**Clarification Questions and Answers for IT Health Check Tender**

Q1. In terms of the Infrastructure vulnerability assessment, will there be a need for a segmentation test between subnets?

A1. Not necessarily as part of the vulnerability assessment. There are two main security zones, and from firewall review, we would anticipate some assessment of traffic permitted from less secure to more secure zones.

Q2. How many differing builds are there within the Virtual servers and physical estate?

A2. For build review, three: two server and one desktop.

Q3. Could we have more information on the two bespoke applications such as purpose of the applications, basic workflow, authorisation levels, etc.?

A3. Generally authenticated - MYC: cataloguing tool accepting uploads - 5 pages, 2 user roles; Secure: authentication service - 5 pages, no user roles.

Q4. How many rules are there for the Firewall devices and how many devices overall?

A4. Checkpoint: ~250, Fortigate: ~600, Cisco: ~230.

Q5. Could you please elaborate on what you mean by Email access review?

A5. It is possible to access email accounts using Android smartphones. This would be to verify this is done in a secure way.

Q6. In regards to VPN Access, is a network segmentation or configuration review needed?

A6. Primarily segmentation though a configuration review may be useful if it meets the aim: to test the security of VPN access and where any security weaknesses may be.

Q7. In regards to Citrix XenApp, will this be Configuration review or Breakout?

A7. Both: the aim of this would be to determine security robustness of our Citrix service and where any security weaknesses may be.

Q8. There are mentions of subnets hosted in AWS and Azure is there a requirement for an AWS or Azure environment configuration review?

A8. There may be benefit in an Azure configuration review. List this item separately in the tender and we can consider it.

Q9. Will National Archives set up a VM for the consultant to access the AWS and Azure IP addresses? If so, could this assessment be performed offsite?

A9. Azure and AWS (public) IPs could be reached from off-site. Azure and AWS (non-public) IPs are only accessible from on-site. A VM should not be necessary if e.g. the approach is to bring devices on-site to carry out testing and to carry out off-site testing remotely - but include in the proposal the anticipated approach.

Q10. Are all IP addresses in the /25 and /29 subnets in scope for the external pen test? If not, how many IP addresses are in scope, and is a host discovery exercise needed?

A10. All IPs are in scope for host discovery, but not all are expected to be live. We would expect ~35 live IPs with ~20 unique hosts/services.

Q11. For each of the 5 applications in scope, could you please indicate the number of pages and user roles in scope for testing. Please also confirm how the application can be accessed, and whether the testing is authenticated or non-authenticated. Additionally, could you please confirm of any key functionality or test scenarios to be included (Such as upload / download functionality).

A.11 Generally authenticated - MYC: 5 pages, 2 roles; Secure: 5 pages, no roles; WordPress: 25 pages across 3 sites, 3 roles. No particular scenarios to test.

Q.12 How can each application be accessed? (i.e. VM, VPN, remotely over the internet, onsite via consultant/national archives laptop)

A.12 Web browser, in all cases. Most apps/WordPress sites are available remotely, except for admin access to one site, which is only available from on-site.

Q.13 For the firewall configuration reviews, how many rules are in scope? Can the configuration outputs be extracted and sent to our consultants’ offsite for review?

A.13 Checkpoint: ~250, Fortigate: ~600, Cisco: ~230. We would prefer this to be conducted on-site.

Q.14 For the build reviews, what OS versions are in use? (E.g. Windows 2016) Can scripts be run and output sent offsite for analysis?

A.14 Windows Server 2012 R2, Windows Server 2016, Windows 10. We would expect this to be conducted on-site.

Q.15 Will testing of the VPN and cloud proxy service be on a national archives window laptop?

A.15 Yes.

Q.16. Is a Citrix breakout assessment required, or testing of the remote access solution.

A.16 Yes.

Q.17 Which O365 products are in scope for testing please?

A.17 Primarily Office (Word, Excel, and PowerPoint), Outlook and Sharepoint are in use.

Q.18 What is the location for all onsite testing?

A.18 The National Archives, Kew, Richmond TW9 4DU

Q.19 For the five applications, which require testing, is authenticated testing required. If yes, how many user roles does each application have?

A.19 Generally authenticated - MYC: 5 pages, 2 roles; Secure: 5 pages, no roles; WordPress: 25 pages across 3 sites, 3 roles.

Q.20 For Annex A – the Rate Card – please confirm whether you require it as a word document separate to the proposal, or part of the proposal itself?

A.20 Can be part of the proposal itself.

Q.21 Please can you provide the quantity of firewalls to be reviewed (Checkpoint, Cisco, Fortinet), and please could you provide an estimate of the number of rules configured on each?

A.21 Checkpoint: ~250, Fortigate: ~600, Cisco: ~230

Q.22 For the external penetration test, please can you confirm how many of the IP addresses are hosting known services?

A.22 We would expect ~35 live IPs with ~20 unique hosts/services.

Q.23 For the 3 WordPress sites, is testing from an authenticated user perspective required, if so, how many user roles are to be tested? [See below]

Q.24 For the bespoke web applications, please can you confirm the approximate number of dynamic and static pages, and the number of user roles to be tested?

A.24 Generally authenticated - MYC: 5 pages, 2 roles; Secure: 5 pages, no roles; WordPress: 25 pages across 3 sites, 3 roles.

3.4.2.     Secure deletion of all storage media used during the ITHC.

Can this be deleted and confirmed at Nettitude HQ or would this need to be done onsite at National Archives?

* Would expect this can be deleted offsite once reporting is complete.

4.3.1.     An internal infrastructure vulnerability assessment of our IT systems.

Is a sample based approach acceptable for the servers and the workstations or is testing required on all?

Are the Azure and AWS subnets accessible from the on premise location? If not we can deploy Virtual Machines within the VNETs/VPCs to conduct testing.

* Azure and AWS (public) IPs could be reached from off-site. Azure and AWS (non-public) IPs are only accessible from on-site.

4.3.2.     An external penetration test of our Internet-facing IT systems, conducted from off-site using known IP addresses

How many external IP's are expected to be live?

* We’d expect ~35 live IPs with ~20 unique hosts/services.

4.3.3.     Web applications testing, against versions of our public-facing web services:

Please provide the URLs for the WordPress sites and please confirm if unauthenticated or authenticated testing are required for the front end.

* test.nationalarchives.gov.uk
* test.blog.nationalarchives.gov.uk
* test.media.nationalarchives.gov.uk
* Authenticated testing would be requested. Wordpress: 25 pages across 3 sites, 3 roles.

For each web application for the 2 bespoke apps, please answer/provide the following information:

The URL/IP address if publicly accessible. If not, how are the applications accessed?

A brief summary on what the application is used for.

What functionality exists before login, and approximate number of pages (e.g. login, register, forgotten password)?

What functionality exists after login, and approximate number of pages (e.g. add to basket, payment, write blog post, account management – change password)?

How many user roles are there, and what levels of privilege do they have?

Where is the application hosted (cloud etc.)?

* MYC: cataloguing tool accepting uploads - 5 pages, 2 user roles; Secure: authentication service - 5 pages, no user roles. Hosted here on-site.

4.3.4.     A review of perimeter and internal firewall configuration and policies.

How many configuration reviews are required per firewall?

Approximately, how many rules are their per firewall ruleset?

* One each. Checkpoint: ~250, Fortigate: ~600, Cisco: ~230.

4.3.6.     Security testing of mobile devices, wireless and remote access.

Are the wireless access point centrally managed?

Please confirm whether the only SSIDs broadcast are: Corporate, GovWifi, Public.

* Yes, access points are centrally managed. Other SSIDs are present with limited secured uses.

Mobile device and policy review questions:

Number of policies to be assessed

Number of devices to be tested and their brands/models/platforms

If a device test is required is it possible to ship the sample devices to Nettitude’s offices?

Which Mobile Device Management solution is currently implemented?

How many policy profiles are in use?

Can the MDM policy be exported for remote assessment?

* One policy, one device. On-site only, both device and policy. Citrix XenMobile.
* Is there a requirement for network segmentation testing between the in-scope subnets?
  + There are two main security zones, and from firewall review we’d anticipate some assessment of traffic permitted from less secure to more secure zones.
* For the infrastructure assessments, is there a preference for full coverage or testing a representative sample of systems? Or a mix, all servers and a sample of workstations?
  + 100% of the estate.