European GNSS Supervisory Authority

TENDER SPECIFICATIONS

Attached to Invitation to Tender No. GSA/OP/03/09

PROTECTOR

PRS Operational Tool to Evaluate and Counteract Threats Originating from Radio-sources

TABLE OF CONTENTS

I. STATEMENT OF WORK

I.1. BACKGROUND

The deployment of the European GNSS system Galileo should be completed and fully qualified by the end of 2013 (FOC: Full Operational Capability). The first Public Regulated Service (PRS) signals should be made available in the second half of 2010 (as part of the In-Orbit Validation phase) for validation and testing of the Galileo SIS, and later on to external users at FOC. The European GNSS Supervisory Authority (GSA) Security Centre is planned to be deployed as part of the FOC procurement phase and should be operative in 2012.

In order to have the PRS available at the very moment the Galileo system is operational, it is necessary to start, well in advance of the infrastructure deployment, the validation of the PRS users' functions (i.e. all the phases of the PRS receiver lifecycle, groups' management, denial orders, organisation of messages at MS level, etc.).

The PRS validation is planned to be achieved through a PRS Pilot Project, being the pre-operational phase of the PRS that the GSA will be defining in the first half of 2009 and that should run in the timeframe 2009-2013.

The PRS Pilot Project will consist in a series of activities devoted to the validation and/or preparation of PRS operations. In particular, the first activity will be the evaluation of the PRS management via the use of the PRS Management Simulator Tool.

In this time frame the GSA is also preparing the deployment of the PRS user segment, managing in the 7th FP the following programs:

- PROGRESS, for the definition and standardization of the PRS receivers;
- PROPHET, for the development of a S/W tool for the optimization of PRS management;
- FORTRESS, for the realization of a demonstrator of tamper-respondent techniques applied to the Security Module of PRS receivers.

I.2. PURPOSE OF THE CONTRACT

PROTECTOR is the acronym of "PRS Operational Tool to Evaluate and Counteract Threats Originating from Radio-sources". The contract's scope is the definition of the means needed to protect the European GNSS (Galileo and EGNOS) systems and services against radio-sources interferences in L-band, S-band, Ku-band and C-band (as detailed in par.I.4), to prevent service disruptions.

Within the present contract the technical and economical definition of a European system and service for the management of interference and jamming will be performed.

The objectives of the PROTECTOR contract are:

§ To produce an inventory of sources of interference and jamming in the EU GNSS bands, including SIS in L-band, TT&C in S-band, and navigation data up-link in C-band and in Ku-band;

§ To produce evolutionary requirements for the protection of Galileo/EGNOS against interference and jamming;

§ To propose and assess techniques to mitigate the impact of jamming and interference on GNSS receivers (at user segment and at infrastructure level);

§ To define the technical requirements of the Jamming and Interference Monitoring System (JIMS) and to define the interaction with the GNSS Security Centre (GSC);

§ To identify and assess possible models for managing JIMS service in the EU in order to facilitate cost-effective implementation of the service in the medium to long term;

- To gain clear understanding on the cost and practical implication of managing JIMS in the EU, in order to inform and support the GSA during the negotiations on the development of the services.

In the next paragraphs a detailed description of PROTECTOR tasks is shown.

I.3. LIST OF ACRONYMS

ATM	Air Traffic Management
C/No	Carrier over Noise_density ratio
CD-ROM	Compact Disk – Read Only Memory
CMS	Common Minimum Standards
CRPA	Controlled Reception Pattern Antenna
CW	Continuous Wave
DCN	Document Change Notice
DOA	Direction of Arrival
DVD	Digital Versatile Disk
EC	European Commission
ECSS	European Cooperation on Space Standardization
EGNOS	European Geostationary Navigation Overlay System
ESA	European Space Agency
ESM	Electronic Support Measures
ESNIS	European Satellite Navigation IndustrieS
EU	European Union
FAR	Final Acceptance Review
FOC	Full Operational Capability
FORTRESS	FORge for Tamper-RESpondent Security module
GDL	Guidelines
GNSS	Global Navigation Satellite System
GSA	GNSS Supervisory Authority
GSC	GNSS Security Centre
GSM	Global System for Mobile communications
GSMC	Galileo Security Management Centre
GSS	Galileo Sensor Station
ICD	Interface Control Document
IEC	International Electro-technical Commission
IOV	In Orbit Validation
IR-1	Intermediate Review 1
IR-2	Intermediate Review 2
ISO	International Organization for Standardisation
ITT	Invitation To Tender
JA	Joint Action

JIMS	Jamming and Interference Monitoring System
LSO	Local Security Officer
MAGIC	Management of Galileo Interference and Countermeasures
MCC	Master Control Centre
MRD	Mission Requirement Document
MS	Member State
MTR	Mean Term Review
NDA	Non Disclosure Agreement
NLES	Navigation Land Earth Station
NOTAM	NOtice to Air Men
OS	Open Service
OURD	Operator User Requirements Document
PACIFIC	PRS Application Concept Involving Future Interested Customers
POCP	Point Of Contact Platform
PP	(PRS) Pilot Project
PRN	Pseudo-Random Noise
PROGRESS	PROgramme for Governmental REceivers Specification and Standardisation
PROPHET	PRs Operations Performance Handy Evaluation Tool
PROTECTOR	PRS Operational Tool to Evaluate and Counteract Threats Originating from Radio-sources
PRS	Public Regulated Service
RD	Reference Document
RIMS	Ranging and Integrity Monitoring Station
SAL	Security Aspects Letter
SFREQ	Service Facility REQuirements
SIS	Signal In Space
SitCen	Joint Situation Centre of the European Union
SM	Security Module
SoL	Safety of Life
SoW	Statement of Work
SRD	System Requirements Document
SSRS	System-specific Security Requirements Statement
T&V	Threat and Vulnerability
TBC	To Be Confirmed
TETRA	TErrestrial Trunked Radio
To	Initial Time
TT&C	Telemetry Tracking and Control
UE	Union Européenne
VAT	Value Added Tax

I.4. NEED FOR A EUROPEAN JAMMING AND INTERFERENCE MONITORING CAPABILITY

It has been highlighted by several studies that intentional (jamming) and unintentional interference are serious and realistic threats to existing and future GNSS. Even GNSS services and systems with enhanced robustness against these threats, such as the Galileo PRS, would only bring full benefits to users and European governments if they come together with interference and jamming monitoring capability.

Any GNSS receiver could be disrupted by enough interference or jamming power. Moreover, GNSS sites are also vulnerable objectives. Therefore, to cope with jamming and interference, it is necessary:

- To define a system for the protection of GNSS signals and services, to be developed to safeguard the continuity and the protection of GNSS systems and services: the Jamming and Interference Monitoring System (JIMS);
- To develop techniques to mitigate the impact of jamming and interferences on GNSS receivers (at user segment and at infrastructure level).

The JIMS is basically a system for the monitoring (i.e. detection, characterisation and localisation) of power radiofrequency emitters that could have an impact on the availability and the reliability of GNSS services. It is an automated service based on a network of sensors (gathering a high number measurement of, say, the C/No in GNSS bands) and an intelligent central processing to elaborate the data. The centre then generates a regular update of the jamming radio maps all over Europe, to provide alarm to relevant institutions (Council of EU, GSA, ATM authorities etc) in case of detection of jamming or interference. The JIMS will also have some specific additional functions, such as mobile units for the precise localization of the jamming sources.

The JIMS is therefore a necessary capability to localise sources of disruption to GNSS and allow the public bodies to prevent and mitigate intentional and unintentional attacks to European GNSS.

To better focus on the issue of JIMS definition, it is useful to consider (Figure 1) how the different elements of GNSS (in rows)

- Galileo sites
- EGNOS sites
- PRS receivers
- National capabilities
- European deployable means

can contribute to the various steps of the system and service protection (in columns)

- Detection
- Characterization
- Localization
- Mitigation of impacts
- Removal of sources

and what are the specific targets of each element of GNSS.

	Detection	Characterization	Localization	Mitigation of impacts	Removal of sources	Specific target
Galileo sites	●	●	●	●		Protection of the system Local contribution to ESM
EGNOS sites	●	●	●	●		Protection of the system Local contribution to ESM
PRS Receivers	●	●	**(2)**	●		Protection of the receivers Local contribution to ESM
National capabilities	●	●	●		●	Local contribution to ESM Removal of sources
EU deployable means **(1)**	●	●	●		●	Local contribution to ESM Removal of sources

1) Under the control of the Joint Action, including potentially specific payloads on helicopters, trucks or other deployable ground means

2) Possible localisation of interferences by national or EU mapping of PRS receivers' C/No by DOA (with dedicated antennas)

Figure 1: Structure of the EU interference and jamming management

In the cells the black points indicate that a component of the GNSS can contribute to a specific step of protection of the system and the service; where no black point is present (grey cells) this component is not able to contribute.

The green cells represent the combination of GNSS elements and protection steps that primarily constitute the JIMS. In addition, the light-blue cells represent the contribution to the services and systems protection provided by the mitigation step, and that we can still consider a specialised function of the JIMS.

I.4.1. GALILEO AND EGNOS SITES

Let us consider the main elements inside the GNSS system (Galileo and EGNOS): all radio-frequency communication links are vulnerable to interference and jamming, and they can contribute to the JIMS (if equipped with specific devices) to detect, characterise, localise interference and jamming, and to mitigate their effects.

Concerning Galileo, we can identify:

- C-band up-link stations, for the upload to the satellites of the navigation and integrity message;
- S-band TT&C up/down-link stations, for the command and control of the satellites constellation and the monitoring of their status;
- L-band receiving Galileo Sensor Stations (GSS).

For EGNOS we can identify:

- Ku-band (towards Artemis satellite) and C-band (towards Inmarsat satellites) Navigation Land Earth Station (NLES) up-link stations;
- L-band receiving Ranging and Integrity Monitoring Stations (RIMS).

These elements of the GNSS systems can obviously contribute to the steps of detection, characterization and localisation of the sources of interference (green cells in the figure).

Mitigation of the effects of the sources is possible if the stations are equipped with specific means to reject the interference via spatial and/or frequency discrimination (light-blue cells). All these elements can actively contribute to the protection of the systems and contribute locally to the Electronic Support Measures (ESM).

I.4.2. PRS RECEIVERS

PRS receivers can play an important role as elements in the JIMS, if equipped with a secondary channel of communications, as explained below.

PRS receivers, as the Galileo and EGNOS sites, can detect and characterise interferences, measuring, for instance, the C/No at the antenna output.

Moreover, mitigation of the effects of moderate interference and jamming is achieved in PRS receivers by the peculiar characteristics of PRS (long PRN codes, larger bandwidth) and by specific techniques not used in commercial receivers for OS, due to the cost impact (blanking) and to export control constraints (CRPA).

Conversely, localisation of radio-sources via PRS receivers is possible:

- As a contribution to EU mapping of C/No: due to their diffusion, PRS receivers can represent an interesting set of sensors of C/No, distributed on large territories, and able to report this information to the JIMS centre;
- Via DOA (Direction of Arrival) technique, if the receiver is also equipped with dedicated high-gain antennas.

The targets of PRS receivers, as elements of the JIMS, are the local contribution to ESM, and their own protection. Of course, the contribution of PRS receivers to the JIMS is only possible if the receivers can transmit the relevant data of monitoring (detection, characterisation and possibly localisation of radio-sources) to some coordination centre via the secondary communication channel.

I.4.3. NATIONAL CAPABILITIES

As to National capabilities (for example, specific payloads embarked on helicopters or aircrafts, trucks or deployable ground means), they are able of course to detect, characterise and localise the sources of interference, and to contribute to the removal of the interference.

I.4.4. EUROPEAN DEPLOYABLE MEANS

European deployable means aim at the same targets of the National capabilities, but they operate under the control of the Joint Action (please refer to reference document [RD4]) in a different institutional context.

Please note that specific targets for National and European capabilities are also the local contribution to ESM and the removal of the interference/jamming sources.

I.5. CHARACTERISTICS OF A EUROPEAN JAMMING AND INTERFERENCE MONITORING SERVICE

The JIMS is a global concept of protection of EU GNSS systems and services against intentional and unintentional interferences, including:

- Monitoring (detection, characterisation, localisation) of interference and jamming;
- Mitigation of interference and jamming;
- Discrimination if interference is likely to be intentional (jamming) or unintentional;
- Identification of the capabilities that Member States should have for the management of interference[1];
- Identification of the missing elements to fully develop the PROTECTOR objectives.

The JIMS will be devoted to the continuous monitoring, mitigation and removal of "high" power GNSS interferers and jammers, where "high" is to be intended as the level that cannot be mitigated by the intrinsic GNSS system or receivers robustness.

Due to the complexity of the European GNSS and its distribution on Europe-wide extension, the JIMS will be composed by several elements having different tasks, to be connected and coordinated by the GSC[2] (the GNSS Security Centre, which includes the GSMC, the Galileo Security Monitoring Centre).

It is worth noting that a trade-off between monitoring (detection, characterisation, localisation) functions and mitigation function must be performed in the frame of PROTECTOR study, when defining a complex system like the JIMS.
Actually, very good monitoring functions, capable to identify with high accuracy and in a short time sources of interference, are extremely helpful to remove these sources, making the mitigation less interesting.
On the contrary, a less accurate monitoring system must rely more on the mitigation function in order to avoid disruption of the service, before the sources are effectively identified and removed.

The general structure of the JIMS should potentially comprise (if confirmed by PROTECTOR study) all the elements discussed in par. 1.4, namely:

- GNSS (Galileo/EGNOS) sites, equipped (as shown in fig. 1) with dedicated monitoring and mitigation functions;
- PRS receivers equipped with the secondary communication channel, acting as a network of sensor stations;
- National capabilities, to be deployed on the territory following instructions of the respective governments, upon reception from the GSC of the information of the presence of interference;
- European deployable means operating under the control of the Joint Action.

Furthermore, the JIMS should also comprise:

- The GSC, as the coordinating entity in Europe of the activities of interference management of the GNSS systems and services;
- The Point of Contact Platforms (POCPs), the interfaces used at National level and by other European institutions to send PRS management orders to the GSMC;
- A communication infrastructure that gathers from all the above elements the information about presence of interference/jamming in a specific area, and send it to the GSC.

1 One of the conclusions of the PACIFIC Study, outlined in the roadmap for the user exploitation of PRS, is that each Member State will have to define its approach to interference monitoring and response to threats.

2 Recent discussions among GSA and Member States representatives led to the conclusion that the role of the GSC (GNSS Security Centre) shall be defined to include the interference monitoring capability into its main missions.

I.6. MANAGEMENT AND COST OF THE JIMS

Besides the technical definition of the JIMS, PROTECTOR will have the following fundamental objectives:

- To identify and assess the possible models for managing JIMS services in the European Union, to facilitate cost-effective implementation of the service in the medium to long term
- To provide a clear understanding of the cost and practical implications of managing JIMS in the European Union, to inform and support the GSA into ongoing European negotiations on the development of the service.

PROTECTOR shall identify the EU Institutions and Member States' roles and responsibilities in managing the JIMS. It shall also clarify the roadmap towards the implementation, considering that part of the needed functions could be available in the initial implementation and part will be ongoing operational requirements.

Further point is the understanding of the necessary interfaces with Member States Government bodies, with European authorities (GSC, Council SitCen) and with existing infrastructure already used in Europe.

The programme shall also identify a range of possible organisational structures and models for discharging the responsibilities of managing the JIMS in the European Union.

Finally, the programme shall give reasonable estimations of costs and potential revenues associated with EU and national management of the JIMS, and user price sensitivity.

I.7. PAST WORK ON GALILEO INTERFERENCE MANAGEMENT

In the 6th FP the project MAGIC (MAnagement of Galileo Interference and Countermeasures) was launched, aiming at analysing the potential interfering scenarios for the Galileo signals, in particular in the OS and SoL bands.

The main tasks of the project included the study of suitable detection, characterisation, localization and mitigation strategies to be implemented in a dedicated mobile infrastructure.

Typical Interferences taken into account by the MAGIC Project were:

- CW and Chirp signals coming from spurious emission and/or from intentional disturber;
- Pulsed signals coming from RADAR equipments;
- Modulated signals coming from standard data transmission;
- Any disturb whose energy was enough to be detected.

The studied algorithms proved able to detect and classify interfering signals and provide their geographical coordinates; mitigation strategies were studied to minimize their impact on the Galileo signals.

As MAGIC gathered a high-level information and experience in the management of interference on Galileo bands, the contractor will be invited to take in consideration the main outcomes of the study and their applicability to the definition and design of the JIMS, in the frame of PROTECTOR contract.

I.8. REFERENCE DOCUMENTS

In the following table the documents labelled [RD1] to [RD9] are the initial set of inputs that the tenderers are invited to take into consideration for the preparation of the proposal.

Documents marked [RD1] to [RD4] constitute a selection of institutional framework documents of the Galileo programme, including the Council Joint Action 2004/552/CFSP.

For the preparation of the offer the tenderer shall apply:

- [RD5], the relevant ECSS Standards

- [RD6], the main ISO/IEC standards for IT security ([RD6]), in particular the Common Criteria for IT Security Evaluation, ISO/IEC 15408.

As well, the awarded contractor shall apply the above mentioned standards for any stage of the production of deliverables in the frame of the project.

The GSA will provide the tenderers with:

- [RD7], a selection of relevant deliverables of the PACIFIC study
- [RD8], the Operator User Requirements Document of the GNSS Security Centre
- [RD9], a GSA document establishing the Policy for the use and management of PRS in Member States

upon request and after the conclusion of a non-disclosure agreement for the classified documents. In that respect, tenderers shall send a request through their Local Security Officer (LSO), at least 30 calendar days before the deadline, to the e-mail address tenders@gsa.europa.eu indicating the name and address of the tenderer and the name of the LSO, as well as proof that the LSO is appointed in this position by the Company. Tenderers shall send with their request a scanned version of the Non Disclosure Agreement provided in Annex 8, duly completed, while the original signed documents (two original copies) shall be sent in parallel by conventional mail at:

European GNSS Supervisory Authority
Rachelle Antal
L56 07/18
B-1049 Brussels (Belgium)

Tenderers who fail to submit the offer must return all documents provided by the GSA within two months following the deadline for the submission of the offer.

Tenderers who submit the offer but are not awarded the contract must return all documents provided by the GSA within two months following publication of the award notice.

The contractor, to perform its activities, will be granted access to at least the set of documents marked [RD10] to [RD24], namely:

- [RD10], further deliverables of PACIFIC study, some of which are RESTREINT UE
- [RD11], a set of deliverables of the MAGIC study
- [RD12] to [RD20], Galileo IOV and C/D/E1 documents produced by ESA or ESNIS, which are classified from RESTRICTED to SECRET level
- [RD21], the Galileo Security Classification Guide (see also par. I.12)
- [RD22] to [RD23], relevant deliverables of PROGRESS programme, either in draft or final issue, according to the availability allowed by the PROGRESS work plan
- [RD24] is the Galileo SSRS.

The mechanism for receiving a copy of the listed documents will be defined in the Security Aspects Letter (SAL), which will be attached to the Contract.

The GSA could decide to provide the contractor with further documents, if deemed relevant for the activities of PROTECTOR programme.

As well, the contractor is requested to provide at the KOM an initial list of input documents not listed in this SoW, which are expected to be used during the contract. The list shall report title, reference number and owner of the document, availability in the company/ies, justification of the request ("need-to-know").

Input Documents	
Documents to prepare the offer[3]	
RD1	Council Regulation (EC) No 1321/2004 of 12 July 2004 on the establishment of structures for the management of the European satellite radio-navigation programmes (see http://ec.europa.eu/dgs/energy_transport/galileo/documents/official_en.htm)
RD2	Council Regulation (EC) No 1942/2006 of 12 December 2006 amending Regulation (EC) No 1321/2004 on the establishment of structures for the management of the European satellite radio-navigation programmes (see http://ec.europa.eu/dgs/energy_transport/galileo/documents/official_en.htm)
RD3	Regulation (EC) No 683/2008 of the European Parliament and of the Council of 9 July 2008 on the further implementation of the European satellite navigation programmes (EGNOS and Galileo) (see http://ec.europa.eu/dgs/energy_transport/galileo/documents/official_en.htm)
RD4	Council Joint Action 2004/552/CFSP of 12 July 2004 on aspects of the operation of the European satellite radio-navigation system affecting the security of the European Union (see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004E0552:EN:NOT)
RD5	ECSS Standards (see http://www.ecss.nl)
RD6	Main ISO/IEC Standards for IT Security (i.e., 13335, 17799, 27001, 15408)
RD7	Selection of relevant PACIFIC Study Deliverables (some RESTREINT UE)
RD8	GSMC OURD (RESTREINT UE)
RD9	Policy for the use and management of PRS in Member States (RESTREINT UE)
Project documents[4]	
RD10	Further deliverables of the PACIFIC study
RD11	Relevant deliverables from MAGIC study
RD12	Galileo Global Component SRD
RD13	Galileo Global Component SRD Classified Annex
RD14	Galileo SIS ICD
RD15	Galileo SIS ICD Classified Annex
RD16	GSMC SFREQ
RD17	GSMC SFREQ Classified Annex
RD18	GSMC-GMS ICD
RD19	GSMC-GMS ICD Classified Annex
RD20	Galileo Threats and Vulnerabilities Analysis
RD21	Galileo Security Classification Guide
RD22	Functional requirements of the SM [TBC]
RD23	ICD of the PRS SM
RD24	Galileo SSRS

[3] Documents publicly available or released upon specific request to the GSA in accordance with section I.7.
[4] Documents released only to the contractor.

I.9. WORK STRUCTURE

The specific tasks to be developed by the contractor in the frame of the PROTECTOR are:

Task 1 Management

Task 2 Analysis and risk assessment of interference sources in GNSS bands

Task 3 JIMS concept definition

Task 4 Galileo and EGNOS in JIMS

Task 5 PRS receivers in JIMS

Task 6 National and European deployable means in JIMS

Task 7 Interaction JIMS-GSC

Task 8 Management and costing models of the JIMS

Task 9 Way forward towards JIMS implementation

In the following sections, T_0 is defined as the day of the kick-off meeting, unless otherwise agreed between the GSA and the contractor at the kick-off meeting.

I.9.1. TASK 1: MANAGEMENT

I.9.1.1. Description

The Task comprises the overall management for the contract.

The main activities related to the management of the project are:

- Technical project coordination
- Contractual management
- Organization and coordination of internal communication flows
- Documentation management
- Tracking of project status
- Establishment and maintenance of the travel plan
- Review and verification of deliverables
- Organization of progress meetings (calling notice, agenda, chairing and reporting)[5]
- Organization of reviews
- Coordination between the different activities as necessary
- Project status reporting
- Travel plan

In case of grouping, the contractor coordinator shall also prepare a Management Plan document to facilitate co-operation within the project, by defining a set of rules for the organization of the day-to-day co-operative work. This document basically serves to ensure that each member of the team has the same references and will follow the same project's rules.

A Draft Management Plan shall be included in the offer.

[5] First level progress meetings will be chaired by the Customer

I.9.1.2. Deliverables

Ref	Title	Delivery	Comments
D1-1	Management Plan	T_0+1 month	
D1-2.x	Status Report, including updated Travel Plan	Every 3 months	It shall include both technical and administrative status and activities, and risk mitigation plan
D1-3	MTR Report	T_0+8.5 months	2 weeks prior to the Mid-term Review (To + 9 months)
D1-4	FAR Report	T_0+17.5 months	2 weeks prior to the FAR (To + 18 months)

I.9.1.3. Meetings

A progress meeting shall be organized every 3 months to present the status of the work and steer the next period.

Project status reports shall be submitted to the GSA two weeks ahead of the project meetings.

Technical coordination meetings shall be held (via teleconference) on GSA request to progress on each specific topic as necessary.

A MTR meeting shall be held at the half of the duration of the project. The MTR report shall be submitted two weeks prior to the MTR meeting.

A FAR meeting shall be held at the end of the project. The FAR report shall be submitted two weeks prior to the FAR meeting.

Section I.11 contains an overview of project meetings, milestones and associated deliverables.

I.9.2. TASK 2: ANALYSIS AND RISK ASSESSMENT OF INTERFERENCE SOURCES IN GNSS BANDS

In this Task the contractor shall perform an inventory of the possible interference or jamming sources that could degrade the system performance or block the services at Galileo and EGNOS system level, in particular considering:

- Galileo sites
  - C-band uplink stations (navigation and integrity messages)
  - S-band TT&C stations
  - L-band Galileo Sensor Stations (GSS)
- EGNOS sites
  - Ku-band and C-band up-link Navigation Land Earth Station (NLES)
  - L-band Ranging and Integrity Monitoring Stations (RIMS)

Starting from the T&V analysis made for Galileo ([RD20]), the contractor shall identify the threat on the systems originating by the identified interference and jamming sources, assess the risk and propose countermeasures involving update in the security requirements (i.e., in the SSRS for Galileo, in dedicated security requirements in the EGNOS MRD), including the review of technological capabilities that could be used.

The residual vulnerabilities shall be identified for the Galileo and EGNOS radio-links.

The contractor shall also propose scenarios showing the credibility of the analysed threats.

I.9.2.1. Duration

This activity will have a duration of 3 months starting at T_0.

I.9.2.2. Deliverables

Ref	Title	Delivery	Comments
D2-1	Report on analysis and risk assessment of interferences to the Galileo and EGNOS systems	T_0+3 months	
D2-2	Report on threats scenarios involving Galileo and EGNOS systems	T_0+3 months	
D2-3	GNSS T&V update, including Galileo SSRS updates and EGNOS MRD updates	T_0+3 months	

I.9.3. TASK 3: JIMS CONCEPT DEFINITION

I.9.3.1. Description

The contractor shall elaborate a global concept of a European interference and jamming detection and mitigation, defining the MRD of the system.

The Task shall include the review of the existing capabilities suitable to be part of the JIMS and the definition of the JIMS structure.

In particular, the contractor shall develop the concepts shown in par. I.4 and I.5, including:

- The GNSS (Galileo/EGNOS) sites, equipped with monitoring and mitigation functions;
- The set of PRS receivers equipped with the secondary communication channel, acting as a network of sensor stations;
- National capabilities to be deployed on the territory following instructions of the respective governments;
- European deployable means operating under the control of the Joint Action ([RD4]) in a European institutional context;
- The communication infrastructure, which gathers from all elements the information about presence of interference/jamming;
- The interface with the GSC, POCPs or any other identified entity.

Output of the Task shall be a "Phase A study output" of the JIMS, indicating how in the JIMS the monitoring, mitigation and removal functions are distributed among the various components. In doing the analysis, the contractor shall make the trade-off between monitoring and mitigation capabilities, as shown in par. 1.5.

I.9.3.2. Duration

This activity will have a duration of 3 months starting at T_0+3 months.

I.9.3.3. Deliverables

Ref	Title	Delivery	Comments
D3-1	Identification of European capabilities to monitor, mitigate and remove interferences and jamming	T_0+6 months	
D3-2	Report of JIMS concept definition	T_0+6 months	
D3-3	Phase A output package for the JIMS concept definition	T_0+6 months	

I.9.4. TASK4: GALILEO AND EGNOS IN JIMS

I.9.4.1. Description

The Task shall include the detailed definition of the contribution of Galileo and EGNOS sites to the JIMS, following the JIMS concept developed in Task 3.

The contractor shall identify, for the sites of Galileo and EGNOS, the possible contributions to JIMS, and analyze the protection needs of the sites against interference.

According to a GSMC requirements ([RD8]) , the GSC "shall be able to request that the GCC or relevant Service Facilities provide all past user data broadcast on the Galileo CS and External Regional Integrity Systems (ERIS), in order to allow security analysis if required".

Furthermore, "On request, the GSMC shall provide the GSA with information on broadcast ERIS, Galileo CS user data and Galileo OS/SOL authentication data."

Therefore, Galileo and EGNOS interference monitoring shall also be conducted by monitoring the Galileo SoL/CS data and EGNOS ERIS data.

Following these needs, the contractor shall detail the need for new capabilities to be implemented, and shall elaborate proposals of DCN's to the Galileo MRD and SSRS, and to the EGNOS MRD.

I.9.4.2. Duration

This activity will have a duration of 3 months starting at T_0 + 6 months.

I.9.4.3. Deliverables

Ref	Title	Delivery	Comments
D4-1	Report on the use of Galileo sites as element of the JIMS, including new capabilities to be implemented	T_0+ 9 months	
D4-2	Report on the use of EGNOS sites as elements of the JIMS, including new capabilities to be implemented	T_0+ 9 months	
D4-3	Proposals of updates (DCNs) to the Galileo MRD and SSRS	T_0+ 9 months	
D4-4	Proposals of updates (DCNs) to the EGNOS MRD	T_0+ 9 months	

I.9.5. TASK 5: PRS RECEIVERS IN JIMS

I.9.5.1. Description

This Task is devoted to the definition of the use of PRS receivers in the JIMS.

The contractor shall identify and assess the suitable techniques for the improvement of interference mitigations at PRS receiver level (say, blanking techniques etc.), to enhance the intrinsic robustness against jamming due to the specific characteristics of the PRS SIS.

According to what is detailed in par. I.4 and I.5, the contractor shall produce an analysis of the requirements of a PRS receiver equipped with enhanced mitigation capabilities and secondary communication (a "Phase A study"), and a detailed implementation file of these features in a PRS receiver (a "Phase B study").

The contractor shall moreover detail the possibility to use PRS receivers as a contribution to EU mapping of, for example, C/No, provided they can be linked to the GSC and/or the POCPs via terrestrial link (say, TETRA, GSM).

The contractor shall also define the requirements of the communication links (bandwidth, link availability etc) and introduce or update the relevant GSC and POCP requirements accordingly.

I.9.5.2. Duration

This activity will have a duration of 6 months starting at T_0+6 months

I.9.5.3. Deliverables

Ref	Title	Delivery	Comments
D5-1	Intermediate report on PRS receivers use in JIMS	T_0+9 months	
D5-2	Report on the architecture of the communication link PRS - JIMS	T_0+9 months	
D5-3	Final report on PRS receiver use in JIMS	T_0+12 months	
D5-4	System requirements (Phase A) and implementation requirements (Phase B) for PRS receivers' contribution in JIMS	T_0+12 months	
D5-5	DCNs to the GSC and POCP requirements	T_0+12 months	

I.9.6. TASK 6: NATIONAL AND EUROPEAN DEPLOYABLE MEANS

I.9.6.1. Description

In this Task the contractor shall define the use in JIMS of possible deployable means that could be needed at National and European level, for the removal of interferences and jamming.

In both options, deployable means should be represented by specific payloads embarked on helicopters or aircrafts, trucks or other deployable ground means, able to detect, characterise and localise the sources of interference, and so to contribute to the removal of the interference.

National capabilities (as described in par. 1.4 and I.5) will be normally deployed on National territories following instructions of the respective governments, upon reception from the GSC or POCPs of the information as to the presence of interference.

European deployable means aim at the same targets of the National capabilities, but they operate under the control of the Joint Action in a different institutional context.

The contractor shall analyse the capabilities of deployable means for both ground-based and airborne cases, identify the needs in terms of communication links with the GSC or POCPs, time to reaction to an alert (especially in case of Joint Action implementation) and time needed to identify the interference.

The contractor shall therefore prepare a definition file (a "Phase A study") for both European and National deployable means, presenting also some characteristic scenario of intervention in case of National alert and in case of Joint Action implementation.

Following the definition file for National deployable means, the contractor shall also draft a document of Guidelines and Common Minimum Standards (GDL/CMS) for the implementation of interference management in Member States

I.9.6.2. Duration

This activity will have a duration of 3 months starting at T_0+9 months

I.9.6.3. Deliverables

Ref	Title	Delivery	Comments
D6-1	Phase A output package for the use of National deployable means in JIMS	T_0+12 months	
D6-2	Phase A output package for the use of National deployable means in JIMS	T_0+12 months	
D6-3	Guidelines and Common Minimum Standards for the implementation of interference management in Member States	T_0+12 months	

I.9.7. TASK 7: INTERACTION JIMS – GSC/POCPs

This Task is devoted to the definition of the communication link between JIMS and GSC/POCPs. The contractor shall define the network architecture (fully terrestrial, terrestrial + satcom) and the related parameters (required bandwidth, data encryption etc).

The contractor shall also verify if the current architectures of the GSC and POCPs are compliant with the new functions introduced by the interaction with the JIMS, and propose possible changes and updates in the GSC OURD.

During this Task the contractor shall also identify, in cooperation with the GSA, 3rd parties interested in the information produced by the JIMS, and define the way to disseminate the relevant data (for instance, as it is done in aviation field with the NOTAM communications).

I.9.7.1. Duration

This activity will have a duration of 3 months starting at T_0+12 months

I.9.7.2. Deliverables

Ref	Title	Delivery	Comments
D7-1	Report on architectural design of the link JIMS – GSC/POCPs	T_0+15 months	
D7-2	DCNs to update the GSC OURD and the Galileo SSRS	T_0+15 months	
D7-3	Report on dissemination strategy of JIMS data to 3rd parties	T_0+15 months	

I.9.8. TASK 8: MANAGEMENT AND COSTING MODELS OF THE JIMS

In this Task the contractor shall identify and assess the possible models for managing JIMS services in the European Union, to facilitate cost-effective implementation of the service in the medium to long term. The contractor shall also provide a clear understanding of the cost and practical implications of managing JIMS in the European Union, to inform and support the GSA input into ongoing European negotiations on the development of the service

In particular, the contractor shall prepare a report, identifying:

- EU Institutions and MSs' roles and responsibilities in managing the JIMS;
- whether the needed functions in JIMS relate to the initial implementation of the service or are an ongoing operational requirement;
- consideration of the necessary interfaces between:
  - MSs Government bodies,
  - European authorities (GSC, Council SitCen),
  - existing infrastructure already used in Europe;
- a range of possible organisational structures and models for discharging in EU responsibilities of managing the JIMS.

The contractor shall identify possible options, setting out the minimum feasible level of EU and Government involvement on organisational and financial levels.
The options shall clearly identify whether EU and Government involvement should be continuous or related only to the initial establishment of the service, and assess the advantages and disadvantages of the options above identified against appropriate criteria including, for instance:

- cost to public purse;
- extent of any structural/administrative changes required;
- security requirements;
- expected willingness of identified players (whether public or private sector organisations) to participate;
- the flexibility to cope with possible user numbers (options should be considered against a number of plausible user demand ranges);
- specific assessment of the risks of each option to the various elements of the EU bodies and national interests (e.g. financial, security, industrial).

Moreover, the contractor shall identify the first practical steps to assess feasibility of favoured options, namely:

- identification of organisations (public or private) which could manage, or contribute to the management of, JIMS in EU bodies and EU MSs;
- initial sounding out on ability to carry out this/these role(s), and identification of the key factors or barriers that would affect both their level of interest and costs;

- assessment of likely timetable for implementation of JIMS and estimation of speed of uptake of service by users in EU;
- consideration of what this means for the GSA in terms of establishing structures to manage the service..

Finally, the contractor shall elaborate an estimation of costs and potential revenues associated with EU and national management of the JIMS service, and user price sensitivity.

I.9.8.1. Duration

This activity will have a duration of 9 months starting at T_0+9 months

I.9.8.2. Deliverables

Ref	Title	Delivery	Comments
D8-1.1	1st Interim report on the definition of models for managing JIMS services in Europe	T_0+12 months	
D8-2.1	1st Interim report on cost and practical implications for the managing of JIMS services in Europe	T_0+12 months	
D8-1.2	2nd Interim report on the definition of models for managing JIMS services in Europe	T_0+15 months	
D8-2.2	2nd Interim report on cost and practical implications for the managing of JIMS services in Europe	T_0+15 months	
D8-1.3	Final report on the definition of models for managing JIMS services in Europe	T_0+18 months	
D8-2.3	Final report on cost and practical implications for the managing of JIMS services in Europe	T_0+18 months	

I.9.9. TASK 9: PREPARATION OF THE WAY FORWARD TO THE JIMS IMPLEMENTATION

In this Task the contractor shall draw the conclusions of the overall programme, and prepare the way forward for the implementation of the JIMS.

In particular, the contractor shall:

- Support the definition and development of PRS receivers as elements of the JIMS;
- Support the preparation of the Phase C/D of the PRS receivers with enhanced mitigation capability and secondary communication channel;
- Finalise a Phase B package for the contribution of National and European deployable means to the JIMS.

I.9.9.1. Duration

This activity will have a duration of 3 months starting at T_0+15 months

I.9.9.2. Deliverables

Ref.	Title	Delivery	Comments
D9-1	Report on the way forward for the implementation of the JIMS	T_0+18 months	
D9-2	Preparation of Phase C/D of enhanced PRS receivers	T_0+18 months	
D9-3	Phase B output package of European deployable means contribution to JIMS	T_0+18 months	

I.10. PROJECT DURATION

The project activities shall start at T_0 and will end after an estimated period of 18 months.

I.11. PROJECT MEETINGS AND MILESTONES

The following table summarises the meetings that shall be held between the contractor and the GSA. The table also summarises the deliverables that shall be ready by the meeting.

Milestones of the project are KOM, MTR and FAR (in bold in table). The milestones will be considered as having been achieved once all the relevant deliverables have been received and approved by the GSA. The achievement of a milestone will trigger the (interim) payment as further detailed in Article I.4 of the draft contract (Annex 7 hereto).

Deliverables that are not included in the milestones below must be delivered at the latest by the contractor's request for payment of the balance.

It is to be noted that, unless the GSA and the contractor have agreed in writing on the postponement of a deliverable, the GSA may reduce or recover payments according to Article II.1.9 draft contract if the contractor delays the performance of the contract.

Project Meeting	Review	Venue	Objective	Sched.	Deliver.
Kick-Off Meeting	KOM	GSA	To authorize the start of project activities by GSA and to clarify open points and details of the project	T_o	
1st Progress Meeting	PM-1	Contractor	To review the work performed during the first trimester of the project duration	T_o + 3 months	D1-1 D1-2.1 D2-1 D2-2 D2-3
2nd Progress Meeting	PM-2	Contractor	To review the work performed during the second trimester of the project duration	T_o + 6 months	D1-2.2 D3-1 D3-2 D3-3
Mid-term Review	MTR	GSA	To assess the accomplishment of the project over the 1st half of activities and to steer the activities for the 2nd half of the project	T_o + 9 months	D1-2.3 D1-3 D4-1 D4-2 D4-3 D4-4 D5-1 D5-2

Project Meeting	Review	Venue	Objective	Sched.	Deliver.
3rd Progress Meeting	PM-3	Contractor	To review the work performed during the 4th trimester of the project duration	T_o + 12 months	D1-2.4 D5-3 D5-4 D5-5 D6-1 D6-2 D6-3 D8-1.1 D8-2.1
4th Progress Meeting	PM-4	Contractor	To review the work performed during the 5th trimester of the project duration	T_o + 15 months	D1-2.5 D7-1 D7-2 D7-3 D8-1.2 D8-2.2
Final Acceptance review	FAR	GSA	To draw conclusions on the project outcome, collect recommendations for future work, approve final deliverables and disseminate accomplishments.	T_o + 18 months	D1-2.6 D1-4 D8-1.3 D8-2.3 D9-1 D9-2 D9-3

I.12. CLASSIFICATION OF DOCUMENTS

In performing the different activities, the contractor and the involved sub-contractors shall handle information which is classified up to CONFIDENTIEL UE level.

The capacity to handle classified information up to CONFIDENTIEL UE level is a selection criterion for the awarding of the contract.

Neither actual PRS operational parameters nor cryptographic material will be handled during the performance of the contract.

At the beginning of the activities, the GSA will provide the contractor with the necessary information regarding the classification of the information (the Galileo Security Classification Guide, [RD21]) with the relevant regulations protecting this information.

During the project, depending on the results, the GSA might also decide on the appropriate level of classification of the information.

I.13. DELIVERABLES

The precise nature of the deliverables and reports required is specified under each individual task description in section I.9.

The GSA shall have 30 calendar days from receipt of the deliverables to approve or reject them.

Within 15 calendar days of receiving the GSA's comments or request for clarification, the contractor shall submit additional information or a new deliverable.

Reports and other written deliverables (e.g. presentations, recommendations and plans) shall be given to the GSA in one hardcopy and two softcopies (one in MS Word and the other in PDF format).

A consolidated version of all reports and other written deliverables due by FAR shall be given to the GSA on a CD-ROM/DVD at FAR. The CD-ROM/DVD shall have a registry file (an Excel table) listing each deliverable, the task it relates to, its title, its reference number, its issue/version number and the date it was released on.

I.14. PLACE OF PERFORMANCE

The contract shall be performed at the contractor's premises, except when indicated otherwise in this SoW.

Meetings between the contractor and the GSA shall be held at GSA premises in Brussels, unless agreed otherwise. All costs incurred by the contractor in the performance of the contract, including travel, accommodation and subsistence costs, shall be borne by the contractor.

I.15. CONTRACT VALUE

The estimated allocated budget for the contract is € 1.000.000 (VAT excluded). The price is not subject to revision or escalation.

II. TERMS OF CONTRACT

In drawing up his offer, the tenderer should bear in mind the provisions of the draft contract attached to this invitation to tender. Any limitation, amendment or denial of the terms of contract will lead to automatic exclusion from the procurement procedure.

Tenderers should especially take into consideration Article II.3 of the draft contract regarding conflict of interests. Specifically, tenderers in their offers will be requested to demonstrate their independence from main companies/actors involved in the development of the EU GNSS systems and how potential conflict of interests with such companies/actors would be solved.

Special attention should also be brought to the requirements as contained in the SAL (see Annex III of the draft contract).

The GSA may, before the contract is signed, either abandon the procurement procedure or cancel the award procedure without the tenderers being entitled to claim any compensation.

The GSA may suspend the procurement procedure and may take whatever measures are necessary, including the cancellation of the procurement procedure under the conditions laid down in Article 103 Council Regulation (EC, Euratom) No 1605/2002 of 25 June 2002 on the Financial Regulation application to the general budget of the European Communities, as amended by Council Regulation (EC, Euratom) No 1995/2006.

II.1. Terms of payment

Payments shall be made in accordance with the provisions specified in the service contract.
Tenderers may choose to refuse the planned pre-financing. In that case, they shall inform the GSA as soon as possible, preferably within the financial section of their offers.

II.2. Financial guarantees

Guarantee on pre-financing
For any pre-financing higher than 100 000 EUR, a financial guarantee equivalent to the amount of the pre-financing will be requested. Depending on the financial situation of the tenderer, GSA may ask for the financial guarantee for amounts lower than 100 000 EUR.

II.3. Subcontracting

If the tenderer intends to subcontract part of the service, he shall indicate in his offer which part(s)/task(s) will be subcontracted and to what extent (% of the total contract value).

Tenderers must inform the subcontractor(s) that Article II.17 of the contract will be applied to them. The contractor shall be responsible for ensuring that all subcontracting activities are undertaken in accordance with the rules set out in the SAL.

Once the contract has been signed, Article II.13 of the above-mentioned contract shall govern the subcontracting.

II.4. Legal form to be taken by the grouping of service providers to whom the contract is awarded

Groupings, irrespective of their legal form, may submit bids. Tenderers may, after forming a grouping, submit a joint tender on condition that it complies with the rules of competition. Such groupings (or consortium) must specify the company or person heading the project and must also submit a copy of the document authorising this company or person to submit a bid. If awarded, the contract will be signed by the company of the person heading the project, who will be, vis à vis GSA, the only contracting party responsible for the performance of this contract.

Tenders from a consortium of firms or groups of service providers, contractors or suppliers must specify the role, qualifications and experience of each member of the consortium or group. Each member must provide all the necessary documents for assessing the bid as a whole with regard to the exclusion criteria, selection criteria (all of them) and award criteria.

III. FORM AND CONTENT OF THE TENDER

III.1. General

Tenders must be written in one of the official languages of the European Union. However, and due to the technical nature of the project, tenderers are invited to submit their bids (or at least the technical part thereof) preferably in English.

Tenders must be clear and concise, with continuous page numbering, and assembled in a coherent fashion (e.g. bound, stapled). Since tenderers will be evaluated on the content of their submitted bids, they must make it clear that they are able to meet the requirements of the specifications.

IMPORTANT NOTE: in order to assess the required effort, the GSA will provide tenderers with documents [RD7], [RD8] and [RD9] (see for more details point I.8 above), upon request, and after the conclusion of a NDA for the classified documents (see Annex 8). Tenderers shall send a request through their LSO, at least 30 calendar days before the specified deadline for the submission of offers, to the e-mail address tenders@gsa.europa.eu, indicating the name and address of the tenderer and the name of the LSO, as well as proof that the LSO is appointed in this position by the requesting tenderer. They shall also fill in and sign the Non Disclosure Agreement provided in Annex 8, send a scanned version by e-mail to tenders@gsa.europa.eu, while the original signed documents (two original copies) shall be sent in parallel by conventional mail at:

European GNSS Supervisory Authority
Rachelle Antal
L56 07/18
B-1049 Brussels
Belgium

III.2. Structure of the tender

All tenders must include three sections i.e. an administrative, a technical and a financial offer.

III.2.1. Section One: Administrative offer

This section must provide the following information, set out in the standard identification forms attached to these tender specifications (Annexes 1, 2 and 3):

- Tenderers' identification (Annex 1)

– All tenderers must provide proof of registration, as prescribed in their country of establishment, on one of the professional or trade registers or provide a declaration or certificate.

– If the tenderer is a natural person, he/she must provide a copy of the identity card/passport or driving licence and proof that he/she is covered by a social security scheme as a self-employed person.

  Each service provider (including subcontractor(s) or any member of a consortium or grouping) must complete and sign the identification forms in Annex 1 and also provide above-mentioned documents.

- Financial identification (Annex 2)

The bank identification form must be completed and signed by an authorised representative of the tenderer. In the case of a grouping, this form must only be provided by the person heading the project.

- Legal entities (Annex 3)

  The legal entity form in Annex 3 must be completed in and should be accompanied by requested supporting documents. In the case of a grouping, this form must only be provided by the person heading the project.

- Declaration regarding exclusion criteria (Annex 4)

  Please refer to Article IV.1 below.

- Declaration of background and third party intellectual property (Annex 5)

  All background IPR, including, if applicable, third party's IPR, must be declared by completing the form in Annex 5. It is recalled that "background" means information which is held by the tenderer and consortium members prior to the award of the contract, as well as copyrights or other intellectual property rights pertaining to such information, the application for which has been filed before the award of the contract, and which is needed for performing the contract or for using the deliverables of the contract.

  The form must be completed by all tenderers (including all consortium members). The contractor shall give the GSA access rights to all the necessary background.

- Security (SAL) (Annex 6)

  Each service provider (including subcontractor(s) or any member of a consortium or grouping) must provide all the information that may be required by the SAL with respect to the management of classified information.

- In case of consortium or grouping: document authorising the company or person heading the project to submit a bid and sign the contract. Such a document shall be provided by each member of the consortium or grouping.

The tenderer shall also include in this section the documents required under Article IV.3.1 below (economic and financial capacity).

The GSA reserves the right to request additional evidence in relation to the bid submitted for evaluation or verification purposes within a time-limit stipulated in its request.

III.2.2. Section Two: Technical offer

This section is of great importance in the assessment of the bids, the award of the contract and the future execution of any resulting contract.

Some guidelines are given below, but attention is also drawn to the selection and award criteria, which define those parts of the technical offer to which the tenderers should pay particular attention. The technical offer should address all matters laid down in the specifications. The level of detail of the tender will be extremely important for the evaluation of the tender.

Tenderers shall describe as part of their technical offer all prior experience relevant to perform the work requested.

Tenderers shall submit, as part of the technical offer, CVs for key personnel involved in the different tasks. They shall also include all necessary justifications regarding the selection criteria (technical and security-related) as described in points IV.3.2 and IV.3.3 below.

They shall provide a detailed offer of how Tasks described in section I.9 are intended to be carried out, and by whom, including the division of work among the different categories of staff on a man/days basis, key milestones, deliverables, date by which the tenderer may complete the task, etc. In case of a grouping, the tenderer may include this information in the Draft Project Management Plan, which must also be submitted in the offer (see section I.9.1.1 above).

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

The technical offer must provide all the information needed for the purpose of awarding the contract.

III.2.3. Section Three: Financial offer

All tenders must contain a financial offer. The tenderer's attention is drawn to the following points:

- Prices must be quoted in Euro, including the countries which are not in the euro-area. As far as the tenderers of those countries are concerned, they cannot change the amount of the bid because of the evolution of the exchange rate. The tenderers choose the exchange rate and assume all risks or opportunities relating to the rate fluctuation.
- Prices must be fixed amounts and include all expenses, such as foreseen travel expenses and daily allowances. All additional meetings (i.e. meetings other than those outlined in sections I.10 & I.12 above) will be reimbursed to the contractor on the basis of the reimbursement scheme contained in Article II.7 of the draft contract.
- Prices should be quoted free of all duties, taxes and other charges, i.e. also free of VAT, as the Communities are exempt from such charges in the EU under Articles 3 and 4 of the Protocol on the Privileges and Immunities of the European Communities of 8 April 1965 (OJ L 152 of 13 July 1967). Exemption is granted to GSA by the governments of the Member States, either through refunds upon presentation of documentary evidence or by direct exemption. For those countries where national legislation provides an exemption by means of a reimbursement, the amount of VAT is to be shown separately.

  In case of doubt about the applicable VAT system, it is the tenderer's responsibility to contact his or her national authorities to clarify the way in which the European Community is exempt from VAT;
- Prices shall be fixed and not subject to revision during the performance of the contract.
- Bids must indicate the number of actual man-days needed to carry out the work split up per staff member involved
- For each category of staff involved in the project, the tenderer must specify:
  - § the total labour costs;
  - § the daily rates
  - § other categories of costs, indicating the nature of the cost, the total amount, the unit price and the quantity.

Bids involving more than one service provider (consortium) must specify the amounts indicated above for each provider.

IV. ASSESSMENT AND AWARD OF THE CONTRACT

The assessment will be based on each tenderer's bid.

All the information will be assessed in the light of the criteria set out in these specifications. The procedure for the award of the contract, which will concern only admissible bids, will be carried out in three successive stages.

The aim of each of these stages is:

1) to check, on the basis of the exclusion criteria, whether the tenderer is qualified to participate in the tendering procedure;

2) to check, on the basis of the selection criteria, whether the tenderer has the financial, economic, technical and professional capacity to carry out the work;

3) to choose, on the basis of the award criteria, the best offer out of those submitted by tenderers which are not excluded and which meet the selection criteria.

The contract will be concluded with the tenderer ranked best as the result of the evaluation of admissible tenders.

IV.1. Exclusion criteria (exclusion of tenderers)

To be qualified for participating in this contract award procedure, tenderers must not be in any of the following exclusion grounds [6]:

(a) they are bankrupt or being wound up, are having their affairs administered by the courts, have entered into an arrangement with creditors, have suspended business activities, are the subject of proceedings concerning those matters, or are in any analogous situation arising from a similar procedure provided for in national legislation or regulations;

(b) they have been convicted of an offence concerning their professional conduct by a judgement which has the force of res judicata;

(c) they have been guilty of grave professional misconduct proven by any means which the contracting authority can justify;

(d) they have not fulfilled obligations relating to the payment of social security contributions or the payment of taxes in accordance with the legal provisions of the country in which they are established or with those of the country of the contracting authority or those of the country where the contract is to be performed;

(e) they have been the subject of a judgement which has the force of res judicata for fraud, corruption, involvement in a criminal organisation or any other illegal activity detrimental to the Communities' financial interests;

(f) following another procurement procedure or grant award procedure financed by the Community budget, they have been declared to be in serious breach of contract for failure to comply with their contractual obligations;

[6] Article 93 of Council Regulation (EC, Euratom) No 1605/2002 of 25 June 2002 on the Financial Regulation applicable to the general budget of the European Communities (OJ L 248 of 16.9.2002)

IV.1.1. Evidence to be provided by the tenderers

1. GSA shall accept, as satisfactory evidence that the tenderer is not in one of the situations described in point (a), (b) or (e) above, the production of a recent extract from the judicial record or, failing that, a recent equivalent document issued by a judicial or administrative authority in the country of origin or provenance showing that those requirements are satisfied.

2. GSA accepts, as satisfactory evidence that the tenderer is not in the situation described in point (d) above, a recent certificate issued by the competent authority of the State concerned.

   Where no such certificate is issued in the country concerned, it may be replaced by a sworn or, failing that, a solemn statement made by the interested party before a judicial or administrative authority, a notary or a qualified professional body in his country of origin or provenance.

The documents referred to in paragraph 1 and 2 shall relate to legal and/or natural persons including, if applicable with regard to points b) and e), company directors or any person with powers of representation, decision-making or control in relation to the tenderer.

The GSA may waive the obligation for the tenderers to submit documentary evidence if such evidence has already been submitted to it for another GSA procurement procedure and provided the documents were issued not more than one year earlier and are still valid. In such cases, the tenderer must declare on his honour that the documentary evidence has already been provided in a previous procurement procedure, state the reference number and subject matter of the procedure, and confirm that there has been no change in the situation.

IV.1.2. Other cases of exclusion

Contracts will not be awarded to tenderers who, during the procurement procedure:

a) are subject to a conflict of interest;

   Tenderers must declare:

   - that they do not have any conflict of interest in connection with the contract; a conflict of interest could arise in particular as a result of economic interests, political or national affinities, family or emotional ties, or any other relevant connection or shared interest;
   - that they will inform the contracting authority, without delay, of any situation constituting a conflict of interest or which could give rise to a conflict of interest;
   - that they have not made and will not make any offer of any type whatsoever from which an advantage can be derived under the contract;
   - that they have not granted and will not grant, have not sought and will not seek, have not attempted and will not attempt to obtain, and have not accepted and will not accept, any advantage, financial or in kind, to or from any party whatsoever, constituting an illegal practice or involving corruption, either directly or indirectly, as an incentive or reward relating to the award of the contract.

   GSA reserves the right to check the above information.

b) are guilty of misrepresentation in supplying the information required by the contracting authority as a condition of participation in the contract procedure or fail to supply this information.

IV.1.3. Declaration

Tenderers must fill in and sign the form attached to the specifications (Annex 4).

Where the tender involves more than one service provider (consortium or grouping), each provider must fill in and return the form, as well as the evidence specified in pt IV.1.1.

Subcontractors (when the subcontracted part does not exceed 20% of the contract value) must only provide the form in Annex 4.

Bids submitted where subcontractors have not provided the abovementioned documents may not be taken into consideration.

GSA reserves the right, however, to request any additional document relating to the proposed tender for evaluation and verification purpose, within a delay fixed in its request.

IV.2. Administrative and financial penalties

1. Without prejudice to the application of penalties laid down in the contract, candidates or tenderers and contractors who have been guilty of making false declarations or have been found to have seriously failed to meet their contractual obligations in an earlier procedure will be excluded from all contracts and grants financed by the Community budget for a maximum of two years from the time when the infringement is established, as confirmed after an adversarial procedure with the contractor.

   That period may be extended to three years in the event of a repeat offence within five years of the first infringement.

   Tenderers or candidates who have been guilty of making false declarations will also incur financial penalties representing 2% to 10% of the total value of the grant being awarded.

   Contractors who have been found to have seriously failed to meet their contractual obligations will incur financial penalties representing 2% to 10% of the value of the grant in question.

   This rate may be increased to 4% to 20% in the event of a repeat offence within five years of the first infringement.

2. In the cases referred to in points IV.1, a), c), d), the candidates or tenderers will be excluded from all contracts and grants for a maximum of two years from the time when the infringement is established, as confirmed after an adversarial procedure with the contractor.

   In the cases referred to in points IV.1, b) and e), the candidates or tenderers will be excluded from all contracts and grants for a minimum of one year and a maximum of four years from the date of notification of the judgment. Those periods may be extended to five years in the event of a repeat offence within five years of the first infringement or the first judgment.

3. The cases referred to in point IV.1, e) cover:

   a) cases of fraud as referred to in Article 1 of the Convention on the protection of the European Communities' financial interests established by the Council Act of 26 July 1995 (OJ/C 316 of 27.11.1995, p. 48);

   b) cases of corruption as referred to in Article 3 of the Convention on the fight against corruption involving officials of the European Communities or officials of Member States of the European Union, established by the Council Act of 26 May 1997 (OJ/C 195 of 25.6.1997, p. 1);

   c) cases of participation in a criminal organisation, as defined in Article 2(1) of Joint Action 98/733/JHA of the Council (OJ/L 315 of 29.12.1998, p. 1);

d) cases of money laundering as defined in Article 1 of Council Directive 91/308/EEC (OJ/L 166 of 28.6.1991, p.77).

IV.3. Selection Criteria (selection of tenderers)

Tenderers must have the financial, economic, technical and professional capcity necessary to perform the tasks required in this call for tender.

IV.3.1. Economic and financial capacity – References required

Tenderers must provide proof of their financial and economic capacity by means of the following documents: the balance sheets or extracts from balance sheets for the last three financial years, and a statement of overall turnover and turnover relating to the relevant services for the last three financial years.

This rule applies to all service providers, regardless of the percentage of tasks they intend to execute, once they have chosen to submit a tender. However, if the tender includes subcontractors whose tasks represent less than 20% of the contract, those subcontractors are not obliged to provide evidence of their economic and financial capacity.

The GSA may waive the obligation for the tenderers to submit documentary evidence if such evidence has already been submitted to it for another GSA procurement procedure and provided the documents were issued for the requested period (last three financial years) and are still valid. In such cases, the tenderer must declare on his honour that the documentary evidence has already been provided in a previous procurement procedure, state the reference number and subject matter of the procedure, and confirm that there has been no change in the situation.

IV.3.2. Technical and professional capacity – References required

Tenderers must provide evidence of their technical and professional competence in the following fields:

- Knowledge and experience of ECSS standards.
- Capacity to handle classified information.
- Knowledge of Galileo and GNSS programmes.
- Knowledge of the security framework of the EU GNSS programmes, and especially of Galileo.
- Knowledge of the Galileo Public Regulated Service functions and interfaces.
- Experience in the Information Security (IS) and Information Technology Security (ITSEC) international standards and techniques, and the relevant certification processes.
- Experience in risk analysis and assessment.
- Experience in the implementation of industrial security rules, both at national and EU levels.
- Experience in definition of requirements for the protection of GNSS against interference and jamming
- Experience in techniques to mitigate the impact on jamming and interference on GNSS receivers
- Knowledge of the structure and relationships among European political Institutions and Organisation
- Experience on the definition of cost and management models of complex organisations.

If several service providers/subcontractors are involved in the bid, each of them must have and show that they have the professional and technical capacity to perform the specific tasks assigned to them.

Tenderers should provide with their bid a detailed curriculum vitae of each staff member responsible for carrying out the work, including his or her educational background, degrees and diplomas, professional experience, research work, publications and linguistic skills.

The curricula vitae shall be presented, preferably, in accordance with Commission Recommendation (2002/236/EC) of 11 March 2002 on a common European format for curricula vitae published in OJ L79 of 22 March 2002, p. 66.[7]

IV.3.3. Security

Tenderers must provide evidence of their experience and ability to comply with security instructions applicable to contractor and subcontractors, as described in the draft SAL attached to this invitation to tender. Selection criteria in security field will be:

- Description of the security organisation of each company involved as prime contractor or subcontractor, for the management of classified information up to CONFIDENTIEL UE level, including EU classified information. This description should contain also the following details for each company involved: country, company name, address, Local Security Officer (LSO) contact details (Name, Tel, Fax, E-Mail), Project Leader contact details (Name, Tel, Fax, E-Mail);
- Analysis of the SAL requirements and provision of a compliance matrix, providing only if needed the status "Partial Compliance (PC)" or "Non Compliance (NC)" with a justification for each of them;
- Demonstration that contractor's personnel as well as sub-contractors' personnel with a need to handle EU or national classified information up to the level of CONFIDENTIEL UE in the framework of the contract, hold a valid and appropriate PSC for that purpose;
- Description of the specific elements used or produced in the framework of the contract which should be classified and specifying the applicable security classification levels required;
- Demonstration that all industrial or other entities which need an access to information classified CONFIDENTIEL UE hold a national FSC. The FSC is granted by the NSA/DSA of the Member State to confirm that a facility can afford and guarantee adequate security protection of EU or national classified information to the appropriate classification level;
- No contract or subcontract may be awarded to entities registered in a non-EU Member State, except if agreements on security procedures for the exchange of classified information have been established with them, defining the purpose of cooperation and the reciprocal rules on the protection of the information exchanged and following article 26 of the Commission Decision 2001/844/EC, ECSC, Euratom of 29 November 2001 amending its internal Rules of Procedure.
- The contractor and the subcontractors for whom an access to the classified information provided by the ESA GalileoSat programme is required, must be in EU Member States participants of the European GNSS PSI[8], without prejudice to the article 26 of the Commission Decision 2001/844/EC, as mentioned above.

[7] Available at: http://www.europa-pages.com/jobs/europass-cv-downloads.html.

[8] Programme / Project Security Instruction concerning European GNSS Programmes (short title: European GNSS PSI) issued by Galileo Security Board (GSB), 19 December 2008; participants are: EU Member States, EU Council, EU Commission, ESA, GSA, Norway, Switzerland.

IV.4. Evaluation of tenders – Award criteria

The contract will be awarded to the tender offering the best value for money according to the criteria given below.

Consideration will be given only to those bids that reach a minimum of 70 out of the possible 100 points for the technical score, of which at least:

- 12 of the possible 20 pts must be achieved in section 1 of the technical evaluation criteria;
- 36 of the possible 60 pts must be achieved in section 2 of the technical evaluation criteria; and
- 12 of the possible 20 pts must be achieved in section 3 of the technical evaluation criteria.

a) Technical evaluation criteria as weighted (70%)

N°	Award Criteria	Weighting
1	"General understanding of the requirements and the context thereof" § Quality of the content of the offer o Bidder's analysis of GSA's requirements and critical review thereof (if necessary) o Understanding of the specific environment under which the tasks are to be carried out o Understanding of GSA's needs and preliminary analysis of solutions § Compliance and completeness of the offer with the tender specifications	20
2	"Proposed approach and methodology" § Quality of the proposed team responsible for carrying out the task(s) § Adequacy of the allocation/distribution of the tasks within the proposed team and adequacy of management level and efforts related to each task § Confidence that the approach and methodology is appropriate to meet the requirements and quality within time limits set § Analysis of interface requirements between the different tasks § Relevance of proposed options	60
3	"Adequacy of management and planning for the execution of the tasks" • Adequacy of reporting scheme • Adequacy of management level of effort • Quality of proposed planning • Heritage and experience of the team	20
Total number of points		100

b) Total price (30 %)

Total number of points for price: X (Where X is the highest score for technical evaluation reached by an eligible offer).

Score for price for offer (a) will then be computed as follows: X * lowest price among eligible offers / price of offer (a)

The contract will be awarded to the tenderer offering the best quality price score as measured by the following formula:

70 % * (Total number of points for technical evaluation) + 30 % * (Total number of points for price)

IV.5. Information for tenderers

The GSA will inform tenderers of decisions reached concerning the award of the contract, 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.

V. ANNEXES

1. Identification of the Tenderer
2. Financial Identification
3. Legal Entity Form
4. Declaration by the Tenderer (relating to the exclusion criteria)
5. Declaration of Background and Third Party Intellectual Property
6. Security Aspects Letter
7. Draft Contract
8. Non-Disclosure Agreement

European GNSS Supervisory Authority

ANNEX 1

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)

Call for tender GSA/OP/03/09

Identity	
Name of the tenderer	
Legal status of 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)[9]	
Address	
Address of registered office of tenderer	
Where appropriate, administrative address of tenderer for the purposes of this invitation to tender	
Contact Person	
Surname: First name: Title (e.g. Dr, Mr, Ms) : Position (e.g. manager): Telephone number: Fax number: E-mail address:	
Legal Representatives	
Names and function of legal representatives and of other	

[9] For natural persons

representatives of the tenderer who are authorised to sign contracts with third parties	
Declaration by an authorised representative of the organisation[10] I, the undersigned, certify that the information given in this tender is correct and that the tender is valid.	
Surname: First name:	Signature:

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

ANNEX 2

FINANCIAL FORM
(to be completed by the tenderer)

The tenderer's attention is drawn to the fact that this document is a model and that a specific Financial Form for each Member State is available at the following Internet address: http://gsa.europa.eu/, under the "Call for Tender" section.

European GNSS Supervisory Authority

FINANCIAL IDENTIFICATION

ACCOUNT HOLDER

NAME

ADDRESS

TOWN/CITY POSTCODE

COUNTRY VAT NUMBER

CONTACT PERSON

TELEPHONE FAX

E - MAIL

BANK

BANK NAME

BRANCH ADDRESS

TOWN/CITY POSTCODE

COUNTRY

ACCOUNT NUMBER

IBAN (optional)

REMARKS :

BANK STAMP + SIGNATURE of BANK REPRESENTATIVE
(Both Obligatory)

DATE + SIGNATURE of ACCOUNT HOLDER :
(Obligatory)

ANNEX 3

LEGAL ENTITY FORM
(to be completed by the tenderer)

The tenderer's attention is drawn to the fact that this document is a model and that a specific Legal Entity Form for each Member State is available at the following Internet address: http://gsa.europa.eu/, under the "Call for Tender" section.

Please note that we can only accept either original documents or certified copies, which must be less than 6 months old.

In the case of a grouping, this form must only be provided by the person heading the project.

ANNEX 4

DECLARATION BY THE TENDERER

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

1. In accordance with Article 93 of the Financial Regulation of the European Communities (Council Regulation 1605/2002 of 25.6.2002) published in Official Journal L 248 of 16 September 2002, I declare on my honour that I am not in any of the following situations which would exclude me from participating in this procurement procedure:

   a) I am not bankrupt, being wound up or having my affairs administered by the courts, I have not entered into an arrangement with creditors, I have not suspended business activities, I am not the subject of proceedings concerning any such matters, and I am not in any similar situation arising from a similar procedure provided for in legislation or regulations;

   b) I have not been convicted of an offence concerning my professional judgement by a judgment which has the force of res judicata;

   c) I have not been found guilty of grave professional misconduct proven by any means which the contracting authority can justify;

   d) I have not failed to fulfil obligations relating to the payment of social security contributions or the payment of taxes in accordance with the legal provisions of the country in which I am established or with those of the country or the contracting authority or those of the country where the contract is to be performed;

   e) I have not been the subject of a judgment which has the force of res judicata for fraud, corruption, involvement in a criminal organisation or any other illegal activity detrimental to the Communities' financial interests;

   f) as a consequence of another procurement or grant procedure financed by the Community budget, I have not been declared to be in serious breach of contract for failure to comply with my contractual obligations,

2. In addition, the undersigned declares on his or her honour:

   a) that on the date of submission of the tender, the company or organisation I do represent and the staff proposed for this tender are not subject to a conflict of interests in the context of this invitation to tender; I undertake to inform GSA without delay of any change to this situation after the date of submission of the tender.

   b) that the information provided to GSA within the context of this invitation to tender is accurate, sincere and complete.

Done at …… on……
Company: ……
Name ……...
Title ……
Signature:

ANNEX 5

DECLARATION OF BACKGROUND AND

THIRD PARTY INTELLECTUAL PROPERTY

Please refer to separate document (Excel)

ANNEX 6

SECURITY ASPECTS LETTER

Please refer to separate document (PDF).

ANNEX 7

DRAFT SERVICE CONTRACT

Please refer to separate document (PDF).

ANNEX 8

NON-DISCLOSURE AGREEMENT

Please refer to separate document (PDF).

The GSA will provide the Tenderers with documents [RD7], [RD8] and [RD9] upon request and after the conclusion of a non-disclosure agreement for the classified documents.

In that respect, Tenderers shall send a request through their Local Security Officer (LSO), at least 30 calendar days before the deadline, to the e-mail address tenders@gsa.europa.eu indicating the name and address of the Tenderer and the name of the LSO, as well as proof that the LSO is appointed in this position by the Company. Tenderers shall send with their request a scanned version of the Non Disclosure Agreement, duly completed, while the original signed document (two original copies) shall be sent in parallel by conventional mail at:

European GNSS Supervisory Authority
Rachelle Antal
L56 07/18
B-1049 Brussels
Belgium

Tenderers who fail to submit the offer must return all documents provided by the GSA within two months following the deadline for the submission of the offer.

Tenderers who submit the offer but are not awarded the contract must return all documents provided by the GSA within two months following publication of the award notice.