TAMPA-HILLSBOROUGH COUNTY EXPRESSWAY AUTHORITY

Letter of Clarification No. 1

FOR

REQUEST FOR QUALIFICATIONS (RFQ)

Administrative & Operations Network Security Assessment

RFQ No. O-00418

Letter of Clarification No. 1 ~ RFP No. O-00418

Date of Letter of Clarification: June 7, 2018

To all prospective respondents:

The following responds to questions received on the solicitation reference above:

Question 1:	How long will the assessment take?
Response 1:	**Vendors are expected to discuss timeline in their response. THEA would like all work completed before 12/31/18.**
Question 2:	Once the assessment is done, if the consultant deems the network security needs an upgrade, will an RFP/RFQ be released to acquire a new system? If so, when?
Response 2:	**THEA does not anticipate any further RFP/RFQ as a result of the assessment.**
Question 3:	What is the estimated cost of a new system?
Response 3:	**This RFP is for a scope of services; not a new system.**
Question 4:	How would it be funded?
Response 4:	**This RFP is funded by THEA's operational budget.**
Question 5:	How many Physical locations will be evaluated in the testing?
Response 5:	**2 = Main Building and nearby DR Site**
Question 6:	What is the function of each location? Office? Co-location facility? Branch site?
Response 6:	**Main Office and DR Testing Site**
Question 7:	How many unique subnets are in use in the entire network?
Response 7:	**There are 2 separate isolated Networks each with 1-3 internal subnets**

Question 8:	How many Internet gateways are in use in the entire network? i.e. Wide Area Network connections from ISP's.
Response 8:	**1 per Network**
Question 9:	Will the test involve remote user policies and testing? i.e. Telecommuters, "Road Warriors".
Response 9:	**Yes**
Question 10:	Roughly how many policies need to be reviewed?
Response 10:	**2-5 Existing policies**
Question 11:	How many locations are in scope for physical penetration test?
Response 11:	**2 Locations: TMC Main Office and East Plaza DR Site**
Question 12:	How many personnel are in scope for the social engineering penetration testing? Does this include, email and phone-based attacks?
Response 12:	**About 25 personnel. Yes email and phone based attacks.**
Question 13:	How many personnel will need to be interviewed for the assessment? Number of IT, management, and administrative, operations personnel.
Response 13:	**Total staff is approximately 25.**
Question 14:	How many network devices, such as firewalls, routers, switches, VPN, etc. are in scope for any external and internal testing?
Response 14:	**2 separate and isolated networks; Admin network has about 1 firewall, 5 access points, 6 switches; Operations Network has about 2 fires walls, 3 routers, 10 switches**
Question 15:	How would you rate the size and complexity of the Administrative and Operations networks?
Response 15:	**Small to medium sized simple networks**

Question 16:	How many target servers and workstations included for the penetration testing? What is the mix of physical and virtual servers?
Response 16:	**Admin Network has about 3 host servers, 3 virtual servers, and 30 workstations; Operations Network has about 6 servers, 0 virtual servers, 15 workstations**
Question 17:	Are there any web applications in scope for testing and how many? • If yes, how many web pages can we expect for each web app?
Response 17:	**Yes, About 1-2 ;** • **About 15 -20 each**
Question 18:	Do you want us to test for denial of service (DoS) vulnerabilities? We don't add DoS testing by default.
Response 18:	**Yes**
Question 19:	Does the Authority have a preference how the information in the Price Proposal Form is laid out? We usually price out the phases of the engagement.
Response 19:	**Pricing out the phases of the engagement is acceptable. THEA will ask for details or clarification if needed.**
Question 20:	Number of offices (please specify approximate number of users, devices, and end-user ports at each)
Response 20:	**Approximately 25 – 30 users, 55 devices**
Question 21:	• Outside of physical offices, what connected physical facilities does the Tampa Hillsborough Expressway Authority have? • How many users, devices and ports can be found at these facilities?
Response 21:	• **1 DR site within 15 minutes of the main office** • **Approximately 0 users, 4 devices, 8 ports**
Question 22:	What technology is used to connect physical installations?
Response 22:	**Fiber and Ethernet and WiFi**

Question 23:	Number of devices (approximated if necessary): Routers, switches, firewalls, hardware appliances (e.g. load balancers, security appliances, etc.)
Response 23:	**2 separate and isolated networks; Admin network has about 1 firewall, 5 access points, 6 switches;** **Operations Network has about 2 fires walls, 3 routers,** **10 switches**
Question 24:	Physical servers a. Virtualization environment i. Physical hosts ii. Virtual Machines iii. Containers
Response 24:	**Admin Network has about 3 host servers, 3 virtual servers, and 30 workstations** **Operations Network has about 6 servers, 0 virtual servers, 15 workstations** **a. Admin Network has about 3 virtual servers, and 30 workstations** **Operations Network has about 0 virtual servers, 15 workstations**
Question 25:	Does the Expressway Authority use any Operational Technologies, such as connected sensors, toll collectors or other devices? a. What types of devices are used? b. Approximately how many are used? c. How do these devices connect back to the datacenter(s)? d. Are these devices considered “in-scope” for scanning and/or penetration testing?
Response 25:	**We will not be assessing or testing any of the Toll collecting devices. That is a separate Network.**
Question 26:	Does the Expressway Authority use any infrastructure installed on public or 3rd-party clouds? a. Does the Expressway Authority use Microsoft Office 365, Google Documents or a similar product? i. If so, what product? ii. How does the Expressway Authority connect to the cloud?

Response 26:	**Yes.** **a. Yes** **i. Microsoft Office 365** **ii. Internet**
Question 27:	What cloud provider(s) are used to provide Infrastructure-as-a-Service? i. How many virtual machines and containers at each? ii. How does the Expressway Authority connect to the cloud? iii. What type of authentication mechanism(s) is/are used (e.g. local authentication, Active Directory Federation, etc.)?
Response 27:	**None**
Question 28:	What traffic baselining tools already exist within the environment and can be made available to the consultant?
Response 28:	**Respondents should assume they are providing tools for establishing baselines**
Question 29:	How many IP addresses total (both internal and external) will be in scope for testing?
Response 29:	**Approximately 100**
Question 30:	How many web applications (websites) will be in scope for testing?
Response 30:	**Approximately 1 - 2**
Question 31:	Are any mobile applications in scope for testing? If so: How many?
Response 31:	**Approximately 25**
Question 32:	When should penetration activities of in scope assets (scanning, exploitation) occur? (e.g. business hours, after business hours, weekends)
Response 32:	**After Hours and Weekends**

Question 33:	For internal testing, will the WWT Penetration Tester have VPN access, or need to be onsite to perform testing?
Response 33:	**VPN Access will be acceptable**
Question 34:	Will the WWT Penetration Tester be required to use client equipment for the test? (Please note, if WWT is required to use customer equipment, WWT will need to install a suite of penetration testing software and the machine in use will need to meet WWT specifications.)
Response 34:	**No**
Question 35:	How many email addresses will be phished?
Response 35:	**Approximately 50**
Question 36:	How many phone numbers will be in scope?
Response 36:	**Approximately 30**
Question 37:	Is a physical penetration testing of one or more business location(s) or physical installation(s) in scope for the assessment? If so, how many?
Response 37:	**Yes. 2**
Question 38:	Was there a pre-bid meeting for this project?
Response 38	**No.**
Question 39:	How many Public IP addresses? (approximate required to effectively quote)
Response 39:	**15 but not all are used**
Question 40:	How many applications? (ie. instances of IIS, WebSphere, Oracle, Peoplesoft etc)
Response 40:	**2 premise applications; 1 cloud application**

Question 41:	Is a physical security assessment of the infrastructure in scope of the Network Assessment?
Response 41:	**Yes**
Question 42:	Is the IT organization centralized or decentralized?
Response 42:	**Centralized**
Question 43:	Has a security control framework been adopted? If yes, which one?
Response 43:	**No**
Question 44:	When was your last network security assessment performed?
Response 44:	**Internal reviews are done quarterly, but this is a special project with broader scope and purpose as stated in the RFP**
Question 45:	Are there documented policies, procedures, standards, and guidelines in place? If so, how many?
Response 45:	**The agency intends to develop new policies and procedures because of this RFP**
Question 46:	For the external network vulnerability assessment and penetration testing, what is the approximate number of active IPs?
Response 46:	**15 but not all are used**
Question 47:	What is the number of firewalls? Are the firewalls in HA mode?
Response 47:	**Two. No.**
Question 48:	What is the approximate number and types of switch devices?
Response 48:	**WatchGuard, Cisco and HP equipment (various models)**
Question 49:	For the internal network vulnerability assessment and penetration testing, what is the approximate number of active IPs?

Response 49:	**3 private subnets; all Class C**
Question 50:	How many staff security training and agency policies are in scope for review?
Response 50:	**All**
Question 51:	For physical security penetration testing, how many server rooms/racks/DR sites require visitation?
Response 51:	• **1 server room and 1 communications room at main office** • **1 DR location approximately 10 minutes from the main office**
Question 52:	How many targets are in scope for user-focused penetration testing?
Response 52:	**User account testing is not part of this scope.**
Question 53:	Is web application testing in scope for this project? If so, how many applications require assessment?
Response 53:	**Application testing is not part of this scope.**
Question 54:	Is a wireless network assessment in scope? If so, how many controllers support the wireless network?
Response 54:	**One controller (firewall) and 5 access points**
Question 55:	Will THEA accept reference letters in lieu of client contact information?
Response 55:	**Submit the most complete bid you can and it will be evaluated per the RFP.**
Question 56:	Will THEA provide its budget for this project?
Response 56:	**No, THEA is looking to the Respondent for price proposal for this project.**
Question 57:	We do have a partner who handles this work and we have worked with on numerous occasions. Will a joint proposal be permitted for the services requested?

Response 57:	**Per page 6 of the RFQ, joint proposals will not be accepted but subcontracting is acceptable.**
Question 58:	We requests that contact info for our references only be provided should we be selected as a finalist. Is this acceptable to THEA?
Response 58:	**Incomplete proposals will be subject to the evaluation per the RFP.**
Question 59:	Is THEA seeking a fixed price or time and materials bid for this project?
Response 59:	**Responses are expected to be stated as a fixed price.**
Question 60:	How many employees total does THEA have? How many IT employees?
Response 60:	**Approximately 30 staff and 1 IT Manager.**
Question 61:	Approximately how many pages of written policies and procedures currently exist? How many documents?
Response 61:	**Less than 100 pages in multiple documents.**
Question 62:	Approximately how many staff must be interviewed for understand the organization strategy and new planned network architecture and design?
Response 62:	**Approximately 1 staff and 2-3 vendor representative.**
Question 63:	How many groups are associated with running the network (eg. Network, Security, Operations)
Response 63:	**THEA has one IT department with one IT Manager responsible for running the network(s).**
Question 64:	How many of the THEA locations have an independent Internet connection?
Response 64:	**The Main Office has the only internet connection.**

Question 65:	Are any cloud services in use and in scope for this assessment - How many SaaS solutions? - How many PaaS solutions? - How many IaaS solutions?
Response 65:	**With the exception of Microsoft Office 365, all infrastructure is premise.**
Question 66:	How many firewalls are in the network?
Response 66:	**Two.**
Question 67:	Is rules analysis on firewalls desired to look for common issues? If so, how many firewalls, and what make, model, and software version?
Response 67:	**No.**
Question 68:	On about what percentage of devices is SNMP or a similar discovery protocol enabled?
Response 68:	**Estimated 75%.**
Question 69:	How much bandwidth is involved in traffic pattern analysis? How many separate locations must this be performed on? Can a network tap be inserted in these locations?
Response 69:	**Unknown. One physical location. Yes, the network can be tapped if necessary.**
Question 70:	How many physical sites are required for physical security penetration testing? Are any of these large sites, such as a distribution center?
Response 70:	**2 physical locations; both small sites.**
Question 71:	Approximately how many users should phishing attempts be made on? Is phishing to be performed in both insider and outsider modes?
Response 71:	**THEA has approximately 30 staff.**

Question 72:	Can testing be performed during business hours?
Response 72:	**Limited testing can be done during business hours; most testing is requested for after hours and weekends.**
Question 73:	Is 'Outsider' testing to be performed from the outside of the network, the inside of the network, or both?
Response 73:	**Provide your recommendation in your response.**
Question 74:	Does THEA have an estimated duration for Outsider testing? An attacker may invest significant time, which can dramatically increase the cost of a proposal without time bounds Is 'Insider' testing to be performed from the outside of the network, the inside of the network, or both? If testing is to be performed from inside the network, can remote access to a testing server be provisioned?
Response 74:	**THEA does not have any estimates.** **Remote access can be provisioned.**
Question 75:	Will the insider/outsider testing be performed from a perspective of assumed compromise (regular user on workstation compromised?)
Response 75:	**Provide your recommendation in your response.**
Question 76:	Is the IT service delivery organization centralized or decentralized?
Response 76:	**Centralized.**
Question 77:	Are there documented policies/procedures for the core IT processes?
Response 77:	**Some policies/procedures are documented.**
Question 78:	What centralized authentication is used (Novell, Windows AD, something else?)? ○ If Windows, how many Domains?

Response 78:	**One Windows Domain structure manages authentication; it synchronizes to Office 365.**
Question 79:	Are all the operational units/divisions logically accessible on the network from a centralized location? ○ I.e. can the systems be tested from a central location?
Response 79:	**Yes.**
Question 80:	Please clarify who the client is in this objective statement. • "Develop physical and logical network diagrams and flow charts to compare with client's"
Response 80:	**THEA maintains internal diagram and is the "client" referred to.**
Question 81:	To what level of detail are you requesting for the inventory of network equipment?
Response 81:	**Make/Model/Serial #/ Identified Role/ Assessment Status would be considered a minimum.**
Question 82:	As an attempt is made to execute the logical/physical penetration test, what is the goal? At some point people become suspicious with various aspects of testing being engaged (phishing, tailgating, USB, etc.) and the effort becomes an exercise in futility because word is passed around and people become suspicious. Bottom line question is "What is considered success?"
Response 82:	**See RFP for the goal; all testing will be limited to reasonable efforts and it is not expected to be a major impact to THEA staff.**
Question 83:	Is Server room in a hosted facility or on THEA premise? ▪ DR Facility?
Response 83:	**Yes, plus a nearby DR site.** • **Yes, within 15 minutes of the main office.**

Question 84:	A Network and/or server diagram
Response 84:	**The development of a network diagram is a component of the scope of work and will not be provided in advance.**
Question 85:	What is the term of the engagement?
Response 85:	**THEA expects the scope to be completed no later than 12/31/18.**
Question 86:	Does the THEA have to have services completed by a specific date to meet demands of an audit or some other date?
Response 86:	**THEA expects the scope to be completed no later than 12/31/18.**

Respondents MUST acknowledge receipt of this Letter of Clarification by signing, dating and returning the completed Acknowledgement of Receipt of Letter of Clarification/Addendum form **with Respondent's proposal.**

All other items, conditions, and specifications in the ITB document not specifically changed by the Addendum remain unchanged.

Please send all questions to THEA's Procurement Manager, Man Le, via email at Man.Le@tampa-xway.com.

ACKNOWLEDGEMENT OF RECEIPT OF Letter of Clarification/Addenda

Were Addenda issued on this Solicitation?

☐ Yes

☐ No

Were Letter of Clarification issued on this Solicitation?

☐ Yes

☐ No

I (We) hereby acknowledge receipt of the following Addendum/Addenda issued in reference to this solicitation by listing the Addenda by number, date and signing the form:

Addendum _____ Date: _____

Letter of Clarification _____ Date: _____

Letter of Clarification _____ Date: _____

PROPOSER:

By: _____
(AUTHORIZED SIGNATURE)

_____
(Printed Name of Signer)

_____
(Title of Signer)

_____
(Date Signed)