Following the Evaluation Phase, Vendors selected to move into negotiations will be requested to provide responses to the questions below using the yellow space provided by close of business on March 18, 2021. The information will be a part of the information used by the negotiation team in determining which Vendor offers the best value for Citizens.

**INSTRUCTIONS:** Vendors shall provide responses to the questions below using the yellow space provided. The space for answers will expand as necessary. Please be thorough but concise in your response. If an attachment (such as a product brochure) is referenced in the response to a question, the attachment should be provided in Adobe PDF format.

| **Section I – Infrastructure and Technical Architecture** |
| --- |
| 1. Describe the solution’s infrastructure architecture:    1. Cloud, hybrid, or client on-prem hosting?       1. Describe the resiliency architecture available, provide diagram if available.       2. Describe the process and timeframe to scale the solution for variable volume.    2. Describe any specific technical requirements or recommendations related to using the solution.       1. If applicable, include client-side technical requirements. i.e. browser configurations, add-ins, desktop software, etc.       2. If applicable, include server-side on-prem technical requirements, third party requirements, database type, operating systems, etc.    3. Does the solution support mobile devices? If so, please identify mobile app, responsive design, etc.    4. Are there any content or storage limitations that we should be aware of? i.e. Size limits for file uploads, file type exceptions, data purge schedules.    5. Is data encrypted at rest? In Transit?    6. Geographically, where are production and backup data stored? |
| Click here to enter text. |

|  |
| --- |
| **Section II – Integration** |
| 1. Describe the solution’s integration architecture. Include the following details:    1. Protocols supported/preferred (e.g. SOAP/REST, WS-I, sFTP, EDI etc.)    2. Does the solution have a shared/public API or are integrations customized for each customer? If applicable, describe your support for custom integrations.    3. Can all business data be accessed through your API or integration architecture? Is there any functionality/data that is not available?    4. Describe your experience integrating through middleware platforms. |
| Click here to enter text. |
| 1. Describe any prior experience integrating with the following:  * Guidewire (ClaimCenter or comparable Claims Management System) * Alfresco Document Management * Kaltura Media Management * Oracle Fusion ERP |
| Click here to enter text. |
| 1. Describe functionality and processes involved for secure transfer of large data sets to and from the solution, include information on the following:    1. Preferred protocols for passing large data sets    2. File format preferences    3. Availability of solution’s data dictionary and data models |
| Click here to enter text. |

|  |
| --- |
| **Section III – Access Control and Security** |
| 1. Describe the solution’s Access Control capabilities, include information on the following:    1. Ability to manage roles and apply permissions.    2. Ability to restrict access to fields, screens, administrative controls, etc.    3. Ability to restrict access so that a vendor (the firm and its users) cannot access another vendor’s data, while still allowing Citizens to see across all vendors    4. How is administrative access managed?    5. Describe your support for multifactor authentication (either natively or through integration with customer’s solution) |
| Click here to enter text. |
| 1. Describe the solutions ability to support federated authentication through Azure AD or other common authentication protocols (for example SAML, OpenID, etc.) |
| Click here to enter text. |
| 1. Describe the solutions ability to manage against cyber security attacks, include the following information:    1. Describe your cadence and process for security patching.    2. Describe your cadence for security testing including penetration attacks and vulnerability testing.    3. Describe your ability to secure data both in transit and at rest. Specifically describe the ability to encrypt restricted-confidential and confidential data (see definitions on last page)    4. Are all parts of the solution SOC 2 Type II certified? If so, will you provide Citizens with your SOC 2 reports? If not, which parts are not certified and what is the roadmap to achieve certification? |
| Click here to enter text. |
| 1. Describe the process and policies for auditing user access and changes to data.    1. What data points are captured for each log type? For example: date, time, username, content accessed, etc.    2. How would Citizens access audit logs?    3. What is the data retention policy for each type of log? |
| Click here to enter text. |
| 1. Describe the ability to protect the system from vulnerabilities that could be introduced due to file uploads? |
| Click here to enter text. |
| 1. Do you have an established Data Security Incident Response Plan?    1. How often is it tested?    2. How often is it revised?    3. How do you communicate with customers during a security incident? |
| Click here to enter text. |

| **Section IV – User Experience** |
| --- |
| 1. Describe the solutions ability to configure and optimize the user experience.    1. Describe features that optimize the user experience in data collection. (i.e. interaction controls such as auto-complete, data look-up etc.)    2. Describe features that optimize the user experience in screen flow.    3. Describe features that allow for style and branding.    4. How do you ensure compatibility and support for various platforms including browsers, mobile devices, etc.?    5. Describe the level of accessibility compliance, e.g. WCAG 2.0 A, AA, etc.    6. Describe reporting and analytics features. Can users access pre-built reports and dashboards? |
| Click here to enter text. |

| **Section V – Maintenance and Configuration** |
| --- |
| 1. What aspects of the Solution are configurable and to what extent can the solution be customized from within the application or through services.    1. Are configurations and/or customizations done by the vendor, the client or both? If by vendor, how are these communicated and coordinated and what are the SLAs associated to configuration changes?    2. How are the integrity of configurations and/or customizations kept during upgrades/releases? |
| Click here to enter text. |
| 1. Describe your release schedule and processes for making releases/features available to your customers. 2. Will releases be available in a test environment ahead of production release? If so, how long do customers have to test? 3. What are the expectations, if any, for post release (non-business hours) UAT from Citizens? |
| Click here to enter text. |

| **Section VI – Resiliency and Business Continuity** |
| --- |
| 1. Describe the Solution’s performance/health metrics and reporting capabilities.    1. Describe the RPO (Recovery Point Objectives) and RTO (Recovery Time Objective).    2. How often do you test resiliency scenarios?    3. How are customers alerted to performance/health degradation?    4. Describe your current replication, backup and restore processes. |
| Click here to enter text. |
| 1. Describe your process for ensuring quality during implementation and future enhancements, i.e. testing practices and processes. 2. What are your internal processes to ensure quality for post implementation releases including ensuring integrity of configurations and customizations made for Citizens? 3. How many test environments are available to the client? Are there any restrictions to test environment access? 4. Are releases made available to client test sites ahead of releases? 5. Explain how you can support integration with Citizens non-production environments. 6. Describe the process for defect tracking and resolution. Describe both implementation and post-implementation processes, if different. |
| Click here to enter text. |
| 1. Does the solution have any specific data retention and deletion guidelines that we should be aware of? How long would Citizens be able to keep both structured and unstructured data in the solution? How is data disposed of or destructed? |
| Click here to enter text. |
| 1. How is data being backed up? How do you protect against data loss events? |
| Click here to enter text. |
| 1. Describe any data security events that have occurred since January 1, 2019. For employees who work remotely, how do you monitor company provided hardware vs. personal hardware to protect the client from data breeches. |
|  |

**Data Classification Definitions (see Question 7c)**

**Restricted Confidential Information**

Restricted Confidential information is highly sensitive, personally identifiable information that, if lost, compromised or disclosed without authorization, could result in substantial harm, inconvenience or unfairness to an individual or to Citizens. Restricted Confidential information must be protected due to legal, regulatory or contractual requirements. The following information, when in combination with a first name or initial and last name, is Restricted Confidential:

* Social Security numbers
* Driver’s license or any other government identification numbers
* Non-citizens financial account numbers in combination with any required security code, access code, or password that is necessary to permit access to a financial account
* Medical treatment information or account numbers
* A username or e-mail address, in combination with a password or security question and answer that would permit access to an online account

**Confidential Information**

Confidential information is personally identifiable information or other information that does not meet the definition of Restricted Confidential information, but that, if lost, compromised or disclosed without authorization, has the potential to cause harm to individuals or to Citizens. Information that is protected from public records disclosure under section 627.351(6)(x), Florida Statutes (Citizens’ enabling statute), or any other rule or law, will be classified as Confidential, unless it meets the definition of Restricted Confidential information.

Examples include, but are not limited to:

* Information contained in underwriting and claims files
* Policyholder names, addresses, phone numbers and email addresses
* Exam questions and answers created or used for licensure, certification or employment
* Proprietary and confidential information licensed to Citizens under contract, trade secret information, or other confidential information provided to Citizens by its business partners
* Records or information related to internal audit, risk assessments, vulnerabilities, data incident response or other aspects of Citizens’ information security program the disclosure of which would facilitate unauthorized access, modification, disclosure or destruction of information resources