Organization for Security and Co-operation in Europe

CLARIFICATION NOTE
– Version 2.0

Issue Date: 10.06.2022 **(**added new questions Nr. 6 to 17)

Tender No: RFP/SEC/10/2022

Subject: Request for Proposal Nr. SEC/10/2022 for provision of IT security consultancy services

In regards to the issued RFP/SEC/10/2022 for the provision of IT security consultancy services, the OSCE would like to provide the following clarifications in regards to the raised clarification questions by participating suppliers:

Nr.	Type	References	Question	Answer
1	Technical	**Terms of Reference – Article 6 (page 5)**	*"Is it an absolute necessity to be in certified partnerships with major vendors in use in the OSCE infrastructure"?* *"Is it an absolute necessity for a Bidding company itself to have a valid ISO 27001 certificate? If it is a necessity, would be assuring to get compliant in a specific period of time sufficient?"*	The below provision from the ToR on page 6 remains valid: "The Contractor shall have certified partnership agreements **with at least three major vendors in use in OSCE infrastructure** as listed in the Appendix 1 and **hold the ISO27001 certificate**." which means it is absolute necessity to have ISO 27001 or equivalent certification at the point of Bid submission and not to be obtained later. In addition, there is a mandatory requirement Nr. 7 in the Table 1 from Annex E, requesting each Bidder to provide "detailed methodology and work plan for provision of the requested services, **demonstrating substantial responsiveness and compliance with the requirements listed in the Terms of Reference**." This criterion is interpreted to also include the mentioned specific requirement of having these partnership agreements in place, as they are valued as a necessity for a Contractor to be able to successfully perform the requested services.

ID	Type	References	Question	Answer
2	Technical	**Terms of Reference – Article 3 (page 1)**	*Is it possible to participate in this tender by proposing / providing just one of the services, ie. Penetration testing?*	No, all services must be provided as per the ToR requirements
3	Technical	**Terms of Reference – Article 3.1 (page 1)**	*Is the primary scope of penetration testing assignments:* *a) to research new vulnerabilities (not published - zero-day) in OSCE proprietary software and develop exploit proof-of-concept? This includes possible development of new tools and techniques?* *b) to utilize known vulnerabilities databases, published exploits and existing tools & techniques to identity presence of vulnerabilities in OSCE software?* *If a) is correct - does this research also cover software components of third-party vendors (such as Cisco, CheckPoint and possibly others) and subsequent reporting of respective CVE vulnerabilities?*	a) This is desirable, but not mandatory. b) YES, that is the primary scope Yes, but this is up to the Contractor to cover these.

ID	Type	References	Question	Answer
4	Technical	**Terms of Reference – Article 6 (page 5)**	*In the Annex D Terms of Reference, it is said: „The Contractor shall have certified partnership agreements with at least three major vendors in use in OSCE infrastructure". Could you please provide the list of the vendors in use in OSCE infrastructure?*	These are provided in the Appendix 1 - "Technical infrastructure overview" which is part of Annex D – Terms of Reference.
5	Technical	**Terms of Reference – Appendix 1 (page 6)**	*Do we need to include the license cost also for the testing software?*	Any licensing costs should be included in your financial bid as part of the cost for the provided services. OSCE will not purchase any licenses in addition.

ID	Type	References	Question	Answer
6	Technical	**Terms of Reference – Article 4 (page 3 & 4)**	In this Article 4 the following is stated: "In case there is an urgent operational requirement, qualified key members from the Contractor shall provide support primarily on-site at the OSCE Secretariat in Vienna, Austria but also be ready to conduct on-site visits to any OSCE Mission, Institution and Field Operation if required." *Is it an elimination criteria if a Bidder can only provide on-site visits at the OSCE Secretariat in Vienna and is only able to provide remote support by qualified key members to the other OSCE Mission, Institutions and Field Operations?*	Bidder's consultants are expected to be available to travel to any OSCE location, should the operational need arise and only in case of major information security incidents and/or emergencies upon request by the OSCE. In such cases the OSCE will cover the travel expenses incl board and lodging costs, which will be agreed beforehand. **However this is not an elimination criteria**, and we refer to Table 2 from Annex E-"Technical Compliance Response Form" – Criteria No. 3 where Bidders should elaborate on their engagement model. Bidders that will confirm to be able to travel to different OSCE locations (only when needed in case of major red category security incident) will score more points on this Criteria over those Bidders that will indicate that they cannot travel to another OSCE location.
7	Technical	**Terms of Reference – Article 3.4 (page 2 & 3)**	*Is it an elimination criteria if a Bidder cannot provide support services for all in the Appendix I listed tools and products?* *If not, please could you categorize the tools and products listed in Appendix I in two groups, like one for which the bidder must provide support and the other for which the support services are only optional?*	Support services are mandatory and expected only for security-related incidents (e.g. if a security incident occurs on an Exchange server, then the Bidder should have the expertise to extract/collect logs and investigate the incident). Operational support services are mandatory and expected for the layers and key applications but related to IT security, i.e. for the following as per Appendix I: network firewall, network, desktops & end user workplace, email, security event logging and management, mobility, remote access. **Bidders will not be requested to provide operational support for any other of the layers or key applications in Appendix I.**
ID	**Type**	**References**	**Question**	**Answer**

Organization for Security and Co-operation in Europe

<table>
<tr><th>ID</th><th>Type</th><th>References</th><th>Question</th><th>Answer</th></tr>
<tr><td>8</td><td>Technical</td><td>Terms of Reference – Article 4.1 (page 3)</td><td>According to Chapter 4.1. Incident response timeframes, resolution time should be 2nd NBD, NBD, 6 hours, respectively.

While the requested response time is well feasible, a guaranteed resolution time in case of a security incident cannot be guaranteed due to the nature of the matter. We would kindly ask if possible to remove this part</td><td>We recognize the raised concern and therefore propose to add the word “mutual agreement” for all three priority levels. The new table for the Incident response timeframes will then look as follows:

<table>
<tr><th>No.</th><th>Priority</th><th>Impact</th><th>Response time, Mon–Fri</th><th>Response time, Sat–Sun MW/OH</th><th>Resolution time</th></tr>
<tr><td>1.</td><td>Yellow</td><td>User impact</td><td>8 hours</td><td>N/A</td><td>2nd NBD** /mutual agreement</td></tr>
<tr><td>2.</td><td>Orange</td><td>Service degradation</td><td>6 hours</td><td>N/A</td><td>NBD / mutual agreement</td></tr>
<tr><td>3.</td><td>Red</td><td>Service unavailable</td><td>4 hours</td><td>3 hours</td><td>6 hours “work through”* / mutual agreement</td></tr>
</table>
</td></tr>
<tr><td>9</td><td>Financial</td><td>Annex F – Pricing form Table 1</td><td>Regarding Annex F: For the benefit of the OSCE we would kindly ask to distinguish between different cost rates related to consultants and Incident response, since a service with SLA is to be quantified differently than a service without SLA.</td><td>We agree and accept this suggestion, so in the updated Annex F1 pricing form we added a 2nd table which asks Bidders to specify rates for incident response.

Please use the new provided Annex F1 form when submitting your financial proposal</td></tr>
</table>

ID	Type	References	Question	Answer
10	Technical	**Terms of Reference – Article 4.1 (page 3)**	*According to Article 4.1 Incident response timeframes, the Contractor's certified staff shall be onsite at the OSCE Secretariat or DR site […].* *Could you please provide us an address of the DR site?*	The address of the DR site is **Fernkorngasse 10/3/501, 1100 Vienna, Austria**
11	Admin	**Annex A – article 6.2 and Annex B – article 16 (Subcontractors)**	*Subcontractors: „According to your General Conditions of Contract for Services document (Annex B), it is prohibited to use Subcontractors expect if OSCE is explicitly permitting their use.* *On the contrary, your Annex A - Article 6.2 states a necessity to specify Qualification Information Form if a Subcontractor is performing more than 10% of the work.* *Is our assumption correct, that every Subcontractor needs to be permitted by OSCE?* *The second question is, which information does OSCE need for the approval of a Subcontractor?"*	Subcontractors are allowed and can be used on this contract and there is no need for the Contractor to seek formal approval from the OSCE to use a subcontractor. However, the Contractor will be obliged **to inform the OSCE** about the use of subcontracted staff. The required information to be provided will be in a form of short explanation/description/summary of the subcontracted entity (name, background, fields of expertise etc.) no need to send a formal CV. The OSCE reserves the right to reject a nominated subcontractor without providing any explanation and in such case the Contractor will have to use another subcontractor.

ID	Type	References	Question	Answer
12	Admin	**Annex B – article 22 (Audit)**	*Right to Review: „The OSCE is allowed to review the recordings of the order fulfillment 7 years after the end of the contract. It is also possible for the OSCE to outsource this review to a third company."* *Is our understanding correct that this third company won´t be a competitor of the contractor?* *Is it correct to assume OSCE will announce the reviews at least 4 weeks in advance?"*	Yes, the understanding is correct. In case this happens, the 3rd party company will be carefully selected not to be a competitor of the Contractor. Such potential review if it happens, will be announced 4-8 weeks in advance.
13	Admin	**Annex B – article 24 (invoices and VAT)**	*According to our knowledge, deliveries and other services to international organizations are taxable in Austria and the invoices therefore include VAT.* *OSCE has an opportunity to submit application for a refund of the sales tax at the Austrian Federal Ministry of Finance.* *Is our understanding correct those Austrian suppliers shall invoice their services with VAT?"*	Yes, the understanding is correct. All Austrian suppliers can and shall include the VAT in their invoice to OSCE and OSCE will pay the VAT towards them in full. Afterwards OSCE is claiming back the paid VAT from the Federal ministry of finance.

ID	Type	References	Question	Answer
14	Admin	**Annex B – article 36 (FORCE MAJEURE)**	*In the General Conditions you have your own definition of a force majeure.* *Is our assumption correct that restrictions related to the COVID-19-pandemic, problems with semiconductors and the conflict in Ukraine/Russia are cases of force majeure too?"*	Yes, the assumption is correct.
15	Admin	**Annex B – article 13 (Confidentiality)**	*Is it correct to assume that the disclosure of information to affiliated companies pursuant to Section 15 of the Austrian Stock Corporation Act (AktG) for the purpose of fulfilling reporting obligations within the Group or subcontractors is permitted, provided that the receiving third party is also obligated to maintain confidentiality analogous to this agreement?"*	Yes, the assumption is correct.

ID	Type	References	Question	Answer
16	Admin	**Annex B – article 13 (Confidentiality)**	*Liability: In order to limit the uneconomical risk premium for OSCE, we would like to ask, weather it is possible to limit the contractor's liability as follows:* *"The contractor shall be liable for damage within the scope of the law, provided it has demonstrably acted with intent and gross negligence. The liability for slight negligence is limited to 50% of the yearly contract value per year. Any liability for indirect damage, lost profit, consequential damages as well as third-party claims, shall be excluded. The contractor is liable for data loss only to the expense of restoration if backup-services were part of the services, in all other cases, liability for data loss is excluded.""*	We are not in a position now at this stage of the tender to answer this question, as these negotiations will be done with the selected Bidder before signing the contract. We propose that any proposals for change in text you have related to the OSCE General terms and conditions, to include them as part of the Technical Proposal and in case you are selected for contract award, we will enter into negotiations to reach a mutually acceptable contract provision.
17	Technical	**Terms of Reference – Article 4.1 (page 3)**	*When it comes to the incident response timeframes we suggest all scenarios to be dealt with remotely (since for all of the tasks under this RFP the accepted practice worldwide is that they are performed/carried out remotely) and this will suffice to resume normal operation of the organization. This means that the Contractor's certified staff needs to be available and reachable (remotely) at any time and deal with all threats/attacks remotely.*	As answered in the Question Nr. 6, the Bidder's consultants are expected to be available on-site in Vienna, should the operational need arise and **only in case of major information security incidents and/or emergencies (only red priority incidents).** **However this is not an elimination criteria**, and we refer to Table 2 from Annex E-"Technical Compliance Response Form" Criteria No. 3 where Bidders should elaborate on their engagement model. Bidders that will confirm to be able to travel to different OSCE locations (only when needed in case of major red category security incident) will score more points on this Criteria over those Bidders that will indicate that they cannot travel.


osce
Organization for Security and
Co-operation in Europe