RFP/SMM/11/2018 "Performance of Independent Activities on IT Security Assurance for the OSCE Special Monitoring Mission to Ukraine"

Questions and answers

Batch 1

Question 1:

Is the target object a dedicated test environment, or any production data and/or systems will be used during the assessment?

Answer: The environment is not in operations yet. It is assumed that the production environment would be used for testing.

Question 2:

Are there any preferred security methodologies or standards for the assessment?

Answer: There are no preferred methodologies. A proper methodology is expected to be suggested by the Contractor.

Question 3:

Is only Android used as a mobile platform?

Answer: Android OS only

Question 4:

Are insiders (OSCE employees) considered as a part of the attacker model, or it includes only an external persons?

Answer: External threat agents are considered as the main risk, however controls against accidental user actions should be tested as well

Question 5:

Social engineering methods cannot be applied during the assessment. Is it correct?

Answer: Yes, it's correct.

Question 6:

The approximate quantity of the IP addresses for an internal and/or external testing.

Answer: Very limited number of IP addresses.

Question 7:

The versions of the supported mobile applications and the versions of the supported mobile operation systems.

Answer: The latest Android OS version

Question 8:

What kind of the hardware and/or software permissions are required for the mobile application?

Answer: For the end user the mobile device shall be in a kiosk mode providing very limited access to its applications and settings.

Question 9:

What information contain in the mobile application log file? Where and in what format is the mobile application log file stored?

Answer: Not applicable

Question 10:

Is the analysis of information systems security settings needed?

Answer: Yes, security settings analysis is needed.

Question 11:

Is the physical security testing needed to identify weaknesses in the physical security monitoring system?

Answer: This is not an organization or mission wide penetration test. The scope is limited to a specific information system only.

Question 12:

Are there any requirements for security code review in terms of types: should it be manual or automated or the supplier can choose preferred way?

Answer: It is up to the supplier to propose a code review approach that will best fit to our purposes.

Question 13:

For better understanding the scope of code review, can you please answer the following:

a. How many lines of source code are currently in the codebase?
b. Is it possible to receive the sample of approx. 300 lines of source code?

Answer: Unfortunately this cannot be provided.

Question 14:

Are target applications integrated or any 3rd party service is used? If yes, is it possible to review the list of them and get the description of how they interact, what functions are used, etc.? (example: GIS service)

Answer: It is assumed that as of the testing date the application is not integrated with any 3rd party services, except Active Directory for authentication purposes.

Question 15:

Are there any requirements for security testing methodologies and standards for web and mobile security testing? Or the supplier is free to choose any suitable one? (e.g.: OSSTMM, PTES, OWASP top 10, OWASP Testing Guide, etc.)

Answer: It is up to the supplier to propose a security testing methodology that will fulfill the purposes of the project.

Question 16:

Would that be possible to get the firsthand experience with web and mobile applications prior to submitting the bid?

Answer: Any internal documents, access to resources will be provided after a contract and NDA are signed after the selection process.

Question 17:

Since the scope of assessment includes SOVA supporting infrastructure – is it possible to review the infrastructure and network design prior to submitting the bid? This affects the effort estimation.

Answer: Any internal documents will be provided after a contract and NDA are signed after the selection process.

Question 18:

As for compliance with "Security Requirements Document for an Integrated Data Collection and Data Management System" – is it possible to review this document prior to submitting the bid?

Answer: This is an internal document and will only be provided after a contract and NDA are signed after the selection process. However, it might be helpful to know that it is based on OWASP documentation.

Question 19:

Annex C from the RFP document pack states that "the Activities are expected to be performed in OSCE SMM office in Kyiv". Does it mean that absolutely all activities must be done from OSCE office and access to source code, database and applications from outside will not be allowed?

Answer: Some components may be accessible from outside for a short period of time, but the preferred approach is to have the assessment conducted on site.

Question 20:

Annex D, item 8: The contractor must be able to arrange the provision of services within shortest possible time upon receiving the notification from the OSCE SMM (please specify numbers of working days needed for preparation, but not longer than 40 days)
This item states 40 day limit to start the works after notification from OSCE, not to complete them, correct?

Answer: Correct, within 40 days the contractor should start the work.

Question 21:

Since there are a lot of uncertainties at this stage, it's hard to give precise estimate for the works. Are you open to the model, when the budget is fixed, but supplier can choose the depth of testing to meet budget constraints?

Answer: This is a tender process. And all participants are in equal conditions. The awarded amount cannot be increased and the proposed/awarded scope of services cannot be decreased. The results of the activities have to meet the described expectations and requirements.

Question 22:

Does OSCE assume fix price model for all the works? Are you open to extending the budget if supplier discovers and provides grounded explanation of obstacles, which might require extending the budget to achieve higher quality of assessment?

Answer: This is a tender process. And all participants are in equal conditions. The awarded amount cannot be increased and the proposed/awarded scope of services cannot be decreased. The results of the activities have to meet the described expectations and requirements.
However, in case of the awarded contractor provides the grounded explanation of obstacles that were not taken into account in the initial requirements and which are not anticipated within the framework of the specified requirements, this may be a subject of the additional procedure.

Question 23:

To leverage our technology and our Vendor platforms we need to send the SOVA code to our Data Centers in Madrid, Spain - Would this be an acceptable practice?

Answer: Subject to discussion.

Question 24:

ToR states that – The Activities are expected to be performed in OSCE SMM office in Kyiv – will it be acceptable to perform some activities relates to the project, that may be required to be done outside of OSCE SMM network perimeter (for example vulnerability assessment or penetration testing) remotely from our offices or other location.

Answer: Some components may be accessible from outside for a short period of time but the preferred approach is to have the assessment conducted on site.

Question 25:

Deliverables section of ToR states that documentation should be delivered within 2 weeks of execution of activity – does it mean that overall time from beginning of activity will be activity execution time + documentation time (2weeks) (e.g. activity execution time =3 weeks, then overall time for activity is 5 weeks)

Answer: Correct. However it is preferred to have the draft report in the shortest possible time.

Question 26:

Should the review, testing be performed on live data / system in production?

Answer: In production environment.

Question 27:

Are there any standards and requirements of corporate or government policy that should be met?

Answer: To be discussed during the contracting phase.

Question 28:

What kind of vulnerability scanning is expected (discovery, credentialed)?

Answer: Contractor's methodology is expected.

Question 29:

What kind of code review is expected (manual, automatic)?

Answer: Consultant's methodology is expected.

Question 30:

What are requirements for system availability?

Answer: Expected to be low as of the test time

Question 31:

How sensitive is the data in the database? Is there Personal data?

Answer: The data is sensitive. No personal data.

Question 32:

Do you have any compliance requirements (i.e. GDPR)?

Answer: Not applicable

Question 33:

How are the backups organized? Are they In scope?

Answer: Backups are not in the scope

Question 34:

What are the endpoints (Win, Linux, MacOS, Android)?

Answer: Android OS, Windows Server

Question 35:

The penetration testing is expected to be white/black box? Will we be provided with user access to the app?

Answer: User access will be provided. Mostly White box. Black box will be as an advantage.

Question 36:

What is the number of IPs to be tested?

Answer: Very limited.

Question 37:

Do you undertake the responsibility to notice their Internet Service Providers about the planned penetration testing activities including the time frame of the testing?

Answer: Yes, if there will be a need to do so.

Question 38:

What criteria are expected to use while prioritizing the risks during assessment?

Answer: Not applicable

Question 39:

Any open source used (Laravel PHP framework version 5.4 and OpenSSL)? Should we review it for security risk as well?

Answer: Yes.

Question 40:

How the working materials should be destroyed? Are there nny requirements on their storing?

Answer: All working materials, logs of the results, hardcopy docs, etc. shall be handed over to SMM.

Question 41:

Hosting type: on-premise / cloud?

Answer: On-premise.

Question 42:

Should we cover system hardening (endpoint/server/hypervisor)?

Answer: Yes, but only for the limited scope provided and not for the whole IT infrastructure.

Question 43:

Is there any IPS (or related technology that restricts access to the app) in use?

Answer: Testings will be conducted on both sides of FW/ISP systems.

Question 44:

Is there a possibility to create a clone of production environment so production environment is not affected?

Answer: Production environment is planned to be used.

Question 45:

Will you conduct interviews with the core engagement team?

Answer: Interviews or induction meetings are possible, but are not foreseen on this stage.

Question 46:

We would like to sign NDA before sharing financial information. Could you please tell if we should use your NDA template or we can share ours?

Answer: This is a tender process. And all participants are in equal conditions. No NDA or any similar documents can be signed before the contractual stage. Financial statement is a part of the bidding documents that proves the viability of the company. All the bidding documents have a very limited access and the non-disclosure of the provided vendor's sensitive data is a responsibility of the OSCE.
The NDA will be signed with the awarder contractor. The form of the NDA is a subject of discussion.

Question 47:

Please let us know if all project team members should be present in OSCE SMM office in Kyiv or only core team?

Answer: Subject to the contractor's approach in condition that all the specified security restrictions are met.

Question 48:

Could you please clarify regarding the question 6, bullet 2 in ANNEX D. We are asked to provide financial statement for the last 3-5 years. Would you like to see the financial statement only for the security services? Also, in the RFP document, we have a requirement to provide Financial Statement for the last 3 years. Are those two requests connected to one document – company`s financial statement?

Answer: The Company's professional experience and the financial statement are the separate requirements. The Company's Financial Statement for the last 3 years is requested as an evidence of the viability of the company.

Question 49:

What kind of information will the vendor be able to share in terms of cooperation with OSCE either publicly (website, presentations to other potential customers, calls, etc.), or after signing an NDA, once the project is complete (i.e. name of the customer (OSCE), type of work, reference contact details upon request)?

Answer: According to the cl.14 of OSCE General Conditions of Contract (Services) https://procurement.osce.org/resources/document/general-conditions-contract-services : "*Unless authorized in writing by the OSCE, the Contractor shall not advertise or otherwise make public for the purpose of commercial advantage the fact that it is a contractor to the OSCE, or use the name, emblem, logo, official seal or any abbreviation of the OSCE.*"