CONTRACTS FINDER ADVERTISMENT

Project Reference 2019-410

INVITATION TO TENDER FOR

Static & Dynamic Analysis Tool

TABLE OF CONTENTS

1. Introduction

AHDB

The Agriculture and Horticulture Development Board (AHDB) is a non-departmental government body, funded by levy income from farmers, growers and others in the supply chain, and managed as an independent organisation (independent of both commercial industry and of Government). The role of the AHDB is to help improve the efficiency and competitiveness of various agriculture and horticulture sectors within the UK. Our statutory functions encompass meat and livestock (cattle, sheep and pigs) in England; horticulture, milk and potatoes in Great Britain; and cereals and oilseeds in the UK. Our purpose is to inspire our farmers, growers and industry to succeed in a rapidly changing world.

As AHDB is funded in this manner, value for money is paramount, we welcome suppliers who can offer innovative and cost-efficient solutions to meet our needs, whilst also offering superlative service that will enable us to create a world-class food and farming industry. Solutions should look to help us not only reduce costs but increase business flexibility, lift productivity, bring people together to collaborate, innovate and drive change throughout.

Further information about AHDB can be found here: https://ahdb.org.uk/

The Service

AHDB are looking to introduce a Security Testing Standard which Information Systems will need to comply with. We have been trialling a static and dynamic analysis tool within IS over the last 12 months for a single application and this trial has provided the leverage to roll out a suitable static and dynamic tool across the department rather than just been limited to one application.

The primary purpose of this tender is to seek a static and dynamic analysis tool/s (and potentially any other products which could help meet the objectives below).

AHDB are looking for:

- A tool to provide reports that the code scanned meets security requirements for both static and dynamic testing Open Web Application Security Project Standards (OWASP) Top 10
- Support for the product
- A security partner able to proactively advise and steer AHDB in delivering to our strategic priorities and achieve maximum return on investment

This will be for the contract period of 1st April 2020 or the soonest date after that is possible for 2 years followed by an option to extend twice for 1 more year (a total possible of 4 years) thereafter the opportunity will be put out to tender again.

2. Background

When AHDB introduces a new piece of software such as a web application, web site or other system or indeed makes substantial changes to one of its current systems this can introduce additional risk to our information, especially if we are collecting or processing sensitive information belonging to our Farmers, Growers & Processors.

Security testing of applications and the infrastructure they are built on requires a consistent and repeatable approach across all systems as the defence of the organisation's information systems is only as strong as its weakest link.

3. Services required

Security Testing - General

Security testing is conducted throughout the lifecycle of an Information system using various techniques to ensure any vulnerabilities that can be exploited by an attacker are removed before the project goes live.

This is only part of the story as new vulnerabilities are found, either through new techniques available to the hacker or as an unintended consequence of an update to an application or system.

Security testing can carried out using various methods and AHDB are looking for a tool to help us comply with the below;

1) Code Scanning - code scanning is conducted on the source code of an application as an aid to discovering any security flaws in the code, generally using OWASP (Open Web Application Security Project) Standards.

2) Vulnerability Scanning – a third party scanning tool is used to discover and analyse known vulnerabilities.

Figure 2 below shows the approximate alignment between AHDB project stages and security testing techniques;

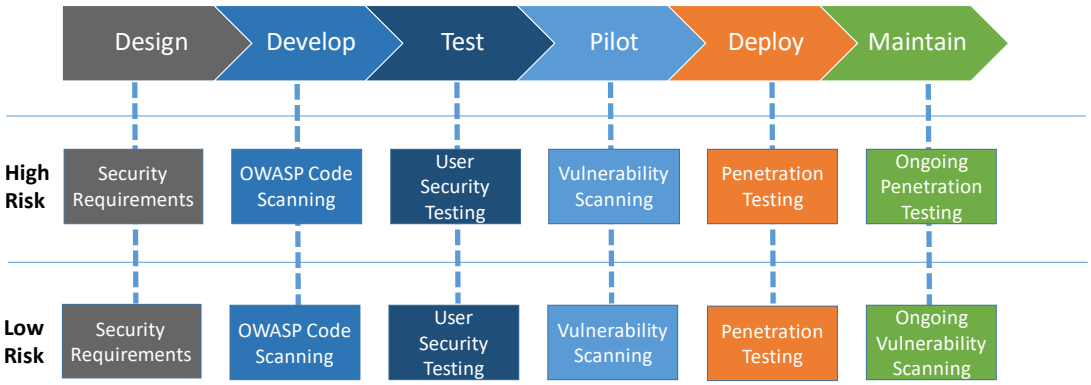

Figure 2 – Best Practice Testing

For the requirement of security testing during the maintenance stage, a view must be taken and agreed by all major stakeholders at as to how often the ongoing tests need to be, for low risk items with superficial changes may not need to be tested during the maintenance phase more than once every 4-5 years, however a complex business critical application undergoing multiple significant changes may need to be tested as frequently as every 6 months (although this is probably at the worst case scenario)

Security Testing – Specifics

a) OWASP Code Scanning (Essential)

AHDB need code scannning software to aid developers to locate potential flaws and determine areas of improvement within their code base. Code scans are conducted internally using these commercially available tools. The scan may be performed during program creation or as enhancements are made to provide insight regarding potential vulnerabilities. OWASP (Open Web application Security Project) is the most well-known and will be used by AHDB to provide assurance that the code base does not have any known security vulnerabilities. Any failure reported in the scan results within the medium to the very high range must be addressed before the project goes any further as code changes are difficult to support when the systems or service goes live.

Requirement - Code Scanning must be performed when the application is first tested and again after every significant change including the correction of known issues. (To ensure new vulnerabilities have not been added with the code improvements).

b) Vulnerability Scanning (Essential)

Vulnerability scanning (in some areas called Dynamic Security Testing) is the network scanning of an application and/or infrastructure for known vulnerabilities, it uses a database of known vulnerabilities and compares it with the configuration of the system and provides a prioritised list of the known vulnerabilities it has found together with risk score as to how easily the vulnerability can be exploited.

AHDB are looking to utilize a vulnerability scanning tool to proactively prevent the exploitation of IT vulnerabilities that exist within AHDB systems (either internally facing or externally facing) which will allow us to reduce or eliminate the potential for exploitation and involve considerably less time and effort than responding after any exploitation has occurred.

Requirement - Each application, website or other service or system must be vulnerability scanned at the end of the development process before it has been released into production.

Additional Vulnerability Scanning should also be undertaken after significant configuration changes or where new high-risk exploits are identified either by the software vendor or other trusted third party.

The scanning report (in plain English) and Remediation Action Plan detailing the identified vulnerabilities will be produced, it will include a list of vulnerabilities rated on a number of criteria that show the risk each of these vulnerabilities expose.

c) Reporting

To provide clear reports of the outcomes of the scanning process reporting on all the issues that were found after each scan. These reports should be in a pdf format or other suitable format to circulate to the manager / business. The other report should create a task list of the flaws so the developers can address any issues highlighted in the scan. These should be able to be access through Visual Studio and/or DevOps.

d) Remediation

To provide advice and guidance on how to fix the issues that the software flags up, AHDB require a variety of remedial actions, where possible, to resolve issues cost effectively and efficiently with a drive for continuous improvement. Examples of remedial action may be:

- sharing a knowledge article
- sharing a website or video for the developer
- time with a consultant

This list is not exhaustive.

4. Personnel

The AHDB Information Services team will consist of (but not limited to and not all will be users):

1 Manager
2 Lead Developers
1 Senior Developer
2 Contractors used frequently
2 Business Analysts – no coding but gather the requirement

5. SDLC methodology used for application development and testing

We use Visual Studio as our coding platform

We use Dev Ops as our code repository

We use add-ins such as JavaScript libraries,

Paid for add-ins like Re-Sharper

We don't automate build or testing currently, but we do plan to introduce some type of automated testing in the next 12-18 months

6. Inventory of Applications

Solution Name	Size	Platform	Code	Method
Levy Admin Portal	42MB & 15MB	Azure SQL DB	C#, javscript,	MVC Framework
Levy Returns Portal	41MB & 14MB	Azure SQL DB	C#	
Levy Agresso Sync Windows Service	50MB & 16MB		C#	
Levy WebApi			C#	
Dairy Wholesale	39MB & 14MB	Azure SQL DB	C#	
RL Portal (Will be spilt into 2 during the update)		MS SQL 2008 R2 on premise	C#	
MI Portal		Azure SQL DB	C#	
MI Portal Exchange Rates WebApi			C#	
IMPC Portal	13MB & 4MB	Azure SQL DB	C#	
IMPC Business Layer	2.3MB & 0.6MB	Azure SQL DB	C#	
RB209 API		Azure SQL DB	C#	
RB209 management Portal		Azure SQL DB	C#	
RB209 web client			C#	
Weather Hub	23MB & 8MB	Azure SQL DB	C#, Logic Apps	
AMDAC		MS SQL 2017 on premise	VB.Net	Console and WinForms Application
DWPIG		MS SQL 2017 on premise	VB.Net	Console and WinForms Application
DWCAT		MS SQL 2017 on premise	VB.Net	Console and WinForms Application
DWSHE		MS SQL 2017 on premise	VB.Net	Console and WinForms Application
Trade Data		Azure SQL DB	VB.Net	Console and WinForms Application
Sheep Scan		MS SQL 2017 on premise	VB.Net	Console and WinForms Application

7. Clarifications

If you have a specific question related to this tender please email Jayne.Chalmers@ahdb.org.uk stating the Tender reference 2019-410. All responses to questions received as part of the process will be recorded, anonymised and shared as an edit on this notice, so it is highly recommended that, **if you are interested in this opportunity that you select "Watch this notice" against this advertisement therein**.

8. Response

In order to facilitate and standardise responses to this tender, we have provided forms alongside this document which we require you to populate.

1) Quality Assessment (60%)
   Please provide your response to section 1, 2 and 3 on the accompanying quality response form.

   PLEASE NOTE – Section 2 Mandatory Question:
   Please confirm you seamlessly integrate with Visual Studio?
   IF the answer to the above is No, please do not proceed any further as your bid will not be considered

2) Price (40%)
   Please provide your quotation for the supply of the services in section 3 of the accompanying commercial response form.

This populated Response Form and supporting documents should then be emailed to: **Jayne.Chalmers@ahdb.org.uk by 5pm on the 10/04/2020.**

Submissions will remain unopened until after the closing date and time has passed.

9. Evaluation

AHDB will then assess those suppliers based on the combination criteria of totalling the weighted criteria of Price (40% available - the lowest price achieves the maximum weighting) and the total marks achieved in Quality (60% available).
We will then be holding a webinar session for the top 3 scored responses which will include the AHDB lead developers and head of IS systems. We would require the presence of your security architect/product specialist. Should this be unsuitable we will adjust timings as necessary. This will not affect your proposal in any way. The final award decision will be arrived at as a result of the Webinar POC.

Please note that AHDB will not reimburse any expenses incurred by interested parties in preparing their responses to this Tender.

10. Timetable

The below are provisional timelines only and may be subject to change.

Opportunity Published	w/c 06/04/2020
Last date for suppliers to ask clarification questions	w/e 24/04/2020
Deadline for receipt of submissions/quotes	w/e 01/05/2020
Webinar assessments/demonstrations (top 3 responses)	Between 11/05/2020 & 22/05/2020
Award of contract	w/c 25/05/2020
Contract commencement	01/06/2020

11. Conditions of contract

Please note that AHDB Standard Terms and Conditions will apply to the contract, a copy of which can be found on the AHDB website: http://www.ahdb.org.uk/about/Procurement.aspx

Tenderers are advised to familiarise themselves with these Terms and Conditions prior to submitting the proposal. The successful supplier will be required to sign a contract with AHDB before commencement of services.

The prices quoted in the response will form part of the contract.