OSCE Organization for Security and Co-operation in Europe

Date: 12 July 2016

Clarification Note No. 1

Invitation to Bid No. ITB/SEC/15/2016

Provision of IT Security Consulting Services on IT Information Security Incident Response

The Organization for Security and Co-operation in Europe has received a request for clarifications from potential bidders. In accordance with “Submission of Bids” Article 22 of the ITB Document, the OSCE would like to provide the following clarification:

Question 1:
How many incidents per year/month take place, for which assistance is needed?

Answer 1:
On average 2-4 incidents per year

Question 2:
In the case that you request assistance from a service provider for security incident response, how many days & how many consultants are needed on an average to resolve an incident?

Answer 2:
Estimated involvement is 2-5 mandays

Question 3:
Section I, Item 24 - Rechnungen und Mehrwertsteuer: According to our knowledge, the deliveries and other services to OSCE are taxable according to Austrian law and should be invoiced by the Contractor with sales tax. Is our information accurate?

Answer 3:
The financial proposal should exclude VAT as the OSCE is VAT exempt. Austrian companies can add the VAT on the invoices and the OSCE will get the VAT refunded.

Question 4:
Section I, Item 29 - Guarantee; Section II, Item 11 - Performance Bond
Is the provision concerning the performance bond relevant for this tender?

Answer 4:
No performance bond is required.

Question 5:
The financial proposal is based on hourly rates, because of this we would like to ask what it is expected to be the minimum engagement time per work order/purchase order. (e.g. 4 hours, 1 working day...)

Answer 5:
We have not defined any minimum engagement time. If you have such a restriction, please indicate it in your proposal.

Question 6:
Regarding the one-day kick-off meeting upon signature of the contract, we assume that only the Key account manager should attend this meeting, is this correct? Though it is stated in the ToR that it will take place at OSCE premises in Vienna, could this kick off meeting be done via Webex?

Answer 6:
The assumption is correct, the Key Account Manager should be sufficient. It can be done through remote video conferencing.

Question 7:
We assume that if the vendor is already registered in OSCE because of previous contracts, then there is no need to send again the registration form, could you confirm this?

Answer 7:
If the vendor was registered with the OSCE long time ago, we prefer to receive an updated vendor registration form with current information.

Question 8:
For many of our customers we cannot disclose the company name or give contact information due to their sensitive nature and possible still ongoing legal proceedings. Therefore we can only provide you with anonymized references for most of our clients. Would you take into consideration references from our customers where our work was pro-active (implementing safeguards before any breaches happened) as it would be easier to gain customer approval on disclosing this information?

Answer 8:
With the reference to Annex A – Technical Compliance Form, Mandatory Requirements, Requirement no. 1.3, “Bidder shall provide at least three references for which services of a similar size and complexity as stated within this tender document have been provided within the last three years and must have successfully managed the type of services that the OSCE is seeking for the last three consecutive years. Documentation to support these requirements must be submitted. The OSCE reserves the right to call the references provided by the Bidder.
Bidder shall list the company name, address, telephone number and contact person for each reference.”
In view of the mandatory requirement, anonymized references are not acceptable.

Question 9:
Could you explain to us how a possible remote access could be handled and if there are any requirements we need to fulfill in order to have that access?

Answer 9:
The remote access will be provided through VPN connection (we have Checkpoint VPN infrastructure). Contractor needs to provide us with names of consultants using remote access and OSCE will provide you with the necessary certificates.

Question 10:
From a contractual perspective is a retainer agreement considered/would that be agreeable?

Answer 10:
This does not align with our General Conditions of Contract where by default we pay only after the services are delivered satisfactorily.

Question 11:
Does the client need to outsource SOC. services or this project is just to provide consultants to help the client?

Answer 11:
No. The scope of the RFP is to provide consultants to help OSCE based on individual request.

Question 12:
If the client need SOC services, do the vendor need to provide security monitoring tools/hardware/appliance or the client already have these kinds of tools?

Answer 12:
SOC services are not in the scope. We already have our tools as described in the RFP document.

Question 13:
Which sector is the client in?

Answer 13:
OSCE is an international organization. Please check our webpage for further information.

Question 14:
Does the prime contractor have security consultants to cooperate with the client onsite?

Answer 14:
There are no prime contractors. The Bidders need to propose the services in the RFP.

Question 15:
Can the prime contractor share more information about this client such as pricing model, how big the client is, is this the 1st time that they set up this project or renew?

Answer 15:
There are no prime contractors.

Question 16:
Is there any automated tool used for information security incident management and response?

Answer 16:
There are no specific automated tools for security incident management and response.
We have a number of monitoring and security tools including firewalls, IDS, antivirus and vulnerability monitoring, as described in the RFP.

Question 17:
Is monitoring of tools, part of this scope? If Yes, what are the devices that needs to be monitored?

Answer 17:
No, incident detection and monitoring of tools is not part of the engagement. The scope is only support in incident response, based on specific request from OSCE in case of an incident.

Question 18:
Does the organization have specific incident response instructions or guidelines?

Answer 18:
Yes, we have a Standard Operating Procedure on security incident response (see attached).

Question 19:
How is cyber security incidents currently identified and handled in your organisation?

Answer 19:
See attached SOP.

Question 20:
Which security infrastructure components exist in the environment? (e.g., firewall, anti-virus, etc.)

Answer 20:
This is defined in the RFP document, section "Current technical infrastructure overview".

Question 21:
What is the security posture of the IT infrastructure components? How recently, if ever, was it assessed for vulnerabilities?

Answer 21:
At the Secretariat in Vienna, the vulnerabilities are assessed at least yearly. We have regular Nessus scans on critical infrastructure elements.
At other OSCE locations, these scans are ad-hoc based on risk.
Recently we are implementing Qualys, which will provide an organization-wide automated scanning system.

Question 22:
Is the scope limited to recommending the corrective and preventive action? Or are consultants expected to follow up with the closure of incident?

Answer 22:
The scope of services is described in section "Objectives of engagement". Follow up on incident closure is expected to be performed by OSCE.

Question 23:
Is the incident management process integrated with any ticketing tool? If yes, which tool is used?

Answer 23:
Yes, we use Assyst as ticketing tool.

Question 24:
Is the existing security incident management process based on any specific standard requirement? Like – ISO 27001, PCI DSS, etc. is this process defined to provide output to any specific compliance?

Answer 24:
The process is based on ISO27001 and ITIL. However, there are no specific compliance requirements to outputs.

Question 25:
Is there compliance or legal obligations tied to the incident? (e.g., PCI, breach notification laws, etc.)

Answer 25:
No.

Question 26:
Ref – (4.4 Section IV – Technical proposal form) :- While it is expected that most Cyber Incident response activity will be managed in Vienna, Austria. Can these service provided from outside European region?

Answer 26:
Yes, the services can be provided remotely. It is not mandatory to provide on-site services in Vienna. However, it is an optional requirement to provide the services on-site, which will be taken into account at the proposal evaluation stage.

Note!

Proposals must be received by the OSCE at the address shown in section 17 no later than **14:00 hours (CET), on 18 July 2016**. Proposals received after the designated time will be automatically rejected. **Submission of proposals by fax or email is not accepted**.