Intellectual Property Office

INVITATION TO QUOTE FOR THE PROVISION OF AN IT HEALTH CHECK OF REMOTE WORKING SOLUTION

IT-2015-080

Table of Contents

1. INTRODUCTION

1.1. Intellectual Property Office (IPO)

1.1.1. IPO (an operating name of the Patent Office) is an Executive Agency of the department of Business, Innovation and Skills (BIS). It aims to stimulate innovation and enhance the international competitiveness of British industry and commerce. It offers customers an accessible, high quality, value for money system both nationally and internationally, for granting intellectual property rights.

1.1.2. The IPO is a highly successful organisation which, over its 162 year history, has adapted its approach and services to meet changing demands. Its core business and products deliver high quality, cost effective Intellectual Property (IP) rights to customers and its success in these core areas is tied to a much wider range of activities, such as awareness-raising and enforcement. Its customers operate within both the UK and global economies. Further information about the IPO can be found on its website at: www.ipo.gov.uk

1.1.3. The number of people currently employed by the IPO is approximately 1000. It is based at three sites: Newport, South Wales; a front office at Abbey Orchard Street, London and a file repository at Nine Mile Point, Cwmfelinfach, South Wales. It is primarily located at the following site.

1.2. Concept House

1.2.1. The headquarters of the IPO is located at Concept House, Cardiff Road, Newport, South Wales, NP10 8QQ. The office is approximately 3 km south-west of the city centre.

2. OBJECTIVES OF THIS PROCUREMENT

2.1. Introduction

2.1.1. This document identifies the Target of Evaluation for an IT Health Check of the IPO Airwatch MDM and associated systems, in support of the IPO Accreditation of the Remote Working Solution.

2.1.2. The Remote Working Solution is currently at Beta phase with testing for DR due to complete by w/e 23rd October 2015, it is anticipate that this ITHC will be undertaken with effect from 12th November 2015.

2.2. Objective

2.2.1. To conduct detailed IT Health Checks (ITHC) of the Remote Working Solution which comprises of an Airwatch MDM, RSA and VPN infrastructure, its interfaces and Administration as hosted by IPO at Concept House, Newport within CESG Guidelines, using a CHECK Green Team. The Work is to be undertaken by a CHECK Team Leader, supported as necessary by CHECK Team Members.

2.2.2. The test will be ‘open’ in nature and the CHECK Team will be provided with all necessary information , system data and user accounts to enable them to conduct the tests in the most effective manner.

2.2.3. While there is no data held within the Remote Working Solution it holds a Security Classification of OFFICIAL as that is the highest rating that will traverse it.

3. SCOPE

3.1. Description

3.1.1. The ITHC is required as a check on the architecture and security controls implemented in the Remote Working Solution for the Intellectual Property Office. The tests must identify vulnerabilities in all layers of the system, from administrative accesses to configuration and integration layers and the underlying OS unless identified in the Out of Scope statement below.

3.1.2. The application and infrastructure is located in Concept House. The Airwatch, RSA and VPN infrastructure uses a number of virtual servers which are summarised below and described diagrammatically in Section 3.8.

3.2. Test Scope

3.2.1. The ITHC on the solution must test the following components: -

Description	Scope
Strength of existing controls – External Threat	Assess the Airwatch, RSA and VPN solutions for any vulnerabilities from an external i.e. Internet-based threat factor. Firewalls, Load Balancers, Airwatch and RSA servers are in scope as are SSL/TLS configurations and certificates.
Strength of existing controls - Internal Threat	Assess the Remote Working Solution for any vulnerabilities from an internal threat. Firewalls, Load Balancers, Airwatch and RSA servers are in scope as are SSL/TLS configurations and certificates.
End User Device configuration	Review of device configuration of the Peripatetic devices identified in End User Devices against the HMG EUD advice or industry best practice where EUD advice is non-existant. Included elements are AV installation, any HIDS configuration & user & system authentication. Certificates and encryption algorithms are in scope. Attempt to break into a device to gain access to user details and authentication data or sensitive data useful to a hacker. Attempt to spoof a known good device using a known backup as a source (e.g. a full iCloud backup).; not applicable to Wyse terminals or laptops. Review of device configurations against the Government EUD guidance and Vendor Leading

	Security Practice, including AV installation, any HIDS configuration & user & system authentication. Certificates and encryption algorithms are in scope.
Mobile Device Management Configurations	Review of the Management Console for configuration and installation vulnerabilities against Leading Security Practice as defined by the vendor, including network and authentication protocols, including user & system authentication. Out of scope are configurations appertaining to the Active Directory, MS Exchange and other Office services used independently of the Airwatch Solution, any Mobile GPOs or LDAP configurations are in scope.
Operating System Hardening and Build	Underlying OS of the AirWatch and RSA servers AntiVirus and AntiMalware configurations Vulnerability scan & patching status VM Tool Configurations
Protocol Analysis	Identify network vulnerabilities including protocols, ports, SNMP configurations.
Auditing	Completeness of audit logs.

3.3. Technical System Description

3.3.1. Airwatch MDM, RSA and VPN services make up the IPO's Remote Working Solution. This comprises of a number of virtual Microsoft Windows servers and appliances to provide connectivity to specific internal resources from externally managed devices. This infrastructure exists across two locations:

i. Concept House - Newport
ii. Companies House - Cardiff

3.3.2. Concept House hosts the live servers whereas Companies House hosts the equivalent set for High Availability only; load balancers exist to provide an active passive service only.

3.4. Airwatch MDM

Location	Server	Operating System	Purpose
Concept House	AWDSPR1	Microsoft Windows Server 2012 R2	Airwatch Device Services which handles enrollments, manages end user devices, deploys profiles, apps etc.

Concept House	AWEGPR1	Microsoft Windows Server 2012 R2	Airwatch Secure Email Gateway which allows end user devices to access the internal email servers via ActiveSync.
Concept House	AWMRPR1	Microsoft Windows Server 2012 R2	Airwatch Mobile Access Gateway Relay is the secure communications in the DMZ which handles secure communications from the end user device to the MAG to allow access to internal resources as described below.
Concept House	AWMEPR1	Microsoft Windows Server 2012 R2	Airatch Mobile Access Gateway which provides the means for end user devices to access internal resources such as fileshares or web servers.
Concept House	AWCPR1	Microsoft Windows Server 2012 R2	Airwatch Console which provides the management interface to the Airwatch solution for internal administrators only.
Concept House	AWPRLB1	Loadbalancer Ent. VA V7.6.2	This together with AWPRLB2 forms the load balance cluster for the Device Services, Secure Email Gateway and Mobile Access Gateway Relay services in the DMZ.
Concept House	AWPRLB3	Loadbalancer Ent. VA V7.6.2	This together with AWPRLB4 forms the load balance cluster for the Mobile Access Gateway and Console servers.
Companies House	AWDSPR2	Microsoft Windows Server 2012 R2	Airwatch Device Services which handles enrollments, manages end user devices, deploys profiles, apps etc.
Companies House	AWEGPR2	Microsoft Windows Server 2012 R2	Airwatch Secure Email Gateway which allows end user devices to access the internal email servers via ActiveSync.
Companies House	AWMRPR2	Microsoft Windows Server 2012 R2	Airwatch Mobile Access Gateway Relay is the secure communications in the DMZ which handles secure communications from the end user device to the MAG to allow access to internal resources as described below.
Companies House	AWMEPR2	Microsoft Windows Server 2012 R2	Airatch Mobile Access Gateway which provides the means for end user devices to access internal resources such as fileshares or web servers.

Companies House	AWCPR2	Microsoft Windows Server 2012 R2	Airwatch Console which provides the management interface to the Airwatch solution for internal administrators only.
Companies House	AWPRLB2	Loadbalancer Ent. VA V7.6.2	This together with AWPRLB1 forms the load balance cluster for the Device Services, Secure Email Gateway and Mobile Access Gateway Relay services in the DMZ.
Companies House	AWPRLB4	Loadbalancer Ent. VA V7.6.2	This together with AWPRLB3 forms the load balance cluster for the Mobile Access Gateway and Console servers.

3.5. RSA

Location	Server	Operating System	Purpose
Concept House	BRAINS	RSA Authentication Manager 8.1	Primary Authentication Mananger
Companies House	TINTIN	RSA Authentication Manager 8.1	Secondary Authentication Manager

3.6. VPN

Location	Server	Operating System	Purpose
Concept House	CiscoASA	ASA 9.1 (6) ASDM 7.4 (2)	Provide access to internal resources for certain authenticated IPO End User Devices via VPN.

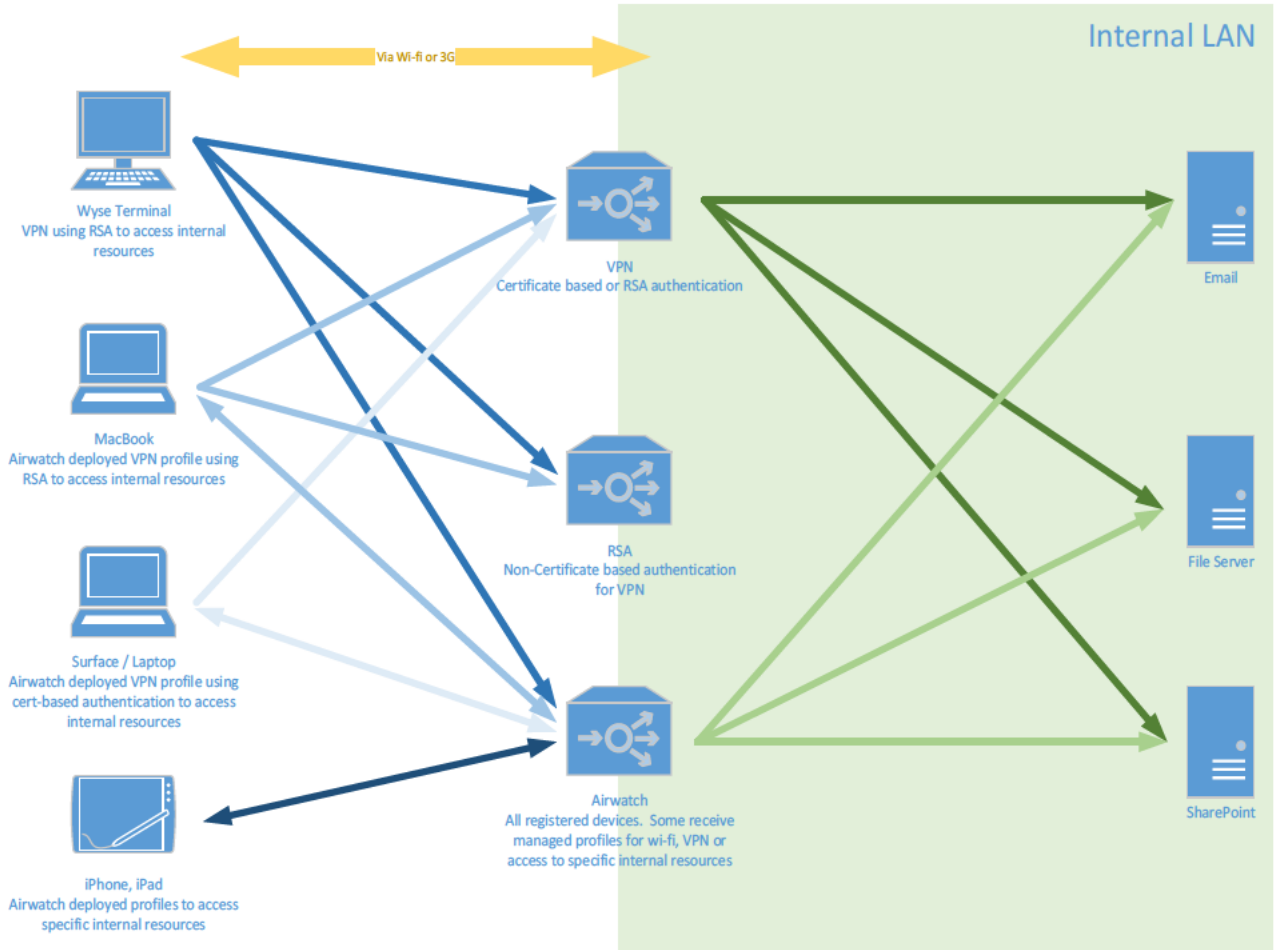
3.7. End User Devices

Location	Device	Operating System	Purpose
Peripatetic	iPhone	iOS 8+	IPO managed device via Airwatch to gain authorised access to restricted internal services such as email, SharePoint or network shares.
Peripatetic	iPad	iOS 8+	IPO managed device via Airwatch to gain authorised access to restricted internal services such as email,

			SharePoint or network shares.
Peripatetic	Surface Tablet	Microsoft Windows 8+	IPO managed device which has authorised access to internal network via RSA and VPN.
Peripatetic	Laptop	Microsoft Windows 7+	IPO managed device which has authorised access to internal network via RSA and VPN.
Peripatetic	MacBook	OS X	IPO managed device which has authorised access to internal network via RSA and VPN.
Homeworker	Wyse Terminal	Microsoft Windows 7 Embedded	IPO managed device which has authorised access to internal network via RSA and VPN.

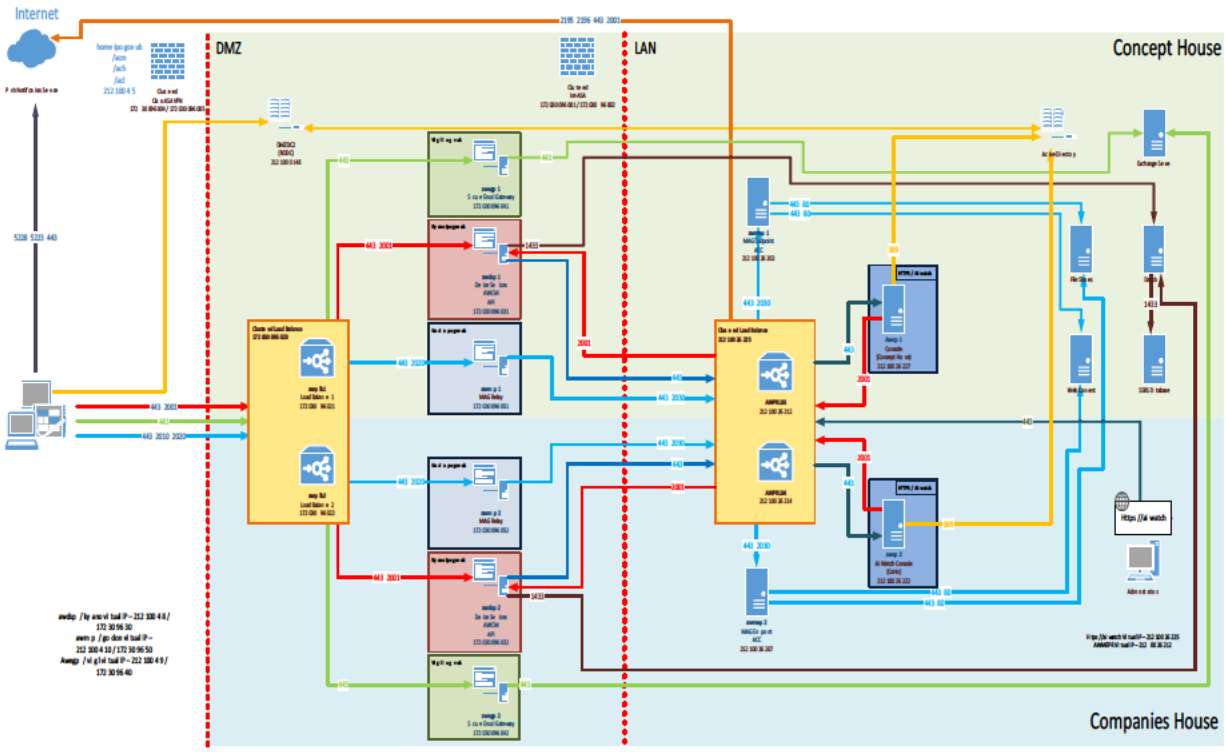
3.8. Functional Diagrams

3.8.1. Logical View

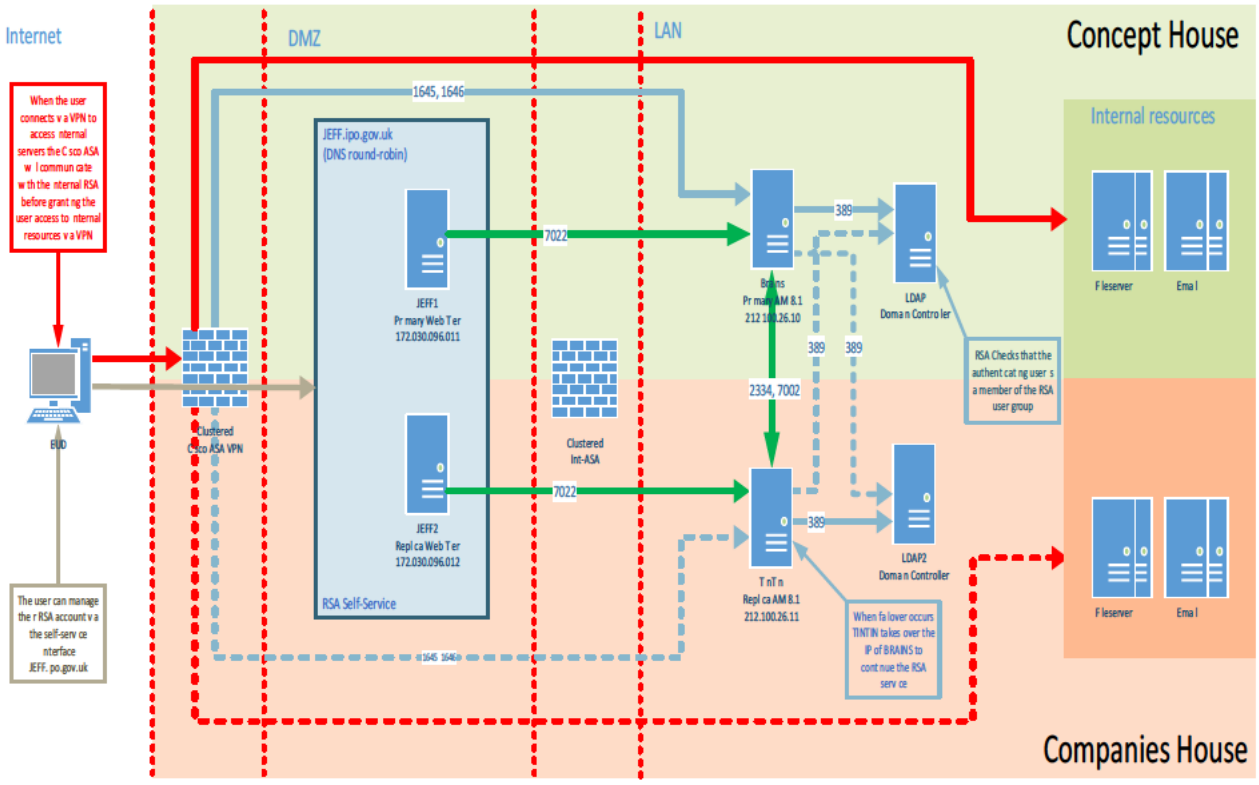


3.9. Infrastructure View (Servers/Networks)

3.9.1. Airwatch



3.9.2. RSA



3.10. Dates of Tests

3.10.1. The tests shall be conducted at Concept House, the window of opportunity being 5 days between 12th November and 18th November, with the final report delivered within five working days after tests are completed (no later than 25th November 2015), unless otherwise agreed as part of the tender process.

3.10.2. The supplier must indicate the availability of resources and any difficulties with meeting our requirements as part of the tender response.

3.11. CHECK Supplier Requirements

3.11.1. The CHECK supplier is expected to:

i. Provide a Risk Assessment detailing the anticipated risk of the planned tests against the availability or performance of any live infrastructure and applications to the IPO ITSO and Accreditor.

ii. During the Scoping Meeting identify CHECK Team requirements/pre-requisites, including but not limited to:-

- Authority for CHECK ITHC.
- Authority for use of CHECK ITHC team laptops.
- IP address requirements for CHECK Team.
- Identification of potential effects of testing on system/application under test, i.e. affect of ITHC activities on system logs, alert mechanisms and possibly firewalls. ANY testing that will result in a loss of service must be flagged to the IP team before that testing is undertaken.
- Confirmation of the address of the test location, along with contact details for the on-site technical contact (who should be available throughout the test period).
- Current versions of all relevant documentation including network diagrams.
- Confirmation of the provision of IP addresses of the devices to be tested.
- Details of the type of Ethernet connectivity within the network (e.g. 100 Base-T).
- Details of any intrusion detection or reaction systems that may affect testing.
- If required, access to or privileged (root or administrator) login accounts for each of the servers for which on-host audits are to be conducted.

iii. Plan for, and execute the CHECK IT Health Check (working with IPO staff and suppliers).

iv. Provide a Scoping document/TOR for the tests planned for this ITHC to the IPO ITSO and Accreditor, including tools to be used.

v. Actively lead the CHECK IT Health Checks, and manage CHECK team members.

vi. During CHECK IT Health Checks bring to the immediate attention of IPO Security and IT staff any identified critical or high impact vulnerabilities that present a risk to the system under test or other IPO connected systems.

vii. Where a Critical or High impact vulnerability identified during the ITHC is resolved while the ITHC team are still on site, the CHECK team will endeavour to confirm the vulnerability has been resolved, if time allows.

viii. During CHECK IT Health Checks attend daily 'wash up' meeting with IT and Security Staff and provide an update on CHECK team activities and findings (identified vulnerabilities with an initial severity rating) in the form of a text file containing issue titles, a low / medium / high risk rating and the hosts affected.

ix. At the end of CHECK IT Health Checks, submit an informal report to IPO staff that identifies the findings (vulnerabilities) of the CHECK team during the health check before leaving site.

x. Formally report on vulnerabilities (and recommended associated remedial solutions) identified during such CHECK IT Health Checks in line with CESG CHECK reporting guidelines.

xi. Provide informal technical Information Assurance advice to IPO in respect of the system under test.

3.12. IPO Responsibilities

i. IPO are responsible for providing access and support for the ITHC, including but not limited to:-

- Contractual issues relating to the conduct of the CHECK ITHC.
- Providing written permission for CHECK ITHC organisation to undertake the ITHC, following the provision of a risk assessment from the CHECK team.

- Attendance at all 'wash up' meetings for the ITHC.
- Completion of IS Audit Checklist of Conformance.
- Allowing access for the ITHC team members to the systems/applications under test.
- Providing IP addresses/URLs for devices/applications in scope for the ITHC.
- Provide mobile devices, configured with AirWatch.
- Providing IP and hostname details of devices excluded from this test.
- Providing guidance to CHECK ITHC organisation on the obfuscation of IP addresses (First two octets to be replaced with "A.B.".
- Provision of requested diagrams and documentation.
- Provision of requested and authorised access to user credentials/system access.
- Provision of a resource to manage support for the checks of the user credentials.
- Providing chaperones for ITHC.
- If required, provision of business focussed explanation and possibly training of how users and administrators would use the application.
- Provision of typical user accounts to the CHECK ITHC team.
- Technical support to the ITHC team during the on-site testing period at Concept House.

3.13. Restrictions

i. Details of the results of tests conducted during this Penetration Test must not be transmitted across the Internet unless suitable approved encryption is used.

ii. All IP addresses noted in the report should be obfuscated in line with guidance provided by the IPO ITSO. However, where screen shots are taken to support the explanation of vulnerability there is no need to obfuscate any IP address within the screen shot.

iii. The Penetration Test specifically excludes:-

- Any activity on the PSN.
- Activity relating to other services hosted at Concept House.

- Active Directory configurations that are not part of the AirWatch Solution
- The conducting of any tests (Denial of Service, brute forcing passwords, etc) with a high probability of impacting on the live operation of other services hosted at Concept House.

iv. This ITHC is restricted to the devices identified in this specification. Other servers and switches are specifically out of scope.

3.14. Reporting

i. The proposal is to be presented in both electronic and hard copy formats. It should be presented to the Accreditor at the address given under **Error! Reference source not found.** below.

ii. The CHECK IT Security Health Check report is to be protectively marked to the same level as given for the test, under **Error! Reference source not found. Error! Bookmark not defined.**.

iii. Reports on the findings of the CHECK IT Security Health Check will be provided to IPO Accreditor, IPO ITSO, IPO Head of Network Services and to the CHECK administrator at CESG.

iv. Three bound copies and an electronic copy (on CD) of the final report should be submitted to IPO by post, within ten working days of testing being completed. In addition to the main report the ITHC provider is required to supply an extract of identified vulnerabilities in Microsoft Excel for inclusion in our Defect Management system. This extract to include detail on:-

- Task Reference
- Issue Number
- Affected Host(s)
- Severity
- Impact
- Threat
- Summary of Finding, including evidence where applicable
- Recommendation

3.15. Contacts

Activity	Title	Contact Details
Invitation to Tender & Procurement	Procurement Manager	[redacted], Room GY33, Concept House, Cardiff Road, Newport, NP10 8QQ [redacted] [redacted]
Delivery of the report	Accreditor	[redacted] Room 2Y05, Concept House, Cardiff Road, Newport, NP10 8QQ [redacted] [redacted]
Security Team Contact	IT Security Officer	[redacted] Cox, Room 2Y05, Concept House, Cardiff Road, Newport, NP10 8QQ [redacted] [redacted]
Infrastructure Team Contact	Infrastructure Technical Lead	[redacted] Room 2R33, Concept House, Cardiff Road, Newport, NP10 8QQ [redacted] [redacted]

4. GENERAL REQUIREMENTS

4.1. Information Required

4.1.1. As part of their proposals suppliers must include the following information:

i. The proposed approach and methodology that will be used to meet the requirements detailed in Section 3 above. Please note paragraph 4.2 below, when preparing this approach and methodology.

ii. Full details of the actual personnel, distinguishing between Staff and Consultants, who will deliver the ITHC to the IPO. This must include summaries of the proposed personnel's relevant skills and qualifications. When proposing staff for this requirement please pay particular attention to Section 2.2.

4.1.2. If you believe any further information would be relevant, this also may be included.

4.1.3. The personnel proposed by the Supplier to deliver the ITHC's to the IPO must not be changed without the prior written approval of the IPO. In the event that changes to personnel are unavoidable the replacements proposed to the IPO must be of equal or greater experience. Any replacement personnel used on the ITHC must be approved by the IPO. Suppliers must confirm their acceptance of this.

4.2. Bid Preparation

4.2.1. Given the short timescales allowed for response to this ITQ and the relatively straightforward nature of the requirements, Suppliers should note that the IPO are not expecting excessively large proposals in response to this ITQ.

5. CHARGES

5.1. Purpose

5.1.1. The purpose of this Section is to define the information that Suppliers must supply in respect of their proposed charges.

5.2. Composition

5.2.1. Charges must be detailed for the requirement specified in Section 3 above.

5.2.2. These charges must be provided as follows:

i. Daily rates in respect of every grade of personnel you foresee would be involved in the provision of the ITHC;

ii. The number of days required detailed by each individual grade to complete the requirements detailed in Section 3 above;

iii. Any other costs you foresee arising;

iv. An overall fixed price cost for testing and reporting.

5.3. Instructions

5.3.1. Expenses, if any, should be detailed at IPO standard rates, shown in section 5.4.

5.3.2. To avoid doubt, all costs not listed within your bid will be deemed to have been waived.

5.3.3. Any improvements you propose that are additional to our stated requirements, and any additional service options being offered, must be separately costed if applicable.

5.3.4. You must confirm that all charges submitted are exclusive of VAT.

5.3.5. You must confirm that all charges submitted will be held firm for a period of 30 days commencing from the quote return date.

5.4. Expenses

5.4.1. SUPPLIERS must detail what travel and accommodation expenses you would apply to a contract (if any).

5.4.2. For the avoidance of doubt, any expenses paid under the contract must only be reasonably and necessarily incurred as a result of carrying out the contracted services, with due regard to economy. They will only be

paid on proof of occurrence and will be paid at the IPO's standard rates which are as follows:-

i. Overnight accommodation: London – maximum £145.00 (inc. VAT) per night, B&B. Elsewhere maximum £110.00 (incl. VAT) per night B&B;

ii. Car mileage rates at 0.45p per mile. This is for round trips of up to 150 miles. Journeys in excess of that must be undertaken by public transport;

iii. Rail fare at standard (or advanced or off-peak) fares;

iv. Flights at economy class;

v. Taxi fares will only be reimbursed where public transport or use of a private car is unsuitable or inappropriate;

vi. Parking fees / and toll charges, necessarily incurred may be claimed where supported by a valid receipt;

vii. No other form of expenses will be payable by the IPO.

6. TERMS AND CONDITIONS

6.1. Contractual Approach

6.1.1. Any contract subsequently awarded will operate in accordance with IPO's standard terms and conditions of contract for services contained below:


BIS Standard Terms and Conditions of Cor

6.1.2. No other Terms and Conditions will apply. Suppliers must confirm their acceptance of this.

6.2. Intellectual Property Rights

6.2.1. As per clause 27 of the above Terms and Conditions, and subject to any pre-existing rights of third parties and of the Tenderer, the Intellectual Property Rights (other than copyright) in all reports, documents and other materials which are generated or acquired by the Tenderer (or any of its sub-contractors or agents) in the performance of the Services shall belong to and be vested automatically in the IPO.

6.2.2. Tenderers must confirm their acceptance of the above as part of their proposal.

7. ACHIEVING TRANSPARENCY OF PUBLIC SECTOR PROCUREMENT

7.1. Requirement to Publish Contractual Information

7.1.1. Government has set out the need for greater transparency across its operations to enable the public to hold public bodies and politicians to account. This includes commitments relating to public expenditure, intended to help achieve better value for money.

7.1.2. As part of the transparency agenda, Government has made the following commitments with regard to procurement and contracting:

i. All new central government ICT contracts over the value of £10,000 to be published in full online from July 2010;

ii. All new central government tender documents for contracts over £10,000 to be published on a single website from September 2010, with this information to be made available to the public free of charge;

iii. New items of central government spending over £25,000 to published online from November 2010;

iv. All new central government contracts to be published in full from January 2011.

7.1.3. Suppliers and those organisations looking to bid for public sector contracts should be aware that if they are awarded a new government contract, the resulting contract between the supplier and government will be published. In some circumstances, limited redactions will be made to some contracts before they are published in order to comply with existing law and for the protection of national security.

7.1.4. With the above in mind Tenderers must confirm that, except for any information which is exempt from disclosure in accordance with the provisions of the FOIA, the content of any subsequent Contract is not Confidential Information.

7.1.5. The IPO shall be responsible for determining in its absolute discretion whether any of the content of the Contract is exempt from disclosure in accordance with the provisions of the FOIA. Notwithstanding any other term of the Contract, the Tenderer hereby gives consent for the IPO to publish the Contract in its entirety, (but with any information which is exempt from disclosure in accordance with the provisions of the FOIA redacted) including from time to time agreed changes to the contract, to the general public.

7.1.6. The IPO may consult with the successful Tenderer to inform its decision regarding any exemptions but the IPO shall have the final decision in its absolute discretion.

7.1.7. The successful Tenderer shall assist and cooperate with the IPO to enable the IPO to publish this Agreement.

7.1.8. Tenderers must confirm their acceptance of the above or their bid may not be considered further.