

REQUEST FOR PROPOSAL – #5632LHC
PROVISION OF VULNERABILITY ASSESSMENT AGAINST EXTERNAL FACING WEB
SITE, INTERNAL NETWORK ENVIRONMENT AND WIRELESS ASSESSMENT AND
PERIMETER ASSESSMENT WHICH INCLUDES SECURITY POLICIES

RESPONSE TO RESPONDENT QUESTIONS
ADDENDUM #1

Lakeridge Health's (LH) responses to Respondent Questions received by the deadline date of June 5, 2010 (Section 3.0 of the RFP) are noted below. These responses do not change the scope or the intent of the Request For Proposal (RFP).

- Q.1.** *In order for us to accurately estimate effort can you please provide the total # of internal hosts to be evaluated. The list of subnets contained in Appendix "B" does not provide # of hosts per subnet. There is a significant difference in effort between a Class C with 20-30 hosts, and a Class C with 250 hosts...*

RESPONSE

Assume 250 host per subnets since we have used all of the host addresses prior to deploying the next subnet.

- Q.2.** *LHO VLAN 503 Wireless Phone – Is Lakeridge using VoIP, or is this 802.11 access for smartphones? If Lakeridge is using VoIP, and if the VoIP infrastructure is in scope for the VA, please provide the name/model/manufacture of the IP PBX and relevant hardware, and the approx # of hardphones and softphones.*

RESPONSE

We are using the Ascom solution which is to some extent proprietary but flexible in design to be used within an open system architecture. This is a very small implementation in a specific area and does not really need to be within scope.

Q.3. *Page 10 Physical Access Security Reviews – Is the scope of the Physical Access Security Reviews restricted to specific zones, such as a Server Room and Cabling Closets, or are the entire premises in-scope? If the scope is focused on specific zones such as Server room and LAN closets, can you please provide a detailed list covering all the zones expected to be in scope of the assessment, and approx sq/ft for each zone. If the scope is all inclusive, and Lakeridge requires “Base Building” Threat & Vulnerability Assessments, please provide the total # of sites, # of buildings at each site, and if possible floorplans of each building.*

RESPONSE

The LH-Oshawa campus data centre physical access is the only area within scope.

Q.4a *Page 10 Wireless Network Vulnerability Assessment – Are all the Cisco Access points centrally managed?*

RESPONSE

Yes they are using a 6509 WISM appliance(s) with 600 licenses.

Q.4b *Page 10 Wireless Network Vulnerability Assessment - Please clarify desired scope. Is the scope limited to an assessment of the existing 250 cisco access points by reviewing configuration settings, etc pulled from a centrally managed point (assuming central management), or does Lakeridge require the proponent to perform an exhaustive review of the 2.4Ghz and 5Ghz spectrums throughout all of Lakeridge's operating premises to search for unauthorized access points, validate that all access points use encryption and strong authentication etc? If the latter, then this task will require extensive physical onsite work at all Lakeridge Health Network locations and we will require a list of all addresses to properly estimate effort. The list of addresses should include: Address, # of floors, total approx sq/ft, shared premises (y/n)*

RESPONSE

The scope should limited to a random selection of A/P determine by them since we have standardized with version and configuration settings (i.e. Encryption algorithm). A rogue sweep is also expected as part of the VA.

- Q.5.** *Security Awareness Program Review – Scope definition – Does Lakeridge require the proponent to validate the effectiveness of the existing Security Awareness Program by way of Social Engineering tests, or are you looking for the proponent to review the content, delivery, and management of the program by way of documentation review, or both?*

RESPONSE

We are you looking for the proponent to review the content, delivery, and management of the program by way of documentation review only.

- Q.6.** *Incident Response Program Review – Scope definition – As per Q5 – Does Lakeridge require the proponent to initiate a pre-authorized Security Incident/Breach and assess the effectiveness of the existing Security Incident Management team/processes, or are you looking for more of a document review exercise, or both?*

RESPONSE

Same answer as question #5