

CLARIFICATION NOTE

– Version 1.0

Issue Date: 30.05.2022

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)	<p><i>"Is it an absolute necessity to be in certified partnerships with major vendors in use in the OSCE infrastructure?"</i></p> <p><i>"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?"</i></p>	<p>The below provision from the ToR on page 6 remains valid:</p> <p>“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.</p> <p>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.</p>

ID	Type	References	Question	Answer
2	Technical	Terms of Reference – Article 3 (page 1)	<i>Is it possible to participate in this tender by proposing / providing just one of the services, ie. Penetration testing?</i>	No, all services must be provided as per the ToR requirements
3	Technical	Terms of Reference – Article 3.1 (page 1)	<p><i>Is the primary scope of penetration testing assignments:</i></p> <p><i>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?</i></p> <p><i>b) to utilize known vulnerabilities databases, published exploits and existing tools & techniques to identity presence of vulnerabilities in OSCE software?</i></p> <p><i>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?</i></p>	<p>a) This is desirable, but not mandatory.</p> <p>b) YES, that is the primary scope</p> <p>Yes, but this is up to the Contractor to cover these.</p>

ID	Type	References	Question	Answer
4	Technical	Terms of Reference – Article 6 (page 5)	<i>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?</i>	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)	<i>Do we need to include the license cost also for the testing software?</i>	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.