****

**IT HEALTH CHECK**

**CLOSING DATE FOR RESPONSES – 5PM, Monday 2nd December 2019**

1. **OBJECTIVE**

The National Archives’ IT Operations Department requires an IT Health Check (ITHC) to be carried out on its IT infrastructure located at its main office at Kew, Richmond, TW9 4DU.
Testing is carried out at least annually, to meet our obligations for ISO 27001 compliance and contribute to the overall information security posture of The National Archives.

In this tender, IT Operations is seeking a supplier for ITHC, CHECK testing and other security audit activities to The National Archives for two years, with the option of a one-year extension (2+1). Security audit activities may optionally include ISO 27001 internal audit, ISO 27005 risk assessment, and Cyber Essentials auditing.

IT Operations will not be obliged to take up services in subsequent years.

1. **BACKGROUND**

The National Archives (TNA) is the official archive and publisher for the UK government, and for England and Wales. Its role is to collect and secure the future of the government record, both digital and physical, to preserve it for generations to come, and to make it as accessible and available as possible. It is based in Kew, South West London. More information on TNA can be found at [www.nationalarchives.gov.uk](http://www.nationalarchives.gov.uk)

1. **THE REQUIREMENT**
	1. The requirement is for an IT Health Check (ITHC) to meet our obligations for ISO 27001 compliance and contribute to the overall information security posture of The National Archives.
	2. A rate card will be expected for future testing by CHECK certified individuals, as given in Appendix A. Optionally, a rate card for ISO 27001 internal audit, ISO 27005 risk assessment and Cyber Essentials audit work may be provided in the proposal.
	3. ITHC testing must be carried out by one or more CHECK certified individuals who hold at least security check (SC) clearance, from a Supplier who has CHECK “Green Light” status and who follows the CHECK Service Provision Guidelines.
	4. The required outcomes of the ITHC must be:
		1. An **on-site workshop** between the Supplier and IT Operations teams, to discuss the findings of the test and suggestions on how to resolve those findings.
			1. A final **report** covering all aspects and findings of the ITHC. This report should include a mapping of hostnames to IP addresses as observed at the time of testing, and be accompanied by a spreadsheet (CSV or Excel) of report findings, for example in the style of HMG’s Remediation Action Plan (RAP) template: <https://www.gov.uk/government/publications/remediation-action-plan-rap-example-template>
		2. **Secure deletion** of all storage media used during the ITHC.
2. **SCOPE**
	1. Where Azure, Office 365 or other Microsoft Cloud components are mentioned below, any testing activities must follow the Microsoft Cloud Rules of Engagement:
	https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement
	2. Where Amazon Web Services (AWS) is mentioned below, any testing activities must follow AWS’s policy regarding security assessments:
	https://aws.amazon.com/security/penetration-testing/
	3. The scope of the ITHC will be the following tasks:
		1. An internal infrastructure vulnerability assessment of our IT systems:
	* The network devices in scope are assigned RFC 1918 (private) IP addresses within four /16, one /18, two /20, four /21, one /22, one /23, eleven /24, one /27 and one /29 IP subnets.
	* Of these, one /24 subnet is hosted in Azure, and one /18, one /20 and one /24 subnet are hosted in AWS.
	* The ranges above are sparse and host discovery should be carried out first. This assessment will include approximately 300 virtual servers, 100 physical servers and up to 1000 workstations running variants of Windows, Linux and Chrome OS.
		1. An external penetration test of our Internet-facing IT systems, conducted from off-site using known IP addresses:
	* On-site: One /25 and one /29 IP ranges, and six other IP addresses, with no more than ten individual web servers;
	* Azure: Three IP addresses.
		1. Web applications testing, against versions of our public-facing web services:
		+ Three WordPress sites, including our main website ([www.nationalarchives.gov.uk](http://www.nationalarchives.gov.uk)). Two of these sites are hosted on AWS.
		+ Two bespoke web applications.
		1. A review of perimeter and internal firewall configuration and policies:
	* Checkpoint;
	* Cisco;
	* Fortinet.
		1. A build review of each of our operating system builds:
	* Two Windows server builds, two Windows workstation builds, one Chrome OS build
		1. Security testing of mobile devices, wireless and remote access:
	* On-site wireless access using Corporate, GovWifi and Public Wifi networks;
	* Email access and mobile device review of an Android mobile device;
	* VPN access and cloud proxy access using a Windows laptop;
	* Citrix XenApp and XenDesktop remote access via the Internet.
		1. Security appraisal of our Office 365 tenant, including access controls and security configuration.
3. **PROPOSAL**
	1. The proposal must contain:
		1. A **statement of work**, including the tasks to carry out and the methods, which will be used.
		2. Any **prerequisites**, which are needed from TNA for the assessment to take place.
		3. A breakdown of the **people and time** required for each task.
		4. A total **price** for the scoped work, which is inclusive of any Travel & Subsistence or any other expenses. The price for the work in section 4 must not exceed the expected price as according to the rate card.
		5. A **rate card** covering security testing by CHECK certified individuals, and optionally including ISO 27001 internal audit, ISO 27005 risk assessment, and Cyber Essentials auditing. This will be inclusive of T&S or other expenses. **Please complete Appendix A with these details.**

1. **EVALUATION CRITERIA**
	1. Tender submissions will be evaluated using the following criteria:
* Statement of work 40%
* Prerequisites 20%
* People and time 20%
* Price / rate card 20% (Please complete Appendix A with these details)

The above areas will be scored according to the table below.

|  |  |
| --- | --- |
| **10 Points** | **Outstanding:*** Potential Supplier has provided a response that addresses all parts of the requirement
* Potential Supplier has provided evidence to support all elements of their response
* The evidence supplied is convincing and highly relevant to the requirement
* Potential Supplier’s response is clear and easy to understand
* Where relevant, Potential Supplier has demonstrated a high level of capability to deliver new and innovative service approaches
 |
| **7 Points** | **Good:*** Potential Supplier has provided a response that addresses all parts of the requirement
* Potential Supplier has provided evidence to support most elements of their response
* The evidence supplied is good and relevant to the requirement
* Potential Supplier’s response is clear and easy to understand
* Where relevant, Potential Supplier has demonstrated some level of capability to deliver new and innovative service approaches
 |
| **5 Points** | **Average:*** Potential Supplier has provided a response that addresses most parts of the requirement
* Potential Supplier has provided evidence to support most elements of their response
* The evidence supplied has some relevance to the requirement
* Potential Supplier’s response is clear and easy to understand
* Where relevant, Potential Supplier has demonstrated limited capability to deliver new and innovative service approaches
 |
| **3 Points** | **Poor:*** Potential Supplier has provided a response that addresses some parts of the requirement
* Potential Supplier has provided evidence to support some elements of their response, but not all
* The evidence supplied is weak and has limited relevance to the requirement
* Potential Supplier’s response is not always clear and easy to understand
* Where relevant, Potential Supplier has demonstrated limited capability to deliver new and innovative service approaches
 |
| **1 Point** | **Very Poor:*** Potential Supplier has provided a response that fails to address most parts of the requirement
* Potential Supplier has provided little or no evidence to support most elements of their response
* The evidence supplied is very weak and has very limited relevance to the requirement
* Potential Supplier’s response is not always clear and easy to understand
* Where relevant, Potential Supplier has demonstrated little or no capability to deliver new and innovative service approaches
 |
| **0 Points** | **Fail:*** No response provided
 |

1. **HOW TO RESPOND**

Please respond by 5pm on 2nd December 2019 to procurement@nationalarchives.gov.uk by providing:

* 1. **A proposal, which** addresses the requirements in Section 5 above.
	2. **Guaranteed dates for test activities**, which allow for all scoped work to be completed before 29thFebruary 2020.
1. **TIMESCALES**

|  |  |  |
| --- | --- | --- |
| **Ref.** | **Description**  | **Date(s)** |
| 1 | Deadline for potential suppliers to submit clarification questions | 5pm, 20th Nov 2019 |
| 2 | Deadline for TNA to respond to clarification questions | 5pm, 25th Nov 2019 |
| 3 | Deadline for potential suppliers to submit tender responses | 5pm, 2nd Dec 2019 |
| 4 | Deadline for evaluation of tender responses and award notification | 5pm, 13th Dec 2019 |
| 5 | Last date for completion of work | 29th February 2020 |

1. **CONTRACT TERMS**

The Contract, and any subsequent Contract variations, shall be governed by our standard terms and conditions, available [here](https://www.gov.uk/government/publications/short-form-terms-and-conditions) and by submitting a response to this ITT, you accept these terms and conditions.

Please note that the information you supply in your tender submission may be used, in whole or in part, to populate the Contract. As such, please make clear and unambiguous statements about the commitments you are making.