	Vendor Question	Answer
1	Given the current pandemic situation, can all services be performed remotely?	Yes, if the vendor has a strategy for completing a remote assessment. Please include remote strategy in the technical proposal.
2	Can a global delivery center outside the U.S. be utilized for any of the services, i.e., vulnerability scanning, report analysis, etc.?	Only from North America (US, Mexico, or Canada)
3	Will the Physical Security Review be applicable to only Ohio DC Headquarters location, or are there additional ancillary sites or datacenter(s) in scope?	Only Ohio DC offices located at 257 East Town Street Columbus OH
4	Will VPN access be provided for internal scanning?	Yes, if the vendor has a strategy for completing a remote assessment.
5	Which vulnerability scanning tools does Ohio DC currently leverage? Does Ohio DC own the licenses for these scanning tools already?	Ohio DC does not own or use any vulnerability scanning tools. In the past, the consultant has used their own tools
6	What is the estimated number of web pages in PWP?	40 pages with input/update capability
7	What is the estimated number of web pages in ORIS?	60 pages with input/update capability
8	Does Ohio DC currently leverage centralized firewall management tools for managing firewall rules and configurations?	Yes, Cisco ASDM
9	Does Ohio DC currently leverage a firewall rule optimization technology (e.g., AlgoSec, Tufin or Skybox)?	No
10	Please provide estimated number of NSG rules in Azure and firewall rules in Cisco ASA.	Azure firewall: 40 and Cisco ASA: 50
11	Approximately how many lines of code will be required to be reviewed for the PWP?	200,000
12	When is expected that the Ohio DC offices be available for a physical review given the current pandemic situation?	Its difficult to project this but hopefully by June 2021. It is possible for the vendor to have physical access prior to June with a very limited number of consultants (1-2). Maybe subject to change.
13	Can you please share the names of the vendors who sent in Letter of Intent?	Its Ohio DC practice to not share information about the vendors who have responded.
14	Is there an incumbent contractor performing this work?	Yes
15	Are the quarterly system vulnerability scan inclusive of all Program on-premises assets?	Yes

16	Will the Microsoft Azure Cloud environment be included in the quarterly vulnerability scans?	Yes
17	Due to COVID-19, do you anticipate resources to be remote? Vendor personnel may need to work remotely for extended periods of time and will use commercially reasonable efforts to mitigate any effects that remote work has on the performance of the services. Post COVID-19, do you anticipate resources to be onsite in Ohio?	Remote access is acceptable if the vendor has a strategy for completing a thorough assessment remotely
18	Will the vendor be responsible for providing security testing/assessment tools for use during the assessment or does the Program have security tools that can be utilized?	This will be the vendor's responsibility
20	Can remote access be provided for penetration testing from within the Program network, such as a Virtual Private Network (VPN) or jump server?	Yes
21	Has the PWP Application undergone a prior information security assessment and security code review? Or will this be the first such assessment?	PWP has undergone 2 penetration tests and 2 code reviews.
22	Can the vendor provide evidence of alternative cyber security leading practices in lieu of a SOC 2?	Yes - to be determined by Ohio DC
23	Does the Program have a collaboration space for the contractor to utilize in handling data and information to keep data and information secure?	Yes if access is avaiable due to COVID pandemic restrictiona
24	Can the Program provide equipment (e.g., laptops) or a Virtual Desktop Infrastructure (VDI) to the contractor for the technical assessment work? This will help ensure that all Program data is maintained inside the Program environment.	Yes, a VM or a limited number of laptops could be made available if needed.
25	Do you want an event and log analysis included as part of this assessment?	No
26	Is there a budget defined for the Network Security Assessment and if so, what is it?	There is a budgeted amount for the assessment but the amount will not be disclosed prior to the vendor selection
27	How many sites are expected to be visited as part of the Network Security Assessment (i.e., can all work be performed from a single location)?	One single physical location
28	a. Number of endpoints requiring access.	<50
29	# of Wired/# of Wireless/# of VPN	Varies depending on the number of employees/contractors working from home versus in the office.

30	b. Endpoint authentication mechanism (802.1X, MAC filter, Open Port, Captive Portal Redirect, PSK)	YES, we use one of the listed mechanisms
31	b cont.: If 802.1X – method? (EAP-TLS, EAP/PEAP-MSCHAPv2, etc.)	YES, we use one of the listed mechanisms
32	c. Endpoint/User Directory (AD, LDAP, Static List, Internal DB on Security Appliance)	AD
33	How many firewalls are in high availability?	2
34	Are virtual firewalls being used and if so how?	Yes - usage will be discussed with the vendor selected
36	Type of NAT being used per firewall?	This information will not be disclosed in a public document and will be discussed with the selected vendor.
37	Are the firewalls integrated with any user directories?	This information will not be disclosed in a public document and will be discussed with the selected vendor.
38	Are the firewalls integrated with any 3rd party tools?	Yes
39	Are the logs centralized and correlated?	No
40	What advanced features are utilized?	This information will not be disclosed in a public document and will be discussed with the selected vendor.
	Application Identification / Awareness	This information will not be disclosed in a public document and will be discussed with the selected vendor.
	User Identification / Awareness	This information will not be disclosed in a public document and will be discussed with the selected vendor.
	Anti-Virus	This information will not be disclosed in a public document and will be discussed with the selected vendor.
	Anti-Malware / APT	This information will not be disclosed in a public document and will be discussed with the selected vendor.
	IPS	This information will not be disclosed in a public document and will be discussed with the selected vendor.
	URL Filtering	This information will not be disclosed in a public document and will be discussed with the selected vendor.
	DLP	This information will not be disclosed in a public document and will be discussed with the selected vendor.
41	Please provide the vendor, vendor model, and quantity of IDP/IDS configuration	This information will not be disclosed in a public document and will be discussed with the selected vendor.
42	What type of IDP/IDS configuration is in use: Active Inline, Active Out of Band (SPAN/TAP), Passive Out of Band (SPAN/TAP)?	This information will not be disclosed in a public document and will be discussed with the selected vendor.

43	Please provide the vendor, vendor model, and quantity of your Network Access Control configuration	This information will not be disclosed in a public document and will be discussed with the selected vendor.
44	Please provide vendor, vendor model, and quantity of your router configuration	This information will not be disclosed in a public document and will be discussed with the selected vendor.
45	What routing protocol(s) is in use in router configuration?	This information will not be disclosed in a public document and will be discussed with the selected vendor.
46	Please provide the vendor, vendor model, and quantity of your VPN configuration	This information will not be disclosed in a public document and will be discussed with the selected vendor.
47	Please provide the vendor, vendor model, and quantity of your WLAN hardware:	This information will not be disclosed in a public document and will be discussed with the selected vendor.
48	What networking standards are use on WLAN hardware? (802.11 a, b, g, n, ac)	This information will not be disclosed in a public document and will be discussed with the selected vendor.
49	Please provide following operational parameters:	This information will not be disclosed in a public document and will be discussed with the selected vendor.
	a. WLAN Architectural/design location (core/distribution/access/redundancy)	This information will not be disclosed in a public document and will be discussed with the selected vendor.
	b. WLAN Operating mode (L2/L3)	This information will not be disclosed in a public document and will be discussed with the selected vendor.
50	Please provide information regarding any additional network-based security controls in use (content filtering, anti-spam, etc.)	This information will not be disclosed in a public document and will be discussed with the selected vendor.
51	What virtualization technology is being leveraged?	This information will not be disclosed in a public document and will be discussed with the selected vendor.
52	How many IPS firewall profiles/rules?	This information will not be disclosed in a public document and will be discussed with the selected vendor.
53	How many application layer filtering profiles/rules?	This information will not be disclosed in a public document and will be discussed with the selected vendor.
54	How many URL filtering profiles/rules?	This information will not be disclosed in a public document and will be discussed with the selected vendor.
55	How many AV profiles?	This information will not be disclosed in a public document and will be discussed with the selected vendor.
56	How many content filtering profiles?	This information will not be disclosed in a public document and will be discussed with the selected vendor.
57	How many DLP profiles?	This information will not be disclosed in a public document and will be discussed with the selected vendor.

58	How many APT rules?	This information will not be disclosed in a public document and will be discussed with the selected vendor.
59	How many external authentication systems are in use?	This information will not be disclosed in a public document and will be discussed with the selected vendor.
60	Are there policies in scope that are outside the realm of cybersecurity (E.g., Physical Security, Enterprise Resilience incl. BC/DR, Product Security, etc.)?	Please refer to RFP scope of services
61	This looks focused on unauthorized access, and the network security implications from that. Are you looking for a more holistic physical security review? For example, considering aspects such as workplace violence, environmental hazards, theft, and others - outside of just access to a physical site and its effect on the network access. Or just network security focused?	Please refer to RFP scope of services
62	The title says IR program, but the description is specific to the IR plan and BC/DR plan. Is the scope to review the entire IR program or is it limited to reviewing the IR and BC/DR plans.	Please refer to RFP scope of services
63	Is the scope of the review of the BCDR is resilient/secured against cyber-attacks in addition to physical/environmental outages?	Please refer to RFP scope of services
64	What mechanisms does Ohio DC currently leverage to deliver and manage completion of the security trainings to its employees?	KnowBe4 Training assigned quarterly and phishing tests performed monthly
65	Does the scope of the security awareness and training review extend to trainings for third party personnel, contractors, and vendors of Ohio DC?	No
66	Should the vendor provide the findings and results of the risk assessment against SPARK's data security control objectives or leveraging NIST Cybersecurity Framework? Please indicate if Ohio DC has a preferred standard for reporting results in order to be able to compare 2021 results with the output of 2019 risk assessment.	The SPARK data security control objectives were the basis of the previous risk assessment but portions of the NIST Cybersecurity Framework was used to validate the SPARK objectives
67	As part of obtaining buy-in from upper management for the IT strategic plan, is the vendor expected to conduct discussions with the members of the Board or is it limited to the Executive Director and staff?	Discussions will be limited to the ED and staff for the development of the plan. However, the vendor will be expected to participate with staff in presenting the plan to the Board.

68	Please describe the building (e.g., number of ingress/egress points, number of floors, are there armed guards?)	The building is a four story building with three physical entrances. The Ohio DC office is located on the fourth floor and can be accessed by either a stairwell or elevators. An unarmed security guard is posted outside the elevators and stairwell. The Ohio DC office is always locked and requires either a key card or a staff member to allow entrance.
69	How many lines of functional (.Net) code are there? (This excludes blank lines, comments, and spaces.)	Approximately 200,000
70	Can you tell us the size and scope of the IR team? (personnel and existing runbooks)	Ohio DC only has 23 employees. The IR team is made up of the 7 members of the management team
71	When was the IR plan last updated?	10/24/2019
72	Is any aspect of the Nationwide support in scope for this proposal? In other words, should we also be evaluating any of their security controls?	Nationwide support is out of scope
73	How many pages/screens does the web application have?	ORIS 60 pages and PWP 40 pages with input/update capability
74	How many input fields does the web application have?	PWP 150 ORIS 600
75	Does the application have any payment processing components?	No
76	What data connections does the web application use, if any (SQL, other REST API, etc.)?	SQL, REST API/WCF
77	Which third party frameworks or libraries are in use?	PWP: .Net / Angualr ORIS: .net, Razor, javascript, jquery
78	Is the organization already using any Application Security Testing tools?	No
79	What Interactive Development Environment (IDE) tool(s) are used for application development (For example Visual Studio)?	Visual Studio
80	What frameworks or libraries are used for development (For example NodeJS, Angular, .Net Core)?	PWP: .Net / Angualr ORIS: .net, Razor, javascript, jquery
81	What tools are used for Software Code Management (For example Git, SVN)?	Git
82	What, if any, build automation tools are used (For example Jenkins, Azure DevOps)?	Jenkins, Azure DevOps
83	What issue/bug tracking/ticketing tools are used (For example Jira)?	Azure DevOps
84	What is the typical release cadence for the application software?	Production support weekly, major releases monthly

85	How many modules or lines of code does the application have?	
86	What is the size of the software development team?	Currently there are 3 Ohio DC employed developers and 11 contractors
87	How many staff are in the organization?	23
88	Can you provide an organizational chart?	Yes
89	Is there an overall strategic plan for the organization?	Yes