Following the Evaluation Phase, Vendors selected to move into negotiations will be requested to provide responses to the questions below by close of business on April 29, 2022. The information will be a part of the information used by the negotiations 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. Be thorough but concise in providing responses. If an attachment (such as a product brochure) is referenced in the response to a question, the attachment must 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 such as browser configurations, add-ins, and desktop software.       2. If applicable, include server-side on-prem technical requirements such as third party requirements, database type, and operating systems.    3. Does the solution support mobile devices? If so, describe technical specifications of the mobile app such as responsive design.   Are there any content or storage limitations such as size limits for file uploads, file type exceptions, data purge schedules?   * 1. Will Citizens’ data be stored in the solution? If so…      1. Describe how Citizens will have access to data and describe methods for access.      2. Describe any data retention restrictions regarding how long the data will be stored in the solution.      3. Describe where, geographically, the data will be stored.   2. Provide a Software Bill of Materials. |
| Click here to enter text. |

|  |
| --- |
| **Section II – Integration** |
| 1. Describe the solution’s integration architecture. Include the following details:    1. Protocols supported/preferred such as SOAP/REST, WS-I, sFTP, EDI.    2. Does the solution have a shared/public API or are integrations customized for each customer? If applicable, describe Vendor’s support for custom integrations.    3. Can all business data be accessed through the API or integration architecture? Is there any functionality/data that is not available?    4. Describe Vendor’s 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) * 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.    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 Vendor’s support for multifactor authentication (either natively or through integration with customer’s solution). |
| Click here to enter text. |
| 1. Describe the solution’s ability to support federated authentication through Azure AD or other common authentication protocols (for example SAML, OpenID). |
| Click here to enter text. |
| 1. Describe the solution’s ability to manage against cyber security attacks, include the following information:    1. Describe Vendor’s cadence and process for security patching.    2. Describe Vendor’s cadence for security testing including penetration attacks and vulnerability testing.    3. Describe Vendor’s 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. Does Vendor have a SOC 2 Type II report? If so, are all parts of the solution SOC 2 Type II certified? If all parts are not certified, which parts are not certified and what is the roadmap to achieve certification? In Vendor’s response to this questionnaire, include the most recent SOC 2 Type II report if available and, as applicable, include a bridge letter. |
| 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.    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 solution from vulnerabilities that could be introduced due to file uploads? |
| Click here to enter text. |
| 1. Does Vendor have an established data security incident response plan?    1. How often is it tested?    2. How often is it revised?    3. How does Vendor communicate with customers during a security incident? |
| Click here to enter text. |

| **Section IV – User Experience** |
| --- |
| 1. Describe the solution’s ability to configure and optimize the user experience.    1. Describe features that optimize the user experience in data collection (such as interaction controls such as auto-complete, data look-up).    2. Describe features that optimize the user experience in screen flow.    3. Describe features that allow for style and branding.    4. How does Vendor ensure compatibility and support for various platforms including browsers, mobile devices?    5. Describe the level of accessibility compliance such as WCAG 2.0 A, AA.    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 Vendor, the client or both? If by Vendor, how are these communicated and coordinated and what are the service levels associated with configuration changes?    2. How are the integrity of configurations and/or customizations kept during upgrades/releases? |
| Click here to enter text. |
| 1. Describe Vendor’s release schedule and processes for making releases/features available to customers.    1. Will releases be available in a test environment ahead of production release? If so, how long do customers have to test?    2. 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 Vendor’s solution availability service level, specifically RPO and RTO service levels. |
| Click here to enter text. |
| 1. Describe the architecture and supportive infrastructure implemented to deliver a resilient and recoverable solution that provides high availability and data loss protection. |
| Click here to enter text. |
| 1. Describe Vendor’s solution’s replication and/or backup strategies to ensure high availability and avoid data loss. |
| Click here to enter text. |
| 1. Describe what components are being replicated and/or backed up, their scheduled frequency, and the capability for how Vendor’s solution will restore/recover in the event of data corruption, cyber security, and/or accidental deletion incident. |
| Click here to enter text. |
| 1. Describe how Vendor’s solution leverages strategic partners, external vendors and/or service providers to deliver the service capabilities defined in Vendor’s proposal? To what extent are they integral to the delivery of the proposed solution? What are the mitigation strategies in place to address disruptions with strategic partnerships? |
| Click here to enter text. |
| 1. Describe the approach used to proactively monitor and alert interested parties of an anomaly that could adversely affect availability of Vendor’s proposed solution. |
| Click here to enter text. |
| 1. Describe Vendor’s approach to ensure business continuity capabilities for Vendor’s solution if there is an event that impacts a strategic location, facility, power/communications utility, service provider, critical system(s), and/or key personnel. |
| Click here to enter text. |
| 1. Describe Vendor’s approach for providing disaster recovery capabilities for Vendor’s solution to respond to a significant technology-based disruption. |
| Click here to enter text. |
| 1. What is the frequency by which Vendor conducts validation exercising for business continuity and disaster recovery and how does Vendor provide the results to the customer? Can the customer participate in the validation exercises? |
| Click here to enter text. |
| 1. Describe the crisis management/crisis communication protocol that will be used to communicate with the customer in the event of a crisis/business interruption while using Vendor’s proposed solution. |
| Click here to enter text. |

**Data Classification Definitions (see Section III.G.c)**

**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