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 January 29, 2021. 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:** The space for answers will expand as necessary. Answers should be specific to the proposed Solution functionality described in Attachment E. Please be thorough but concise in your response. ***The entire response, excluding attachments, should not exceed twenty-five (25) pages.*** 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. Include client-side technical requirements. i.e. Browser configurations, add-ins, desktop software, etc.       2. Include server-side technical requirements, third party requirements, database type, operating systems, etc. |
| Click or tap 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. Support for custom integrations    3. Describe your experience integrating through middleware platforms. |
| Click or tap here to enter text. |
| 1. Describe any prior experience integrating with the following:  * Guidewire BillingCenter®, Guidewire ClaimCenter® |
| Click or tap 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: |
| Click or tap here to enter text. |

|  |
| --- |
| **Section III – Access Control and Security** |
| 1. Describe the solution’s Access Control capabilities, include information on the following and identify if the capability is achieved through configuration or customization:    1. Ability to manage roles and apply permissions.    2. Ability to restrict access to fields, screens, administrative controls, etc. |
| Click or tap here to enter text. |
| 1. Describe the solutions ability to support for SSO and 3rd party authentication integrations and supported protocols i.e. SAML. |
| Click or tap here to enter text. |
| 1. Describe your security management procedures, 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)* |
| Click or tap 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 for all information described?    3. How often are each type of log purged? |
| Click or tap 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?    5. Describe the level of accessibility compliance, e.g. WCAG 2.0 A, AA, etc. |
| Click or tap 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?    2. How are the integrity of configurations and/or customizations kept during upgrades? |
| Click or tap here to enter text. |
| 1. Describe the Solution’s performance/health metrics and reporting capabilities. **(Cloud Options Only)**    1. How are customers alerted to performance/health degradation?    2. Describe the RPO (Recovery Point Objectives) and RTO (Recovery Time Objective).    3. Describe the resiliency architecture related to the solution. i.e. High Availability, Warm Disaster Recovery, etc.    4. How often do you test resiliency scenarios?    5. Describe procedures related to back up and restores. |
| Click or tap here to enter text. |
| 1. Describe your process for ensuring quality during implementation, i.e. testing practices and processes.    1. What are your internal process to ensure quality for post implementation releases including ensuring integrity of configurations and customizations made for Citizens?    2. What and how many test environments are available to the client?    3. Are releases made available to client test sites ahead of releases?    4. Explain how you can support integration with Citizens non-production environments.    5. Describe the process for defect tracking and resolution. Describe both implementation and post-implementation processes, if different. |
| Click or tap here to enter text. |

**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