Summary

Call for Nomination

IT SECURITY SERVICES

1 BACKGROUND AND OBJECTIVE

These technical specifications address the set-up of a framework contract via call for tender. The IO IT (ITER Organization Information Technology) intends to acquire services in the field of IT Security.

The objective of this call for tender is:

- To select providers recognized for their expertise in the supply of IT Security Services; and
- To conclude one or more framework contract(s) (up to one for each of the 3 lots) for the supply of services in area of IT Security consultancy.

2 REQUIRED EXPERIENCE

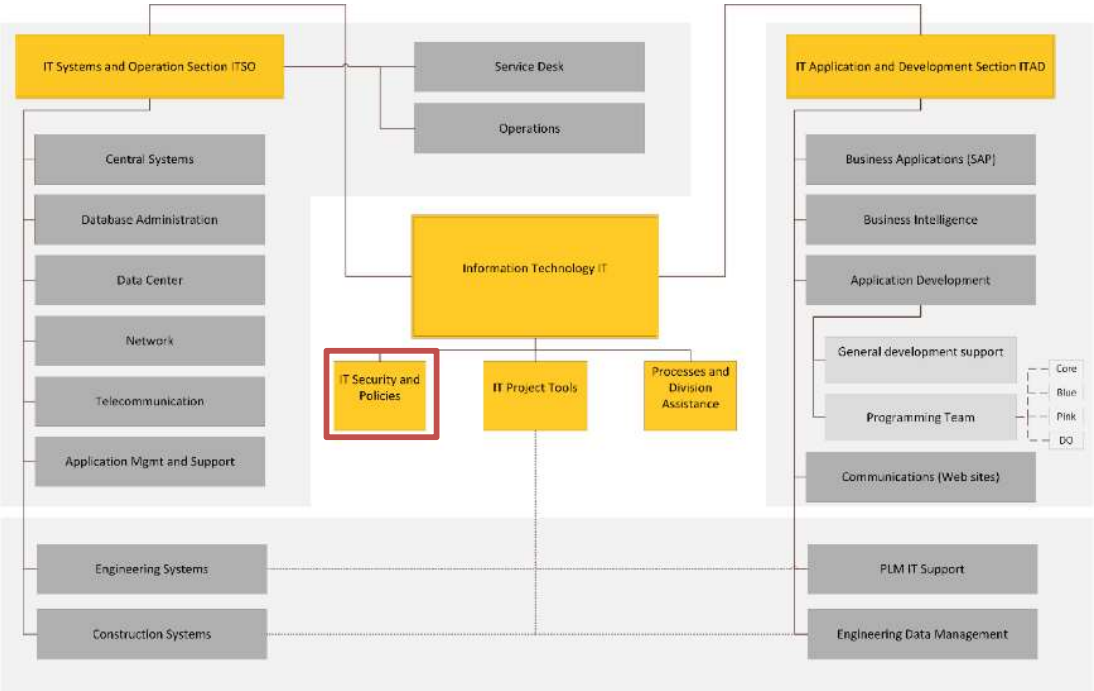
The candidate companies shall have demonstrated capabilities in providing consulting and expertise services for assessing, reinforcing and managing IT Security preferably in an international environment and in a complex organization setup comparable to the ITER project.

IOs cost containment objectives also favor companies with a proven track record of delivering projects on time and within budget. The specific experience and qualities sought by IO include but are not limited to:

- Proven expertise in the technical fields listed in part 4;
- Adequate skills level for the resources proposed by the company demonstrated through higher diplomas or certificates in Engineering, Computer Science or equivalent;
- Proven track record of successful deliveries of the same type of services;
- Ability to respond rapidly to changing resource requirements, to accommodate peak demands, and to provide specific expertise; and
- Capability to mobilize and manage centralized, site-based resources.

3 INFORMATION SYSEM AND IT LANDSCAPE

IO/IT Organisational structure



Technical environment

- Servers environment
  - HyperV clusters
  - Windows Server 2012 – 2016
- Business applications
  - SAP
  - .NET VB
  - SmartPlant, PLM
  - Catia/Enovia
- Scientific computing
  - HPC Linux (Puppet, RedHat Satellite, 2500 cores, 200 users, 25TB of data);
- Networking
  - Cisco Networking
  - Cisco Wifi
- IT Security
  - F5 BigIP
  - Checkpoint FW
  - PaloAlto FW
  - Elastic Search Cluster, Logstash, Kibana, Elastalert, SearchGuard
  - Windows Event forwarding
  - Splunk

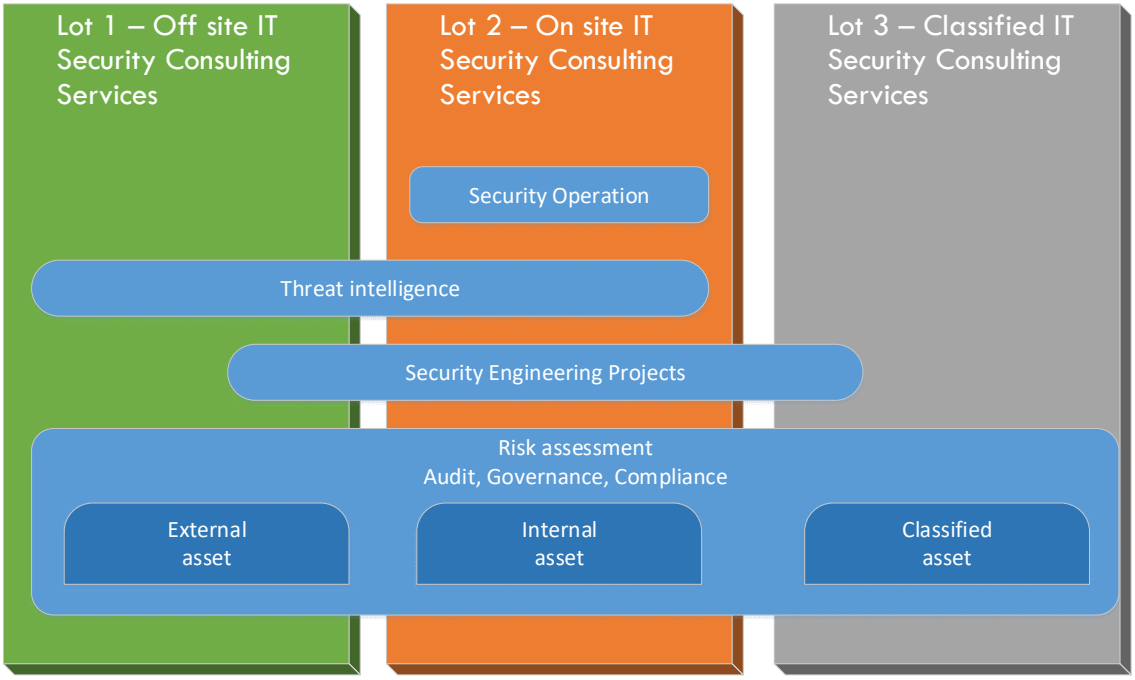
4 SCOPE OF WORK

The scope of work is divided into 3 areas each represented by one Lot:

Lot 1 – Off site IT Security Consulting Services

Lot 2 – Onsite IT Security Consulting Services

Lot 3 – Classified IT Security Consulting Services



4.1 Requested Services:

The requested services will mostly, but not exclusively, comprise:

4.1.1 Lot 1– Off site IT Security Consulting Services

- Malware analysis
- Incident response remote assistance
- Security assessment
  - Penetration Testing
  - Code auditing
  - Social Engineering
  - Web Site Penetration Testing
  - Information Risk Assessment
- Security related Policy review and drafting
- Other occasional IT consulting

4.1.2 Lot 2 – Onsite IT Security Consulting Services

- Regular IT Security operation ('run')
  - SIEM alert qualification and handling
  - Security incident handling
  - Vulnerability monitoring
  - IT Security performance reporting
- IT Security Improvement program
  - SIEM improvements: rules, alerting, upgrade maintenance
  - Vulnerability assessment and follow up
  - Compliance and policy maintenance
  - Project management related to IT Security;
    e.g.:
    - Authenticated Wifi
    - IT Security awareness raising campaign
    - Password management solution
    - Bastion
    - Hardened VM infrastructure
    - Etc.

4.1.3 Lot 3 – Classified IT Security Consulting Services

Lot 3 includes services in Lot 1 or 2 involving classified information and requesting security clearance (Confidentiel défense).

Lot 3 also includes audits and management of critical infrastructures classified SIIV (*Système d'Information d'Importance Vitale)*. IO/IT wishes to perform audits on *SIIV* that conform to the requirements referenced from ANSSI - Agence nationale de la sécurité des systèmes d'information, see: PASSI – référentiel d'exigences – v2.1.

These audits shall be conducted by qualified *Prestataires d'audit de la SSI*. Vendors bidding for Lot-3 shall therefore be listed as *PASSI* on the ANSSI registry.

CONFIDENTIALITY REQUIREMENT FOR LOT 3

Lot 3 scope of work will include elaboration, handling and storage of French Classified Information, classified as "Confidentiel Défense" level.

Candidates for Lot 3 shall be familiar with the Instruction Générale Interministérielle n° 1300 dated 30 November 2011. This Instruction covers Contractor's obligations resulting from having knowledge or possession of French Classified Information and/or media falling under French national defense confidentiality measures.

A Security Annex will be included in the Contract for Lot 3.

In order to participate to the procurement process of Lot 3, any non-French company must be legally registered in a State which has signed a security agreement with the French State for exchanging French Classified Information.

In particular, some work premises of the Candidate shall be configured in order to guarantee French national defense confidentiality under the conditions defined in the Instruction Générale Interministérielle n° 1300.

5 IT ENVIRONMENT and requested skills

The IT environment of IO concerned by this call for tender includes the following elements for which the candidate(s) may be required to demonstrate their expertise.

- Servers environment
  - HyperV clusters
  - Windows Server 2012 – 2016
- Business applications
  - SAP
  - .NET VB
  - SmartPlant, PLM
  - Catia/Enovia
- Scientific computing
  - HPC Linux (Puppet, RedHat Satellite, 2500 cores, 200 users, 25TB of data);
- Networking
  - Cisco Networking
  - Cisco Wifi
- IT Security
  - F5 BigIP
  - Checkpoint FW
  - PaloAlto FW
  - Elastic Search Cluster, Logstash, Kibana, Elastalert, SearchGuard
  - Windows Event forwarding
  - Splunk

The candidate(s) shall compose team members involved in the requested services with proper IT Security skills and demonstrated experience. The following qualifications are expected by the IT Security specialists proposed to perform the requested services.

Field of expertise	Indicative Junior Experience	Indicative Senior Experience
IT Security operations	2 years	5 years
Windows security environment	2 years	5 years
SIEM – Spunk or ELK stack	2 years	5 years
Recognised IT Security certification e.g.: CISSP, OSCP, CEH, GPEN, CASP, GIAC GSEC, …	Preferred	Mandatory

6 QUALITY ASSURANCE REQUIREMENTS

For the entire duration of the framework contract, Contractors shall hold, and maintain, a valid and relevant ISO 9001 and 14001 certification or comparable.

The missions and tasks executed under this framework contract shall be carried out in compliance with the ITER IT policies, and the IO Quality Requirements.

7 ESTIMATED DURATION

The duration of the framework contract shall be 3 years. The IO may exercise the options to extend these services for 2 times 1 year. Such options shall be exercised by written notice to the contractor no later than 30 days before the expiration of the initial term of the contract or of the additional period.

This Framework Contract will be implemented by means of "Task Orders" (TO), signed by the Contractor and the IO. The TOs will be organized in work packages (WP) reflecting the ITER needs.

Work packages will be defined as combination of services.

8 TIMETABLE

The tentative timetable is as follows:

Call for Nomination	October 2018
Issue Pre-qualification package	November 2018
Deadline for receipt of pre-qualification	December 2018
Issue the call for Tender	February 2019
Deadline for receipt of Tenders	March 2019
Contract Signature	June 2019

9 CANDIDATURE

Participation is open to all legal persons participating either individually or in a grouping (consortium). All legal persons including all consortium members should be established in an ITER Member State. A legal person cannot participate individually or as a consortium partner in more than one application or tender. A consortium may be a permanent, legally-established grouping or a grouping, which has been constituted informally for a specific tender procedure. All members of a consortium (i.e. the leader and all other members) are jointly and severally liable to the ITER Organization.

The consortium groupings shall be presented at the pre-qualification stage. The tenderer's composition cannot be modified without the approval of the ITER Organization after the prequalification.

Legal entities belonging to the same legal grouping are allowed to participate separately if they are able to demonstrate independent technical and financial capacities. Candidates (individual or consortium) must comply with the selection criteria. The IO reserves the right to disregard duplicated reference projects and may exclude such legal entities from the prequalification procedure.

More information on ITER Organization Procurement process can be found at:

https://www.iter.org/proc/generalinfo