CONTENTS

1. PURPOSE

DVSA is looking to purchase vulnerability scanning software to monitor and report on vulnerabilities within software dependencies.

Managing 3rd party software dependencies is an onerous but necessary task to ensure vulnerable software is not released onto production servers. Use of open-source dependencies is commonplace within DVSA software.

The only logical choice in this space is to procure services that have technology to monitor and contribute to CVE databases.

Snyk, is software as a service, the proposal is to seed with accounts for all developers (development and test team – a developer is classed as anyone who has committed in the last 90days) so 100 will allow for existing requirements and any project transition into CI.

2. BACKGROUND TO THE CONTRACTING AUTHORITY

DVSA is an executive agency, sponsored by the Department for Transport. We help you stay safe on Great Britain's roads by helping you through a lifetime of safe driving, helping you keep your vehicle safe to drive and protecting you from unsafe drivers and vehicles

We employ around 4,600 people across Great Britain to do this. They include:

2..1 driving examiners

2..2 vehicle standards assessors

2..3 vehicle examiners

2..4 traffic examiners

2..5 customer service agents

2..6 registration and licensing officers

2..7 digital services and technology experts

2..8 corporate services experts, such as communications, finance and HR

3. OVERVIEW OF REQUIREMENT

Requirement is for Snyk open source, use across all teams 100 developer licence and also to scan terraform code for any configuration vulnerabilities 50 IaC licences.

Requirement	Quantity
Snyk Open Source - 50 Pro UserPack	2
Snyk IaC - Pro User	50

The contract is for a period of 1 year with an option to extend for a further year.

4. SCOPE OF REQUIREMENT

Modern software development at pace hinges on the inclusion of third party, typically open-source packages and components, regardless of the language.

Introducing these packages results in faster delivery, arguably more robust software and ease of development. However, there are also risks – a reliance on 3rd party software, reliance on hosted package management systems and potential for vulnerability injection. By far the most severe of these is vulnerability injection.

DVSA will benefit from a security scanning tool, integrated into out pipelines and processes. Analysis of the market has considered internal integrations, language support and customisation for the DVSA need. Several tools have been looked at but tooling option recommended Snyk open source, use across all teams 100 developer licence and also to scan terraform code for any configuration vulnerabilities 50 IaC licences.

5. KEY MILESTONES AND DELIVERABLES

The following tendering milestones (anticipated timelines subject to change) shall apply:

Milestone/ Deliverable	Description	Timeframe or Delivery Date

1	Publish invitation to tender	29 April 2021
2	Clarification questions deadline although DVSA will address questions as they arise	4 May 2021 23:59
3	Responses to clarification questions	5 May 2021 23:59
4	Submit tenders	7 May 2021 23:59
5	Evaluation decision	10 May 2021
6	Notification letters to suppliers	11 May 2021
7	Contract Award	11 May 2021

6. CONTINUOUS IMPROVEMENT

The Supplier should update DVSA with new features and fixes as they are made available in each release.

7. PRICE

Prices must be populated within Commercial Envelope in Jaggaer. All rates must exclude VAT.

8. SECURITY AND CONFIDENTIALITY REQUIREMENTS

14.1 The supplier shall maintain and comply with a security policy which specifically addresses the protection of all Authority information/data that is generated and/ or managed in the provision of the service.

The supplier must allow audit of all controls under this section by the Authority to agreed schedules as well as notification of any sub processing prior to implementation.

14.2 The supplier's security policy shall address as a minimum:

- security management (risk assessment, response, evaluation, responsibilities and roles)
- supplier personnel integrity (recruitment, training, staff responsibilities, vetting, and disciplinary procedures)

- compliance with legislation
- business continuity arrangements
- handling of information from creation to destruction or deletion
- management of suspected/ actual breaches of security.

14.3 The supplier shall comply with all the relevant legislation, organisational and cross Government policy and guidelines in relation to data and asset security including but not limited to: Data Protection Act 2018, General Data Protection Regulation (GDPR), HMG Security Policy Framework, Cabinet Office Minimum Cyber Security Standard (2018), National Cyber Security Centre Cloud Security Principles.

14.5 The supplier shall ensure that the Authority's information and data is secured in a manner that complies with the Government Security Classification Policy rating of OFFICIAL. The Supplier shall ensure that the Government Security Classification Policy rating is also applied when information and data is transmitted across all applicable networks and/or in line with the Authority's requirements.

Handling of OFFICIAL SENSITIVE data must ensure no removal or obfuscation of GSC classification in metadata.

14.6 The supplier must notify the Authority of any data being offshored outside of the UK and for what purpose. Any changes to the handling of data, including changes to offshoring, must be notified and have the approval of the Authority before any change happens.

14.7 The supplier shall ensure that any suspected or actual security breaches are reported to the Authority's representative immediately. Breach reporting must be defined with named contacts and escalation paths.

14.8 The supplier shall ensure that they support the Authority in meeting their legislative obligations including, but not limited to, those set out in:

- General Data Protection Regulations 2018
- Data Protection 2018
- Freedom of Information Act 2000
- Human Rights Act 1998
- Privacy & Electronic Communications Regulations 2006 (PECR)
- Regulation of Investigatory Powers Act (RIPA) 2000
- The Investigatory Powers Act 2016

This includes assisting the Authority carrying out a data protection impact assessment and identifying and mitigating privacy risks to a level acceptable to the Authority.

14.9 The supplier shall not charge a premium to the Authority for any additional standards and/ or security compliance applicable to a Call Off Contract, unless otherwise agreed in advance by the Authority

9. PAYMENT AND INVOICING

Payment can only be made following satisfactory delivery of pre-agreed certified products and deliverables.

Before payment can be considered, each invoice must include a detailed elemental breakdown of work completed and the associated costs. Purchase order must be included on each invoice.

Invoices should be emailed to: ssa.invoice@sharedservicesarvato.co.uk or posted to the following address:

Shared Services Arvato
5 Sandringham Park
Swansea Vale
Swansea
SA7 0EA

10. CONTRACT MANAGEMENT

Contract Review meetings are not expected. But DVSA is open to review meetings every 4 months during the life of the licence and at a further review meeting when it ends.

11. LOCATION

The location of the Services will be carried out at:

The Axis

112 Upper Parliament Street

Nottingham

NG1 6L