GSA/OP/09/14

"General ICT Support"

ANNEX I.D to the Tender Specifications
Technical Terms of Reference

Contents

1 Purpose of the Framework Service Contract

The objective of this call for tenders is to establish a contractual framework for the provision of services in the areas of:

- User support
- System maintenance and administration
- System and software development

The scope includes all the administrative information and communication systems operated by the GSA including those processing EU classified information up to the level Secret UE.

Information systems linked directly to the operations of the European Global Navigation Satellite Systems (GNSS, Galileo and EGNOS) are not in scope of this tender.

The specific tasks will be achieved via the execution of specific contracts.

The Contractor shall be able to dedicate one or more persons to the work for the GSA and these persons shall be able to work either remotely or in any of the GSA sites.

The company must be proficient in the core technologies used by the GSA and the expertise must be supported by the relevant certifications issued by the software or hardware vendors.

Whenever technically possible and financially favourable, the Contractor shall be directly involved in all new developments and changes of the GSA's information and communication systems.

2 Description of GSA ICT Systems

2.1 Sites

Currently, there are 3 permanently occupied sites:

European GNSS Agency (GSA) Janovskeho 438/2 17000 Prague 7 Czech Republic	GSA Headquarters
GSA Galileo Security Monitoring Centre (GSA GSMC) Quartier Général des Loges 8, avenue du Président Kennedy 78102 Saint-Germain-en-Laye France	GSA GSMC site in France
GSA Galileo Security Monitoring Centre (GSA GSMC) NATS Sopwith Way Swanwick Hants SO317AY United Kingdom	GSA GSMC site in the UK

Prague hosts the core technology of the IT systems, the other sites are considered branch sites and contain a subset of the IT systems.

In the future other sites located within Europe may become operational.

2.2 Technologies

The core technologies of the GSA are based on Microsoft and Cisco:

- Server Hardware
  - Dell, HP, IBM x86 servers
  - Cisco x86 Blade servers
  - EMC VNX Storage
  - EMC Data Domains
- Network Hardware
  - Cisco Catalyst switches
  - Cisco Nexus switches
  - Cisco ASA Firewalls
  - Netasq VPN Encryptors and related software products
- Backoffice
  - Microsoft Server 2008, 2012 R2,2012 R1
  - Microsoft Active Directory
  - Microsoft SQL Server 2012, 2008
  - Microsoft Exchange 2010, 2013
  - Microsoft SharePoint 2013, 2010

- Microsoft Lync 2013
- System Centre Configuration Manager 2012 R2
- System Centre Operations Manager 2012 R2
- System Centre Service Manager 2012 R2
- System Centre Data Protection Manager 2012 R2
- Microsoft certificate services
- Microsoft Threat Management Gateway 2010
- Symantec Antivirus
- McAfee Antivirus

- Front Office
  - Windows 7, 8
  - Office 2010, 2013
  - Lync 2013
  - Polycom Video Conference
  - Windows Phone 8
  - Apple iPhone / iPad

NOTE: The software versions listed are the versions currently utilised by the GSA, the Framework Service Contract t covers current versions and all future evolutions of the systems.

3 Description of Services

3.1 Basic Service

The GSA requires the Contractor to provide the following services for a monthly fixed price:

- Contract management
- On-call standby ICT specialists service
- Purchasing service

3.1.1 Contract Management

The Contractor must provide a contract manager and a deputy that will ensure continual access to the contract manager throughout the duration of the life of the framework contract.
These persons shall perform as a minimum the following duties.

- Manage the framework contract, its specific contracts and deliverables
- Assign a project team and provide the GSA with the team composition and contact details
- Arrange the proper execution of all the project tasks
- Manage its resources allocated to the project, monitor and document the use of resources
- Monitor the use of the "Provisional amounts for unplanned work" allocated to the specific contracts
- Be proactive and prevent any risks related to the correct functionality of all supported systems by informing the GSA counterparts whenever a risk is identified
- Ensure all communication with GSA, in particular regarding the organisation of work and any changes and exceptions that may happen during the project

execution; inform GSA in advance (at least 5 working days) of any actions or resources required to assist the Contractor
- Chair project and contract meetings
- Draft minutes of all the 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
- Draft project documentation if required
- Monitor mission costs of the specialists working for the GSA and collect the necessary evidence for the purpose of reimbursement of these costs where applicable
- Create monthly reports covering the execution of all running specific contracts and providing lists of all activities and products delivered to the GSA over the respective time period; any invoicing to the GSA can be done only on the basis of these reports approved by the GSA

3.1.2 On-call Standby ICT Specialists Service

The Contractor shall arrange the availability of on-call standby support of ICT Specialists that are able to provide support at very short notice in the following areas:

- Cisco Network
- Cisco Firewalls
- Microsoft Exchange 2010 and/or 2013
- Microsoft SharePoint 2013
- Microsoft Lync 2013
- Microsoft TMG

The term "on-call" includes support on phone and/or via remote access. All specialists available under this service must be adequately equipped to connect remotely to the GSA system while respecting the provisions on the Security Convention document (annex) and perform the necessary actions.

The purpose of the service is the remedy of anomalies on GSA systems requiring immediate or rather quick action and therefore only senior personnel with sufficient working experience is allowed.

The require intervention time for this service varies from 1 hour for phone or remote intervention and 4 hours for on-site intervention including travel to the GSA HQ in Prague[1]. Travel to other GSA sites will not be required for the standby service.

The standby service must be

- available at least 12 hours every business day without interruption (for example from 8:00 to 20:00)[2]
- available for activation directly by the designated GSA personnel without the involvement of the Contract Manager; however, the service provider must inform the Contract Manager about the activation as soon as the Contract Manager resumes his working activity, typically on the business day following the activation.

[1] See the provisions of the Service Level Agreement and the tables in the Financial Offer document.

[2] Local time and holiday schedule in Prague, Czech Republic

Once activated, the actual remote and/or on-site intervention must be performed even outside the above time range.

3.1.3 Purchasing Service

The Contractor is expected to provide a service for the purchase of:

- ICT material
- Supplies
- SSL certificates
- Services either for unexpected use or in situations that the services are available only via online payments.

This applies to individual items of value less than 5000 EUR. The typical items to be purchased are spare parts or items available only from Internet online transactions, like SSL certificates, software utilities, hard disks, memory, supplies and accessories (namely toner cartridges), cables etc. or services like a repair of a broken device out of warranty, payment to a specialized technician coming to GSA premises etc.

These purchases must be authorised by the GSA on a case-by-case basis.

The Contractor shall also handle all activities related to warranty, repair, return and replacements of such materials and supplies purchased for the GSA. No handling fees or price mark-ups shall be charged for these purchases (this activity shall be included in the basic service price).

In order to allow for more flexibility in handling urgent support needs (urgent missions, unforeseen work and purchases) under the Basic service, a provisional amount of money may be allocated for this purpose via a specific contract without a link to a specific task or project.

3.2 ICT Specialist Support

The Contractor **must be able to provide** persons with the following profiles, on long, medium or short term basis, to any of the sites mentioned in section 2.1 (other sites within Europe may be requested in the future) upon request of the GSA:

	Profile	**Requirements**
1	Helpdesk Operator	At least 4 years working on a helpdesk
		Experience in supporting: • Standard x86 Desktop and Laptop computers • Microsoft Windows 7 • Microsoft Office 2010 or 2013 • Mobile devices • Adobe Reader or Acrobat • A corporate Antivirus product
2	Helpdesk Operator with System Administration skills	Identical to Helpdesk Operator plus at least 2 years of experience in monitoring and administrating:

		• Microsoft Server 2008 and/or 2012 R2 • Microsoft Active Directory • Microsoft Exchange 2010, 2013 • Installation and deployment of client workstations • A corporate Antivirus product
3	User Trainer	Experience in providing end user training in Microsoft products
4	System Builder	At least 6 years working as a system administrator of Microsoft based systems
		Experience in installing and administrating: • Microsoft Server 2008 and/or 2012 R2 • Microsoft Active Directory • Microsoft SQL Server 2012 • Microsoft Exchange 2010, 2013 • Microsoft SharePoint 2010 and/or 2013 • A corporate Antivirus product.
5	System Administrator	At least 6 years working as a system administrator of Microsoft based systems
		Experience in monitoring and administrating: • Microsoft Server 2008 and/or 2012 R2 • Microsoft Active Directory • Microsoft SQL Server 2012 • Microsoft Exchange 2010, 2013 • Microsoft SharePoint 2010 and/or 2013 • A corporate Antivirus product.
6	System Specialist *For each profile we require a Senior with more than 5 years' experience and a Junior with 2-5 years' experience in the area of specialization, preferably with a formal certification*	Required profiles: Cisco technologies: • Cisco Network • Cisco Firewalls Netasq Technology: • NetAsq VPN Encryptors and related software products Microsoft Technology: • Microsoft Server 2008 and/or 2012 R2 • Microsoft Server 2012 R2 Hyper-V Clusters

		• Microsoft SQL Server 2012 • Microsoft Exchange 2010 and/or 2013 • Microsoft SharePoint 2013 • Microsoft Lync 2013 • System Centre Configuration Manager 2012 • System Centre Operations Manager 2012 • System Centre Service Manager 2012 • System Centre Data Protection Manager 2012 • Microsoft certificate services • Microsoft Threat Management Gateway 2010 Antivirus • Symantec Antivirus • McAfee Antivirus
7	SharePoint Developer	With at least 3 years' experience in developing SharePoint 2010 and 2013 solutions
8	Software Developer	Experience and/or certification in: • .NET • MS SQL
9	Project Manager	At least 10 years of relevant work experience
		Certification in one of the major project management methodologies (preferably Prince2),
10	IT Security Specialist	Able to provide advice, guidance and assistance in both network and software based technology.
		Experience in: • IDS and IPS • System and file encryption • Network encryption • Certificate authorities • Authentication systems • PKI
11	Network specialist	Able to provide advice, guidance and assistance in network topology, design, component selection, configuration and performance tuning.
		Experience in: • Cisco technologies • Microsoft networking products • SIP and videoconferencing • Internet DNS services

		• Load balancing • VPN technology • Traffic analysis
12	Test Engineer	Experience in software testing
		Experience in system testing
13	System Architect	Experience in: • Interfacing with the users in order to determine their (evolving) needs. • Generating the highest level of system requirements, based on the user's needs and other constraints such as cost and schedule. • Ensuring that this set of high level requirements is consistent, complete, correct, and operationally defined. • Performing cost-benefit analyses to determine whether requirements are best met by manual, software, or hardware functions; making maximum use of commercial off-the-shelf or already developed components. • Interfacing with the design and implementation engineers and architects, so that any problems arising during design or implementation can be resolved in accordance with the fundamental design concepts, and user needs and constraints. • Ensuring that a maximally robust design is developed. • Generating a set of acceptance test requirements, together with the designers, test engineers, and the user, which determine that all of the high level requirements have been met, especially for the computer-human-interface. • Generating products such as sketches, models, an early user guide, and prototypes to keep the user and the engineers constantly up to date and in agreement on the system to be provided as it is evolving.
14	Application Analyst	Experience in:

		• Limiting choices available during development by - choosing a standard way of pursuing application development - creating, defining, or choosing an application framework for the application • Recognize potential reuse in the organization or in the application • Subdivide a complex application, during the design phase, into smaller, more manageable pieces • Grasp the functions of each component within the application • Understand the interactions and dependencies among components • Communicate these concepts to developers
15	Webmaster	Must have experience in administering websites at least using basic HTML
		Preferably experience in SharePoint
		Preferably experience in Apache, MySQL, PHP, Drupal CMS
16	System documentation writer	Experience in drafting IT system documentation of all kind, typically for security purposes, system development and administration and last but not least for the end users. The GSA may request the documentation to be created in a special format, for example as Intranet / SharePoint sites or pages.

The assistance shall be provided in the following ways:

- Short-term = 1 - 60 working days
- Medium-term = 61 – 120 working days
- Long-term = 121 and more working days
- Physical presence and/or intervention on the GSA systems on-site (in all GSA sites, mainly in Prague)
- Remote work and/or intervention on the GSA systems over Internet (secure connection to be prepared by the GSA)
- On phone assistance and/or consultancy

NOTE:

- Please refer to the Service Level Agreement (Annex I.K) for details of the candidate selection procedure
- All staff must be able to communicate both verbally and in writing in ENGLISH, their level of written English must be to a suitable level to be able to produce technical documents

3.3 System and Application Development

The Contractor **must be able to provide** the following, to any of the sites mentioned in section 2.1 (other sites within Europe may be requested in the future);

- Resources to perform the development and programming of new systems or components.
- Minor enhancements of the system or even major changes including the purchase of new system components from 3rd parties.
- Provide qualified specialists and developers available to work for GSA upon a special request in the following technologies:
  - Microsoft SharePoint 2013
  - .NET
  - MS SQL
- To design and build new IT systems, which may contain any of the following profiles:
  - Project managers
  - System administrators/builders
  - System architects
  - Application analysts
  - IT Security specialists
  - Network specialists
  - Test engineers

3.4 Application Maintenance Service

The GSA is developing a number of applications in SharePoint 2013 and 2010, for example quite recently we have developed an application for paperless processing of financial workflows and in the moment of publication of these tender specifications we are building a new Document Management System. A number of further applications is in our working plan for the coming months and years.

The Contractor is expected to provide, as a service working remotely from his premises, the maintenance of these applications, which means implementation of small changes, customizations, configuration of components and other interventions required in real-time by the end users.

For example, the Contractor shall be able to put at the GSA disposal the following resources:

- Application analyst, 10 hours per month
- SharePoint 2013/2010 developer, 20 hours per month
- Test engineer, 8 hours per month

The resources shall be available at the latest on the 2nd business day following a request.

The actual scope and amount of this service shall be described in Specific Contracts

3.5 Offsite Storage of Unclassified Backup Media

Ensure that GSA supplied backup media sets[3]:

- Are collected from GSA offices (normally in Prague but it should be possible in any of the 3 main GSA sites) on regular basis (frequency 1x,2x, 3x, 4x or 5x a week)
- The exact location(s), frequency and number of media sets will be determined in the specific contracts
- Are stored in secure and environmentally controlled conditions
- There is a rigorous chain-of-custody and audit trail, both in transit and when the media sets are stored
- The GSA has the ability to locate and request the delivery of a specific media set at any time day or night any day of the year following the predefined procedure and authorization

3.6 Access to 3rd Party Cloud-Based Services

The Contractor shall be able to provide GSA with access to the cloud computing market. Upon request, the Contractor shall procure on GSA behalf the selected cloud services and further assist the GSA in the setup and exploitation of these services. This may be applicable for the development and testing of new applications, for the operation of websites or the provision of other specialized services like audio and videoconferencing, e-mail services, security services (malware protection).
An example of a possible scenario is to host the GSA websites, which are based on LAMP (Linux, Apache, MySQL, PHP) and Drupal CMS.

4 General Requirements

4.1 General Security Requirements

The security principles contained in Commission Decision 2001/844[4] shall govern the execution of the contract. They are supplemented by other Commission's rules as well as the GSA rules and requirements as necessary more specifically with regard to Contractor's staff and way of working.

[3] In order to quantify better the service, we define "a media set" as "5 standard DLT IV data cartridges or equivalent size (for example, a box of 10 CD/DVDs)".

[4] Commission Decision 2001/844/EC, ECSC, Euratom published in OJ L 317 of 3.12.2001 as last amended by Commission Decision 2006/548/EC, Euratom published in OJ L 215 p.38 of 5.8.2006

Referring to article 27.2 (i) of Commission Decision 2001/844[5], the overall level of security classification of the contract is SECRET UE as contractor's staff may access area or data classified up to SECRET UE while performing their tasks. However the tender and the contract documentation are unclassified.

4.1.1 Main Security Requirements for the Contract

4.1.1.1 Security clearance

While working in GSA premises Contractor's (or subcontractors') personnel may access a security area accredited at the level SECRET UE. However, no EUCI is expected to be handled or stored in the (sub) Contractor's premises.

A Personnel Security Clearance (PSC) at the level SECRET UE is required for GSA Helpdesk personnel and system administrators or any other person requiring frequent access to the GSA security area and for any person working on long-term basis in the GSMC. The rules are following:

- If GSA selects a candidate proposed by Contractor for the above specified positions and the candidate has not a valid PSC at the level SECRET EU, the Contractor will be required to submit the request for the PSC to the relevant National Security Authority within 2 weeks after the candidate is selected; the proof must be provided to the GSA.
- In case of failure to deliver to the GSA a missing PSC within the time limit required for the procedure by the relevant NSA, the personnel must be replaced by another with a valid PSC; if not, the contract may be terminated by the GSA immediately.

All personnel working in GSA premises longer than 60 working days have to submit to the GSA a proof of clean criminal record.

A PSC at the level SECRET UE is strongly recommended for any other personnel involved in support activities within the GSA security area as it will allow smooth access to that area.

4.1.1.2 Security Convention for Remote Access to the GSA Information Systems

Contractor will have to sign and respect Security Convention for Remote Access to the GSA Information Systems (Annex I.L to the Tender Specifications).

[5] Ibidem

5 Desired Content of the Technical Offer

The Tenderer's offer shall include the following aspects:

Desired Content of the Technical Offer	
1	Information about the services offered by the Tenderer and its subcontractors in context of this open call for tenders
2	Proof that the Tenderer is a current Microsoft Silver or Gold Partner in the Server Platform
3	Proof that the Tenderer is a current Microsoft Silver or Gold Partner in at least 3 of the following competencies: a. Application Development b. Data Platform c. Collaboration and Content d. Communications e. Messaging f. Project and Portfolio Management g. Devices and Deployment h. Identity and Access i. Management and Virtualization
4	Proof the Tenderer or one of its subcontractors is Cisco Certified Partner
5	Proof the Tenderer or one of its subcontractors is Netasq Certified Partner or Netasq itself
6	Methodology of the Tenderer or one of its subcontractors used to perform the following audits or health checks: a. IT Security b. Microsoft Active Directory and Domain Services c. Microsoft Exchange d. Microsoft SQL e. Microsoft Lync f. Microsoft Forefront TMG
7	Methodology of the Tenderer or one of its subcontractors used to perform the following audits or health checks: a. Network Security b. Cisco Firewalls c. Cisco Network d. Antivirus systems
8	The CV of the Contract Manager and their deputy that will be proposed to the GSA fitting the profile as described in section 3.1 of this document
9	Confirmation that all the profiles as described in section 3.2 of this document are

	available to work: • Short-term = 1 - 60 working days • Medium-term = 61 – 120 working days • Long-term = 121 and more working days • Physical presence and/or intervention on the GSA systems on-site (in all GSA sites, mainly in Prague) • Remote work and/or intervention on the GSA systems over Internet (secure connection to be prepared by the GSA • On phone assistance and/or consultancy
10	Software development methodology used by the Tenderer and its subcontractors including the profiles they have at the their disposal as detailed in section 3.2
11	Detailed description of at least 3 software development project that the Tenderer did in the last 5 years for customers - comparable in size with and relevant to the requirements of GSA *Description of every project has to include following elements:* • *Customer's requirements* • *Methodology used for the project* • *Profiles used in this project plus number of days* • *Result of the project*
12	Details about the provision of the purchasing service as specified in section 3.1.3
13	Details about the offsite storage of unclassified backup media as specified in section 3.5
14	Confirmation that the Tenderer is capable of conforming to and signing the Security Convention (Annex I.L to the Tender Specifications) that shall form part of the Framework Contract.
15	Duly filled-in and signed SLA (Annex I.K to the Tender Specifications)