

## General Questions

1. With regards to the execution team, are there any objections with the responding vendor using a combination of offshore and onshore resources or must team members all be onshore?

The preference is to use local or national (onshore) resources but will not rule out using global (offshore) resources; however, that is subject to change

2. Will the State agree to negotiate certain terms related to the contract resulting from this RFP including, but not limited to, the inclusion of a reasonable limitation of liability?

Correction-the Request for Qualifications (RFQ) was published by the City of Indianapolis/Marion County not the State of Indiana and . Certain terms may be negotiable.

## External Network Vulnerability Assessment Questions

3. The RFQ requests a third party to perform a series of “vulnerability assessments.” Please confirm if ISA desires “vulnerability assessments,” “penetration testing,” or both based on the following definitions:
  - a. Vulnerability Assessment – perform automated scanning using a tool to attempt to identify any one of the thousands of publically known vulnerabilities. This task primarily follows an automated approach with some manual techniques.
  - b. Penetration Testing – perform manual hacking techniques to attempt to gain unauthorized access to resources, the data contained within and the overall network. This task primarily follows a manual approach with the use of some automated tools.

For this engagement our requirement is to conduct vulnerability assessments; however, should it make financial sense and we have the funds we would consider some penetration testing

4. The RFQ requests that a component of the External Vulnerability Assessment include “Denial of Service Emulation” and “Man-in-the-middle” attacks.” Both of these are highly intrusive tests and will disrupt production services. Does ISA want the third party to actually perform both of these attacks in a production environment, or simply attempt to identify vulnerabilities that may result in these conditions through automated vulnerability scanning?

It is understood by ISA that some of the testing could be intrusive. However, a respective vender’s expertise on the risks and rewards of this kind of testing is subject to evaluation by ISA (i.e., recommending a test that could permanently damage a production system would represent a poor choice by the vender. Discovery of such a problem would best be done passively.) ISA will work with the vender to minimize outages and anticipates running some test during maintenance windows on advice from the vender, etc.

5. Are any ISA external resources hosted by third party service providers within scope for the assessment?

No.

## Internal Network Vulnerability Assessment Questions

6. Based on the RFQ description, we understand ISA wants both an automated vulnerability assessment and manual penetration testing of the internal network environment. Please confirm this assumption.

Please see response to Question #4

7. The RFQ requests a series of security tests for the below areas. Does ISA want detailed technical configuration assessments against industry standard “hardening” practices for each of these areas or is the main focus of the assessment to identify vulnerabilities? Additionally, please confirm the following questions below:

a. Access lists and account settings

- i. What is the intended scope of this area? Specifically, what access lists and account settings would you like assessed? (e.g., Active Directory, OS- or application-specific access lists, VPN, Network Devices, other)

This will be subject to negotiation. Gaining the most information for the best price is the goal.

b. Desktop operating systems

- i. Do you desire that all desktops be assessed, or a representative sample? If a sample, what is the sample size of desktops you would like assessed? If all desktops, how many are there?

This will also be subject to negotiation.

c. Network architecture and address scheme

- i. No further questions.

d. Network operating systems

- i. No further questions.

e. Routers and network devices

- i. What specific network devices are in scope other than routers? E.g., firewalls, switches, intrusion detection/prevention systems, other?

- ii. How many of each network device is in scope and what vendor is used (e.g., Cisco)?

The scope will be subject to negotiation.

### Wireless Network Vulnerability Assessment Questions

8. The RFQ states there are 50 wireless access points (WAP) located within 10 miles of the city county building.
- a. What is the WAP vendor or vendors (e.g., Cisco, Aruba, other)?

This information will be provided during negotiation.

b.

- c. Is a centralized management console used to manage the 50 WAP's or are each of the 50 WAP's individually managed?

This information will be provided during negotiation.