



GSA/OP/17/18

"SECURITY MONITORING SERVICES TO THE GSA"

Annex I to Invitation to Tender- 'Tender Specifications'

Ref: GSA/OP/17/18

Issue: 1 Rev 0

Date: 7 April 2018



1.	Overview	3
1.1	CONTEXT OF THE TENDER	3
1.2	OUTLINE OF THE TENDER AND PROCEDURAL PROCESS	3
1.3	PRINCIPLES	3
1.4	PURPOSE OF THE INVITATION TO TENDER	3
1.5	PROCUREMENT PROCEDURE TIMELINE.....	4
2.	Terms of reference.....	5
2.1	TECHNICAL TERMS OF REFERENCE	5
2.1.1.	Scope of the activities under the FWC	5
2.1.2.	Simulation exercise.....	9
2.2	LEGAL AND CONTRACTUAL TERMS OF REFERENCE.....	10
2.2.1	Procurement process	10
2.2.2	Form of Contracts	14
2.2.3	Place of performance	15
2.2.4	Duration	15
2.2.5	Language of the FWC	15
2.2.6	Volume of the FWC	15
2.2.7	Subcontracting	15
2.2.8	Participation of consortia	17
2.2.9	Confidentiality and conflict of interest.....	17
2.2.10	Application of FWC to contractor's staff	18
2.2.11	Access to GSA premises	18
3.	Assessment of Tenders.....	18
3.1	EXCLUSION CRITERIA.....	19
3.2	SELECTION CRITERIA	19
3.2.1.	Legal capacity	19
3.2.2	Economical and financial capacity criteria.....	21
3.2.3	Technical and professional capacity criteria	22
3.3.	MINIMUM REQUIREMENTS.....	25
3.4.	AWARD CRITERIA.....	26
3.4.1	Qualitative Award Criteria.....	26
3.4.2.	Financial Award Criteria	30
4.	CONDITIONS OF SUBMISSION OF TENDERS.....	31
4.1	DISCLAIMERS.....	31
4.2	VISITS TO PREMISES OR BRIEFING	31
4.3	VARIANTS.....	31
4.4	PREPARATION COSTS OF TENDERS	31
4.5	CONTENT OF THE TENDER TO BE SUBMITTED	31
4.6	CHECKLISTS OF THE CONTENT OF THE TENDER.....	33
4.7	SUBMISSION.....	37
4.8	PUBLIC OPENING OF THE TENDERS.....	37
4.9	PERIOD OF VALIDITY OF THE TENDERS.....	38
4.10	CONTACTS WITH THE TENDERERS	38
4.11	INFORMATION FOR TENDERERS	38
4.12	DATA PROTECTION SPECIFIC TO THE TENDER PROCESS	39
5.	List of Annexes.....	40

1. Overview

The present specifications are attached to the invitation to tender and are intended to complement the information contained in the Contract Notice 2018/S 090-201120 providing to the tenderers further information on the procurement procedure and elements to allow them to prepare for the procurement process.

1.1 Context of the Tender

The European GNSS Agency (“**GSA**”) is an agency formed by the European Union to accomplish specific tasks related to the European GNSS programmes (Galileo and EGNOS).

Further information can be found on the GSA’s web site (<http://www.gsa.europa.eu>). This website contains also information about

- European GNSS programmes (<https://www.gsa.europa.eu/european-gnss/what-gnss>)
- Legal framework applicable to the GSA (<https://www.gsa.europa.eu/gsa/about-gsa>)

1.2 Outline of the Tender and procedural process

Name: GSA/OP/17/18 "Security Monitoring Services to the GSA"

Procedure: Open procedure in accordance with Article 127(1)(2) of Regulation No 1268/2012 (“**RAP**”) for procurement of single framework service contract (“**FWC**”).

Where the reference is made to the FWC in these tender specifications, it should be assumed that any such reference is also meant to cover any specific contracts concluded on a basis of the FWC, in particular when there is a reference covering any obligation of the tenderers.

1.3 Principles

Tenderers are required to accept all the terms and conditions set out in the invitation to tender, the tender specifications and draft FWC. Tenderers are required to waive their own general or specific terms and conditions. The terms and conditions set out in the invitation to tender, the tender specifications and draft FWC shall be binding on the tenderer to whom the FWC is awarded for the duration of the FWC and for the duration of all individual contracts concluded under the FWC.

Any attempt by a tenderer to obtain confidential information, enter into unlawful agreements with competitors or influence the evaluation committee or the GSA during the process of examining, clarifying, evaluating and comparing tenders will lead to rejection of his tender and may result in administrative penalties.

1.4 Purpose of the Invitation to Tender

The objective of this invitation to tender is to establish one single supplier FWC having duration of up to 4 years for provision of security services to the GSA.

The GSA has under its mandate to operate the Galileo Security Monitoring Centre (“**GSMC**”), having its main site in France, near Paris and its backup site near Madrid, Spain. One of its main

responsibilities is to ensure the security of the Galileo system under its mission of Security Monitoring.

This GSMC mission relies on 24/7 security operations performed by a pool of GSMC staff, trained and certified to the highest level. In order to reinforce this mission, the GSA is looking to procure one equivalent 24/7 position. In addition, one of the aims of this tender is also to be able to call upon, on short notice, a pool of external experts, trained and certified to the same level as the GSMC ones in order to ensure the continuity of the mission in case of contingencies within the GSMC operational staff.

In conjunction with this operational mission, the GSA is also looking for local support in coordinating security activities involving the security staff of the Galileo Operator located in the 2 Galileo Control Centres, one in near Rome, Italy and the other in near Munich, Germany.

Finally, GSA is looking for support in the implementation of cyber security requirements across the Galileo system, more specifically in the areas of vulnerability management and risk assessment.

IMPORTANT NOTE: The purpose of this procurement and the FWC is not to replace GSA staff. Tasks shall be provided for complementing GSMC security monitoring and other security support services not available in-house - a duplication of tasks is not intended and shall be avoided. Neither this procurement nor any activities under the FWC (i) are meant to establish any employment relationship between the GSA and the contractor's personnel performing the services or (ii) shall be permitted to be interpreted as establishing such a relationship. The contractor shall take all measures to ensure this understanding with its personnel and shall indemnify and hold the GSA harmless against any claim which the GSA would face in this respect. The tenderer/contractor shall ensure that the entire content and legal implications of this note are clearly communicated, understood, and endorsed by any consortium member and subcontractor, as the case may be.

1.5 Procurement procedure timeline

Timetable	Date	Comments
Submission for publication of contract notice to the supplement to the Official Journal by the GSA.	07/05/2018	All documents of the Invitation to Tender available at: http://www.gsa.europa.eu/gsa/procurement
Deadline for submission of signed NDUs and request to access proprietary information relevant for the tender preparation	11/06/2018	Details for the request procedure and required documents are provided in section 2.2.1.3.
Deadline for requests of clarifications.	22/06/2018	Requests to be sent in writing only to: tenders@gsa.europa.eu . Tenderers are invited to send requests for clarifications as early as possible.
Last date on which clarifications are issued by GSA.	26/06/2018	All clarifications will be published at the GSA's procurement website: http://www.gsa.europa.eu/gsa/procurement Tenderers are invited to check GSA's procurement



		website on a regular basis.
Deadline for submission of tenders.	02/07/2018 at 17.00 CET	According to conditions of submissions set out in section 4.7 of these specifications.
Opening session and start of evaluation session.	09/07/2018	10h00 (local time) in GSA premises in Prague, Czech Republic.
Completion of evaluation and award	August/ September 2018 (estimated)	

2. Terms of reference

2.1 Technical Terms of Reference

2.1.1. Scope of the activities under the FWC

The scope of the activities under the FWC consists in the following two main areas: (i) providing support to the GSMC security monitoring mission by supplying security expertise in the field of information security, and more specifically, in the area of incident handling for the whole Galileo system, and (ii) providing cyber security expertise support to both GSMC and GSA Security Department.

The scope of the activities can be divided in six tasks:

- Task 1: Contractor's own project management and reporting
- Task 2: Operational support to the GSMC Security Monitoring mission
- Task 3: Cyber security expertise support to the GSMC
- Task 4: Cyber security expertise support to the GSA Security Department
- Task 5: Remote operational support to the GSMC Security Monitoring mission
- Task 6: Reinforcement of the GSMC Security Monitoring mission

2.1.1.1. Task 1: Contractor's own project management and reporting

2.1.1.1.1 Objective of the Task

The objective of this Task is to manage the resources provided by the Contractor and to communicate efficiently with the GSA (including all project reporting activities).

Each specific contract awarded for implementation of the FWC will constitute a project to be managed by the Contractor. The Contractor may choose any of the recognised project management methodologies to perform the management and reporting tasks, and will have to describe and justify its chosen methodology in the specific contracts proposals. The capability to manage these projects properly will have to be clearly demonstrated in the proposal, ideally using the selected methodology wherever applicable.

The Contractor shall appoint a Service Supervisor Manager (and a substitute) who will act as single point of contact for the GSA, working closely with the GSA Project Officers for each Task. This person is expected to handle all requests received from the GSA Project Officers and report back to them while taking care of its own personnel and the personnel of its subcontractors subject to the FWC.

A short operational status/progress meeting between the GSA Project Officers and the Contractor's Service Supervisor Manager shall be held at least once every three months.

The Contractor shall implement proper configuration and change management procedures.

2.1.1.1.2. Detailed activities

The Contractor shall:

1. assign a Service Supervisor Manager who will act as a single point of contact for the GSA, as well as a substitute to ensure that a point of contact is available at all times (i.e. reachable on a 24/7 basis), which shall be responsible of the contractual management and the technical project coordination;
2. assign a project team and provide GSA with the team composition and contact details;
3. if deemed necessary by the Contractor, assign a technical manager for each of the area of the support;
4. arrange the proper execution of all the project tasks, in particular it shall track the project status and the reporting;
5. manage its resources allocated to the project;
6. ensure all communication with GSA in due time, in particular regarding the organisation of work and any changes and implementation issues that may happen during the project execution;
7. inform GSA in advance (at least 5 working days) of any actions or resources required to assist the Contractor;
8. organise (including sending invitations and agenda) and chair progress meetings and technical coordination meetings;
9. draft minutes of all the progress meetings and technical coordination meetings, submit them for GSA comments and/or approval within 3 working days so that the final meeting minutes are available 5 working days after the meeting;
10. deliver a Project Management Plan, including risk register, security management, establishment and maintenance of the travel plan;
11. create, review and submit to the GSA all other deliverables according to the descriptions of the individual tasks below (in particular put together all deliverables from the Tasks to into one activity report to be submitted on a monthly basis); and
12. ensure that the Galileo Programme Security Instructions are applied to all the project activities and that GSA is aware of any risk or incident.

2.1.1.2. Task 2: Operational support to the GSMC Security Monitoring mission

2.1.1.2.1 Objective of the Task

This task deals with the execution of the Security Monitoring operations of GSMC, which runs its operations under a 24/7 shift rotation work scheme composed of GSA internal staff.

In order to ensure the full continuity of the GSMC operations, GSA is looking, through this Task, to build a pool of operators available on short-term notice. In order to build up their GSMC knowledge and be operational as a GSMC Security Incident Handler for as long as needed, these operators will follow – once this task is activated by the GSA - dedicated GSMC trainings supplied by the GSA, as part of the GSMC operator certification process as described in Annex I.K .

2.1.1.2.2 Place of performance

The place of performance will be mainly the GSMC master site near Paris, France but it could also be required from the Contractor that its operators perform the activities from other locations such as the GSMC backup site near Madrid, Spain or one of the Galileo Control Centres, near Munich (Germany) and/or Rome (Italy).

2.1.1.2.3 Detailed activities

Upon GSA request and as per the Service Level Agreement (Annex I.F), the Contractor will be asked to supply one or several persons which shall inter alia be capable of:

1. Supervision of the security and system status of the Galileo system using dedicated GSMC security tools (e.g. memory /disk acquisition tools, network monitoring, IDS, firewalls and log centralisation/correlation software);
2. Incident handling of any security alerts raised by the GSMC security tools by following the GSMC operational procedures which cover security alert monitoring, incident categorisation and triage, incident response strategy and definition of recovery strategies;
3. Operating the GSMC Ticketing System to log and trace the full incident handling process;
4. Contributing to the review and refinement of the incident handling processes in order to optimize GSMC incident response capabilities;
5. Maintaining the lessons learnt knowledge base following incidents closure;
6. Supporting the GSA Operational Analysts in developing the information security vision for Galileo system evolutions.

2.1.1.3. Task 3 Cyber security expertise support to the GSMC

2.1.1.3.1 Objective of the Task

The objective of this task is to provide onsite support services to GSMC by the provision of cyber security expertise to the GSMC Cyber Security Manager (CSM).

The areas where the GSMC is looking for support in terms of expertise are the following:

- Vulnerability Management
- Threat Landscape Analysis

2.1.1.3.2 Detailed activities

A more detailed description of the tasks related to each area of expertise can be found in Annex I.E (please refer to section 2.1.2 for more information regarding access to this annex).

2.1.1.4. Task 4 Cyber security expertise support to the GSA Security Department

2.1.1.4.1 Objective of the Task

The objective of this task is to provide onsite support services to GSA by the provision of cyber security expertise to the GSA Cyber Security Manager (CSM).

The areas where the GSA is looking for support in terms of expertise are the following:

- Vulnerability Tracking and Mitigation
- Defensive Security Design
- Cyber Internal Auditing

2.1.1.4.1 Detailed activities

A more detailed description of the tasks related to each area of expertise can be found in Annex I.E (please refer to section 2.1.2 for more information regarding access to this annex).

2.1.1.5. Task 5 Remote operational support to the GSMC Security Monitoring mission

2.1.1.5.1 Objective of the Task

The objective of this task is to provide support services to the GSMC mission of Security Monitoring in making the operational link between the GSOP Central Security Facility team and the GSMC.

2.1.1.5.2 Place of performance

Up to two FTEs, one collocated in GCC-I and the other in GCC-D, will work as a nexus between teams, and will allow to strengthen the operations, increase the GSA visibility and understanding of the system configuration, participate to GCC planning and meetings and support the investigations and resolution of incidents.

2.1.1.5.3 Detailed activities

A more detailed description of the tasks related to each area of expertise can be found in Annex I.E (please refer to section 2.1.2 for more information regarding access to this annex).

2.1.1.6. Task 6: Reinforcement of the GSMC Security Monitoring mission

2.1.1.6.1 Objective of the Task

This task deals with the execution of the Security Monitoring operations of GSMC through the provision of one 24/7 position, running under the GSMC 24/7 shift rotation work scheme.

In order for the operators ensuring this 24/7 position to have the same knowledge as GSMC Security Incident Handlers, these operators will follow – once this task is activated by the GSA - dedicated GSMC trainings supplied by the GSA, as part of the GSMC operator certification process as described in Annex I.K .

This task and Task 2 in section 2.1.1.2 are comprising the same scope of detailed activities with exception that Task 2 is meant to cover temporary contingencies in the GSMC Security Monitoring mission while this Task aims at delivering those services on a permanent basis. Therefore, while the Contractor is free to use a pool of certified operators to cover both tasks, it must demonstrate that this flexibility does not bring prejudice to the delivery of one of the tasks, more specifically, when both tasks are activated by GSA at the same time.

2.1.1.6.2 Place of performance

The place of performance will be mainly the GSMC master site near Paris, France but it could also be required from the Contractor that its operators perform the activities from the GSMC backup site near Madrid.

2.1.1.6.3 Detailed activities

Upon GSA request, the Contractor will be asked to supply this 24/7 position capability which shall be capable of:

1. Supervision of the security and system status of the Galileo system using dedicated GSMC security tools (e.g. memory /disk acquisition tools, network monitoring, IDS, firewalls and log centralisation/correlation software);
2. Incident handling of any security alerts raised by the GSMC security tools by following the GSMC operational procedures which cover security alert monitoring, incident categorisation and triage, incident response strategy and definition of recovery strategies;;
3. Operating the GSMC Ticketing System to log and trace the full incident handling process;
4. Contribute to the review and refinement of the incident handling processes in order to optimize GSMC incident response capabilities;
5. Maintaining the lessons learnt knowledge base following incidents closure;
6. Supporting the GSA Operational Analysts in developing the information security vision for Galileo system evolutions.

2.1.2. Simulation exercise

2.1.2.1 Introduction

The simulation exercise has been designed to provide the tenderers a good overview of the range of activities they may be asked to perform under the FWC, based on the tasks described above. It is further a likely scenario for the implementation of the FWC through specific contracts for individual tasks. Accordingly, the simulation exercise will serve as a common scenario against which the quality and the price of the submitted tenders will be compared.

The tenderers have to reply to this simulation exercise while presenting their tenders, explaining for each Work Package (WP) at least the following:

- The methodology they intend to use
- Preliminary outcomes
- Any other elements to evidence their understanding and suitability to perform the Tasks

The tenderers are hereby informed that their offer for the simulation exercise will be deemed relevant to be used as a basis for the establishment of specific contracts under the FWC with the successful tenderer if the request for services will be identical. In addition, the GSA may calibrate:

1. The expected **minimum** quality and quantity of outputs that the contractor shall be **able** to commit to provide within the suggested elapsed periods of time.
2. The expected **maximum** quantity of resources/costs that the contractor would charge to the GSA **for the corresponding output**.
3. Note: the GSA shall be entitled to request the same quality at higher or lower quantity, and thus pro-rata charging. The tenderer shall indicate in its tender any constraints it would face in terms of increasing the quantity within any 3-month period.

2.1.2.2 Description of the Simulation Exercise Tasks

The detailed description of the Simulation Exercise can be found in Annex I.E (please refer to section 2.1.2 for more information regarding access to this annex).

2.2 Legal and Contractual terms of reference

2.2.1 Procurement process

The tenderers shall submit a complete tender within the deadline indicated in section 1.5. The tender shall include all the content described under section 4.5 allowing the GSA to fully assess the exclusion and the selection criteria and to perform the evaluation of the technical proposal and the financial offer on the basis of award criteria as described under section 3.

2.2.1.1 Specific participation conditions

- I. For reasons related to the protection of the essential interests of the security of the European Union, including that of its Member States and/or to public security, the participation to this procurement procedure as a prime contractor, or as a subcontractor where its activities present security aspects, is limited to economic operators which, at the moment of the submission of their tender and during the entire period of the FWC or subcontract if it is awarded to them, are established within the European Union.

An economic operator is considered established within the European Union when it meets all of the following conditions:

- a) the economic operator is formed in accordance with the law of an EU Member State and has its central administration, registered office and principal place of business within the European Union if it is a legal person, or is a national of and resident in an EU Member State if it is a natural person;
 - b) If it is a legal person, the economic operator's decision making centre(s) comply with the conditions specified in point a) of this subparagraph. Decision making centre shall be understood as a legal or natural person which is, with respect to the economic operator, in one or more of the situations set out in article 22(1) of Directive 2013/34/EU¹;
 - c) the facilities (for manufacturing of goods and/or supplying of services) which the economic operator would use for the execution of the FWC or the subcontract are located within the European Union.
- II. In duly justified circumstances related to the nature, cost or availability of specific goods and/or services and on the basis of a duly motivated waiver request submitted in writing by an economic operator, the GSA shall be entitled to waive:

¹ Directive 2013/34/EU of the European Parliament and of the Council of 26 June 2013 on the annual financial statements, consolidated financial statements and related reports of certain types of undertakings, amending Directive 2006/43/EC of the European Parliament and of the Council and repealing Council Directives 78/660/EEC and 83/349/EEC. OJ L 182, 29.6.2013, p. 19–76

- a) one or more conditions specified in points I.b or I.c above if it concerns a prime contractor; or
- b) any of the conditions specified in point I above, if it concerns a subcontractor;

on the condition that the economic operator demonstrates the implementation of sufficient measures in order to guarantee the protection of the essential interest of the security of the European Union including that of its Member States and/or public security.

To fulfil this condition the economic operator requesting a waiver may provide from the relevant National Security Authority of a Member State the assurance that sufficient measures have been implemented and are in place in relation to the subject matter of the FWC to guarantee the protection of the essential interests of the security of the European Union including that of its Member States and public security.

The GSA may require the economic operator to present a duly signed security deed containing appropriate security undertakings, including the assurance from the National Security Authority if any, where the contractor/subcontractor will handle information classified at the level CONFIDENTIEL UE/EU CONFIDENTIAL or above.

When deciding on the waiver, the GSA shall take into consideration the nature, cost or availability of specific goods and/or services. It shall also take the utmost account of the assurance issued by the National Security Authority presented by the economic operator.

The Contractor must comply with participation conditions throughout the duration of FWC.

2.2.1.2. Notice on the United Kingdom's withdrawal from the EU (complementing the participating conditions)

The United Kingdom submitted on 29 March 2017 the notification of its intention to withdraw from the European Union, pursuant to Article 50 of the Treaty on European Union. This means that, unless a ratified withdrawal agreement² establishes another date, all Union primary and secondary law will cease to apply to the United Kingdom from 30th March 2019, 00:00h (CET) ("the withdrawal date"³). The United Kingdom will then become a "third country"⁴.

Subject to any transitional agreement that may be contained in a possible withdrawal agreement, as of the withdrawal date, Tenderers and – where they carry out activities related to the protection of essential interests of the security of the European Union or to public security, including the security of the EU Member States – also their Subcontractors, which are no longer established in the European Union as a result of the withdrawal of the United Kingdom, will no longer comply with the participating conditions as mentioned in 2.2.1.1. Therefore, subject to the following paragraph, those prime contractors and subcontractors will no longer be in a position to carry out their activities under the contract or the subcontract, respectively.

² Negotiations are ongoing with the United Kingdom with a view to reaching a withdrawal agreement.

³ Furthermore, in accordance with Article 50 (3) of the Treaty on European Union, the European Council, in agreement with the United Kingdom, may unanimously decide that the Treaties cease to apply at a later date.

⁴ A third country is a country, which is not a member state of the EU.

In as far as the Tenderer and/or their Subcontractors are in the situation described in the previous paragraph, Tenderers shall provide in their tender adequate explanations, assurances and commitments on how they will ensure that, as from the withdrawal date, they and/or their Subcontractors will continue to comply with the participating conditions set out in Section 2.2.1.1. Such adequate explanations, assurances and commitments may involve substantiated requests for waiver as stated in 2.2.1.1., in accordance with those participating conditions. Failure by Tenderers to provide such adequate explanations, assurances and commitments will lead to rejection of the proposal.

More specifically,

The proposal shall therefore contain adequate explanations, assurances and commitments on how the Tenderers will ensure that, as from the withdrawal date, they and/or their Subcontractors(s) will continue to comply with those participating conditions. This is hereinafter referred to as “Mitigation Plan” and will be evaluated as an integral part of the Tenderer’s Proposal.

The Tenderer shall note the following cases or combination of cases, if/as applicable:

1. UK Prime:

The Mitigation Plan shall contain:

a) a firm, irrevocable and unconditional commitment by the Tenderer to assign the contract at the latest as from 30 March 2019 to another economic operator satisfying the participating conditions (the “Proposed Assignee”), as well as a firm, irrevocable and unconditional commitment and acceptance by the Proposed Assignee to be bound by all ITT requirements, rights and obligations; and

b) shall provide, as a minimum, the following information and documents:

- The Tenderer shall clarify and justify how the Tenderer will continue to ensure compliance with the Security Aspect Letter(s) (Annex I.J) after the withdrawal date;
- The Tenderer shall clarify and justify that the schedule of this activity will not be affected and shall submit relevant information supporting such statement;
- The Tenderer shall confirm and justify that the implementation of the Mitigation Plan will not cause any additional cost to this activity;
- The Tenderer shall provide evidence of compliance of the Proposed Assignee with the participating conditions and additionally, the Proposed Assignee shall state in a duly signed declaration its compliance to section xxx (participating conditions), if applicable;
- The Tenderer shall assume full responsibility, ensure and confirm all formalities which are required for such an assignment to be legal, valid and enforceable under the applicable law it adheres to;
- The Tenderer and the Proposed Assignee shall explicitly state their compliance with Art. I.14 of the Contract (Annex II to this ITT) (clauses related to assignment).

- In order to substantiate the assignment, the Tenderer is further expected to elaborate the mitigation plan to a full extent as an integral part of the baseline proposal, including complete technical, management and administrative, implementation, financial and contractual volumes as defined in the tender specifications.

2. UK Subcontractor (if the Subcontractor carries out activities related to the protection of the essential interests of the security of the European Union or to public security, including the security of the EU Member States):

- The Tenderer (Prime) shall provide a Mitigation Plan.
- The Tenderer shall flow down to the Subcontractor(s) as a minimum the mitigation plan bullets under b) above as applicable and ensure that its Subcontractor(s) meet(s) the participating conditions as of 30 March 2019. This is without prejudice to any substantiated written waiver request that may be granted as per the applicable ITT participating conditions (section 2.2.1.1).

3. UK Parent Company of Tenderer/Subcontractor (if the Subcontractor carries out activities related to the protection of the essential interests of the security of the European Union or to public security, including the security of the EU Member States):

- The Mitigation Plan shall contain a substantiated written waiver request as described in the applicable ITT Participating Conditions (section 2.2.1.1).

Where applicable, the contract shall be assigned in whole or in part to the Proposed Assignee no later than 30th March 2019, to ensure that the participating conditions as stated in section 2.2.1.1 are met. Such assignment is subject to Art. I.14 of the Contract.

The Tenderer shall ensure that its Subcontractor meets the conditions of Art. I.15 of the draft Contract (attached hereto as Annex II).

2.2.1.3 Submission of Non-Disclosure Undertakings – access to proprietary and/or classified information during the tender

For access to proprietary information (contained in Annex I.E, Annex I.K and Annex I.L to the present tender specifications) **and/or classified information** (referred to in the Annex I.J) relevant for drafting the tender **before the deadline for its submission**, tenderers (including consortium members and any subcontractor) shall **each** submit:

- their **Non-Disclosure Undertaking** (“NDU”) using the form attached in Annex I.I **in one (1) signed original and two (2) copies**
- the **Legal Identification Form**⁵ (“LEF”) and
- the **supporting documents** indicated in the LEF.

⁵ Available here: http://ec.europa.eu/budget/contracts_grants/info_contracts/legal_entities/legal_entities_en.cfm

to the following address:

European GNSS Agency
Procurement and Legal Department

Non-Disclosure Undertaking under procurement procedure GSA/OP/17/18

Janovskeho 438/2
170 00 Prague 7
Holesovice, Czech Republic

In parallel, the tenderers shall send **an electronic copy** of the NDU, Legal Entity Form and the supporting documents to tenders@gsa.europa.eu to allow a quicker treatment of the request.

Only entities which, according to the submitted Legal Identification Form and supporting documents, are established in a Member State of the European Union shall be eligible to receiving proprietary information, including any classified information, for preparing their tender. This does not prejudice the verification of the specific participation conditions subject to section 2.1.1, to be performed separately against tenders submitted. In addition, the proprietary information shall only be available to potential tenderers. The GSA reserves the right to refuse the access to entities which cannot pretend to perform the contract.

Without prejudice to further legal measures, exchange of any proprietary and/or classified information subject to NDU with any person who have not previously signed the relevant NDU may lead to exclusion from the procurement procedure under the GSA's discretion.

Agreements previously signed by economic operators for access to the proprietary information not related to this procurement are not regarded as fulfilling the present NDU requirements.

Unless an NDU was already submitted prior to the submission of the tender for access to proprietary information for the tender preparation, tenderers shall submit the NDU together with their tender as described in section 4.6.

Further to the requirement to submit NDUs with the tender as detailed above, please note for the implementation of the FWC that, as a condition for any economic operator to join the consortium of the successful tenderer following signature of the FWC, and without prejudice to further authorisation requirements by the GSA, the economic operator shall submit the **duly signed** NDU (Annex I.I), in **one (1) signed original and two (2) copies** to the GSA.

2.2.2 Form of Contracts

The aim of this procurement is to award one FWC to one Contractor for the provision of services described in present Tender Specifications and their annexes.

The GSA reserves the right to launch an exceptional negotiated procedure for new services **of a value up to 50% of the initial maximum FWC value** with the same Contractor in case of need, as foreseen in Art. 134(1)(e) RAP.

2.2.3 Place of performance

Mainly at the following sites:

- GSMC-FR, 8, Av du Président Kennedy, Saint-Germain-en-Laye, France
- GSMC-ES, INTA, Ctra. de Villaverde Bajo, km 18, 28330 San Martín de la Vega, Spain
- GSA Headquarters, Janovského 438/2, Prague, Czech Republic
- Galileo Control Centre (GCC-D), Oberpfaffenhofen, Germany
- Galileo Control Centre (GCC-I), Fucino, Italy

and potentially in other Galileo infrastructure sites in Europe, currently being:

- Lauch Early Operations Centre, Darmstadt, Germany
- Lauch Early Operations Centre, Toulouse, France
- In-Orbit Testing Centre, Redu, Belgium

2.2.4 Duration

The expected duration of the FWC is 1 year from the signature of the FWC, with the possibility of extension 3 times for 1 year (4 years maximum).

The foreseen start date is the following: July 2018

2.2.5 Language of the FWC

English shall be the working language of the FWC including all correspondence with GSA. Therefore, all proposed personnel should have an excellent level of English as detailed in Minimum Requirements M3 and M4⁶. The GSA reserves the right to request certificates issued by an officially recognised institution.

2.2.6 Volume of the FWC

The indicative budget estimated for the maximum duration of the FWC is EUR 21,500,000 (twenty-one million five hundred thousand Euros).

This budget is only indicative; it will be subject to budget allocations given to the GSA.

2.2.7 Subcontracting

Subcontractors must satisfy the eligibility criteria applicable to the award of the FWC.

According to article 26(1) of the GNSS Regulation the GSA intends to favour wide participation of various economic operators, while securing smooth and effective operations. On this basis and for

⁶ see the Common European Framework of Reference for Languages (CEFR) (<http://europass.cedefop.europa.eu/europass/home/hornav/Downloads/CEF/LanguageSelfAssessmentGrid.csp>)



the purposes of article 26(2) GNSS Regulation, the tenderer is obliged to **subcontract a minimum share of 10 % and maximum share of 70% of the total price of all tasks of the FWC**. These subcontractors shall be selected outside the tenderer's group⁷ (including consortium members).

The tenderer shall subcontract by **competitive tendering outside the tenderer's group a minimum share of 5% of the total price**.

Competitive tendering outside the tenderer's group is considered to have taken place when more than one offer from an entity outside the group has been requested by the tenderer.

Each tenderer is responsible for organising its own competitive tender(s) aimed at finding necessary subcontracting respecting the following procurement principles:

- Fair competition & equality of treatment
- Transparency
- Proportionality
- Best value for money

Given the fact that the GSA cannot assume and/or guarantee that the full budget available under the FWC will be consumed, the percentage of subcontracting will be calculated as the percentage from the actually requested services under the FWC and not as a percentage from the maximum volume of the FWC. In order to ensure that the proposed percentage of subcontracting will be achieved, such subcontracting shall be done at the level of each individual contract concluded under the FWC.

Tenderers shall clearly indicate in their FWC tenders which part of the services they intend to subcontract as well as their approach to implement such subcontracting at each specific contract level to demonstrate compliance with the above mentioned requirements. A proof of competitive subcontracting tender(s), including thorough visibility of technical and financial offer of consulted entities outside the group (envisaged subcontractors) shall be provided together with the tender.

If the tenderer does not manage to complete the competitive tender(s) required by the time of tender submission, it shall submit a signed undertaking presenting credible tendering plan it intends to carry out.

If the competitive tenders are completed only during FWC execution, the concluded subcontracts shall not lead to a change of the FWC unless it is in favour of the GSA.

The contractor shall request the GSA's prior written authorisation to introduce any newly selected subcontractor(s) according to the provisions of FWC. In case of failure to respect the undertaking of subcontracting or obtaining the said authorisation, the FWC may be terminated for contractor's default.

⁷ For the purpose of this requirement the expression "group" is meant to encompass i) the entity or the group of entities acting as a tenderer, ii) the entity /entities to which the tenderer or any of the members of the group acting as tenderer is affiliated, iii) the entities affiliated to the tenderer or to any of the members of the group acting as tenderer. An entity shall be deemed affiliated to the tenderer or any of the members of the group acting as tenderer if their links fall within the scope of article 22 of Directive 2013/34/EU, of 26 June 2013.

In case where no competitive tendering is planned to be undertaken, tenderer shall submit a justification providing compelling reasoning for the non-compliance with the above mentioned requirement. Failure to provide such justification may lead to the rejection of the tender.

Tenderers may at any time after tender submission or during the FWC execution be requested to submit supporting evidences of their application of competitive tendering for the selection of subcontractors and their compliance with the principles established above. Contractors can be subject to possible auditing according to contractual provisions.

Without prejudice to the above, the GSA may reject the proposed subcontractor(s) and ask for another subcontractor(s) to be proposed as part of the tender. Such rejection shall be justified in writing by the GSA and may be based only on the criteria used for selection of tenderers for the FWC.

Sub-contracting shall not relieve the contractor from its obligations under the FWC. In this respect, the contractor shall remain the sole partner and person legally and financially responsible vis-à-vis the GSA.

2.2.8 Participation of consortia

Consortia may submit a tender on the condition that it complies with the rules of competition.

A consortium may be a permanent, legally-established grouping or a grouping which has been constituted informally for a specific Tender procedure.

Such grouping (or consortium) must specify the company or person heading the project (the leader) and must also submit a copy of the document authorising this company or person to submit a tender on behalf of the consortium. All members of a consortium (i.e. the leader and all other members) are jointly and severally liable to the GSA.

In addition, each member of the consortium must provide the required evidence for the exclusion and selection criteria (see section 3 of these Tender Specifications). Concerning the selection criteria “economic and financial capacity” as well as “technical and professional capacity”, the evidence provided by each member of the consortium will be checked to ensure that the consortium as a whole fulfils the criteria.

The participation of an ineligible person will result in the automatic exclusion of that person. In particular, if that ineligible person belongs to a consortium, the whole consortium will be excluded.

2.2.9 Confidentiality and conflict of interest

The tenderer shall pay particular attention to the clauses on confidentiality of the draft FWC. The assignment is to be considered as a highly sensitive issue, considering that the Contractor will not only have direct access and knowledge of the GSA's internal organisation but will also have to deal with proprietary and classified information.

Therefore the selected Contractor needs to be holder of a Facility Security Clearance (FSC) of at least SECRET UE/EU SECRET level.

Personnel providing services under Tasks 2, 3, 4, 5 and 6 shall be holder of a Personnel Security Clearance at the level described under the personnel specifications of the “legal capacity requirements” section.⁸

The Contractor undertakes to treat in the strictest confidence and not make use of or divulge to third parties any information or documents which are linked to performance of the FWC. The Contractor shall continue to be bound by this undertaking after completion of the tasks.

In case of award of the FWC and before start of any service provisions under a specific contract, candidates shall be prepared to declare in writing to the GSA Local Security Officer that its personnel providing the services is suitable for the performance of his/her duties, free from criminal convictions and enjoy full rights as citizen of EU.

The Contractor shall **ensure** through adequate arrangements with its service-providing personnel that they:

- are bound to follow any security rules as may be set by the GSA from time to time for anyone entering into or staying in the premises of GSA – any such rules shall be provided to the Contractor; and
- are ready to sign a “**declaration on confidentiality and absence of conflict of interest**” with the GSA before commencing any service provision. The current form of such declaration is attached as Annex V of the FWC for information on the understanding that such form is liable to evolve and possibly cover additional aspects from time to time and shall not in any way relieve the Contractor from any of its obligations. The GSA reserves further rights to ask the Contractor or its staff performing the services to sign a declaration regarding confidentiality, non-disclosure and/or declaration regarding precise obligations of processing of personal data.

2.2.10 Application of FWC to contractor’s staff

The contractor shall take all necessary steps, towards its staff executing this FWC, to ensure the full applicability of FWC conditions.

2.2.11 Access to GSA premises

Access to GSA premises implies the acceptance by the contractor or any subcontractor to comply with the GSA’s internal security and safety rules.

3. Assessment of Tenders

All tenders will be assessed in the light of the criteria set out in these specifications.

The assessment of the tenders is carried out in successive stages against the exclusion and selection criteria set out below.

⁸ Commission Decision 2001/844/EC, ECSC, Euratom on Information Security and Amendments, of 29 November 2001 (consolidated version)

- 1) **Exclusion stage** - to check, on the basis of the exclusion criteria, whether tenderers can take part in the tendering procedure;
- 2) **Selection stage** - to check, on the basis of the selection criteria, (a) the technical and professional capacity; (b) the economic and financial capacity and (c) the legal capacity of each tenderer.
- 3) **Minimum requirements stage** – to verify the tender of each tenderer that has passed the exclusion and selection stages for compliance with the minimum tender requirements as defined in section 3.3.
- 4) **Award stage** - to assess, on the basis of the award criteria, each tender that has passed the exclusion and selection stages.

A single FWC may be concluded with the tenderer ranked best as the result of the evaluation of admissible tenders.

3.1 Exclusion criteria

Participation in this Tender is only open to tenderers (all entities involved, including sub-contractors) who will be able to sign the Declaration of Honour (Annex I.B to this document). Failure to do so will lead to exclusion from the procurement process.

Supporting evidence requested as part of the Declaration of Honour may be submitted only by the successful tenderer upon notification of award by the GSA. The tenderers are however highly recommended to start preparing the evidence in original version as soon as possible given the time necessary to gather them. The GSA reserves the right to request the supporting evidence during the tendering procedure.

3.2 Selection criteria

To be assessed in selection stage, the tenderer must have passed the exclusion stage described above.

The tenderers (including all entities participating, including subcontractors, unless indicated otherwise in the following tables) in their Declaration of Honour shall confirm their compliance with the selection criteria.

3.2.1. Legal capacity

Tenderers must have the legal capacity to perform the tasks required in this invitation to tender
Legal capacity shall be demonstrated by:

Ref. #	Legal capacity	Evidence
L1.	General requirement All economic operators participating in	Tenderers (including all consortium members and any proposed



	<p>this procurement, i.e. tenderers (including any consortium member and subcontractor) have to be authorised to perform the FWC under the national laws.</p>	<p>subcontractor) shall provide a duly filled in and signed Legal Entity Form (see section 4.6.1, ENVELOPE 1 for more details) alongside a copy of the trade or professional register excerpt of the entity and the supporting documents required in the form, i.e. copy of the value added tax (VAT) registration document.</p> <p>NOTE 1: Where a tenderer has already signed another contract with the GSA, it may provide instead of the legal entity file and its supporting documents a copy of the legal entity file provided on that occasion, unless a change in its legal status occurred in the meantime or the legal entity file or its supporting documents are older than 12 (twelve) months.</p> <p>NOTE 2: Where the tenderer has already provided the legal entity form and the supporting documents for the signature of the NDU (see section 2.2.1.3), it may provide only a reference to those in its offer.</p>
L2	<p>PSC requirement</p> <p>All tenderer's personnel (including any consortium member and subcontractors) involved in Tasks 2, 3, 4, 5 and 6 and planned to access classified information above RESTREINT UE/EU RESTRICTED under the FWC must have - at the time of submission of the offer - a Personal Security Clearance ("PSC") of at least SECRET UE/EU SECRET level to be maintained throughout the duration of the FWC.</p> <p>In case some tenderer's personnel (including any consortium member and subcontractors) involved in Task 1 is planned to access classified information above RESTREINT UE/EU RESTRICTED, they shall have a PSC of at least SECRET UE/EU SECRET level to be maintained</p>	<p>Submission of official documentation proving tenderer's (including all consortium members and any proposed subcontractors) personnel PSC up to SECRET UE/EU SECRET, to be maintained throughout the duration of the FWC.</p>

	throughout the duration of the FWC.	
L3	<p>FSC Requirement</p> <p>All economic operators participating in this procurement, i.e. tenderers (including any consortium member and subcontractor) must have - at the time of submission of their offer - a Facility Security Clearance (“FSC”) of at least SECRET UE/EU SECRET level to be maintained throughout the duration of the FWC, unless the tenderer/contractor can demonstrate the absence of that consortium member’s, or subcontractor’s need to access classified information for performing the tasks under the FWC outside the GSA’s premises.</p>	<p>Submission of official documentation proving tenderer’s (including all consortium members and any proposed subcontractor) FSC up to SECRET UE/EU SECRET, to be maintained throughout the duration of the FWC.</p> <p>Otherwise, tenderers shall submit to the GSA’s satisfaction in writing the absence of that consortium member’s (or subcontractor’s) need to handle classified information above RESTREINT UE/EU RESTRICTED for performing the activities under the FWC outside the GSA’s premises.</p>
L4.	<p>Appointed, available Local Security Officer</p> <p>Tenderers (including any consortium member and subcontractor) handling classified information above RESTREINT UE/EU RESTRICTED under the FWC, must have appointed - at the time of submission of their offer - a Local Security Officer (“LSO”), to be maintained throughout the duration of the FWC.</p> <p>The tenderer’s LSO shall act as principal point of contact between the contractor and GSA concerning all matters related to security and handling of European Union Classified Information.</p>	<p>Any tenderers (including any consortium member and subcontractor) handling classified information above RESTREINT UE/EU RESTRICTED shall submit a proof of the appointment of their respective LSO.</p> <p>NOTE: There is no specific format/template for proof of appointment of the LSO – a signed declaration of the duly authorised representative of the concerned entity shall be sufficient.</p> <p>The tenderer shall clearly list which entity (in case of consortium and subcontracting) will be handling classified information above RESTREINT UE/EU RESTRICTED.</p>

3.2.2 Economical and financial capacity criteria

Tenderers must have the economic and financial capacity to perform the tasks required in this invitation to tender.

Financial and economic capacities shall be demonstrated by:

Ref. #	Economic and financial capacity	Evidence
--------	---------------------------------	----------

S1.	General requirement The tenderer (all members of consortium and subcontractors cumulatively) must have minimum general turnover of EUR 3,000,000 (three million Euro) per year in the last three years	Statement of turnover relating to the relevant services for this Tender for the last three financial years;
S2	The tenderer (including all consortium members) is required to have a stable financial capacity to sustain its business. The tenderer is presumed to have this capacity if it complies with the requirements as stipulated in Table 5 of Annex I.C)	Full financial statements for the last three financial years, including a consolidated balance sheet and the profit and loss account; Duly filled in Financial Statements relating to the Selection Stage in Annex I.C

3.2.3 Technical and professional capacity criteria

Tenderers must have the technical and professional capacity to perform the tasks required in this invitation to tender.

Technical and professional capacities shall be demonstrated by:

Technical Skills and Competences		<u>Tenderers applying as consortium or relying on subcontractors for capacity criteria SHALL clearly indicate the relevant consortium member or subcontractor in the evidence for each task</u>
Criteria	Details	To be evidenced by
T1	Task 1: At least 3 years of experience in 2 different projects management and coordination activities similar to the one that is requested under this procurement;	(i) Provide a list of EU/National/International projects on GNSS, space or security sensitive IT systems that have been coordinated within the past 5 years. Associated budget, number of partners involved, abstract and main achievements of the projects should be reported. For the avoidance of any doubts, the required 3 years of experience shall be gained anytime during the past 5 years within one or more projects. This applies



		to criterion T1 through 10. (ii) Provide the CV(s) of the proposed personnel for this Task.
T2	Task 2 and Task 6: At least 3 years of experience in incident handling gained within a security operational centre or equivalent environment;	(i) Provide a list of EU/National/International projects in incident handling gained within a security operational centre environment, rendered within the past 5 years. Associated budget, number of partners involved, abstract and main achievements of the projects should be reported. (ii) Provide the CV(s) of the proposed personnel for this Task.
T3	Task 3 – Vulnerability Management (as defined in Annex I.E): At least 3 years of experience in vulnerability management, dealing with the drafting of risk reports and security advisories;	(i) Provide a list of EU/National/International projects in vulnerability management, dealing with the drafting of risk reports and security advisories, rendered within the past 5 years. Associated budget, number of partners involved, abstract and main achievements of the projects should be reported. (ii) Provide the CV(s) of the proposed personnel for this Task.
T4	Task 3 – Threat Landscape Analysis (as defined in Annex I.E): At least 3 years of experience in cyber-threat analysis, dealing with collection and analysis of Open Source Intelligence (“OSINT”) sources and private security feeds, drafting of risk reports and security advisories;	(i) Provide a list of EU/National/International projects in cyber-threat analysis, dealing with collection and analysis of OSINT sources and private security feeds, drafting of risk reports and security advisories, rendered within the past 5 years. Associated budget, number of partners involved, abstract and main achievements of the projects should be reported. (ii) Provide the CV(s) of the proposed personnel for this Task.
T5	Task 3 – Forensics Analysis : At least 3 years of experience in cybersecurity dealing with the definition and execution of electronic forensics collection and analysis;	(i) Provide a list of EU/National/International projects in cyber-threat analysis, dealing with collection and analysis of OSINT sources and private security feeds, drafting of risk reports and security advisories, rendered within the past 5 years. Associated budget, number of partners involved, abstract and main achievements of the projects should be reported. (ii) Provide the CV(s) of the proposed



		personnel for this Task.
T6	Task 3 – Malware Analysis : At least 3 years of experience in cybersecurity dealing with code and behavioural analysis of active code	<p>(i) Provide a list of EU/National/International projects in cyber-threat analysis, dealing with collection and analysis of OSINT sources and private security feeds, drafting of risk reports and security advisories, rendered within the past 5 years. Associated budget, number of partners involved, abstract and main achievements of the projects should be reported.</p> <p>(ii) Provide the CV(s) of the proposed personnel for this Task.</p>
T7	Task 4 – Vulnerability tracking and mitigation (as defined in Annex I.E): At least 3 years of experience in vulnerability management, dealing with the drafting of risk reports and security advisories;	<p>(i) Provide a list of EU/National/International projects in vulnerability management, dealing with the drafting of risk reports and security advisories, rendered within the past 5 years. Associated budget, number of partners involved, abstract and main achievements of the projects should be reported.</p> <p>(ii) Provide the CV(s) of the proposed personnel for this Task.</p>
T8	Task 4 – Defensive Security Design (as defined in Annex I.E): At least 3 years of experience in design and implementation of secure systems, with focus on implementation of security in the design and security controls (e.g. patch management, hardening guidelines);	<p>(i) Provide a list of EU/National/International projects in design and implementation of secure systems, with focus on implementation of security in the design and security controls (e.g. patch management, hardening guidelines), rendered within the past 5 years. Associated budget, number of partners involved, abstract and main achievements of the projects should be reported.</p> <p>(ii) Provide the CV(s) of the proposed personnel for this Task.</p>
T9	Task 4 – Cyber Internal Auditing (as defined in Annex I.E): At least 3 years of experience in auditing and reviewing design and implementation documentation of secure systems, with focus on implementation of security in the design and security controls (e.g. patch management, hardening guidelines) in operational ICT systems;	<p>(i) Provide a list of EU/National/International projects where auditing of information security management systems and/or cyber security risk management had been performed, within the past 5 years. It will be also valuable to provide certifications on information security auditing, as ISO27001 or CISA. Associated budget, number of partners involved, abstract and main achievements of the projects should be reported.</p>

		(ii) Provide the CV(s) of the proposed personnel for this Task.
T10	Task 5: at least 3 years of experience in leading a team of technical experts in the field of IT/INFOSEC and/or 3 years of experience in practical INFOSEC security (e.g. network security device administration, user security management, incident response).	<p>(i) Provide a list of EU/National/International projects in leading a team of technical experts in the field of IT/INFOSEC and/or 3 years of experience in practical INFOSEC security (e.g. network security device administration, user security management, incident response), rendered within the past 5 years. Associated budget, number of partners involved, abstract and main achievements of the projects should be reported.</p> <p>(ii) Provide the CV(s) of the proposed personnel for this Task.</p>
T11	Full compliance with the security requirements detailed in the Security Aspects Letter (Annex I.J)	Initialled, dated, completed and signed Security Aspects Letter and submission of all information required therein.

3.3. Minimum requirements

In order to be further evaluated, the tenderers shall be compliant with the following minimum requirements (in meaning of article 105(2) of FR):

Ref. #	Minimum Requirements	Required evidence
M1.	Compliance with applicable environmental, social and labour law obligations established by European Union law, national legislation, collective agreements or the applicable international social and environmental conventions listed in Annex X of Directive 2014/24/EU.	Corresponding statements of compliance in the Declaration of Honour – Annex I.B.
M2.	Compliance with the minimum requirements of the SLA.	Corresponding statements of compliance in the Service Level Agreement – Annex I.F, Table 3.
M3.	B2 level (according to Europass CV Classifications) of English, both written and spoken, of all personnel involved in Tasks 2 and 6	<p>Corresponding statements of compliance in the Declaration of Honour – Annex I.B.</p> <p>The GSA reserves the right to request at any stage evidence of language certification.</p>
M4.	C1 level (according to Europass CV Classifications) of English, both written and spoken, of all personnel involved in Tasks 1, 3, 4 and 5	<p>Corresponding statements of compliance in the Declaration of Honour – Annex I.B.</p> <p>The GSA reserves the right to request at any stage evidence of language</p>



		certification.
M5.	University degree of all involved staff in a relevant discipline, or equivalent relevant professional experience (over 10 years).	Europass CV detailing education and previous experience of the respective tenderer's personnel to be involved in the performance of the services under the FWC.

Table 5 – Minimum requirements

Failure to comply with any of these minimum requirements shall lead to the rejection of the tender.

3.4. Award criteria

To be assessed in award stage, the tenderer must have passed the three previous stages described above.

All Tenders will be assessed in the light of the objectives, specifications and criteria set out in these Tender Specifications in particular regarding the simulation exercise.

The assessment of the Tenders in award stage is carried out in three successive stages against the Technical and Financial Award Criteria set out below.

3.4.1 Qualitative Award Criteria

The technical quality of the Tender will be assessed on the basis of the tenderer's technical proposal.

Tenders will be evaluated on the basis of the following award criteria. The maximum quality score is 100 points. **Tenders which do not obtain the minimum score for each qualitative award criterion and at least 60% of the overall score for all the qualitative award criteria will not be admitted to the next stage of the evaluation procedure.**

Unless otherwise indicated below, all subcriteria (mentioned in bullet points) have the same weighting.

#	Qualitative Award criteria	Minimum points: 60	Maximum points: 100
Q.1	Quality and adequacy of the proposed team (a+b+c+d+e+f+g+h+i) Quality of the proposed personnel, with specific reference to the delivery of the concerned task (both at FWC level and for the specific work packages under the simulation exercise).	25	50



	Quality of the proposed team will be evaluated based on the following elements:		
a	<u>Tasks 2 and 6:</u> <ul style="list-style-type: none"> ○ knowledge in the use of security tools commonly used in computer incident handling like memory /disk acquisition tools, network monitoring, IDS, firewalls and log centralisation/correlation software; and ○ experience in the analysis, interpretation and handling of computer and network security related events. 	6	12
b	<u>Task 3 – Vulnerability Management:</u> <ul style="list-style-type: none"> ○ background in computer security, preferably obtained in a security operating centre or equivalent environment; and ○ understanding of compiler specifics, operating system concepts, security models, and the causes of existing vulnerabilities and the potential to exploit them. 	2	4
c	<u>Task 3 – Threat Landscape Analysis:</u> <ul style="list-style-type: none"> ○ experience in risk assessment methodologies applicable to IT systems; ○ experience in the cybercrime scene and knowledge of its main actors and their attack tactics; and ○ experience in leveraging online research tools to identify and navigate online forums, specialised Web sites, social media, and traditional sources. 	2	4
d	<u>Task 3 – Forensics Analysis:</u> <ul style="list-style-type: none"> ○ experience in electronic evidence collection and analysis; ○ good knowledge of the forensic tools and technologies market; ○ experience in supporting criminal 	2	4



	investigations as a technical expert;		
e	<u>Task 3 – Malware Analysis:</u> <ul style="list-style-type: none"> ○ experience in code analysis; ○ experience in code behaviour and identifying Indicator of Compromise (IOCs) markers; 	2	4
f	<u>Task 4 – Vulnerability tracking and mitigation:</u> <ul style="list-style-type: none"> ○ background in computer security, preferably obtained in a security operating centre or equivalent environment; and ○ understanding of compiler specifics, operating system concepts, security models, and the causes of existing vulnerabilities and the potential to exploit them. 	2	4
g	<u>Task 4 – Defensive Security Design:</u> <ul style="list-style-type: none"> ○ experience in requirements engineering and management; ○ experience in production and enforcement of security policies; and ○ knowledge/experience in security monitoring operations. 	2	4
h	<u>Task 4 – Cyber Internal Auditing:</u> <ul style="list-style-type: none"> ○ experience in auditing technical and organisational security requirements implementation on ICT systems; ○ experience in cyber security risk management; 	2	4
i	<u>Task 5:</u> <ul style="list-style-type: none"> ○ background in computer security, preferably obtained in a security operating centre or equivalent environment; and ○ experience in drafting operational procedures related to root cause 	5	10



	investigation and troubleshooting technical issues.		
Q.2	Adequacy of the proposed approach and methodology of the simulation exercise (a+b+c+d+e+f) Evaluated on the basis of the expected outputs for each WP. The following will be taken into account for the respective WP:	21	42
a	WP 1: <ul style="list-style-type: none"> ○ Quality of best practises and methodologies proposed ○ Identification of key challenges and related risks and proposed means for their mitigation, ○ Adequacy of number of people involved ○ quality of the dummy report 	3.5	7
b	WP 2: Adequacy of <ul style="list-style-type: none"> ○ the team organisation (structure, size) to provide the services (in all necessary locations); ○ the approach to service availability, considering all shift durations and uncertainty of the service provision duration; ○ the proposed approach to service continuity and contingency planning; ○ training of the personnel; ○ shift allocation; ○ dummy monthly activity report. 	3.5	7
c	WP 3: Adequacy of <ul style="list-style-type: none"> ○ team organisation; ○ the proposed approach to service continuity and contingency planning; ○ service availability in both GSMC locations; ○ training of the personnel. 	3.5	7
d	WP 4: Adequacy of <ul style="list-style-type: none"> ○ team organisation; ○ the proposed approach to service continuity and contingency planning; ○ service availability and ability to handle regular missions on other GSA sites; ○ training of the personnel. 	3.5	7
e	WP 5: Adequacy of <ul style="list-style-type: none"> ○ team organisation; ○ the proposed approach to service 	3.5	7



	<p>continuity and contingency planning;</p> <ul style="list-style-type: none"> ○ service availability and ability to handle missions on other GSA sites. 		
f	<p>WP6: Adequacy of</p> <ul style="list-style-type: none"> ○ team organisation to ensure a 24/7 service delivery; ○ the proposed approach to service continuity and contingency planning; ○ dummy roster planning and compliance to the shift labour rules; ○ service availability in both GSMC locations. 	3.5	7
Q.3	<p>Quality of SLA</p> <p>Improved parameters of SLA suggested by GSA (Annex I.F to Tender Specifications) for the activation of Task 2 services will be positively marked as per the following scale:</p> <ul style="list-style-type: none"> - the SLA currently foresees 5 days for the placement of the expert on site; - 1.6 points shall be given for any day by which the contractor will reduce this period of notice for on-site placement; - the best value that can be achieved is 8 points (i.e. the contractor shall place the expert on site on the same day as requested by GSA) <p>In case no improvement is proposed, the tender shall receive 0 point under this criterion.</p>	0	8

3.4.2. Financial Award Criteria

Following the appraisal of the qualitative award criteria the Tender will be evaluated with regard to the price of tender that shall be provided by filling in and signing the Financial Table of Answers (Annex I.D).

The price quotes given in Annex I.D that constitute the price of tender are binding for the tenderer and they will be considered as prices for the FWC.

The price index will be calculated as follows: the tender with the least expensive Overall Total Price and that is above the technical threshold will receive 100 points. The other Prices of Tenders receive the points according to the ratio between the least expensive tender and their one, and then multiplied by 100, as shown in the formula below:

$$\text{Price Index} = \text{Cheapest Price of Tender Received} / \text{Price of the Tender} * 100$$



IMPORTANT NOTE: No article is to be omitted or added to the Financial Table of Answers (Annex I.D) by the tenderer. Omissions will result in an incomplete tender and exclusion from the tender process.

3.4.3 Calculation of final score and ranking of tenderers

The FWC will be awarded to the tenderer offering the best value for money, i.e. the highest final score in the final evaluation, weighting each tenderer's total technical score against the respective tenderer's financial score on a **50/50** basis with the following formula:

Final score of Tender X = Total technical score of Tender X * 0.5 + Financial score of Tender X * 0.5

4. CONDITIONS OF SUBMISSION OF TENDERS

4.1 Disclaimers

Please note disclaimers referred to in the invitation to tender.

4.2 Visits to premises or briefing

Visits to GSA's premises or briefings during the tendering process are not foreseen.

4.3 Variants

Variants are not permitted under this procurement procedure.

Any variant submitted aside from the regular tender will be disregarded. Any changes to the tender documents, requirements or structure not clearly marked or distinguishable as a variant may lead to the rejection of the entire tender.

4.4 Preparation costs of Tenders

Costs incurred in preparing and submitting tenders are borne by the tenderers and will not be reimbursed.

4.5 Content of the Tender to be submitted

4.5.1 Language

Tenders shall be drafted in one of the official languages of the European Union, preferably **ENGLISH**.

4.5.2 Outer envelopes

Each tender must be presented in one (1) outer envelope or parcel, which should be sealed with adhesive tape, signed across the seal.

Each outer envelope shall carry the following information:

- the reference number of the Invitation to Tender **GSA/OP/17/18**
- the project title **“SECURITY MONITORING SERVICES TO THE GSA”**
- **the name of the tenderer**
- the indication **“Tender - Not to be opened by the internal mail service”**
- **the address for submission of tenders** (as indicated in **section 4.7**)
- **the date of posting** (if applicable) should be legible on the outer envelope.

4.5.3 Inner envelopes

Each outer envelope shall contain **three (3) inner envelopes**, namely, **Envelope 1, 2 and 3 stating the content of each:**

- Envelope 1: “ADMINISTRATIVE DOCUMENTS and DOCUMENTS RELATING TO EXCLUSION and LEGAL and FINANCIAL AND ECONOMIC SELECTION CRITERIA”, with the name and stamp of the tenderer and the reference number of the Invitation to Tender “GSA/OP/17/18”;
- Envelope 2: “TECHNICAL OFFER”, with the name and stamp of the tenderer and the reference number of the Invitation to Tender “GSA/OP/17/18”;
- Envelope 3: “FINANCIAL OFFER”, with the name and stamp of the tenderer and the reference number of the Invitation to Tender “GSA/OP/17/18”.

Each inner envelope shall contain **one (1) ORIGINAL and two (2) COPIES**. The original tender shall be marked **“ORIGINAL”**, and the copies signed in the same way as the original shall be marked **“COPY”**. **One electronic copy of each envelope shall also be submitted.**

It is required that tenders be presented in the correct format and include all documents necessary to enable the evaluation committee to assess them. Failure to respect these requirements will constitute a formal error and may result in the rejection of the tender.

In addition to the above, in general the tender must be:

- signed by the tenderer or his duly authorised representative;
- perfectly legible so that there can be no doubt as to words and figures;
- clear and concise, with continuous page numbering, and assembled in a coherent fashion (e.g. bound or stapled or organised in files).

The GSA reserves the right to request additional evidence in relation to the tender submitted for evaluation or verification purposes.

The GSA retains ownership of all tenders received under this procedure. Consequently tenderers shall have no right to have their tenders returned to them.

4.6 Checklists of the content of the tender

4.6.1 Administrative file

The administrative file will consist of the following elements:



Ref #	ENVELOPE 1 – ADMINISTRATIVE DOCUMENTS and DOCUMENTS RELATING TO EXCLUSION and LEGAL AND FINANCIAL/ECONOMIC SELECTION CRITERIA (one (1) ORIGINAL, two (2) PAPER COPIES and one (1) ELECTRONIC COPY per envelope)	
(1)	A cover letter , dated and signed by the tenderer or by any other duly appointed representative, including: <ul style="list-style-type: none">- A declaration of full acceptance of the requirements in this Invitation to Tender;- The tenderer's undertaking to provide the services;- A list of all the documentation included/enclosed in the tender;- A list of the legal entities involved, specifying each entity's role and qualifications;- Tenderer's contact details.	<input type="checkbox"/>
(2)	The duly filled in, signed and dated identification sheet of the tenderer using the template in Annex I.A (One per tenderer presenting all the legal entities involved in the consortium and subcontractors).	<input type="checkbox"/>
(3)	The duly filled in, signed and dated legal entity form (one per tenderer and, in case of consortia, one per economic operator involved in a consortium , and in any case one per subcontractor) using the template available at: http://ec.europa.eu/budget/contracts_grants/info_contracts/legal_entities/legal_entities_en.cfm and any supporting documents required in this template. Please take into consideration the instructions from this link before filling in the documents: http://ec.europa.eu/budget/library/contracts_grants/info_contracts/instructions_fiche_en.pdf	<input type="checkbox"/>
(4)	A duly signed and dated statement of authorization/power of attorney containing the name and position of the representative/signatory and official documentary evidence on the person's legal authority to validly sign the tender and the Contract on behalf of the organisation, should it be awarded it.	<input type="checkbox"/>
(5)	The duly filled in, signed and dated Financial Identification Form using the template available at: http://ec.europa.eu/budget/contracts_grants/info_contracts/financial_id/financial_id_en.cfm In case of consortia, only one financial identification form for the whole consortium should be submitted, nominating the bank account into which payments are to be made under the contract (i.e. the account of the consortium leader) in the event that the respective tender is successful. Please pay attention to the supporting documents that should be submitted together with duly filled in financial identification form.	<input type="checkbox"/>
(6)	The duly filled in, signed and dated Declaration(s) of Honour relating to exclusion criteria and selection criteria using the template in Annex I.B - one per economic operator (i.e. tenderer, all consortium members, all subcontractor(s), if any).	<input type="checkbox"/>
(7)	The duly filled in, signed and dated Financial Statement relating to the selection stage using the template in Annex I.C , complemented by the full financial statements for the last three financial years and a statement of turnover relating to the relevant services	<input type="checkbox"/>

	for this tender for the last three financial years as requested in section 3.2.2 of these tender specifications.	
(8)	All evidence relating to the selection criteria L1 to L4	<input type="checkbox"/>
(9)	<u>In case of consortia</u> , a duly signed and dated statement/declaration by each of the consortium members specifying the company or person heading the project and authorised to submit an tender on behalf of the consortium, sign the general terms and conditions of contract in the name and on behalf of the other consortia members, manage the contracts, including any amendment thereof in the name and on behalf of other consortia members using the template in Annex I.G. .	
(10)	For the proposed subcontractors, duly filled in, signed and dated subcontractor Letter of Intent using the template in Annex I.H.	<input type="checkbox"/>
(11)	For any entity or any individual Receiving Person which has not yet submitted them before the submission deadline, dully filled in, signed and dated NDU	
(12)	An electronic copy of each document submitted in the administrative envelope on CD-ROM or USB stick with the full set of documents in machine readable format (MS Office 2003 or later, or Adobe Reader Version 8.0 or later), strictly identical in full to the original tender	<input type="checkbox"/>

4.6.2 Technical proposal

The tender shall include a technical proposal demonstrating a good understanding of the tender requirements and the capability to satisfy them.

Tenderers shall describe as part of their technical proposal all prior experience relevant for performance of the Tasks requested.

Moreover, tenderers (whether being sole contractor or part of a consortium/grouping) are requested to demonstrate how their proposed methodology/strategy/organisation will guarantee the most efficient implementation and management of the requested Tasks.

In particular, the tenderers must include into the technical proposal:

	ENVELOPE 2 – TECHNICAL OFFER (one (1) ORIGINAL, two (2) PAPER COPIES and one (1) ELECTRONIC COPY per envelope)	
(1)	Duly filled in, signed and dated Executive Summary (max 2 pages) of the technical offer	<input type="checkbox"/>
(2)	Information required for evaluation of technical and professional capacity selection criteria	<input type="checkbox"/>
(3)	Technical Proposal , in accordance with the requirements of the present tender specifications, describing in particular: description of the methodology and quality of services (number and quality of staff members able to provide the service) for each Task; technical and logistics measures taken to ensure the quality of the services provided, including training programs for staff, system for control of quality, measures taken to ensure flexibility and continuity of services, measures on how to limit turnover, language and professional training of staff, etc	<input type="checkbox"/>

(5)	Simulation exercise proposal detailing each work package in accordance with Annex I.E	<input type="checkbox"/>
(6)	Confirmation of the tenderer's personnel readiness to sign a declaration on confidentiality and absence of conflict of interest with the GSA before commencing any service provision.	<input type="checkbox"/>
(7)	An electronic copy of each document submitted in the technical envelope on CD-ROM or USB stick with the full set of documents in machine readable format (MS Office 2003 or later, or Adobe Reader Version 8.0 or later), strictly identical in full to the original tender	<input type="checkbox"/>
(9)	Statement of Compliance to the Service Level Agreement	<input type="checkbox"/>

4.6.3 Financial offer

4.6.3.1 Content

The tender shall include a financial proposal. Here below is a summary of the content requirements of the technical proposal:

	ENVELOPE 3 – FINANCIAL OFFER	
(1)	Duly signed and dated financial proposal using the template in Annex I.D	<input type="checkbox"/>
(2)	An electronic copy of each document submitted in the financial envelope on CD-ROM or USB stick with the full set of documents in machine readable format (MS Office 2003 or later, or Adobe Reader Version 8.0 or later), strictly identical in full to the original tender	<input type="checkbox"/>

The financial offer must respect the following conditions:

4.6.3.2 Unit prices and total prices

Unit prices quoted in **Annex I.D**, must be firm and fixed and are not subject to revision. The unit prices in the financial offer will constitute the price list for the duration of FWC⁹, and shall include all costs and expenses which are necessary for performance of the tasks.

These cost and expenses comprise the effort for all the tasks (including drawing up quotations and reports) necessary for their performance, including:

- all activities included in Task 1 (section 2.1.1.1 of these Tender Specifications), except for the tasks explicitly mentioned in Table 1 of Annex I.D – Financial Tables of Answers;
- all other costs (administrative support and any support resource, coordination, quality control or currency conversion fees);
- all overheads (management of the firm, secretarial services, social security, wages, etc.) necessary for the performance of the tasks described

⁹ Price grid quantities estimates are provided by the GSA in Annex I.D. Such estimates will only be used by the GSA to simulate the cost competitiveness of tenderers against the most realistic scenario of implementation of the FWC. In this respect, quantity estimates are in no way binding. Upon signature of the FWC, only the unit prices provided by the tenderers in the duly completed tables of Annex I.D.

incurred directly and indirectly by the Contractor and/or subcontractors (if any) in performance of the tasks that will be entrusted to him.

4.6.3.4 VAT exemption

As the GSA is exempt from all taxes and dues, including value added tax (VAT), pursuant to Articles 3 and 4 of the Protocol on the privileges and immunities of the European Communities, these must not be included in the price.

4.6.3.5 Currency and exchange rates

The price tendered must be all-inclusive and expressed in Euro, including for countries which are not part of the Euro zone. For tenderers in countries which do not belong to the Euro zone, the price quoted may not be revised in line with exchange rate movements. It is for the tenderer to select an exchange rate and assume the risks or the benefits deriving from any fluctuation.

4.7 Submission

Tenders may be submitted by post mail, express mail, commercial courier or hand-delivered and are to be submitted not later than the relevant date and time specified in section 1.5 above to the following address:

European GNSS Agency
Procurement and Legal Department
Tender ref: GSA/OP/17/18
Janovskeho 438/2
170 00 Prague 7
Holesovice, Czech Republic

Tenders sent by post mail, express mail and commercial courier shall be addressed to this address not later than 23:59 (local time) of date as indicated in section 1.5. In this case, a receipt must be obtained as proof of submission.

In case the tender is hand-delivered, a receipt must be obtained as proof of delivery, signed and dated by the reception desk officer. The reception is open from 08.00 to 17.00 Monday to Thursday, and from 8.00 to 16.00 on Fridays. It is closed on Saturdays, Sundays, European Commission holidays and some Czech national holidays.

Upon submission of tenders by post mail, express mail, commercial courier or hand-delivery, tenderers shall send an email of notification of submission to tenders@gsa.europa.eu. The subject of the email shall be: "GSA/OP/17/18 submission of tender by [insert name of legal entity / consortium]"

4.8 Public opening of the tenders

The tenders will be opened on the date and time indicated in section 1.5 above, in the offices of the GSA, Janovskeho 438/2, Prague 7, Czech Republic.



This opening session will be public. **Maximum one representative of each tenderer may attend the opening of the tenders.** At the end of the opening session, the Chairman of the opening committee will indicate the name of the tenderers and the decision concerning the admissibility of each offer received. The prices indicated in each tender received will not be communicated.

Tenderers who wish to attend shall send a request (at least 5 (five) calendar days before the date of the opening) to the following e-mail address: tenders@gsa.europa.eu, indicating the name(s) of the attending person(s) and the tenderer (s)he represents. The subject of the email shall be: "GSA/OP/17/18: request from *[insert name of legal entity / consortium]* to participate to the opening session"

In order to be able to enter the GSA premises for the opening of the tenders, the attending person shall present an ID card or passport at the reception of the GSA.

4.9 Period of validity of the tenders

Period of validity of the tenders, during which tenderers may not modify the terms of their tenders in any respect: 9 (nine) months from the closing date for the submission of the tenders.

4.10 Contacts with the tenderers

Contacts between the GSA and tenderers are prohibited throughout the procedure save in exceptional circumstances and under the following conditions only:

Before the final date for submission of tenders:

- At the request of the tenderer, the GSA may provide additional information solely for the purpose of clarifying the nature of the contract.
- Any requests for additional information must be made in writing only to tenders@gsa.europa.eu. The subject line of the e-mail has to quote the reference of the procurement procedure: GSA/OP/17/18.
- Requests for additional information received after deadline specified in section 1.5 above will not be processed (*for practical reasons*).
- The GSA may, on its own initiative, inform interested parties of any error, inaccuracy, omission or any other clerical error in the text of the Invitation to Tender.

After the opening of tenders:

- If, after the tenders have been opened, some clarification is required in connection with a tender, or if obvious clerical errors in the submitted tender must be corrected, the GSA may contact the tenderer, although such contact may not lead to any alteration of the terms of the submitted tender.

4.11 Information for tenderers

The GSA will inform tenderers of decisions reached concerning the award of the contract in due course, including the grounds for any decision not to award a contract or to recommence the procedure.

If a written request is received, the GSA will inform all rejected tenderers of the reasons for their rejection and all tenderers submitting an admissible tender of the characteristics and relative advantages of the selected tender and the name of the successful tenderer.

However, certain information may be withheld where its release would impede law enforcement or otherwise be contrary to the public interest, or would prejudice the legitimate commercial interests of economic operators, public or private, or might prejudice fair competition between them.

4.12 Data protection specific to the tender process

Processing the reply to the invitation to tender involves the recording and processing of personal data. Such data will be processed pursuant to Regulation (EC) No 45/2001 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data.

Identity of the Controller: Unless indicated otherwise, replies to the questions and any personal data requested are required to evaluate the tender in accordance with the tender specifications and will be processed solely for that purpose by the Executive Director of the GSA (the Controller), Head of Administration and Head of Legal and Procurement Department (the Delegated Controllers).

Purpose of processing: Upon reception of your tender by the Controller, your personal data is collected and further processed for the purpose of the management and administration of the selection of procurement by GSA services.

Data concerned: personal data collected and further processed concern the tenderer and its staff or subcontractors (natural persons). Information can relate to the following data: name; function; contact details (e-mail address, business telephone number, mobile telephone number, fax number, postal address, company and department, country of residence, internet address); certificates for social security contributions and taxes paid, extract from judicial records; bank account reference (IBAN and BIC codes), VAT number, passport number, ID number; information for the evaluation of selection criteria or eligibility criteria: expertise, technical skills and languages, educational background, professional experience including details on current and past employment; declaration on honour that they are not in one of the exclusion situation referred to in article 93 and 94 of the FR.

Legal bases: The FR and the RAP

Lawfulness of processing: The lawfulness of the processing is based on Article 5(a), 5(c) and 5(d) of Regulation (EC) No 45/2001.

Recipients of the data processed: For the purpose detailed above, access to your personal data is given to the following persons, without prejudice to a possible transmission to the bodies in charge of a monitoring or inspection task in accordance with European Union law: (i) the GSA staff as well as outside experts and members of opening or evaluation committee and contractors who work on behalf of the GSA for the purposes of management of the procurement procedure and evaluation of the tenders, and the bodies charged with a monitoring or inspection task in application of European Union law (e.g. internal audits, Financial Irregularities Panel, European Anti-fraud Office - OLAF); (ii) members of the public; In case you are awarded a contract by the GSA, your personal data will be made public, in accordance with the GSA's obligation to publish information on the outcome of the procurement procedure and on the beneficiaries of funds deriving from the budget of the European Union (Article 90, 110 (2) and Article 30(3) of the FR,

respectively). The information will concern in particular your name and address, the amount awarded and the name of the project or programme for which you are awarded a contract. It will be published in supplement S of the Official Journal of the European Union and/or on the website of the GSA.

Information on the retention period of personal data: Files relating to tender procedures, including personal data, are to be retained by the GSA until procurement procedure is finalised, and in the archives for a period of 7 years following the end of the year when last payment has been made under the contract signed as a result of the procurement procedure. However, tenderers from unsuccessful tenderers have to be kept only for 7 years following the signature of the contract. Files may have to be retained also until the end of a possible audit if one started before the end of the above periods.

Technical storage information: Files relating to tender procedures, including personal data, are retained both in soft (electronic) and hard (paper) format in GSA servers/premises where access is granted in controlled manner strictly on basis of justified need-to-know.

Your personal data may also be registered in the Early Detection and Exclusion System (EDES) of European Commission if you are in one of the situations mentioned in Article 106 of the FR. For more information, see the Privacy Statement on http://ec.europa.eu/budget/explained/management/protecting/protect_en.cfm

The data subject's rights and contact data: Data subjects have the right of access and rectification (modification, correction or deletion) of their personal data at any time. Requests shall be addressed to the Controller via GSA Data Protection Officer at dpo@gsa.europa.eu by describing your request explicitly. Any rectification of your personal data will be taken into consideration from the data protection point of view. Special attention is drawn to the consequences of a request for deletion, as this may lead to an alteration of the terms of the tender and lead to exclusion as stated in Article 148 of the RAP. Data subjects are entitled to lodge an appeal with the European Data Protection Supervisor (EDPS) at edps@edps.europa.eu should they consider that the processing operations do not comply with Regulation (EC) 45/2001

5. List of Annexes

These Tender Specifications (Annex I to Invitation to Tender) have the following annexes:

- Annex I.A - Template Identification Sheet of the Tenderer
- Annex I.B - Template Declaration of Honour
- Annex I.C - Financial Statements relating to the Selection Stage
- Annex I.D - Template Financial Tables of Answers
- Annex I.E – Detailed definition of the Work Packages and Simulation Exercise
- Annex I.F - Service Level Agreement
- Annex I.G - Power of Attorney
- Annex I.H - Subcontractor Letter of Intent
- Annex I.I - Non-Disclosure Undertaking



- Annex I.J - Security Aspect Letter
- Annex I.K - GSMC Certification Procedure ref. GEN-PRO-GSA-GSMC-218309
- Annex I.L - GSMC Internal Rules for Shift Work
- Annex I.M – GSA policy on the Prevention and Management of Conflicts of Interests



ANNEX I.A - TEMPLATE IDENTIFICATION SHEET OF THE TENDERER

IDENTIFICATION OF THE TENDERER

(Each service provider, including subcontractor(s) or any member of a consortium or grouping, must complete and sign this identification form)

Identity	
Name of the legal entity	
Legal status of the legal entity	
Description of role within the Tenderer	
Date of registration	
Country of registration	
Registration number	
VAT number	
Description of statutory social security cover (at the level of the Member State of origin) and non-statutory cover (supplementary professional indemnity insurance) ¹⁰	
Address	
Address of registered office of legal entity	

¹⁰ For natural persons



Where appropriate, administrative address of legal entity for the purposes of this procurement process	
Contact Persons	
For procurement process management¹¹	
Surname: First name: Title (e.g. Dr, Mr, Ms) : Position (e.g. manager): Telephone number: Fax number: E-mail address:	
Contact person for the communications regarding the NDU	
Surname: First name: Title (e.g. Dr, Mr, Ms) : Position (e.g. manager): Telephone number: Fax number: E-mail address:	
Local Security Officer	
Surname: First name: Title (e.g. Dr, Mr, Ms) : Position (e.g. manager): Telephone number: Fax number: E-mail address:	
Legal Representatives	
For the signature of the NDU	
Names and functions of legal representatives and of other representatives of the legal entity who are	

¹¹ One person per tenderer (legal entity, group or consortium) has to be identified for the purposes of this procurement procedure. This person will be responsible for distributing information within the Tenderer.



authorised to sign contracts with third parties	
For the signature of the Contract	
Names and functions of legal representatives and of other representatives of the legal entity who are authorised to sign contracts with third parties	
Declaration by an authorised representative of the organisation¹² I, the undersigned, certify that the information given in this identification sheet is correct and that the identification sheet is valid.	
Surname: First name:	Signature:

¹² This person must be included in the list of legal representatives; otherwise the signature on the tender will be invalidated.



ANNEX I.G - TEMPLATE POWER OF ATTORNEY

(DESIGNATING ONE OF THE COMPANIES AS GROUP COORDINATOR AND GIVING IT POWER OF ATTORNEY)

We the undersigned:

– Signatory 1 [*Name, Function, Company, Registered address, VAT number*]

For [*Company name*] taking up the following role within the consortium with its qualification as [*enter company's qualification for its assigned role*].

– Signatory 2 [*Name, Function, Company, Registered address, VAT number*]

For [*Company name*] taking up the following role within the consortium with its qualification as [*enter company's qualification for its assigned role*].

–

– Signatory N [*Name, Function, Company, Registered address, VAT number*],

For [*Company name*] taking up the following role within the consortium with its qualification as [*enter company's qualification for its assigned role*].

each of us having the legal capacity required to act on behalf of our company,

HAVE AGREED AS FOLLOWS:

- (1) For that purpose, the group members designate company X as group coordinator.
[N.B. The group coordinator/prime must be one of the group members]
- (2) The group members confer on the group coordinator all the necessary powers to act on their behalf in connection with the procurement process **GSA/OP/17/18 – "SECURITY MONITORING SERVICES TO THE GSA"**.
- (3) This mandate involves in particular the following tasks:
 - The group coordinator shall sign any procurement related documents requiring the candidate's/tenderer's signature).
 - The group coordinator shall act as single point of contact for the GSA in connection with the procurement process.
 - If awarded, the group coordinator shall sign the FWC, specific contracts and addenda thereto, issue any invoices related to the supplies or the services and receive payments from the GSA on behalf of the group members.
 - The group coordinator shall act as single point of contact for the GSA in connection with supplies and the related services to be provided under the FWC in case awarded. It shall coordinate the provision of the supplies and the related services by the group members to the GSA, and shall ensure proper performance of the Contract.
- (4) In case of contract award, as co-signatories of the Contract, all the group members:
 - shall be jointly and severally liable vis-à-vis the GSA for the performance of the FWC, including any specific contracts thereunder;



- shall comply with the conditions of the FWC, including any specific contracts thereunder, and ensure the proper execution of their respective share of the supplies and/or the services.

(5) Payments by the GSA for the supplies or related services shall be made through the group coordinator's bank account.

[Provide bank details, name, address, account number, etc.]

Any modification to the present agreement/power of attorney must be explicitly approved by the GSA.

This agreement/power of attorney shall expire when all the contractual obligations of the group members towards the GSA in connection with the supplies and the services to be provided under the FWC, including any specific contracts thereunder, have lapsed. The parties may not terminate it before that date without the GSA's consent.

Signed at _____, on _____

Name		Name	
Function		Function	
Company		Company	
Name		Name	
Function		Function	
Company		Company	



ANNEX I.H - TEMPLATE LETTER OF INTENT

<Letterhead of the sub-contractor or other entity on whose resources to rely>

GSA/OP/17/18

"SECURITY MONITORING SERVICES TO THE GSA"

The undersigned: [...]

Name of the company/organization: [...]

Address: [...]

Declares hereby the commitment to collaborate in the execution of the tasks subject to the above procurement process and contract implementation, in accordance with the terms of the tender to which the present form is annexed, if the contract is awarded to [insert candidate's/tenderer's name] to make it available the competence (resources and other capacities) of our company as described under section 1 in the area described under section 2. below;

Further declares hereby accepting the terms and conditions set out in the draft FWC applying to subcontracting by returning this form filled in and signed.

Sub-contracting is intended as follows:

1. Brief description of the resources of the subcontractor required for the performance of the contract:

[...]

2. Brief description of the performance which will be rendered by the subcontractor:

[...]

3. Estimated proportionate value (in%) of contribution to the total contract value to be subcontracted to the present company/organization:

_____%

Full name

Date

Stamp/Signature

.....



ANNEX I.I – NON-DISCLOSURE UNDERTAKING

(name of undertaking entity)

the undertaking entity, hereinafter referred to as the **“Recipient”**, whose registered office is at:

_____ -

-

-

(Official address of Recipient in full)

represented, for the purposes of the signature of this non-disclosure undertaking (hereinafter the
“Undertaking”),

by

(insert (i) name of representative of Recipient duly empowered to sign the Undertaking and (ii) his/her function).

Article 1 – Definitions

For the purpose of this Undertaking:

“Agency” shall refer to European GNSS Agency (hereinafter also “the GSA”).

“Undertaking” shall refer to the present non-disclosure undertaking (hereinafter also “the NDU”) by the Recipient.

“Proprietary Information” shall mean any information or data of financial, personal, commercial or technical nature, including but not limited to, any reports, analyses, compilations, studies, interpretations, assumptions, estimates, projections, forecasts prospects, whether it relates to technical, pricing, legal or other information, including ideas, know-how, concept, designs, specifications and data, and whether it is in written, electronic, photographic, oral and/or any other form relating to the Purpose and/or disclosed by or on behalf of the GSA to the Recipient.

“Contract” shall refer to the legal commitment envisaged to be entered into between the Agency and the tenderer as a result of the Procurement Procedure.

"Classified" shall refer to the national or European Security classification of information (such as RESTREINT UE/EU RESTRICTED, CONFIDENTIEL UE/EU CONFIDENTIAL, SECRET UE/EU SECRET, TRÈS SECRET UE/EU TOP SECRET).

“Procurement Procedure” shall refer to procurement process with reference GSA/OP/17/18 – "SECURITY MONITORING SERVICES TO THE GSA"

"Purpose" shall refer to the Recipient's activities for preparing the tender subject to the Procurement Procedure and, in case of award, the Recipient's activities related to the provision of services subject to the corresponding Contract.

Article 2 – Confidentiality and conditions of access to and use of the Proprietary Information

2.1 The Proprietary Information is supplied to the Recipient solely and exclusively for the Purpose. The Proprietary Information cannot be used totally or partially, directly or indirectly, for any purpose other than the Purpose of this Undertaking, unless the GSA gives its prior written authorisation. In any case, the Recipient shall not use the Proprietary Information in a manner conflicting with the objectives of the European GNSS programmes.

2.2 The Recipient shall not copy, reproduce, distribute, communicate or otherwise make available the Proprietary Information to public, either in whole or in part, unless the GSA gives its prior written authorisation. The Recipient shall keep the Proprietary Information and any copies thereof secure by effective and reasonable means in such a way as to prevent unauthorised access. The Recipient shall be responsible for any disclosure of the Proprietary Information in breach of the provisions of the present Undertaking.

2.3 Without prejudice to section 2.4, the Recipient shall not disclose the Proprietary Information to persons inside and outside its organisation unless such persons (for the purposes of the present clause “Receiving Persons”) have a proven need to know for the Purpose. The Recipient shall ensure that the Receiving Persons are bound by the provisions of this Undertaking and fulfil the conditions of the tender specifications of the Procurement Procedure before releasing to such persons the Proprietary Information. The Recipient shall assume full responsibility towards GSA for any breach of the present undertakings by the Receiving Persons.

2.4. If the Proprietary Information is Classified, the Recipient shall request GSA authorisation to disclose such Proprietary Information to third parties and provide the GSA with an electronic copy of the non-disclosure undertaking signed by such third party or non-disclosure agreement between the Recipient and such third party with obligations not less stringent that provided in this Undertaking.

2.5 Handling of Classified Proprietary Information shall, in addition to the terms and conditions of this Undertaking, comply with the applicable security rules¹³.

2.6 Nothing contained in this Undertaking shall be construed as granting any right, title or interest in the Proprietary Information including any intellectual property right. The Recipient shall not itself, nor authorise any third party to, write, publish or disseminate any description of the Proprietary Information or elements of it, such as its structure or content for so long as it is bound by this Undertaking.

2.7 The Proprietary Information is provided "as is". The Recipient acknowledges that the GSA disclaims all warranties of any kind relating to the Proprietary Information, whether expressed or implied, including but not limited to, any implied warranty against infringement of third party property rights or as to merchantability or fitness for a particular purpose.

2.8 The Recipient acknowledges and accepts that the GSA will not be liable for any damage related to the disclosure of the Proprietary Information, even when such disclosure has been authorised by the GSA, including, but not limited to, damages for loss of profit, business interruption, loss of business information, or any other pecuniary loss arising out of the use of, or inability to use, the Proprietary Information.

2.9 When the Recipient becomes aware of any unauthorised use of the Proprietary Information or of any unauthorised copy of the Proprietary Information or of any unauthorised derivative work, it shall immediately inform the GSA thereof.

2.10 Should the Recipient breach any of its obligations under this Undertaking, and without prejudice to the right of the GSA to seek damages, the GSA may, by written notice to the Recipient, withdraw the right to use the Proprietary Information for the Purpose.

Article 3 – Limitation on protection of the Proprietary Information

The obligations set out in Article 2 are not applicable to information for which the Recipient can demonstrate that it:

- a) has come into the public domain prior to, or after, the date of receipt of the Proprietary Information from the GSA through no fault or unauthorised act of the Recipient;
- b) was already lawfully developed or acquired by the Recipient at the date of receipt of the Proprietary Information from the GSA;
- c) has been or is published without violation of this Undertaking;

¹³ Commission Decision (EU, Euratom) 2015/444 of 13 March 2015 on the security rules for protecting EU classified information.

- d) was lawfully obtained by the Recipient without restriction and without breach of this Undertaking from a third party, who is in lawful possession thereof, and under no obligation of confidence to the GSA;
- e) is disclosed pursuant to a request of a governmental or jurisdictional authority or is disclosed according to the law or regulations of any country with jurisdiction over the Recipient; in either case the Recipient, subject to possible constraints of such governmental or jurisdictional authority, shall immediately give the GSA a written notice of the above request and shall reasonably cooperate with the GSA in order to avoid or limit such disclosure; or
- f) was disclosed and/or used without restriction pursuant to written authorisation from the GSA.

Article 4 – Duration of this Undertaking and protection of the Proprietary Information

4.1 The effective date of this Undertaking shall be the date on which it is signed. This Undertaking shall remain in force for 10 (ten) years as from its signature unless a Contract is signed including confidentiality obligations according to the following paragraph. Following signature of such a Contract as a result of the tender, any information exchanged for the purpose of conclusion and execution of the Contract signed following the tender is not covered by this Undertaking but by the resulting Contract.

4.2 Upon the expiration of this Undertaking, the Recipient shall, always at its own costs, return to the GSA headquarters to the address indicated in Article 2.5 all the Proprietary Information and any copies made of them or, if the GSA so instructs the Recipient, destroy all the Proprietary Information and any copies of it. The destruction shall be certified in writing by the Recipient and sent to the GSA to legal@gsa.europa.eu without requiring the GSA's further request.

4.3 The Recipient shall use all reasonable endeavours to ensure that any third parties to whom the Recipient has supplied any Proprietary Information according to Articles 2.3 and 2.4 above, return/destroy (in line and with the previous paragraph, applying accordingly) such Proprietary Information and any copies made of them.

Article 5 – Applicable law; Dispute

5.1 This Undertaking shall be governed and construed in accordance with the laws of the European Union complemented when necessary by the law of Belgium.

5.2 The Recipient and the GSA shall make their best efforts to settle amicably all disputes arising in connection with this Undertaking. If such amicable settlement fails, the said dispute shall be finally settled by the General Court of the Court of Justice of the European Union in accordance with its rules of procedure.

Article 6 – Final provisions

If any term of this Undertaking is or becomes illegal, invalid or unenforceable in any jurisdiction, this shall not affect the legality, validity or enforceability in that jurisdiction of any other terms of this Undertaking, nor the legality, validity or enforceability in other jurisdictions of that or any other provision of this Undertaking.



In witness thereof, the Recipient has caused this Undertaking to be executed by its duly authorised representative,

Signature of representative of Recipient duly empowered ¹⁴ to sign the Undertaking	
Name	
Signature	
Position	
Date	

¹⁴ Signatory must enclose the document proving his/her due empowerment to sign on behalf of Recipient.