ADDENDUM ONE
QUESTIONS AND ANSWERS

Date: July 12, 2021

To: All Bidders

From: Jennifer Crouse and Scott Hansen, Buyers
                Department of Health and Human Services

RE: Addendum for iServe Nebraska Portal Work Order #4

███

Questions and Answers

Following are the questions submitted and answers provided for the above mentioned Work Order (WO). The questions and answers are to be considered as part of the Work Order. It is the Bidder's responsibility to check the project information page for all addenda or amendments.

Question Number	Work Order Section Reference	Page #	Question	DHHS Response
1.	II. D.	5	Multiple roles/access levels that can provide or restrict access to different application functionality – please confirm/clarify that you are referring to access to the identity platform or to the application.	While DHHS assumes that the identity platform itself will have role-based controls, this requirement refers to roles in the application(s).
2.	II. D.	5	Is there a defined RBAC model for the application and for the management of the Azure AD B2C platform	DHHS assumes is Role Based Access Control. DHHS has one role expected for our MVP.

3.	II. D.	5	Identity proofing – is there a current standard for this capability. Is there a requirement to partner with a specific proofing service provider or perhaps an internal system at the State of Nebraska.	Identity proofing is outside the scope of this Work Order. References to identity proofing are provided for future context.
4.	II. D.	5	Is there a "system" external to Azure AD B2C that would be an authoritative source of identity. Is there another system or repository that will need to be integrated to Azure AD B2C	Azure AD B2C will be the authoritative source for customer/citizen identity. A possible integration could be with the existing Access Manager system.
5.	II. D.	5	Is there a current IAM provisioning process/solution for constituent services?	There is an existing process for provisioning identities in Access Manager. A new process will have to be developed for IAM provisioning with the new B2C platform.
6.	II. D.	5	Is there a current organization that does customer support – are there mature, documented processes?	Yes. Yes.
7.	II. D.	5	Is there Cyber Security policy or guidelines which must be incorporated?	Yes. Security guidelines from DHHS and OCIO will need to be incorporated.
8.	II. D.	5	There is mention of having different policy enforced based on access method (public web pages was an example) – do you have a list of conditions that need to be used to enforce policy?	There is no exhaustive list, but a common use case would be different levels of access driven by URL patterns.
9.	II. D.	5	There is mention of fine grain and coarse grain security checks – please clarify that these are not enforced by the identity platform. Would the IdP provides the data in the token which is then used for enforcement? Could this enforcement be split between Azure AD B2C and the application?	The identity platform would be responsible for creating a token including the appropriate claims or others parameters. The application would then be responsible for enforcing coarse-grained and fine-grained security based on the contents of the token.
10.	III	8	Is the "Stories" section of the tables relevant for this Work Order?	No. See Revised Work Order 4.

11.	II.D.	5	Can you verify that Access Manager Identity is the product provided by NetIQ?	Yes (although NetIQ is the old company name, now Micro Focus).
12.	II.D.	5	Should permissions reside in the app or within the identity system?	See answer to question #9.
13.	II.D.	5	Is there already an authorization scheme that Nebraska uses today?	Yes.
14.	II.D.	5	Are app roles specific to individual applications or are they common per user across applications?	For the scope of this Work Order there is only one application. Although there could be some overlap, in general, app roles will be specific to individual applications.
15.	II.D.	5	Is different information collected during authentication/registration into each app, or is it just building out a user's profile over the course of multiple logins to a common authentication endpoint?	For the scope of this Work Order there is only one application. Different apps could have unique information that needs to be collected during registration. Some of this data might be stored in the B2C platform, and some might be saved within each application.
16.	II.D.	5	What specific identity verification/proofing provider is Nebraska looking to use?	See answer to question #3.

This addendum will become part of the proposal and should be acknowledged with the Work Order response.