE). Specific CCDs will be made available to the contractor via the CSE Industrial COMSEC Account (CICA) or DND.

CSE Reference documentation that should be reviewed are ITSD-01A and ITSD-06A (available at https://www.cse-cst.gc.ca/en/publication/list/).

9.1 Encryption Keys:

Keys will be required for the following systems: Phone (STE or OMNI), TACLANE, CFU, CGU-X and CGU-S. Discussion about encryption keys kept at a high level may remain UNCLASSIFIED. Development and test keys will be UNCLASSIFIED while operational keys will be classified SECRET.

Encryption Keys are to be handled and secured at the classification level of the key. Short Titles are UNCLASSIFIED. Long Titles are normally UNCLASSIFIED. For additional direction contact CICA.

RCM Crypto are of two types: Type 1 Crypto (CFU/CGU) or Commercial (software-based) crypto. Commercial crypto are UNCLASSIFIED in all cases. The CFU/CGU, when not keyed are UNCLASSIFIED, when keyed they are classified to the same level as the loaded key.

RCM Keys targeted for use on Type 1 Crypto are of three types based on their usage: Development keys, test keys and operational keys. Development keys are produced by the contractor (or sub-contractors); in all cases these are UNCLASSIFIED. Test keys are provided by CSE and are UNCLASSIFIED. There are two types of operational keys: the first type is the UNTEK and is UNCLASSIFIED and the other type is furnished by CSE and is classified SECRET.

Additionally, keys used with Type 1 Crypto can be subdivided into two groups based on their purpose: Traffic Encryption Keys (TEKs) and Key Encryption Keys (KEKs). Keys in the “clear” are as per the above paragraph. BLACK keys (TEKs encrypted with a KEK or KEKs encrypted with a KEK) are considered Protected A. The Protected A rule is a CSE rule (ITSD 03 Annex A).

A key in a BLACK state may be transmitted over any:
- Classified network

- Government of Canada departmental network that has been accredited to protect PROTECTED A or PROTECTED B information, or
- public network (e.g. the Internet), as long as it is protected minimally with Public Key Infrastructure (PKI) encryption or Hypertext Transfer Protocol Secure (HTTPS) encrypted connection.

RCM Keys targeted for use on Commercial-grade Crypto are UNCLASSIFIED in all cases.

Note: "Storage, Handling and Transportation of COMSEC material must be in accordance with ITSD-03A and ITSD-06A only."

10 MARKING AND LABELLING (other than COMSEC)

As per the NDSOD Chapter 6, SECRET documents and data products of PE2 must be labelled CAN SECRET.

Security Warning for Contractor Produced Publications (Chap5 ISM)

Unless otherwise specified in the contract, where a contractor is producing a publication on behalf of the Government of Canada that contains PROTECTED information, the following warning will be printed on both the front cover and title page:

This publication contains PROTECTED information which must be safeguarded under the provisions of Canada's Government Security Policy. It has been produced by (contractor's name) under the provisions of (contract number or other authorization) on behalf of (the Government of Canada or department), as applicable. Release of this publication, or of any information contained herein, to any person not authorized by the originating agency to receive it is prohibited.

All CLASSIFIED publications, pamphlets, handbooks or brochures which are produced by a contractor on behalf of the Government of Canada must have, in addition to the regular security classification markings as prescribed in this chapter, the following security warning on both the front cover and the title page:

"This publication contains CLASSIFIED information affecting the national interest of Canada. It has been produced by (contractor's name) under the provisions of (contract number or other authorization) on behalf of (the Government of Canada or department, as applicable) and is to be safeguarded, handled and transported in accordance with Government Security Policy. Release of this publication, or of any CLASSIFIED information contained herein, to any person not authorized to receive it is prohibited by the Security of Information Act."

The UK, Canadian and US standards for marking classified information are similar except for potential caveats. For the RCM and PE2, no caveat is required.

For non-classified information, the marking standards vary. Documents should be marked according to the nationality of origin and NOT re-classified or re-marked in any manner.

Canadian material marked “Protected A” should be handled in the UK as “Restricted” but not “UK Restricted”.

The following procedures are from the ISM Chap 5 (Marking) except for #9.

1. for PROTECTED information, mark the word "PROTECTED" in the upper right corner of the face of the document and where required, with the letter "A", "B" or "C" to indicate the level of safeguarding;
2. for SECRET information, mark the classification in the upper right corner of each document page;
3. mark covering or transmittal letters or forms or circulation slips to show the highest level of classification or protection of the attachments;
4. mark all materials used in preparing PROTECTED and CLASSIFIED information. Such material includes notes, drafts, carbon copies and photocopies;
5. the letters used in marking should be larger than those used in the text of the document;
6. in addition to marking individual pages as stipulated above, documents must be appropriately marked on the outside of both the front and back covers;
7. **loose documents** must be marked on every sheet;
8. **charts, maps, drawings, etc**. must be prominently marked near the margin or title block in such manner that the marking is clearly visible when the document is folded; and
9. Protective markings on paragraphs are known as paragraph grading indicators and may appear in brackets at the start of each paragraph. The protective marking can be written in full or abbreviated by the first letters of the markings and should be the same colour as the text within the document. For instance, (S/REL FVEY) for SECRET or (U) for UNCLASSIFIED.

11 PROCESSING OF SENSITIVE INFORMATION ON AN IT SYSTEM

In accordance with the Treasury Board policies on Government security, all Level II (SECRET and above) information technology systems must be operated within a security or high security zone. If classified processing is required but is not supported by the current SRCL, contact the applicable Contract’s Technical Authority.

12 STORAGE AND HANDLING

The storage and handling of PROTECTED and CLASSIFIED information and assets will be in accordance with the Industrial Security Manual (RD-16) for industry and in accordance with respective Departments directives for GC organizations.

When information is generated, reproduced, edited, viewed, processed, stored or otherwise accessed, consideration must be given to the security of the assets, equipment and environment where these activities will take place. Information must only be handled in physical security and electronic zones that are appropriate for the sensitivity of that information

13 TRANSPORT AND TRANSMITTAL

Sensitive information must be safeguarded when it is being physically transported from one location to another, and also when it is being transmitted across computer networks, phone lines or any other transmission medium.

Maintaining authorized access to protected and classified assets and valuables is paramount when being transported:

a. When transporting protected and classified assets from one person or place to another, safeguards must include controlling access to the information by need-to-know.
b. When transmitting protected and classified assets from one person or place to another, safeguards must depend on proper packaging, an appropriate and reliable postal or courier service (government or private sector) and the anonymity of the information while in transit.
c. The RCM users will ensure that protected and classified assets are transported or transmitted according to the minimum requirements set out in the Operational Security Standard on Physical Security document. (RD-13).
d. RCM users will refer to RCMP Guide G1-009, Standard for the Transport and Transmittal of Sensitive Information and Assets (RD-06) for detailed specifications for enveloping, addressing and courier services for transporting and transmitting protected and classified assets.
e. PE2 users will refer to NDSOD (RD-10), Security of Information Standards for detailed specifications for enveloping, addressing and courier services for transporting and transmitting protected and classified assets.

14 DISCLOSURE AND SHARING OF SENSITIVE INFORMATION

The security controls of the physical environment must be commensurate with the designation or classification of the information being discussed or shared.

When authorized and before sensitive information is shared, the custodian of the information must ensure that recipients of the information:

a. have an appropriate clearance for access to the information;
b. have a demonstrated need-to-know for the information;
c. are authorized to access the information, if said sensitive information was obtained through the means of a foreign export authorization; and
d. are aware of, understand, and have agreed to the safeguarding requirements for that information.

Like classification and protection, any sharing or disclosure of GC information should comply with the exemption and exclusion criteria of the Access to Information Act, and the Privacy Act.

15 DISPOSAL

The destruction of PROTECTED and CLASSIFIED information and assets will be in accordance with the Industrial Security Manual (RD-9) for industry and in accordance with respective Departments directives for GC organizations.