CONTENTS

1. PURPOSE 2
2. BACKGROUND TO THE CONTRACTING AUTHORITY 2
3. BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT 2
4. DEFINITIONS 2
5. SCOPE OF REQUIREMENT 3
6. THE REQUIREMENT 4
7. KEY MILESTONES 6
8. AUTHORITY'S RESPONSIBILITIES 7
9. REPORTING 7
10. VOLUMES 7
11. CONTINUOUS IMPROVEMENT 7
12. SUSTAINABILITY 7
13. QUALITY 8
14. PRICE 8
15. STAFF AND CUSTOMER SERVICE 8
16. SERVICE LEVELS AND PERFORMANCE 8
17. SECURITY REQUIREMENTS 9
18. INTELLECTUAL PROPERTY RIGHTS (IPR) 10
19. PAYMENT 10
20. ADDITIONAL INFORMATION ..... **ERROR! BOOKMARK NOT DEFINED.**
21. LOCATION 10

1. PURPOSE

1.1 The purpose of this study is to provide an evidence based report outlining the UK aviation industry's current capability and future plans to respond to a serious cyber incident. It will also outline what support and advice industry needs from government to improve their plans.

1.2 The report will then be used within the Department for Transport (DfT) and shared with the National Cyber Security Centre (NCSC) and Civil Aviation Authority (CAA) to inform policy development in this field.

2. BACKGROUND TO THE CONTRACTING AUTHORITY

2.1 The contracting Authority is the Department for Transport (DfT). The Authority is the government department responsible for the safety and security of transport across the UK.

3. BACKGROUND TO REQUIREMENT/OVERVIEW OF REQUIREMENT

3.1 Like much of the UK's Critical National Infrastructure, the UK transport sector is a potential target for cyber-attacks. These may occur across the multitude of different systems and technologies that facilitate travel. There is scope for considerable economic and social disruption from malicious attacks, with the aviation sector in particular being a high profile and attractive target.

3.2 While aviation industry response plans to cope with physical attacks are well understood, tested and exercised, the Authority's experience of running table top exercises with separate areas of industry indicate that response plans for cyber-attacks require further development. There is a need to understand what current and future planning looks like, and what support industry requires from government to make it more resilient to cyber-attack. In this respect the Authority invites bids to provide:

- A comprehensive report outlining the UK aviation industry's current capability and future plans to respond to a serious cyber incident, and what support is required from government. The report is to be based on consultation with key aviation industry stakeholders across the UK.

- A summary of the findings.

3.3 The aims and objectives of the work are to:

- Inform the Authority of the state of incident response capability in the UK aviation industry, highlighting any particular weaknesses or gaps, focussing on pre-incident planning, incident response, and post-incident recovery;

- Outline the future direction of travel for response plans, and what support and advice industry requires from government, including the role it should play.

3.4 Proposals will be evaluated on the basis of demonstrable understanding of both the aviation industry and cyber security issues; how comprehensive the plan for engaging with relevant stakeholders is; proven experience in the field of aviation security, which should include experience of cyber security; the approach to the exchange and protection of the sensitive information that will be obtained and the cost forecast for the work.

4. DEFINITIONS

Expression or Acronym	Definition
DfT	Department for Transport or the Authority
NCSC	National Cyber Security Centre
CAA	Civil Aviation Authority
CPNI	Centre for the Protection of National Infrastructure
ANSPs	Air Navigation Service Providers

4.1 The term "industry" is used within this document. The term is intended to be broad and cover many participants in the aviation sector. It will comprise airlines, airports and Air Navigation Service Providers (ANSPs).

5. SCOPE OF REQUIREMENT

Baseline maturity of the aviation industry's cyber incident response capability

5.1 The study should gather evidence as to the current maturity of the aviation industry's plans to respond to a serious cyber incident, including details of chains of command, information flows, escalation thresholds and in-house/contracted technical response capability. The specific questions the Authority requires the Potential Provider to ask are outlined in section 6.2 below. The Potential Provider may identify additional questions to include in the study, but must first agree these in writing with the Authority. The output should be a report evidencing the current status of industry incident response plans, highlighting common gaps and areas where there is variation.

Assessment of role of government

5.2 A second aim of this study is to assess where government could provide the greatest impact and leadership in ensuring the resilience of the aviation sector to cyber-attack in the future. The report should include an outline of the plans industry has to improve their incident response capability, and what support they believe is required from government to enable them to do so.

Exclusions:

5.3 The report's recommendations should be primarily based on the views expressed in the consultation with the named organisations and enhanced by the Potential Provider's expertise in the relevant fields (rather than solely reflecting the opinions of the Potential Provider).

5.4 The Potential Provider is expected to consult with named organisations from the aviation industry only. The Authority has drawn up a list of target organisations that will be shared with the Potential Provider when the contract is awarded. The list covers ANSPs, airlines and airports, and comprises 25 UK-based organisations. The Authority will provide points of contact within each organisation, however the Potential Provider will be required to work with them to ascertain who the most appropriate individual in the organisation is to answer the questions. The Potential Provider should engage with a minimum of 50% of the organisations listed in each category. The Potential Provider

may identify additional organisations to include in the study, but must first agree these in writing with the Authority.

6. THE REQUIREMENT

6.1 The Potential Provider shall provide an electronic report describing the maturity of the aviation industry's capability and plans to respond to a cyber incident, their intentions to improve their capability in the future, and their views on what support and guidance will be required from government to enable them to do so.

6.1.1 The Potential Provider shall contact the organisations listed by the Authority to gather evidence in response to the questions outlined in section 6.2 below

6.1.2 The report shall provide a summary document of the responses providing a high level overview of the current and future maturity of the aviation industry with regards to cyber incident response.

6.1.3 The summary document shall provide recommendations, based primarily on consultation with stakeholders, but enriched by the Suppliers' own expertise, on what support/advice is required from government in improving the aviation industry's resilience to cyber-attack.

6.1.4 The report shall also provide a main section providing the evidence and reasoning behind the summary document's conclusions.

6.1.5 The report shall further highlight any commonalities and variations in responses across the aviation industry.

6.1.6 The report must be anonymised across all of the respondents so that no individual stakeholder is identifiable.

6.2 The Potential Provider will be required to collect responses to the questions outlined below. The Authority may also ask the Potential Provider to collect information in response to additional questions. These will be discussed and agreed at the inception meeting.

General:

- Do you know what your critical assets are?
- Does your organisation have a cyber incident response plan?
- Does your organisation test or exercise the cyber incident response plan?
- Are all employees aware of and understand the measures within the cyber incident response plan?
- Are you aware of the newly-formed National Cyber Security Centre (NCSC) and its role and capabilities?

Security Monitoring:

- How do you detect malicious content and other forms of attack amongst regular business traffic crossing the system boundary?
- How do you detect suspect activity indicative of the actions of an attacker attempting to breach the system boundary or other deviation from normal business behaviour?
- How do you detect changes to device status and configuration from accidental or deliberate acts by a user, or by malware?
- How do you detect suspicious activity that may indicate attacks by internal users, or external attackers who have penetrated the internal network?
- How do you prevent unauthorised connections to the network made by remote access, VPN, wireless or any other transient means of network connection?
- How do you detect unauthorised activity and access that is suspicious or violates security policy requirements?

Notification of an incident:

- Once an anomaly or suspicious activity is detected, how do you determine its criticality?
- What are the thresholds used to determine the level of response required?
- What are the escalation procedures to initiate the appropriate level of response?
- Are there assets or systems that you do not operate, but whose compromise would affect the operations of your organisation or assets?
- If so, how would you be informed about an anomaly or suspicious activity?
- How would you work with the organisation who owns and operates the asset or system in question to respond?
- What is the communications plan for internal staff i.e. who is informed, what information are they given, what stage are they given that information, and how is that information transmitted?
- What is the communications plan for external stakeholders, including the Department for Transport, the CAA, the NCSC and law enforcement?
- Do you have points of contact at all of the organisations listed above? Are these contacts regularly updated?

Incident response:

- Do you have in-house technical capability to respond to a cyber incident, or is this contracted out?
- If it is contracted out, how do you engage/work with the contractor at all stages of the response?
- Do you have back-up systems and/or strategies for continuing to operate without your critical systems?

Recovery:

- Do you have plans in place to recover from a cyber incident and resume operations?
- Do you have a mechanism for reporting lessons learnt and applying these to your response plans?

Future plans:

- Do you have plans to update your cyber incident response plans and/or improve your capability in this area?
- Are any of your future plans or identified improvements constrained by a lack of available resources or expertise?
- How will your future plans differ from your current plans?
- How will these plans be tested/exercised?

Government support/advice:

- Have you taken any advice/support from DfT, CAA, the NCSC or CPNI with regards to your cyber incident response plans?
- Have you taken any advice/support from DfT, CAA, the NCSC or CPNI with regards to an identified incident? If so, how useful was the support or advice provided?
- What do you see Government's role as being now, and in the future with regards to cyber incident response?
- Are there any areas where you would like to receive further support/guidance from government e.g. in identifying critical assets, identifying vulnerabilities, devising mitigation plans, devising incident response plans, testing and exercising response plans?
- Are there any common areas across industry that Government needs to focus on?

International and cross-industry:

- Have you received any advice or support from international counterparts or cross-industry bodies regarding incident response?
- Have you coordinated with any international stakeholders on incident response plans or in response to a specific incident?
- Given the increased interconnections and interdependencies in the aviation system, what additional support or arrangements do you think will be required to support responses to incidents at an international level?

6.3 It is expected that Potential Providers should be able to demonstrate:

- Expertise in the fields of cyber security and aviation and evidence of how they would apply this to the project. This should include CV's of the people undertaking the work, a list of previous relevant work and example case studies.
- A detailed plan for how they will undertake the work and who within the team will do which parts. For the plan a case study should be used to demonstrate how the work will be conducted and a project plan for the steps involved.
- The Potential Provider should also provide information on the resources and relationships they have available and how these will be utilised.

7. KEY MILESTONES

7.1 The Potential Provider should note the following project milestones that the Authority will measure the quality of delivery against:

Milestone	Description	Timeframe
1	Contract award	20th January 2017
2	Inception meeting	23rd January 2017
3	Delivery of first draft of report	10th March 2017
4	Final report delivery and presentation	24th March 2017

7.2 The Potential Provider shall perform its obligations so as to achieve each Milestone by the Milestone Date.

7.3 Changes to the Milestones shall only be made in accordance with the variation procedure and provided that the Potential Provider 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 Potential Provider's ability to achieve a Milestone by the relevant Milestone Date).

8. AUTHORITY'S RESPONSIBILITIES

8.1 The Authority will need to ensure that sign-off and comments on the final report is provided as per the agreed timetable.

8.2 In order to ensure that respondents are as open as possible about the status of their response plans, the Authority will provide a covering letter to the Potential Provider, explaining that all responses will be anonymised by the Potential Provider, and that the Authority will not take any regulatory or punitive action with individual organisations in response to the findings. The letter will also state that the report will remain confidential within government and will not be made publically available. This is to assure industry that the exercise is purely an information gathering one, intended to give the Authority a holistic view of the status of emergency response plans across industry.

9. REPORTING

9.1 Please refer to the Potential Provider's key reporting responsibilities as mentioned in 6.1.

10. VOLUMES

10.1 This contract is for a one-off piece of work for an estimated 6 week period or until the work is complete within the bounds of the contract.

11. CONTINUOUS IMPROVEMENT

11.1 Changes to the way in which the Services are to be delivered must be brought to the Authority's attention and agreed prior to any changes being implemented.

12. SUSTAINABILITY

12.1 N/A

13. QUALITY

13.1 The Potential Provider shall state how they will ensure a quality product and provide Quality Assurance through the provision of a Quality Plan. They may provide a summary of the Quality Assurance arrangements, principles, standards and checks they will use within the project.

14. PRICE

14.1 The contractor shall provide a fixed cost price for this work. The maximum allocated budget for the contract is £70,000.00 excl. VAT. Bids above this value may be discounted at the discretion of the DfT.

14.2 30% of the total evaluation score will be allocated to evaluation of the prices tendered for the specified requirement.

14.3 Prices are to be submitted via the e-Sourcing Suite, Appendix E excluding VAT.

15. STAFF AND CUSTOMER SERVICE

15.1 The Authority requires the Provider to provide a sufficient level of resource throughout the duration of the writing of the report on the "UK Aviation Industry's Capability to Respond to a Serious Cyber Incident" Contract in order to consistently deliver a quality service to all Parties.

15.2 Potential Provider's staff assigned to writing of the report on the "UK Aviation Industry's Capability to Respond to a Serious Cyber Incident" Contract shall have the relevant qualifications, experience and security clearance to deliver the Contract, as described in section 17.

15.3 The Potential Provider shall ensure that staff understand the Authority's vision and objectives and will provide excellent customer service to the Authority throughout the duration of the Contract.

16. SERVICE LEVELS AND PERFORMANCE

16.1 The Authority will measure the quality of the Supplier's delivery through assessment of their progress alongside the agreed milestones set out in paragraph 6.1.

KPI/SLA	Service Area	KPI/SLA description	Target
1	Progress Report	Progress reports will be supplied to the DfT project manager by phone or email (to be confirmed). This will include a summary of progress against the delivery.	Fortnightly
2	Risk monitoring	The Potential Provider will raise any concerns about the possibility of failing to meet the overall deadline and lack of relevant information to meet the requirements.	Within 1 working day

3	Communication	The Potential Provider shall acknowledge any communications from the contract/project manager within 2 working days via personal email.	2 working days
4	Emergencies	If there is an urgent issue, the Potential Provider shall make the contract manager aware of this within 2 working days.	2 working days

17. SECURITY REQUIREMENTS

17.1 The Provider must be able to handle and store classified material up to and including OFFICIAL SENSITIVE level. The project report will be classified at OFFICIAL SENSITIVE.

17.2 The Provider must be able to provide staff with appropriate clearance. As a minimum staff should have or be willing to apply for and obtain the Baseline Personnel Security Standard (BPSS) but National Security Vetting clearance (to Counter-Terrorist Check level) is preferable.

17.3 The Provider should demonstrate the measures in place to keep this information secure. Specifically, in the bid document the Provider should provide detail on how they will meet the following requirements:

- Information classified at OFFICIAL SENSITIVE level relating to this project should not be communicated electronically, except between the contractor and DfT (and other parties approved by DfT) and then only using the methods below.
- The supplier should ensure the security of the information in transit. Electronically this will involve using software (for example Egress Switch system) to encrypt the files, preferably using AES-256, or other measures that offer an equivalent level of protection.
- Any passwords used to encrypt files should be complex and should be conveyed separately to the files themselves.
- Any electronic files should be stored on an IT system that has access controls that only allow approved personnel with a genuine 'need to know' to access them to read and copy. The IT system should be protected by an appropriate firewall.
- Once electronic files are no longer needed they should be deleted from the IT system in a way that makes recovery unlikely, either by overwriting the storage space or eventual dilution and deterioration on a busy shared storage system.
- Paper copies (including drafts and notes) and any removable electronic storage must be locked away when not in use to prevent unauthorised access. Printed material should be marked OFFICIAL SENSITIVE and numbered to ensure no copies are lost. Paper and printed material should be shredded when no longer needed.
- If any paper copies are to be posted, advice should be sought from the Authority.
- Access to all material generated by this project (not included source data unless supplied by DfT) must be on a limited and controlled basis, by persons approved by the DfT.

17.4 Any personal information obtained under this contract must be controlled in compliance with the Data Protection Act.

17.5 Further information on security classification is available on the Cabinet Office website at the following addresses:

http://www.cabinetoffice.gov.uk/sites/default/files/resources/hmg-personnel-security-controls.pdf

https://www.gov.uk/government/publications/security-policy-framework

17.6 Due to the sensitivity of the work the successful supplier will be required to sign a non-disclosure agreement (NDA) prior to any work on the contract being started. This NDA will be provided as part of the ITT pack and signed as part of the contract award.

18. INTELLECTUAL PROPERTY RIGHTS (IPR)

18.1 All copyright, know-how and other property rights generated from this project remain the property of the Crown. The contractor shall ensure that all documentation and wherever possible all computer media are clearly marked accordingly.

19. PAYMENT

19.1 Prices should be submitted in pounds sterling and be inclusive of expenses and exclusive of VAT.

19.2 The Authority require invoices to be submitted within one month of the end of the project.

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

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

19.5 The Authority shall pay the supplier within Thirty (30) calendar days of receipt of a valid invoice, paid against a valid Purchase Order issued by the Authority; the method of payment will be by BACS.

19.6 Any anticipated travel and expenses incurred from engagement with stakeholders or the Authority must be included in the bid price.

20. LOCATION

20.1 The location of the Services will be carried out at the Potential Provider's premises. Any anticipated travel and expenses incurred from engagement with stakeholders or the Authority must be included in the bid price.