**Solution Description and Pricing**

1. Please provide a general description of your proposed solution based on OCERS requirements for the application as stated above.
2. For cloud and on premise, please provide a breakdown of the pricing for the proposed solution(s). Specifically for on premise, please differentiate between hardware, software licensing, subscription, professional service, support and maintenance costs.
3. Please indicate if third party applications and/or services are required for the solution to function correctly, as well as who is responsible for purchasing and maintaining the associated licenses or subscriptions.

**Product History, Roadmap and Updates**

1. Please describe the history of the proposed application offering(s), including initial release date, current version number and brief development history.
2. Please provide information on the product development roadmaps for the proposed solution.
3. Please describe the process of new version releases, release cadence or timing, and the application of software updates to the application(s).
4. Please describe the quality assurance/testing processes to follow to determine whether a new cloud version, or an upgrade or custom modification, is suitable for release.
5. Please describe the process by which opportunities for system enhancements are identified, screened, programmed, field tested and released to customers.
6. Please describe whether the upgrade methodology includes a tracking system not only to report on the status of the upgrade, but also to record problems and bugs.

**Product Support and Service Warranty**

1. Please describe the support offerings available for proposed solution and the associated costs.
2. Please provide copies and descriptions of all warranties associated with the proposed solution and related applications.

**Training, Skillset and Customer Success**

1. Please describe the training and associated pricing of training that would be required/recommended for OCERS staff to complete to effectively implement and use the proposed solution. Please include required/recommended training for administrators, power users, and standard users.
2. Please describe the skills and typical job positions OCERS will need to implement, support, and use the proposed solution.
3. Please describe the extent and scope of post sales services available for supporting usage and adoption of the proposed solution.

**Security Frameworks, Controls and Regulations**

1. What control and compliance frameworks does your company adhere to (ISO, NIST, COBIT, CSA, HITRUST, etc.)?
2. What data security regulations does your company adhere to (PCI-DSS, HIPAA, GDPR, CCPA, GLBA, FISMA, etc.)?

**System Availability**

1. How do you calculate the average monthly uptime / availability rate of your solution?
2. Do you distinguish between the systems being “up” vs. being “available”?
3. What is the average monthly uptime / availability rate for the proposed solution for the past 12 months?
4. Please describe the resiliency and availability capabilities of the proposed solution. Please note any single points of failure.
5. In the past two years, how many service outages has the proposed solution experienced, and what was the longest period of downtime?
6. Please describe the proposed solutions maintenance schedule and how that may impact availability.
7. How long in advance are customers notified of scheduled maintenance windows and the subsequent estimated downtime?

**Service Level Agreements**

1. Please provide details of your service-level agreements (SLAs), including system availability, system response times, and support ticket resolution times.
2. Please outline the available service levels, the contractually defined response and resolution times for each service level, and the associated costs.
3. What are the penalties for nonperformance according to your SLAs?
4. Are there any penalties for delayed or degraded performance?
5. Do you provide an uptime / availability guarantee?
6. Describe the protections available for customers against loss of data or data integrity issues?
7. Do you automatically notify customers of an SLA miss?
8. What is the notification window for a customer to submit a SLA claim miss? See above
9. Please provide the documented procedure for escalation if SLAs are not met.

**Service and Support**

1. Please provide details on the available professional services implementation and deployment offerings with associated costs.
2. Please provide details on the available post-implementation support offerings and associated costs.
3. What methods are available for contacting technical support?
4. Do you offer a dashboard that shows service health?
5. Do you provide system usage and tracking tools?
6. Will we be assigned a dedicated support manager and account representative?
7. Do you have documented change management procedures?
8. Do you have documented incident prioritization procedures?
9. Describe available migration support to and from your services?
10. What support do you provide for third-party application integrations?
11. What is the process for making feature / enhancement suggestions?
12. Do you have a customer advisory panel?

**Security Assessments**

1. Please provide a copy of your most recent SOC 2 Type 2 report.
2. How often is your organization assessed by an independent third party and a SOC 2 Type 2 report generated?
3. Besides SOC 2 assessments, what other assessments, audits, or penetration tests are performed on your systems? Please state the frequency for each.
4. Do you provide your customer’s (or their designee’s) with the right to audit your systems? If so, how many audits are permitted within a 12 month period?

**Personnel Management**

1. What is the name of your company’s Chief Information Security Officer or security lead?
2. Does your company have a dedicated Information Security department?
3. Do you outsource any of your Information Technology or Information Security functions? If so, what is outsourced?
4. Do you conduct background checks on employees, contractors and consultants?
5. Do you conduct annual mandatory security awareness training for all users of your systems?
6. How do you assess your employee’s understanding of your security policies?

**Risk Management**

1. Does your company have a formal risk management program in place? If so, please describe.
2. Do you have cybersecurity insurance? If so, how much? Additionally, are customers a beneficiary of this insurance too in the event of an insurance reimbursable breach?

**Vendor / Third Party Risk Management**

1. Please describe the reliance you have on other third party suppliers to properly deliver the proposed solution.
2. Please describe the controls you have in place to ensure the failure of a third party to perform their duties does not impact your ability to deliver the proposed solution.

**Data Security and Privacy**

1. Describe the measures your organization takes to ensure data security to protect customer information.
2. What data encryption and security protocols are used to enable clients to protect their data?
3. Please describe the process, noting your security protocols, for how data is uploaded and transferred from your clients to you, and how it is eventually stored in a protected format on your system(s).
4. For primary (production), secondary (test), and tertiary (backup) copies of the data, in which cities, states, and countries is the data stored?
5. What controls are in place to keep client data segregated if the proposed solution is a multitenant environment?
6. Will any personnel from your company have the ability to access our data? If so, please list which job roles and how many individuals may have access to our data.
7. What protocols and security measures are in place so that only authorized individuals from your company have access to our data? How do you prevent authorized individuals from unauthorized access to our data?
8. Does the proposed solution have data loss prevention (DLP) capabilities that can be configured by the customer?
9. What are the defined retention periods for customer data? Can the retention periods be configured by the customer?
10. Please describe the tools and processes for archiving historical data from the solution.
11. Please describe the tools and processes for data destruction and secure deletion when data is purged from the solution. Is a certificate of destruction provided?
12. How are data access requests from law enforcement handled?
13. Does all ownership rights to data, inputs and outputs remain with the customer for the proposed solution?

**Security Incident and Response**

1. Please provide a copy of your incident response policy/plan.
2. Please provide a copy of your breach disclosure policy.
3. Please describe the systems and processes you have in place to detect security incidents.
4. Is security monitoring performed by in-house personnel, third party personnel, or a mixture of both?
5. What criteria do you use to determine whether your customers should be notified of a security incident?
6. How and when are customers notified of security incidents?
7. Please describe how you conduct security incident investigations, capturing of evidence, and the forensic collection process.

**Vulnerability Management**

1. Please identify the methods, processes, and frequency associated with identifying vulnerabilities within your corporate networks and within the proposed solution.
2. When security vulnerabilities are identified in the proposed solution, please indicate the process and expected timelines to remediate the vulnerabilities.
3. Please explain who is expected to pay (customer or vendor) for vulnerability scanning / penetration testing of the proposed solution, as well as who is expected to pay for remediation of any vulnerabilities identified.

**Business Continuity**

1. Do you have a business continuity / disaster recovery plan for the products and services we would receive from you? If so, how often is it reviewed, updated, and tested?
2. Does your Business Continuity Disaster Recovery plan address loss of technology, loss of resources, loss of facilities, and loss of suppliers?
3. Please provide a documented copy of your business continuity / disaster recovery plans, including target periods for recovery point objective (RPO) and recovery time objective (RTO).
4. In the past 12 months, have you conducted an employee Business Continuity / Disaster Recovery training exercise of the systems needed to provide your product and/or services? If so, can you share the results and areas for improvement?
5. How do you communicate to your clients during a disruption of service?
6. Do you evaluate your suppliers’ preparedness as part of your business continuity or risk management functions?
7. What reliance do you have on third parties for the proper execution of recovery when there is a disruption in service?
8. If your service is limited due to a disruption, how will clients be prioritized for service restoration?
9. Is your organization able to operate effectively when key locations are closed?
10. Please describe your backup policy and strategy.
11. How is data replicated, are online and offline backups maintained, how many copies of the data are created, where are backup data sources stored, in what format is backup data stored, and how is backup data recovered?

**Vendor Contacts and Communications**

1. Please identify the process and the contact(s) for resolving all of the following issues:

* Contract/SLA issues
* Technical support issues
* Degraded quality of service and outage issues
* Feature enhancement requests
* Billing/accounting issues

**Termination of Service**

1. If a client’s contract with you expires or if a client terminates their contract with you, is their data destroyed or returned to the client?
2. If data is returned to the client, please describe the process and tools used to retrieve the data, as well as the format of the data when it is returned.
3. What provisions exist if your business terminates, is purchased or merges with another company during the term of the contract?

**Architecture and Infrastructure**

1. Please describe the overall architecture of the proposed solution.
2. Please how the solution will be delivered (cloud, on-premises, hosted or hybrid).
3. If it is a cloud solution, please describe the solution model. For example, the type of cloud (public, private or hybrid, single or multitenant database, etc.).
4. Please identify the number, locations, and ownership of data centers from which the solution is hosted/managed. If third-party public cloud infrastructure as a service (IaaS) providers are used, please name the vendors and describe the nature of the relationship.
5. Are systems that comprise the proposed solution solely managed by your company, solely by a third party, or by a combination of the two?
6. Does your infrastructure (including backup and disaster recovery) reside solely in the United States? Do you have components of the proposed solution that reside outside the United States?
7. How do users access the system (web browser, client application, other)? If accessed through a web browser, is there a preferred browser to use?
8. How many concurrent users can the proposed solution support?

**Network**

1. What is your approach to network capacity planning for the proposed solution?
2. Please describe your support for integration with cloud security gateway and/or cloud access security broker technologies.
3. Do you support the ability to connect our network directly to your network to bypass the internet?
4. Do you utilize a content delivery network (CDN) as part of the proposed solution?
5. Do you have distributed denial of service (DDoS) prevention capabilities?
6. Is all data in transit encrypted (TLS 1.2 or greater)?
7. Do you support geo-fencing to allow access to the proposed solution only from certain countries?

**Storage**

1. Please describe encryption options for protecting data at rest.
2. Please identify the available options for encryption key management.
3. Are there any storage limits for the proposed solution?
4. If there are storage limits, is it possible to surpass the storage limits, and are there any additional costs?
5. What data archiving options are available to the customer?
6. Do you provide e-discovery capabilities so we can search and extract relevant data as necessary?

**Integration**

1. Please describe the API(s) associated with the proposed solution.
2. Please identify if the API(s) can be used by the customer for data access, business functions, operational functions, user management and data import/export.
3. Do you offer an API developer portal?
4. Does the proposed solution provide native application connectors to common desktop applications?

**Identity & Access Management**

1. Please describe authentication controls and levels of security associated with the proposed solution.
2. Please describe how usernames and passwords are managed in the system.
3. Does the system natively support two-factor or multi-factor authentication?
4. Does the proposed solution support federation with external Single Sign-On (SSO) systems using SAML and/or OpenID?
5. Does the proposed solution support batch import / bulk upload of user accounts?
6. Does the proposed solution support directory synchronization with on premise systems such as Active Directory?

**User Permissions and Roles**

1. Does the system support users with different user profiles depending on their functions? Explain how your system supports each of these user profiles.
2. How many unique roles are included in the default configuration? What permissions does each role have within the system?
3. Does the proposed solution support the creation of custom roles and permissions? If so, are those configured by the vendor or the customer?

**Auditing and Logging**

1. Please describe the logging level / audit trail associated with user activity in the proposed solution.
2. Please describe any syslog type functionality for customers to send logs continuously to external sources (e.g. monitoring system, SIEM, etc.).
3. Can the logs be exported, and if so, in what format?