**INSTRUCTIONS:** This Questionnaire must be completed and submitted according to Section 3.6 of the ITN. See Section 3.7 of the ITN for additional information on the evaluation process. Vendor Replies will be evaluated and scored based on the following table:

|  |  |  |
| --- | --- | --- |
| **ATTACHMENT** | **EVALUATION CRITERIA** | **MAXIMUM Points** |
| G | Technology Questionnaire | General Questions | 5 |
| Integration | 5 |
| Access Control and Security | 4 |
| User Experience | 4 |
| Maintenance and Configuration | 3 |
| Service Levels | 2 |
| Testing | 2 |
| **Total Points:** |  | **25** |

Vendors shall provide responses to the questions below using the yellow space provided. The space for answers will expand as necessary. Answers must be specific to the proposed System 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 – General Questions (Up to 5 points)** |
| --- |
| 1. Describe any required or optional server-side or client-side installable components (i.e. Browser components, add-ins, desktop software, etc. Include any minimum system requirements, third party requirements, i.e. database type, operating systems, etc.).
 |
| Click here to enter text. |
| 1. Provide a high-level System architecture diagram. Include descriptions for primary, lower and recovery data centers. Citizen’s preference is Cloud/SaaS based solutions. Hybrid models could be considered, but the goal is to minimize Citizen's internal infrastructure footprint. For Cloud solutions, the data would need to be stored in the United States.
 |
| Click here to enter text. |
| 1. What is your preferred file format(s) for incoming data? Provide a list of file formats supported by the proposed System for storage and access from within the System. Describe any limitations to size and/or formats supported by the System.
 |
| Click here to enter text. |
| 1. Describe the ability and requirements for the System to scale to meet changes in volume over time.
 |
| Click here to enter text. |
| 1. Explain in detail various infrastructure related quality of service elements. Such as load balancing, high availability, fault tolerance, fail over, session replication, transaction support, etc.
 |
| Click here to enter text. |

|  |
| --- |
| **Section II – Integration (Up to 5 points)** |
| 1. Describe your capabilities to support third party API integrations
 |
| Click here to enter text. |
| 1. Describe any prior experience integrating with the following:
* Guidewire Suite – (PolicyCenter, ClaimsCenter and BillingCenter)
* Outside counsel billing systems
 |
| Click here to enter text. |
| 1. Web Services. Are WS-I compliant web services supported? Provide details on web service support and respective WS Security items.
 |
| Click here to enter text. |
| 1. Describe functionality and processes involved for Citizens to extract data individually or in a batch. Please include a list of approved ETL tools, any event trigger mechanisms, and automation.
 |
| Click here to enter text. |
| 1. Describe the various integration mechanisms supported by the System, and the scope of these mechanisms within the System. Such as web services (SOAP/REST), messaging, MFT, etc.
 |
| Click here to enter text. |
| 1. What capability does the System have to perform callouts to external systems to retrieve data, invoke external processes, etc.? What are the integration requirements?
 |
| Click here to enter text. |
| 1. Is the System certified to work with commonly used middleware products such as Oracle Fusion Middleware (OSB/SOA)? Provide a list of all those products. What level of SOA support is provided by the System? Ability to present business functions as reusable service, synchronous and asynchronous communication, extensibility, etc.
 |
| Click here to enter text. |

|  |
| --- |
| **Section III – Access Control and Security (Up to 4 points)** |
| 1. Describe the System’s ability to protect data at rest and in transit. Also, describe how data classified as ‘Restricted-Confidential ‘or ‘confidential’ is protected (see definitions at the end of the questionnaire).
 |
| Click here to enter text. |
| 1. Describe the system’s access policies and abilities to apply those policies. (i.e. Automatic password resets every xx calendar days, use of multi-factor authentication, etc.)
 |
| Click here to enter text. |
| 1. What is the security patch policy and process?
 |
| Click here to enter text. |
| 1. How often is the System tested for security vulnerabilities and penetration attacks? Provide details.
 |
| Click here to enter text. |
| 1. Explain how user information for the System is stored, or mechanisms available for integration?
 |
| Click here to enter text. |
| 1. Can the System integrate with any third party SSO (single sign-on) solutions? Does it utilize SAML 2.0 and/or any other type of "modern authentication?
 |
| Click here to enter text. |
| 1. Describe how the System integrates with a custom authentication solution using web services. [Note: Citizens provides a set of authentication API as secure (WS-Security) web services].
 |
| Click here to enter text. |
| 1. How are the authorization of the user (access rights, etc.) handled by the System? Describe how much is configurable and customizable.
 |
| Click here to enter text. |
| 1. Describe how system access is logged and describe the level of detail of information logged, e.g. username, login time, content accessed, etc.Do you use SIEM integration for monitoring?
 |
| Click here to enter text. |
| 1. Describe what level of access an administrator user has to the system and what type of access they have to content.
 |
| Click here to enter text. |
| 1. Is your product SOC 2 Type II certified? If so, will you provide Citizens with your SOC 2 reports?
 |
| Click here to enter text. |
| 1. Describe your process and policies for access and user management. i.e. If access is vendor managed, how often are access reviews are performed to identify and disable stale accounts? If access is client managed, describe reporting/alerting capabilities surrounding access and user management.
 |
| Click here to enter text. |
| 1. Describe your procedures for incident response. (i.e. How are you monitoring for breeches? What is your process for notifying customers of a breech? How do you test your incident response plan? Etc.)
 |
| Click here to enter text. |

| **Section IV – User Experience (Up to 4 points)** |
| --- |
| 1. Describe the proposed System's capabilities that align with the functionality in the User Experience section of Attachment E.
 |
| Click here to enter text. |
| 1. For browser-based system access, describe your methodology for maintaining cross-browser compatibility and support for browser upgrades.
 |
| Click here to enter text. |
| 1. Please describe any features the proposed solution has in terms of accessibility compliance, e.g. WCAG 2.0, 2.1, etc
 |
| Click here to enter text. |

| **Section V – Maintenance and Configuration (Up to 3 points)** |
| --- |
| 1. Describe professional service practices you provide including your change management process for system enhancements. Including how changes are initiated, pricing process, and process for changing service level deliverables.
 |
| Click here to enter text. |
| 1. Provide your release schedule and describe how customers are notified of upcoming releases. Also, how much advance notice is provided for upcoming releases?
 |
| Click here to enter text. |
| 1. Describe what aspects of the System are configurable from within the application or service.
 |
| Click here to enter text. |
| 1. Describe what aspects of the System can be customized (via custom coding) for Citizens (by Vendor staff or by Internal Staff).
 |
| Click here to enter text. |

| **Section VI – Service Level (Up to 2 points)** |
| --- |
| 1. Describe the System’s performance/health metrics reporting capabilities.
 |
| Click here to enter text. |
| 1. Describe the System’s ability to alert on service performance. How selective can SLA monitoring be for a given service?
 |
| Click here to enter text. |
| 1. Describe what kind of information is logged and maintained. Explain the purge process and audit logs.
 |
| Click here to enter text. |
| 1. Describe any business activity logging, auditing or monitoring support provided by the System.
 |
| Click here to enter text. |
| 1. Describe your disaster recovery capabilities. Include how often you test and validate your disaster recovery strategy and the results of the last test. Describe the RPO (Recovery Point Objectives) and RTO (Recovery Time Objective)?
 |
| Click here to enter text. |
| 1. Describe your back up and restore procedures.
 |
| Click here to enter text. |
| 1. How often do you perform your Disaster Recovery testing?
 |
| Click here to enter text. |

| **Section VII – Testing (Up to 2 points)** |
| --- |
| 1. Describe the test environments that would be provided and the availability of these environments to Citizens. In addition, provide details of how many environments would be provided. Describe functional testing protocols and test environment architecture. Explain how you can support integration with Citizens non-production environments.
 |
| Click here to enter text. |
| 1. Describe the proposed System’s testing and validation processes, including unit, functional, regression and performance testing (including both manual and automated tests). Include all tools used and the process for defect tracking and resolution. Describe both implementation and post-implementation processes, if different.
 |
| Click here to enter text. |
| 1. Describe your performance test strategy (both pre- and post- implementation).
 |
| Click here to enter text. |

**Data Classification Definitions (see Question 9)**

**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 user name 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