Title:

Negotiated procedure for low-value contract for the performance of a "bug-bounty" activity on open-source software

Purpose:

The Commission intends to conduct a small-scale "bug bounty" activity on open-source software with companies already operating in the market. The scope of this action is to:

- run a small-scale "bug bounty" activity for open source software project or library for a period of up to two months maximum;
- the purpose of the procedure is to provide the European institutions with open source software projects or libraries that have been properly screened for potential vulnerabilities;
    - the open source software project or library, to be reviewed, will be selected by the European institutions;
    - the choice will take into account the limited duration of this project, the software use at the European institutions as well as the results of a public survey done in the scope of EU-FOSSA Pilot project;
- fully manage the process of vulnerability submission and vulnerability assessment in a transparent manner allowing full justification of the bounty award;
- fully manage the communication with the teams or communities reviewing the source code of the projects being analysed;
- the process must be fully open to all potential bug hunters (hereafter called the "researchers" or the "bug hunters"), while staying in-line with the existing Terms of Service of the bug bounty platform;
- the company must grant the European Union staff an access to observe the fairness of the awarding process;
- the proposed total cost of the project is a fixed-price and must cover all the costs of exploitation of the project (including the reward budget for bounties and all platform costs);
- the company must prove having run similar bug bounties during one year preceding this publication;
- the company must be able to start the process within 5 working days from the signature of a contract with the European Commission and complete it within maximum 2 calendar months from that point in time;
- the company must report regularly on the progress as well as prepare a project report at the end of the project; all such project documentation becomes property of the European Union.

Access to market:

Participation in the procurement procedure will be open on equal terms to all natural and legal persons coming within the scope of the Treaties, as well as to international organisations. It will be also open to all natural and legal persons established in a third country which has a special agreement with the Union in the field of public procurement on the conditions laid down in that agreement.

Selection criteria:

The candidates must have the necessary technical, professional, economic and financial capacity to execute the contract, and in particular:

- An annual turnover of the last financial year for which accounts have been closed above EUR 60,000.
- The candidate must prove experience in the field of running a "bug bounty" platform and organising "bug bounty" activities (at least three different projects having similar or higher value, scope and complexity, involving the security audit of open source software, running for at least 1 month on the candidate's platform, having at least 10 researchers participating and completed between May 2016 and May 2017).

When expressing their interests, the candidate is invited to provide evidences that it fulfils the selection criteria above.

NB: Each reference must include the following information:

- Client name
- Client's Contract person name, position, phone number and email address;
- Client's official statement (signed by authorized representative) on the accuracy of the reference project details including the customer satisfaction level
- Start date (mm/yy)
- Finish date (mm/yy)
- Description of the contract (type of source code researched and overview of the results of the research);
- Brief description of the services supplied (process used to assess the vulnerabilities and bounty awarding process).

Estimated amount: 60,000 EUR maximum for running "bug bounty" activities on an open-source software. Tenders proposing a budget higher than 60,000 EUR will be excluded from evaluation.

Period of execution of the contract: 2 calendar months from the start date

Estimated launching date of the negotiated procedure: 28/06/2017

Contact information:

Economic operators interested in participating in this call for tenders may express their interest by writing to DIGIT-CONTRACTS-INFO-CENTRE@ec.europa.eu no later than 16:00 pm CET/Brussels time on 17/07/2017. It is strongly advised to verify that you fully comply with the access to market rules and selection criteria announced before contacting the Commission.

The participation or non-participation in this activity has no influence on any potential future procurement procedure regarding security audit of Open-source software that could be

launched by the Commission. To maintain the transparency of the latter, all Final Reports will be published on this website afterwards.