OHIO DEFERRED COMPENSATION
OHIO PUBLIC EMPLOYEES DEFERRED COMPENSATION PROGRAM

2015 Security Assessment RFP Vendor Questions and Answers

4/16/2015

Question #	Topic	Question	Answer
1.00	Evaluation of security risks related to NRS data access	What is the system(s) that hosts NRS data? Approximately how many users have access?	We are not asking the vendor to assess the data stored with Nationwide but only Nationwide's access to our data.
2.00	Firewall Diagnostic Reviews	How many firewalls?	2
2.01	Firewall Diagnostic Reviews	How many rules per firewall?	Not available
2.02	Firewall Diagnostic Reviews	How many objects within the firewall?	Not available
3.00	General	What is driving this initiative?	Our Security Policy requires that we complete a security assessment biennially.
3.01	General	When was the last time you performed this assessment?	2013
3.02	General	What items were included?	The same services that are listed in the current RFP Scope of Services.
3.03	General	What is the ultimate goal of the assessment?	To verify that the proper controls are in place to insure that our participant's data remains secure.
3.04	General	What deliverables other than a presentation to the Board are you hoping to receive?	The vendor should provide a thorough assessment report that includes the findings, the level of risk resulting from the findings and recommendations for remediation.
3.05	General	Are you looking for a risk based approach to this assessment?	Yes
3.06	General	What type of framework do you currently use to understand security risk?	We don't have a specific framework - we base understanding on the recommendations made in past security assessments.
3.07	General	Does the Ohio DC have any special compliance or federal regulations that need to be addressed during this assessment?	No
3.08	General	How in-depth would you like the reviews for the items listed in the scope of services question?	We are looking for a balanced approach with the reviews sufficient to insure that the appropriate security is in place while keeping in mind that are staff size is limited and assessment cost is a consideration.
3.09	General	Do you have a budget for this initiative and if so how much?	We do have a budget but are not willing to disclose the amount.
3.10	General	What are the main decision criteria for the awardee?	Please refer to page 15 of the RFP titled: EVALUATION CRITERIA AND SELECTION PROCESS
3.11	General	Are there any payment terms or options that the Ohio DC prefers?	In the past, we have paid for the assessment after all of the work has been completed.
3.12	General	When would you like to have this project started/completed by and are there any other time considerations?	Please refer to the calendar of events on page 4 of the RFP.
3.13	General	What, if any, are the compliance/regulatory requirements that must be included/assessed? (e.g. PCI, HIPAA)	We do not have any specific compliance/regulatory requirements specific to our line of business.
3.14	General	Has an IT risk assessment been performed recently?	Yes in 2013
3.15	General	Can you please detail and describe the documentation that currently exist? The answers will speak to scoping the amount of review time needed to satisfy the engagement.	A yes or no answer for each of the following documents will indicate whether or not they are available.
3.16	General	· Regulatory Framework (e.g., ISO 17799, HIPAA, SOX)	No
3.17	General	· Policy Management	Yes
3.18	General	· User Awareness & Training	Yes
3.19	General	· Personnel Security	No
3.20	General	· Network Management	No
3.21	General	· Incident Response	Yes
3.22	General	· Access Control	Yes
3.23	General	· Information Management	No
3.24	General	· Physical Security	Yes
3.25	General	· Disaster Recovery & Business Continuity	Yes
3.26	General	· Backup	Yes
3.27	General	· Response Timeline	No
3.28	General	· Disaster Procedures	Yes
3.29	General	· Disaster Recovery Managers	Yes
3.30	General	· Points of Contact (e.g., Security Personnel, IT Admin, Data Owners & Custodians, Incident R	Yes
3.31	General	· Inventories (e.g., Critical Equipment, Assets, Data, Applications)	No
3.32	General	· Software Development	Yes

3.33	General	Are you looking for one person to do as much of the work as can be done in the time available or are you open to a team approach?	A team approach is acceptable
3.34	General	How many applications, physical locations, Hosts, and personnel are in scope?	See previous answers
3.35	General	Do you expect the consultant to the board to do the actual assessments and reviews or would the consultant be providing recommendations and review assessments provided by others?	We are looking for a consultant to do the actual assessment.
4.00	Host Diagnostic Reviews	Approximately how many hosts are anticipated to be included in the review?	One
4.01	Host Diagnostic Reviews	How many target servers/workstations?	See previous answers
5.00	Incident Response Program Review	Is this a paper review or is a table top required?	This question is unclear.
6.00	Internet Vulnerability Assessment and Penetration Testing	How many endpoints (e.g., workstations, laptops) exist within the environment?	We have approximately 25 workstations that have access to our internal network. In addition, Nationwide has about 30 workstations that have access to the IBM iSeries. We also have a wireless access point configured to have both an external guest account and an internal account with access to the network.
6.01	Internet Vulnerability Assessment and Penetration Testing	What is the scope of the vulnerability assessment and penetration testing? Will this include internal and external testing? Will this include web applications?	The scope of services are outlined in the RFP. We are looking for the vendor to recommend additional services that may be required. The vulnerability assessment and penetration testing should include both internal and external testing. There are no web applications included.
6.02	Internet Vulnerability Assessment and Penetration Testing	Will administrator credentials be provided in order to perform authenticated vulnerability scans?	Yes
6.03	Internet Vulnerability Assessment and Penetration Testing	Are NRS networks, applications, facilities, policies, and personnel in scope of this assessment?	No
6.04	Internet Vulnerability Assessment and Penetration Testing	Will the awarded vendor review internet vulnerability assessment and penetration testing reports that have been previously performed?	They can if they so desire.
6.05	Internet Vulnerability Assessment and Penetration Testing	If the answer is yes, how many assessment and testing reports are in scope to review?	One
6.06	Internet Vulnerability Assessment and Penetration Testing	If the answer is no, that the awarded vendor will conduct internet vulnerability assessment and penetration testing, then:	N/A
6.07	Internet Vulnerability Assessment and Penetration Testing	Can you please provide answers to the following scoping questions:	
6.08	Internet Vulnerability Assessment and Penetration Testing	Number of external facing servers & types (mail, web, etc..)	None
6.09	Internet Vulnerability Assessment and Penetration Testing	Number of internal servers & types (database, development, etc..)	See RFP
6.10	Internet Vulnerability Assessment and Penetration Testing	Briefly describe your environment and architecture (i.e. all in-house, some hosted/CoLo, custom apps, SaaS, etc..)	See RFP
6.11	Internet Vulnerability Assessment and Penetration Testing	Number of users on the system	Approximately 50
6.12	Internet Vulnerability Assessment and Penetration Testing	Number of network appliances (routers, firewalls, etc..)	See RFP
6.13	Internet Vulnerability Assessment and Penetration Testing	What operating systems are you using	See RFP
6.14	Internet Vulnerability Assessment and Penetration Testing	What types of remote access is available	Cisco VPN access for IT staff only.
6.15	Internet Vulnerability Assessment and Penetration Testing	Do you provide any third parties access to the systems	Nationwide only
6.16	Internet Vulnerability Assessment and Penetration Testing	What sort of protection mechanisms do you have in place currently (i.e. firewalls, antivirus, etc..)	We have a Cisco PIX firewall at our end of a dedicated T1 line with Nationwide and a Cisco ASA 5505 at our end of a fiber line to access the internet. We use Symantec Endpoint Protection for our antivirus solution.
6.17	Internet Vulnerability Assessment and Penetration Testing	What type of internet connection do you have and the number of (T1, OC3, share service, leased circuit, etc..	See RFP
6.18	Internet Vulnerability Assessment and Penetration Testing	Number of locations and estimated sizes	See RFP
6.19	Internet Vulnerability Assessment and Penetration Testing	How many active IP's will be included in the external vulnerability assessment and pen test?	One
7.00	Physical Security Review	How many physical locations are in scope?	One
7.01	Physical Security Review	How many locations and or buildings are within scope?	One
7.02	Physical Security Review	Are physical locations in scope for the Social Engineering assessment?	Yes
8.01	Remote Access Security Testing	Approximately how many users have remote access?	4
8.02	Remote Access Security Testing	How many analog telephone numbers need to be tested?	Not part of the scope of this assessment.
8.03	Remote Access Security Testing	Does the organization have analog modems connected to production devices?	The IBM iSeries has an internal modem that is used for faxing reports.
8.04	Remote Access Security Testing	What method of remote access are permitted and need to be tested?	See previous answers

9.00	Security Awareness Program Review	How many touch points does the program include?	See previous answers
10.00	Security Policy Review	How many policies will need to be reviewed?	We have one Security Policy document that contains 15 different security policies. In addition, we have a financial security policy.
10.01	Security Policy Review	Is there a Security program document	
11.00	Social Engineering	Do you want onsite or remote exercises or both?	Only one exercise is necessary and whether its onsite or remote is up to the vendor
12.00	Software Security Assessment	How many applications are in scope?	One
12.01	Software Security Assessment	Please provide an overview of in-scope applications.	We have a custom recordkeeping system that runs on an IBM iSeries 520.
12.02	Software Security Assessment	Will the awarded vendor review software security assessment reports that have been previously performed?	They can if they so desire.
12.03	Software Security Assessment	If the answer is yes, how many assessment reports are in scope to review?	One
12.04	Software Security Assessment	If the answer is no, that the awarded vendor will conduct application security assessments, then:	N/A
12.05	Software Security Assessment	Can you please enumerate the number of applications to be assessed for each agency and provide details for each application to assist scoping?	See previous answers
12.06	Software Security Assessment	Approximate size – (lines of code)	We are not asking the vendor to the code.
12.07	Software Security Assessment	Technology/language and system framework	See RFP and previous answers
12.08	Software Security Assessment	General purpose of the application	See RFP and previous answers
12.09	Software Security Assessment	Major functions and features	See RFP and previous answers
12.10	Software Security Assessment	Number and kinds of user roles	There are three main roles: Administrative (full access - IT Staff), Internal User (Update capability - Ohio DC staff), and Customer Service(Mainly inquiry only - Nationwide staff).
12.11	Software Security Assessment	Is the application an existing system or one currently in production?	Yes
12.12	Software Security Assessment	Will source code be available for any or all of the applications?	N/A
12.13	Software Security Assessment	If currently in production, what is the frequency of releases in a fiscal year?	As needed
12.14	Software Security Assessment	Will you require re-testing after a short period during which you will have addressed and remediated outstanding issues to validate fixes before the formal report to the Board?	No
12.15	Software Security Assessment	How many web application will need to be tested?	None
12.16	Software Security Assessment	How many are exposed to the Internet and how many are internal-based?	None
12.17	Software Security Assessment	How many mobile applications need to be tested?	None
12.18	Software Security Assessment	How many roles for each application?	See previous answers
12.19	Software Security Assessment	Will VPN access be permitted to test any internal web applications?	N/A