



Intellectual
Property
Office

INVITATION TO QUOTE
FOR THE PROVISION OF AN
IT HEALTH CHECK OF IPO NETWORK

IT-2016-101

Table of Contents

1. INTRODUCTION	4
1.1. Intellectual Property Office (IPO).....	4
1.2. Concept House	4
2. INSTRUCTIONS ON BIDDING PROCEDURES	5
2.1. Instructions.....	5
2.2. Procurement Information.....	5
2.3. Deadline for receipt of bids.....	5
2.4. Incomplete bid.....	5
2.5. Acceptance of bid.....	5
2.6. Communications	5
3. OBJECTIVES OF THIS PROCUREMENT	6
3.1. Introduction	6
3.2. Objectives	6
4. SCOPE	7
4.1. Tests	7
4.2. External testing	7
4.3. Internal testing.....	7
4.4. System Description	8
4.5. PSN Connectivity	9
4.6. Desktop build	9
4.7. Remote access	9
4.8. IPO Business Infrastructure	9
4.9. System Diagram.....	10
4.10. Dates of Tests.....	11
4.11. Check Supplier Requirements	11
4.12. IPO Responsibilities.....	12
4.13. Restrictions	13
4.14. Reporting	14
4.15. Contacts.....	14
5. GENERAL REQUIREMENTS.....	15
5.1. Information Required.....	15
5.2. Bid Preparation	15

Invitation to Quote for the provision of an IT Health Check
OFFICIAL: SENSITIVE

6. CHARGES	16
6.1. Purpose.....	16
6.2. Composition	16
6.3. Instructions.....	16
6.4. Expenses	16
7. RESPONSE TO THE INVITATION TO QUOTE	18
7.1. Function and Format of Proposals	18
7.2. Structure Of Proposals.....	18
7.3. Procurement Timetable	18
8. TERMS AND CONDITIONS	19
8.1. Contractual Approach	19
8.2. Intellectual Property Rights	19
9. ACHIEVING TRANSPARENCY OF PUBLIC SECTOR PROCUREMENT	20
9.1. Requirement to Publish Contractual Information.....	20

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 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.

3. OBJECTIVES OF THIS PROCUREMENT

3.1. Introduction

3.1.1. The following specification has been developed to support the scoping for CHECK IT Health Checks of the IPO Network infrastructure & applications and is in support of IPO Network accreditation.

3.2. Objectives

3.2.1. To conduct a detailed IT Health Check (ITHC) of the IPO Network infrastructure and associated infrastructure that connects to the PSN as hosted by IPO at Concept House, Newport and Companies House, Cardiff within CESG Guidelines, using a CHECK Green Light Team. The work is to be undertaken by a CHECK Team Leader, supported as necessary by CHECK Team Members and it is intended to give disclosure to enable the team to do their work in the most effective manner.

3.2.2. The assessment will focus on the following testing:

- i. IT Health Check - White Box test on infrastructure components where full disclosure will be allowed to enable the team to do their work in the most effective manner. For this part of the assessment the Check Team will be allowed access to site to perform a full IT Health Check of:
 - The remote access components
 - The mail gateway control components
 - Proxy internet access
 - The IPO Network that provides access to PSN
- ii. Firewall rules review;
- iii. VLAN configuration;
- iv. Mobile device configuration review; and
- v. Desktop build setup and configuration review.

3.2.3. The tests will be focused on demonstrating that IPO has sufficient controls in place and doesn't provide any unauthorised entry points to the IPO networks and onward to the PSN.

3.2.4. The data processed and stored on IPO Network holds a maximum protective marking of Official - Sensitive.

4. SCOPE

4.1. Tests

- 4.1.1. The ITHC team will have access to network diagrams, IP address ranges and VLANs to be tested.
- 4.1.2. The ITHC is required as a check on the design, build and management of the IPO Network infrastructure providing secure email via the PSN and includes external access points. The tests must identify vulnerabilities in all layers of the system, from application, to integration layers and the underlying OS and hardware as necessary.
- 4.1.3. An assessment must be based on current best practices, and designed by the CHECK Team based on current knowledge of the technologies under test. In any case, the test must include at least the following checks:

4.2. External testing

- i. Open Ports and Services.
- ii. Web services exposure.
- iii. Application services exposure.
- iv. File Transfer services.
- v. Script injection.
- vi. Exposure to the Internet and robustness of protective controls between the internal environment and the external DMZs.
- vii. Vulnerability scanning.
- viii. Mobile Worker Access.

4.3. Internal testing

- i. Internal Network Vulnerability scan.
- ii. Firewall rule base review.
- iii. VLAN bridging:
 - Review of DMZ architecture and vulnerability to DMZ 'hopping'.
 - VSS configuration on the corporate LAN.
- iv. Virtualisation review (ESX) of the host in:
 - Corporate network Hosts (excluding the IPO business infrastructure as indicated the diagram in 4.9 below).
 - DMZ Hosts.

- Vsphere configuration.
- v. Server Build:
 - Windows.
 - LINUX.
- vi. Database secure configuration of SQL servers supporting DMZ applications:
 - SQL.
- vii. Web Server secure Configuration:
 - IIS.
 - Apache.
 - Tomcat.
- viii. Audit and Logging – review of configuration.
- ix. Unauthorised access to, or manipulation of, system or application administration utilities.

4.4. System Description

4.4.1. IPO Boundary DMZ

- i. The IPO have a number of internal and externally facing web facing services, including:
 - Web forms linked, internal applications and databases to blogging (e.g. WordPress) and information services;
 - Web browsing for internal users; and
 - Remote access.
- ii. These services are presented via IPO's external DMZ, with further architectural (layer 3) separation provided by subsequent layers within the DMZ. All external web services utilise reverse proxies and utilise services provided by the front node firewall.
- iii. Web browsing by internal users is controlled by group policy applying proxy pac files for user group access.
- iv. Remote access is via the following:
 - Laptop access via an X-Kryptor; and
 - Cisco ASA appliance for iPhone and iPad.
- v. Remote access devices are then provided access to the corporate network via VRF to dedicated internal VLANs.
- vi. All @ipo.gov.uk email transits inbound and out bound through the DMZ via the internet, and is transferred via the MailGate,

which provides the content scanning on the IPO network and a mail forwarding component MailEdge in the DMZ.

- vii. The full range of all IPO's internal and external IP addresses, URLs and protocols will be made available prior to commencement of testing. All VLAN details and number and type of server will also be made available prior to testing.

4.5. PSN Connectivity

4.5.1. The connection to the PSN is routed via a VLAN off the front node Checkpoint Firewall and is used for the following services:

- i. All @ipo.gsi.gov.uk email transits inbound and out bound through the PSN, and is transferred via the MailGate which consists of a content scanning component on the IPO network and a mail forwarding component MailEgde on the PSN LAN, DNS for the PSN is also provided on this server.
- ii. Access to specific web sites hosted on the PSN are controlled via proxy settings within the browser (proxy pac file) and the external PSN Proxy.

4.5.2. Protocols will be HTTP(S) and SMTP with defined endpoints such as the PSN mail gateway and the external proxies.

4.6. Desktop build

4.6.1. The IPO run windows 7 throughout their estate on a combination of physical desktops and VMs through Wyse terminals, these access the Internet and the PSN for services such as email and web access as described above. Web access is via IPOs internet proxies and it is intended to demonstrate that these devices are not vulnerable to attack and do not present threat to the internal IPO network or the PSN.

4.7. Remote access

4.7.1. The IPO run a number of remote access devices including Windows 7 laptops, iPhones and iPads, as with the desktop estate, mobile access use the same email and web browsing services through the external web access through the IPO internet and PSN proxies, it is intended to demonstrate that these devices do not pose a higher threat to the IPO or PSN.

4.8. IPO Business Infrastructure

4.8.1. The IPO infrastructure supporting the business operation of IPO is out of scope of this ITHC and is physically isolated by a combination of the IPOs internal Cisco ASA firewall and the VSS Switch.

4.10. Dates of Tests

- 4.10.1. The tests shall be conducted at Concept House and the reports delivered up to ten working days after tests are completed. If the supplier believes any of the testing (in particular the external testing) needs to happen from the suppliers site then a description of how this is secure to do so should be included.
- 4.10.2. The target start date is week commencing 3rd October 2016.
- 4.10.3. The supplier must indicate the availability of resources that meet our requirements as part of the tender response.

4.11. Check Supplier Requirements

- 4.11.1. The CHECK supplier is expected to:
- i. During the Scoping Meeting identify CHECK Team requirements / pre-requisites, including but not limited to:
 - Authority for Penetration Test and CHECK ITHC.
 - Authority for use of Penetration Test and CHECK ITHC team laptops.
 - IP address and URL requirements for CHECK Team.
 - Identification of potential effects of testing on system / application under test, i.e. effect of Penetration Test and ITHC activities on system logs, alert mechanisms and possibly firewalls.
 - 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.
 - ii. Plan for, and execute the Penetration Test and CHECK IT Health Check (working with IPO staff and suppliers).

Invitation to Quote for the provision of an IT Health Check
OFFICIAL: SENSITIVE

- iii. Provide a Scoping document / TOR for the tests planned for this Penetration Test and ITHC to the IPO DSO / ITSO and Accreditor.
- iv. 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 DSO / ITSO and Accreditor.
- v. Actively lead the Penetration Test and CHECK IT Health Check, 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.

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

4.12. IPO Responsibilities

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

- i. Contractual issues relating to the conduct of the CHECK ITHC.
- ii. Providing written permission for CHECK ITHC organisation to undertake the ITHC, following the provision of a risk assessment from the CHECK team.
- iii. Attendance at all 'wash up' meetings for the ITHC.
- iv. Completion of IS Audit Checklist of Conformance.

Invitation to Quote for the provision of an IT Health Check
OFFICIAL: SENSITIVE

- v. Allowing access for the ITHC team members to the systems / applications under test.
- vi. Providing IP addresses / URLs for devices / applications in scope for the ITHC.
- vii. Providing IP and hostname details of devices excluded from this test.
- viii. Providing guidance to CHECK ITHC organisation on the obfuscation of IP addresses (First two octets to be replaced with "A.B.").
- ix. Provision of requested diagrams and documentation.
- x. Provision of requested and authorised access to user credentials / system access.
- xi. Provision of a resource to manage support for the checks of the user credentials.
- xii. Providing chaperones for ITHC.
- xiii. If required, provision of business focussed explanation and possibly training of how users and administrators would use the application.
- xiv. Provision of typical user accounts to the CHECK ITHC team.
- xv. Technical support to the ITHC team during the on-site testing period at Concept House.

4.12.2. The IPO accreditor will be assigned to the CHECK team for the duration of the Penetration Test to mediate.

4.13. Restrictions

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

4.13.2. All IP addresses noted in the report should be obfuscated in line with guidance provided by the IPO DSO / ITSO.

4.13.3. The Penetration Test specifically excludes:

- i. Activity relating to other services hosted at Concept House.
- ii. The conducting of any tests (Denial of Service, etc) with a high probability of impacting on the live operation of other services hosted at Concept House (unless expressly permitted by the IPO Head of Security / Accreditor).

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

4.14. Reporting

- 4.14.1. The proposal is to be presented in both electronic and hard copy formats. It should be presented to the DSO at the address given under section 9.
- 4.14.2. The CHECK Penetration Test and IT Health Check report is to be protectively marked as Official – Sensitive.
- 4.14.3. Reports on the findings of the CHECK IT Security Health Check will be provided to the project staff and any affected suppliers (if applicable), the IPO DSO, IPO Accreditor, IPO ITSO, IPO Head of Network Services and to the CHECK administrator at CESG.

4.15. Contacts

Activity	Title	Contact Details
Invitation to Tender & Procurement	Procurement Manager	██████████ Room GY33, Concept House, Newport, NP10 8QQ ██ 01633 81██████████
Delivery of the report	DSO / IT Security Officer	██████████ Room 2Y05, Concept House, Newport NP10 8QQ ██ 01633 81██████████
Security Team Contact	Security Architect	██████████ Room 2Y05, Concept House, Newport NP10 8QQ ██ 01633 81██████████
Security / Accreditor	Head of IPO Security / Accreditor	██████████ Room 2Y05, Concept House, Newport NP10 8QQ ██ 01633 81██████████

5. GENERAL REQUIREMENTS

5.1. Information Required

5.1.1. 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 4 above. Please note paragraph 5.2 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 3.2.

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

5.1.3. 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.

5.2. Bid Preparation

5.2.1. 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.

6. CHARGES

6.1. Purpose

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

6.2. Composition

6.2.1. Charges must be detailed for the requirement specified in Section 4 above.

6.2.2. 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 4 above;
- iii. Any other costs you foresee arising;
- iv. An overall fixed price cost for testing and reporting.

6.3. Instructions

6.3.1. Expenses, if any, should be detailed at IPO standard rates, shown in Section 6.4.

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

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

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

6.3.5. You must confirm that all charges submitted will be held firm for a period of 30 days commencing from the quote return date (23rd September 2016).

6.4. Expenses

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

6.4.2. 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

Invitation to Quote for the provision of an IT Health Check
OFFICIAL: SENSITIVE

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

- i. Overnight accommodation: London – maximum £150.00 (inc. VAT) per night, B&B. Elsewhere maximum £85.00 (inc. 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 / 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.

7. RESPONSE TO THE INVITATION TO QUOTE

7.1. Function and Format of Proposals

7.1.1. You must e-mail an electronic version of your quote (in Microsoft Word XP or .pdf format) to [REDACTED] by 1:00pm, Friday 23rd September 2016.

7.2. Structure Of Proposals

7.2.1. SUPPLIERS must structure their proposal as follows:

- i. Part 1: Management Summary – Provide a resume of the proposal.
- ii. Part 2: Understanding of Requirements – Confirm your understanding of the key requirements and scope of the services to be provided to IPO.
- iii. Part 3: Requirements – This section must address the requirements of the ITQ, including a clear and comprehensive methodology, project timescales and how your particular expertise matches IPO's requirements (excluding Charges).
- iv. Part 4: Charges - It is imperative that the IPO is able to form a clear view of the charges in your proposal for the provision of the services. Therefore all charges must be included or summarised in this section of your response. These charges must be provided in accordance with Section 4.
- v. Part 5: Any other information - that you wish to add further to that already requested, that you feel may further demonstrate your ability.

7.3. Procurement Timetable

ACTION	DATE
Issue of this Invitation to Quote	Wednesday 14 th September 2016
Deadline for return of incoming quote	1:00pm, Friday 23 rd September 2016
Contract award	Week commencing 26 th September 2016
Contract Commencement	Week commencing 3 rd October 2016

8. TERMS AND CONDITIONS

8.1. Contractual Approach

8.1.1. 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

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

8.2. Intellectual Property Rights

8.2.1. 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.

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

9. ACHIEVING TRANSPARENCY OF PUBLIC SECTOR PROCUREMENT

9.1. Requirement to Publish Contractual Information

- 9.1.1. 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.
- 9.1.2. 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 be published online from November 2010;
 - iv. All new central government contracts to be published in full from January 2011.
- 9.1.3. 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.
- 9.1.4. 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.
- 9.1.5. 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.
- 9.1.6. 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.

Invitation to Quote for the provision of an IT Health Check
OFFICIAL: SENSITIVE

- 9.1.7. The successful Tenderer shall assist and cooperate with the IPO to enable the IPO to publish this Agreement.
- 9.1.8. Tenderers must confirm their acceptance of the above or their bid may not be considered further.