Planning

DDaT25380 - UKRI - BGS Web Application Firewall (WAF)

UK Research and Innovation

UK2: Preliminary market engagement notice - Procurement Act 2023 - view information about notice types

Notice identifier: 2025/S 000-069946

Procurement identifier (OCID): ocds-h6vhtk-05d798

Published 31 October 2025, 9:46am

Scope

Reference

DDaT25380

Description

The purpose of this survey is to test the market and see what the market can offer and whether suppliers able to deliver what is required.

If UKRI decide to go to market, then In alignment with the Procurement Act 2023, information gathered as part of this Pre-Market Engagement activity shall be shared and made available to all potential suppliers to maintain a fair and transparent process, preventing any Supplier from gaining an unfair advantage and to avoid distorting competition. If there is any information you enter which you deem commercially sensitive and that you wish not to be shared to other suppliers, then please indicate within the specific response(s) in the questionnaire including your reason for them not to be part of the information to be shared to other potential suppliers.

This pre-market engagement notice is to help us understand the market.

UK Research and Innovation (UKRI) have an existing web application firewall in Keyworth and Edinburgh, that is due to go end of life in December 2026 and needs to be replaced to maintain a secure operating environment and Cyber Essentials Plus certification, which critically underpins BGS commercial activities.

The primary objective for deploying the new solution is to enhance application security, ensure high availability, and optimise traffic management across the BGS operating environments in Keyworth and Edinburgh.

Functional and Non-functional Requirements

The Balancer solution must meet the following functional and non-functional requirements to ensure robust performance, security, and scalability.

Functional Requirements

· SSL Offloading: Terminate SSL connections at the load balancer to reduce backend server load.

· Traffic Inspection: Deep packet inspection to detect and block malicious traffic.

· Application Layer Protection: Defend against OWASP Top 10 vulnerabilities including XSS, SQL injection, and CSRF.

· Load Balancing Algorithms: Support for round-robin, least connections, and IP hash methods.

· Session Persistence: Maintain user sessions across multiple requests.

· Health Monitoring: Continuous checks on backend server health to ensure availability.

· Content Switching: Route traffic based on URL, headers, or other application-level data.

Non-Functional Requirements

· High Availability: Redundant architecture with failover capabilities (achieved by dual systems in Keyworth and Edinburgh)

· Scalability: Ability to handle increasing traffic loads without performance degradation.

· Performance: Low latency and high throughput under peak conditions.

· Security Compliance: Adherence to standards such as PCI DSS, ISO 27001, and GDPR.

· Manageability: Centralised management interface with role-based access control.

· Logging & Auditing: Comprehensive logging for security events and administrative actions.

· Interoperability: Compatibility with existing infrastructure and third-party tools.

Security and Compliance

The solution must align with industry-standard security and compliance frameworks to ensure data protection, regulatory adherence, and risk mitigation. Key considerations include:

· Regulatory Standards: Support for compliance with PCI DSS, HIPAA, ISO 27001, GDPR, and other relevant regulations.

· Data Protection: Encryption of data in transit and at rest, secure key management, and tokenisation where applicable.

· Access Control: Role-based access control (RBAC), multi-factor authentication (MFA), and integration with identity providers.

· Audit & Logging: Detailed logging of security events, configuration changes, and user activities to support forensic analysis and compliance reporting.

· Vulnerability Management: Regular updates, patching, and integration with threat intelligence feeds to address emerging vulnerabilities.

· Security Testing: Support for penetration testing, automated vulnerability scanning, and security validation during deployment cycles.

These measures ensure that the solution not only meets technical requirements but also aligns with organisational governance and risk management policies.

Integration and Monitoring

Successful deployment of the solution requires seamless integration with existing infrastructure and robust monitoring capabilities. Key integration and monitoring requirements include:

· Infrastructure Integration: Compatibility with existing network architecture, DNS, firewalls, and application servers.

· Identity & Access Management: Integration with LDAP, Active Directory, and SSO

solutions for centralised authentication and authorisation.

· SIEM & Logging Platforms: Support for integration with Security Information and Event Management (SIEM) tools e.g. Microsoft Sentinel

· Monitoring & Alerting: Real-time monitoring of traffic patterns, performance metrics, and security events with customisable alerting mechanisms.

· API & Automation: RESTful API support for configuration management, automation, and orchestration with tools like Ansible, Terraform, and CI/CD pipelines.

· Reporting & Dashboards: Centralised dashboards for visualising system health, performance, and security posture.

These capabilities ensure operational visibility, proactive threat detection, and streamlined management across diverse environments.

Support and Maintenance

To ensure long-term reliability and performance of the solution, the following support and maintenance practices are required:

· Support: Access to technical support services, including 10/5 assistance, knowledge base, and escalation procedures.

· Software Updates: Regular updates and patches to address security vulnerabilities, improve functionality, and maintain compliance.

· Hardware Maintenance: Scheduled inspections, component replacements, and lifecycle management for physical appliances.

These practices help maintain system integrity, reduce downtime, and ensure that the solution continues to meet evolving business and security requirements.

Support:

5 year support - Level 1-3 Standard Service (10 hours x 5 days: 8am to 6pm Monday to Friday).

Providing - vendor software support, security patches and telephone support for the traffic management operating system (TMOS).

Hardware Maintenance:

5 year support - Next-Business-Day Hardware Replacement Service (RMA) (10 hours x 5 days: 8am to 6pm Monday to Friday). Next business day is acceptable given the high availability configuration.

Providing - replacement for defective hardware.

Implementation Support:

Onsite engineer support at Keyworth and Edinburgh for implementation.

Desired solution unique functionality includes:

WAF - ASM policies

APM - VPN

DNS - Global web site Load Balance (DNS)

LTM - Load Balancing of local traffic

VPN

To operate as an SSL VPN gateway and terminal server gateway.

Support active directory, saml and custom idp configurations.

Client/user attribute based rules.

Host checking including certificate/pathing/AV.

WAF

Advanced WAF (Web Application Firewall)

Be able to inspect API traffic and block malicious requests.

Supports JSON and XML payload inspection, which is essential for API protection.

Defends against common API threats like SQL injection, XSS, and API abuse.

Support ability to import openapi to create an api security defence policy.

Bot Protection

Detects and mitigates automated attacks on APIs (e.g., credential stuffing, scraping).

Uses behavioural analysis and machine learning to distinguish between legitimate users and bots.

Rate Limiting & Throttling

Prevents abuse by limiting the number of requests per user/IP/token.

Helps mitigate DDoS attacks targeting APIs.

Authentication & Access Control

Integrates with OAuth2, JWT, and other token-based authentication mechanisms.

Ensures only authorized users can access specific API endpoints.

API Discovery & Visibility

DNS

Needs to be able to query databases including Oracle to determine their high availability status.

Provide cross site load DNS level balancing

LTM

Being able to programmatically interact with traffic flow and security inspections using a like TCL syntactic language.

Be able to offload uploaded file scanning to antivirus using icap or cava

Specification:

The system specifications for the solution includes:

Hardware Specifications

· Processor:

o 6 vCPUs

o 18 vCPUs available for tenant workloads

· Memory:

o 128 GB DDR4 RAM

· Storage:

o 1 × 1TB M.2 SSD

· Form Factor:

o 1U rack-mountable chassis

o Dimensions: 1.72" (H) × 17.1" (W) × 30.6" (D)

o Weight: 36 lbs (16.33 kg)

Networking & Connectivity

· Management Ports:

o 1 × 1000BASE-T (RJ-45)

o 1 × USB 3.0

o 1 × Serial Console

· Data Ports:

o 2 × 100G/40G QSFP+/QSFP28

o 8 × 25G/10G SFP+/SFP28

Performance Metrics

· Layer 7 (L7) Requests per Second: 3.3 million

· Layer 4 (L4) Connections per Second: 1.4 million

· L4 HTTP Requests per Second: 18 million

· Max L4 Concurrent Connections: 85 million

· Throughput:

o L4: 95 Gbps

o L7: 85 Gbps

Total value (estimated)

- £800,000 excluding VAT
- £960,000 including VAT

Above the relevant threshold

Contract dates (estimated)

- 31 March 2026 to 30 March 2030
- 4 years

Main procurement category

Services

CPV classifications

- 30211300 - Computer platforms
- 48000000 - Software package and information systems
- 72000000 - IT services: consulting, software development, Internet and support

Contract locations

- UK - United Kingdom

Engagement

Engagement deadline

7 November 2025

Engagement process description

The Contracting Authority UK Research and Innovation (UKRI) would like to conduct pre-market engagement.

As part of this information gathering exercise, we have developed a series of questions to ascertain the capability, the capacity and the appetite of the current market and would welcome your responses.

Please see below questions

1.Company name

2.Name of main contact

3.Email address

4.Please confirm if your organisation is able to deliver the requirement as detailed within the specification

5.Are you registered on any Frameworks for the supply of Application delivery and security solutions that would fall in scope of this requirement? Required to answer.

6.Since you have answered yes, please share the details, including the Framework name and Reference number.

7.Please confirm if you have the capacity to deliver the goods by 31/03/2026 and have the systems in operation by 01/04/2026?

8.Do you foresee any potential issues with this requirement that may need to be considered? Particularly any challenges with installation and ongoing usage of the

solution?

9.What is your anticipated cost range to deliver all of the requirement? Please detail the potential element that will contribute to total cost, such as hardware, software, training, maintenance etc.

10.What are the lead times for the hardware required (in weeks)?

11.Are there any barriers (e.g. time constraints) that could discourage you from bidding?

12.Are there any new or emerging technologies, methods or innovations you think the Authority should consider for this requirement?

13.What support do you offer post-installation and what are the cost implications?

14.Are there any software necessary for the installation? If so, what are the costs associated (e.g. maintenance costs)

Due to the timeframe required, please ensure to complete the questions and email your responses to DDaTProcurement@uksbs.co.uk before 14:00 hrs on 07th November 2025 to express your interest.

If you would prefer the specification or questions in a document, please request them by emailing DDaTProcurement@uksbs.co.uk

---

Participation

Particular suitability

Small and medium-sized enterprises (SME)

Contracting authority

UK Research and Innovation

- Public Procurement Organisation Number: PDQJ-7126-JDHG

Polaris House, North Star Avenue

Swindon

SN2 1FL

United Kingdom

Email: commercial@ukri.org

Website: https://www.ukri.org/

Region: UKK14 - Swindon

Organisation type: Public authority - central government

Other organisation

These organisations are carrying out the procurement, or part of it, on behalf of the contracting authorities.

UK Shared Business Services Ltd

Summary of their role in this procurement: Shared Service Provider

- Public Procurement Organisation Number: PMPN-7535-GNTG

Polaris House, North Star Avenue

Swindon

SN2 1FF

United Kingdom

Email: DDaTProcurement@uksbs.co.uk

Region: UKK14 - Swindon

Contact organisation

Contact UK Shared Business Services Ltd for any enquiries.