

Dynamic Purchasing System

for the provision of

Managed ICT Security Service

DPS Admission Qualification Questionnaire

PART B – LOT SPECIFIC

Version	Date	Summary of changes
1.0	06.02.2026	Initial Release (terminated)
2.0	N/A	Update to Lot Details Update to 1.5.6 (c) Service Capabilities
3.0	21.04.2026	Update to Lot Details Update to 1.5.6 (c) Service Capabilities
4.0	15.06.2026	Update to 1.5.5 (E) Business Partner Requirement

Lot Details – CHOOSE ONE LOT ONLY

Interested Party must indicate below which lot this relates to.

For each Lot you are applying you MUST COMPLETE A SEPARATE PART B questionnaire.

Lot No.	Lot Name	Select Lot(s)
Lot 1	IBM QRadar based platform or equivalent, with managed ICT security services	☒
Lot 2	MS Sentinel based platform or equivalent, with managed ICT security services	☐
Lot 3	Splunk based platform or equivalent, with managed ICT security service	☐
Lot 4	Rapid 7 InsightIDR based platform or equivalent, with managed ICT security services	☐
Lot 5	Trend Vision One based platform or equivalent, with managed ICT security services	☐
Lot 6	AT&T AlienVault based platform or equivalent, with managed ICT security services	☐
Lot A	Any SIEM Platform or equivalent with managed ICT security services including SOC State the solution you are proposing under Lot A	☐ <Insert name>

Eligibility Requirements

Interested Party must complete and submit a separate form for every lot being submitted for admittance and upload documents as requested. Instructions under each section will indicate when uploading documents is required. Please input Yes or No as appropriate.

Note: The qualification questionnaire is divided into two sections, Parts A and B.

Part A: only needs to be completed once, regardless of the number of lots for which admittance is requested. It covers items 1.5.1–1.5.3 inclusive and 1.5.7.

Part B (this document): must be completed separately for each lot being submitted for admittance and covers items **1.5.4–1.5.6 inclusive**.

1.5.4 24x7 Security Operations Centre (SOC)	Respond Yes/No
Interested Party must provide their SOC and Incident Response Services on a 24 hour a day, 7 days a week, 365 days a year. Interested Parties are admitted to the DPS on acceptance of the Model Service Level Agreement in Appendix 5. This is the minimum level interested parties must provide. Confirm acceptance of the Model Service Level Agreement in Appendix 5.	
1.5.5 Technical and Professional Proficiency	Respond Yes/No
1.5.5 (a) References Evidence of three customers for whom they have delivered similar services. Details must include: - names, addresses and telephone numbers - a brief outline of their level of involvement with the reference site, - what services were provided - a brief description of the project - number of staff involved - duration of contract HEAnet will only contact any or all referees with prior notice given to the Interested Party. The information provided will be treated in the strictest confidence. Confirm you have uploaded relevant documentation to eTenders.	
1.5.5 (b) Minimum Order Value Evidence of relevant experience of a single minimum order value of €80,000 euros excluding VAT per year. Documentary evidence must be provided in the form of a reference statement relating to a completed contract performed within the last three years, counting backwards from the submission date of the Request for Admission. Confirm you have uploaded relevant documentation to eTenders.	
1.5.5 (c) Security Operations Centre (SOC) Service Evidence of, at a minimum, the following FTE staffing levels: 8 FTE Cyber Security Support Engineers, across L1, L2 & L3 2 FTE CISO equivalent Cyber Security personnel 4 FTE Cyber Security System Architects / Designers Interested Party must also provide certificate of fluency under the Common European Framework of Reference for Languages at level C2 Mastery or Proficiency or equivalent for each non-native speaker who will be part of the service delivery of the services described. Confirm you have uploaded relevant documentation to eTenders.	

1.5.5 (d) ISO or equivalent accreditation Interested Party must demonstrate accreditation to the ISO standard- ISO: 27001 or equivalent. Confirm accreditation and that evidence has been uploaded to eTenders.	
1.5.5 (e) Business Partner Requirement If not the original service of the SIEM platform, Interested Party must: • hold the minimum partner level for the solution they are providing • state the partner level • provide evidence of same Confirm the partner level and that evidence has been uploaded to eTenders.	<state partner level>
1.5.5 (f) Bring Your Own Licence (BYOL) Confirm if the proposed service has a mechanism where clients wishing to migrate to the solution can bring their existing licence(s). Confirm Yes/No	
1.5.6 Solution Requirements	Respond Yes/No
1.5.6 (a) Solution Scalability Interested Party must confirm the proposed services is scalable to meet the requirements of all Asiera clients. Asiera client sites range in size from offices of 50 people up to University Campus's with over 30,000 staff and students on site. A current example of a large university has an average of 15,000 events per second (approx. 400GB per day) with 20,000 end users. Confirm Yes/No	
1.5.6 (b) Professional Services Interested Party must confirm you can provide professional services on an ad-hoc basis where the following applies: Cyber security services will be available on a daily rate with a minimum block of 10 days and access to services of the following security roles: • Chief Information Security Officer • Senior Cyber Security Engineer/Architect • Cyber Security Engineer Confirm Yes/No	
1.5.6 (c) Service Capabilities Interested Party must confirm the SIEM Service has the following capabilities: • Log Management & Reporting • Automatic threat detection and alert • Implementation & integration of intelligence feeds • Collection, logging and storage from both onsite services and cloud • Automated ticketing system (provision or integration with existing) • Support user and entity behaviour analytics (UEBA) • Provide or integrate with Incident management capabilities	

• Ability to perform network discovery for linking incidents and users to physical network port and VLAN on both wired and wireless networks. • Reporting and analysis tools • MFA Confirm Yes/No Interested Parties may be required to provide evidence	
1.5.6 (d) Security Operations Centre (SOC) Service Interested Party must confirm the security operations centre (SOC) service has the following capabilities • SOC onboarding assistance • Security analysis • Threat intelligence • Incident Management • Reporting • Enforce MFA for all admin and management accounts • Information and guidance Confirm Yes/No	
1.5.6 (e) Advanced Security Management Services Interested Party must confirm the availability of a minimum of two (2) advanced security management service elements in <i>Appendix 3 - Admission Requirements - Advanced Security Services.docx</i> Interested parties should indicate the availability of these services within their portfolio and add any additional ones that may be suitable. • Incidence Response services • SOAR Services • MDR Services • MSSP Services • Red, Blue, Purple Teaming • Penetration testing • Vulnerability scanning • End point protection • Remediation of issues for clients • Intrusion detection and Prevention services • AD Health Checks/Auditing • Secure DNS Confirm you have completed Appendix 3 – Admission Requirements – Advanced Security Services.docx	