APPENDIX B

SERVICE DESCRIPTION

CONTENTS

1. INTRODUCTION

1.1 The Department for Transport is responsible for the aviation security policy within the UK, ensuring that the measures balance the need for security with the facilitation requirements of passengers.

1.2 The Department is continually assessing aviation security measures to ensure they mitigate current and potential future threats. Cyber security is a growing issue within the security environment (and beyond), and is becoming more significant in equipment and systems that were previously considered resilient because they were relatively unsophisticated and not networked.

1.3 Whilst cyber-security is fundamental to the integrity of all security screening equipment, this project focuses on equipment used in central search processes, and excludes the insider threat (i.e. it is assumed those with hostile intent do not have legitimate access to systems or equipment).

2. PURPOSE

2.1 The aim of this project is to review existing security screening equipment and systems used for screening passengers and their belongings to identify any cyber-security vulnerabilities and support development of good practice guidance for the airport security industry.

2.2 The output of the project will support development of guidance to the airport security industry that will ensure cyber security is considered alongside other security requirements when implementing and operating security screening equipment.

2.3 The vulnerability of individual equipment types will be considered, along with the environment in which they are deployed (including any corporate networks they may be connected to).

3. BACKGROUND TO THE AUTHORITY

3.1 The department for Transport (DfT) works with its agencies and partners to support the transport network that helps the UK's businesses and gets people and goods travelling around the country. DfT plans and invests in transport infrastructure.

3.2 The project will be overseen by the Research, Analysis and Development (RAD) team within DfT, which is a team of scientists responsible for ensuring that aviation security screening equipment is fit for purpose.

3.3 RAD will be responsible for technical oversight, answering specific technical queries, arranging access to equipment and airports, and providing liaison with relevant customers and Government Departments.

3.4 See https://www.gov.uk/government/organisations/department-for-transport for further information on DFT.

3.5 RAD is referred to as the Authority hereafter.

4. BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

4.1 Equipment used to screen passengers and their belongings before they enter the critical part of an airport is becoming more sophisticated, with a trend towards more networking and remote operations. There are several reasons for this, including:

4.1.1 Efficiency of the screening process and optimal use of staff resource to manage passenger queues.

4.1.2 Reporting of management information to support the operation.

4.1.3 Helping to demonstrate compliance with security directions and other regulatory requirements, such as queuing times.

4.1.4 Supporting remote access for routine maintenance and trouble-shooting of screening equipment.

4.2 The security performance of individual types of equipment has been assessed in detail, but there has been no detailed assessment of potential cyber security issues.

4.3 Specific screening equipment types that must be considered in the review are

- Security Scanners (SSc)
- Baggage X-Rays
- Walk Through Metal Detectors (WTMD)

4.4 For each of the equipment types identified in 4.3, an Evaluation Readiness Review (ERR) will be carried out to identify high-level technical vulnerabilities. Suggestions for mitigating the vulnerabilities (either technical or operational) will also be identified.

4.5 Once the ERRs have been completed, the operational environment in which they are used will be investigated, including a high-level network architecture review. To facilitate this, DfT will identify a specific airport, and provide introductions to relevant technical staff.

4.6 Any examples of existing good practice will be recorded and identified in the final project report.

4.7 RAD will provide access to representative examples of equipment, and access to airport equipment and relevant staff. RAD will also provide opportunities to talk directly to equipment manufacturers.

5. SCOPE OF REQUIREMENT

5.1 Mandatory Requirements:

5.1.1 The successful project will review and document potential cyber security vulnerabilities of at least one example of each type of equipment identified in paragraph 4.3.

5.1.2 For each type of equipment, specific vulnerabilities associated with networking will be identified and mitigations proposed, and results of the ERR documented.

5.1.3 The project will conduct a network architecture review of the operational environment in which the security equipment is deployed, to identify any vulnerabilities and possible mitigations.

5.1.4 A report detailing all of the findings of the project will be delivered in pdf or word format.

5.1.5 Recommendations of effective mitigation options (and examples of good practice) for each type of security equipment will be documented in the final report.

5.1.6 The successful bidder will have experience of carrying out cyber security assessments of systems.

5.1.7 The successful bidder will be a CESG accredited test laboratory (for example, see details here: http://www.cesg.gov.uk/AboutUs/contactus/Pages/Contact-CPA.aspx)

5.1.8 The successful bidder will be a CESG accredited CLAS consultant (see http://www.cesg.gov.uk/ServiceCatalogue/CLAS/Pages/CLAS.aspx).

5.2 Desirable Requirements:

5.2.1 Knowledge of previous research in this technical area.

5.2.2 Working knowledge of aviation security equipment.

6. SERVICE LEVELS AND PERFORMANCE

6.1 The Supplier shall ensure that the Project Plan is maintained and updated on a regular basis as may be necessary to reflect the then current state of the implementation of the project.

6.2 The Customer shall have the right to require the Supplier to include any reasonable changes or provisions in each version of the project Plan.

6.3 The Supplier shall perform its obligations so as to achieve each Milestone by the Milestone date.

6.4 The Supplier will inform the customer of changes to risk which will impact upon delivery to time, cost or quality.

6.5 Changes to the Milestones shall only be made in accordance with the variation procedure and provided that the Supplier shall not attempt to postpone any of the Milestones using the variation procedure or otherwise (except in the event of a Customer default which affects the Supplier's ability to achieve a Milestone by the relevant Milestone Date). The variation procedure is detailed in Appendix G.

6.6 The supplier must ensure that the right people are in place to manage all aspects of delivery for the contract. The supplier must identify named individuals for each role as required as part of their tender submission.

6.7 Tenders must include full CV’s for all named individuals. It is not expected that key staff should change over the course of the contract but if for any change required must be communicated at the earliest opportunity and project members being replaced will be

substituted by those of a similar experience/authority. The Authority may also request the CV's of the new project members for verification if required.

6.8 The project progress will be monitored through regular review meetings. These will be at least monthly, and may be more frequent during the early stages of the project, in order to ensure that the supplier has sufficient information from the Authority.

6.9 The supplier must attend these meetings, which will be held either in DfT offices in London or at the supplier premises, at no additional cost to the Authority.

6.10 During the meetings, the supplier must update the Authority on all progress using the reports as specified in section 6.2, and highlight any new or changed risks that are likely to affect delivery of the project.

6.11 Any delay or issues may also be tabled during the meetings with resolutions agreed and changes addressed by use of the Contract Variation Form, (Appendix G).

7. SECURITY AND INFORMATION HANDLING REQUIREMENTS

7.1 Any information arising from this project (including data, interim or final reports, recommendations, vulnerability assessments and information provided by third parties) must be stored securely and access controlled such that only those with a direct need to know may access it.

7.2 Any information held on an IT system must be encrypted and password protected.

7.3 The supplier may be given access to sensitive information which must only be shared on a strict need to know basis (i.e. selected members of the project team only). The supplier will destroy all classified information on completion of the project.

7.4 Data may be held on a corporate IT network, subject to points 7.1, 7.2 and 7.3 above being complied with.

7.5 Information from this project may only be shared with third parties if prior written approval is obtained from the DfT. This includes publication, presentations at conferences and informal discussions with peers not directly involved with the project.

7.6 Staff with open access to the collated information and the final report must have (or have a willingness to obtain), at least a basic security check which meets the Basic Personnel Security Standard defined by the Cabinet Office.

8. PROJECT TIMETABLE & DELIVERABLES

8.1 The key targets for this project are as follows:

(a) Project initiation: September 2015

(b) Interim Progress Meeting: December 2015

(c) Project Completion: March 2016

8.2 Project Inception

8.2.1 Following the award of the contract, a project inception meeting will be held at the Authority's premises in September. The purpose of the meeting will be:

(a) Introduce key project team members from both organisations

(b) Discuss and agree working arrangements

(c) Review and authorise the project plan

8.3 Project Conclusion

8.3.1 At the conclusion of the contract, the contractor shall provide the Authority with:

(a) A final report detailing the work carried out during the contract and inclusive of details as described within the Delivery Plan (section 6.2).

(b) A list of recommendations for mitigations, and identified good practice, for inclusion in future guidance material.