APPENDIX B - Proposed Solution Requirements Questionnaire

Project Name:

Vendor:

The table lists all of the functional and technical critical requirements, including Optional items JEA is interested in.

1. **ALL ITEMS MUST BE ADDRESSED INDIVIDUALLY AND NO BLANKET RESPONSE TO ALL ITEMS WILL BE ACCEPTED.**
2. **FM/PM/NM -The Respondent must specify if the solution meets the requirement fully (FM – Fully Meet), partially (PM - Partially Meet), or not at all (NM - Not Met.).**
3. **State specific evidence in the "Vendor Evidence" column to allow a determination to made. Failure to complete will be deemed as "NM – Not Met".**
4. **Security controls MUST be equal to or greater than the controls JEA implements to be considered PM or FM.**
5. **ALL QUESTIONS MUST BE COMPLETED BY ALL RESPONDEDENTS PROPOSING A CLOUD, OUTSOURCED OR MANAGED SERVICES SOLUTION.**

Requirement Category	Item	Cloud Item #	Vendor NM/PM/FM Rating (See Next 3 Columns)	NM - "Not Met" Definition (0)	PM - "Partially Met" Definition (1)	FM - "Fully Met" Definition (2)	Vendor Evidence
MINIMUM QUALIFICATION This section lists the Critical requirements that each Respondent must meet.	**PROVIDE REPORT WITH BID** The Company must be SOC 2 Type 2, OR ISO 27001, OR other relevant security related assessment compliant (An auditor's report or independent third party assessment report will be required annually).	1		The provider says nothing on internal control assessments, or states that assessments or audits may be negotiated if the customer pays and both parties agree to the scope of the assessment or audit.	N/A	The company is SOC 2 Type 2 or ISO 27001 Compliant OR the Company is compliant with another relevant security related assessment, and has provided a certificate and an Auditor's Report, or the company has provided an independent third party assessment report.	
	PROVIDE DECLARATION WITH BID The Company Data must only be stored within the Continental United States.	2		The provider is silent on data storage location or the documentation states that data is either stored or backed up outside the Continental United States.	N/A	The Cloud provider contractually commits to keeping personal information in your geographic region, or in an area within the Continental United States with local laws at least as strenuous.	

Requirement Category	Item	Cloud Item #	Vendor NM/PM/FM Rating (See Next 3 Columns)	NM - "Not Met" Definition (0)	PM - "Partially Met" Definition (1)	FM - "Fully Met" Definition (2)	Vendor Evidence
REQUIREMENTS **Solution must have as part of their proposal.** **nts should be listed in the appropriate field in this document.** **ormation Security Policy, Procedures and Practices to be acceptable.** **dures and practices regarding:**	**Secure Messaging**	3		The provider says nothing about their policy.	Provider describes, in the vendor evidence column, their policy and/or procedures and how they apply.	The provider complies with Partially Meets (PM) AND the actual policy or procedure document is provided.	
	Identity and Access Management	4		The provider says nothing about their policy.	Provider describes, in the vendor evidence column, their policy and/or procedures and how they apply.	The provider complies with Partially Meets (PM) AND the actual policy or procedure document is provided.	
	Data Ownership	5		The provider says nothing about their policy.	Provider describes, in the vendor evidence column, their policy and/or procedures and how they apply.	The provider complies with Partially Meets (PM) AND the actual policy or procedure document is provided.	
	Data Sharing	6		The provider says nothing about their policy.	Provider describes, in the vendor evidence column, their policy and/or procedures and how they apply.	The provider complies with Partially Meets (PM) AND the actual policy or procedure document is provided.	
	Data Storage (At Rest Encryption)	7		The provider says nothing about their policy.	Provider describes, in the vendor evidence column, their policy and/or procedures and how they apply.	The provider complies with Partially Meets (PM) AND the actual policy or procedure document is provided.	
	Data Transfer (In Transit Encryption)	8		The provider says nothing about their policy.	Provider describes, in the vendor evidence column, their policy and/or procedures and how they apply.	The provider complies with Partially Meets (PM) AND the actual policy or procedure document is provided.	
	Data Retention	9		The provider says nothing about their policy.	Provider describes, in the vendor evidence column, their policy and/or procedures and how they apply.	The provider complies with Partially Meets (PM) AND the actual policy or procedure document is provided.	
	Data Deletion at Contract Termination	10		The provider says nothing about their policy.	Provider describes, in the vendor evidence column, their policy and/or procedures and how they apply.	The provider complies with Partially Meets (PM) AND the actual policy or procedure document is provided.	
	Intrusion Detection	11		The provider says nothing about their policy.	Provider describes, in the vendor evidence column, their policy and/or procedures and how they apply.	The provider complies with Partially Meets (PM) AND the actual policy or procedure document is provided.	
	Incident Response	12		The provider says nothing about their policy.	Provider describes, in the vendor evidence column, their policy and/or procedures and how they apply.	The provider complies with Partially Meets (PM) AND the actual policy or procedure document is provided.	
	Escalation Process	13		The provider says nothing about their policy.	Provider describes, in the vendor evidence column, their policy and/or procedures and how they apply.	The provider complies with Partially Meets (PM) AND the actual policy or procedure document is provided.	

Requirement Category	Item	Cloud Item #	Vendor NM/PM/FM Rating (See Next 3 Columns)	NM - "Not Met" Definition (0)	PM - "Partially Met" Definition (1)	FM - "Fully Met" Definition (2)	Vendor Evidence
CRITICAL RE This section lists the requirments that each Details on how each Respondent will meet these requireme Your Policies, procedures and practices must be in line with JEA Inf Describe your policies, proce	**Disaster Recovery Management**	14		The provider says nothing about their policy.	Provider describes, in the vendor evidence column, their policy and/or procedures and how they apply.	The provider complies with Partially Meets (PM) AND the actual policy or procedure document is provided.	
	Audit Logging	15		The provider says nothing about their policy.	Provider describes, in the vendor evidence column, their policy and/or procedures and how they apply.	The provider complies with Partially Meets (PM) AND the actual policy or procedure document is provided.	
	Patch Management	16		The provider says nothing about their policy.	Provider describes, in the vendor evidence column, their policy and/or procedures and how they apply.	The provider complies with Partially Meets (PM) AND the actual policy or procedure document is provided.	
	Vulnerability Management	17		The provider says nothing about their policy.	Provider describes, in the vendor evidence column, their policy and/or procedures and how they apply.	The provider complies with Partially Meets (PM) AND the actual policy or procedure document is provided.	
	Monitoring	18		The provider says nothing about their policy.	Provider describes, in the vendor evidence column, their policy and/or procedures and how they apply.	The provider complies with Partially Meets (PM) AND the actual policy or procedure document is provided.	
	Source and Configuration Management	19		The provider says nothing about their policy.	Provider describes, in the vendor evidence column, their policy and/or procedures and how they apply.	The provider complies with Partially Meets (PM) AND the actual policy or procedure document is provided.	
	Malware Security	20		The provider says nothing about their policy.	Provider describes, in the vendor evidence column, their policy and/or procedures and how they apply.	The provider complies with Partially Meets (PM) AND the actual policy or procedure document is provided.	
	Shall store logs for a minimum of 90 days. Ideally 3 years. **(Please state maximum period.)**	21		No Audit information is available	Logs are stored for 90 days.	Logs are stored for 3 years.	
	Data/information storage facility is compliant with ISO 27001,NIST 800-53 OR equivalent.	22		Facility is non-compliant	Vendor states that the facility is compliant with ISO 27001, NIST 800-53 or equivalent.	Vendor states that the facility is compliant with ISO 27001, NIST 800-53 or equivalent AND provides most recent certification audit report.	
	Ability to encrypt content that is transported over non-trusted networks using strong encryption.	23		No data encryption in place.	Partial data encryption in place.	Data encryption is in place for the level of data being protected.	
	Describe your contractual operation & service level monitoring & reporting procedures.	24		The provider does not speak to security monitoring.	The provider specifies that there is in place security information management and/or security event monitoring. Logs are however not provided to the customer.	The provider specifies that they have in place a full SIEM and logs will be provided to the customer upon request. Customer contact is provided.	

Requirement Category	Item	Cloud Item #	Vendor NM/PM/FM Rating (See Next 3 Columns)	NM - "Not Met" Definition (0)	PM - "Partially Met" Definition (1)	FM - "Fully Met" Definition (2)	Vendor Evidence
	Ability to utilize single sign-on function where applicable.	25		The provider does not provide single sign-on function.	The provider uses existing account names to sign on to applications. Passwords and status of accounts are managed separately.	The provider users single sign-on which enables the customer to disable and enable accounts with existing corporate accounts.	
	Ability to prevent caching of sensitive information.	26		The provider says nothing on data caching.	The provider caches sensitive data which expires with session.	The provider does not cache sensitive information.	
	Ability to implement a default ‘deny’ access policy for users and content objects.	27		The provider says nothing on access policies.	The provider implements a default 'deny' access policy for content or users objects.	The provider implements a default 'deny' access policy for user and content objects.	
	Ability to allow the revocation of all privileges from a specified group or selected user(s), thereby preventing access to the system.	28		The provider says nothing on revocation of privileges.	The provided process which provides for revocation of all priviledes from a specified group or selected user(s) preventnig access to the system takes more than 24 hours after notification.	The provided process which provides for revocation of all priviledes from a specified group or selected user(s) preventnig access to the system takes less than 24 hours after notification.	
	Ability to provide, support and maintain industry accepted methodologies of data exchange and interface tools.	29		No ability to provide, support and maintain industry accepted methodologies of data exchange and interface tools.	Ability to provide, support or maintain industry accepted methodologies of data exchange and interface tools.	Able to provide, support and maintain industry accepted methodologies of data exchange and interface tools.	
	Ability to support SSL encryption based on current minimum acceptable standards for all communication from user logon and all user account pages.	30		No data encryption in place.	Partial data encryption in place.	Data encryption is in place for the level of data being protected.	

Requirement Category	Item	Cloud Item #	Vendor NM/PM/FM Rating (See Next 3 Columns)	NM - "Not Met" Definition (0)	PM - "Partially Met" Definition (1)	FM - "Fully Met" Definition (2)	Vendor Evidence
	Ability to provide LDAP authentication processes for user access. If not, explain your user store, authentication and authorization process(es).	31		There is no directory integration in place.	Directory integration is limited to the system itself with manual ties to external systems.	Directory integration is automatic and integrated with the system.	
	What type of logs are available? Application, database, server, network? How often are you able to provide these logs?	32		No Audit information is available	Logical access logging is in place and logged to a SIEM.	There is detailed activity logging in place and logged to a SIEM.	
	Ability to provide application firewalls used for web applications. **(Architecture Diagram Required)**	33		The solution is a multi-tenant model that provides a predefined environment for the customer that is shared with other tenants	Various types of multi-tenant arrangements are possible. Each arrangement pools resources differently, offering different degrees of isolation and resource efficiency	The solution is a multi-instance model whereby the customer has complete control over role definition, user authorization, and other administrative tasks related to security.	
	Explain the data conversion process.	34		The provider says nothing on data conversion.	The provider gives overview but limited supporting documentation for data conversion process.	The provider gives overview and full supporting documentation on the data conversion process.	
	Identify third party backup tools and explain the process by which backups are taken	35		The provider says nothing on data backup or backup tools.	The provider identifies what third party back tools are used to support customer SaaS solution on their infrastructure but gives limited explanation around the process.	The provider identifies what third party back tools are used to support customer SaaS solution on their infrastructure and gives explanation. The third party backups are easily portable to JEA's data center and can be stored because JEA uses the same/similar backup tool.	
	Identify service level agreements for data performance, business continuity and disaster recovery.	36		The provider says nothing on data performance.	Provider identifies various services level agreements, business continuity and disaster recovery in general.	Provides supporting documentation showing statistical reference data performance for on-line transactions processing (OLTP) & on-line analytical processing (OLAP) by service level agreement, business continuity (BC) and disaster recovery (DR). May include but not limited to current customer performance statistics or a chart detailing data speeds for BC and DR.	
	Explain the archival and retention process for storing tiered or historical data.	37		The provider says nothing on data archival and retention.	Provider gives general understanding of their archival and retention data policies.	Specific archival and retention details are provided for data tiered storage regarding historical or transactional data. For example, transactional data like temporary logs can be purged by weekly or monthly. Does provider outline details of what can or can't be purged, retained and tools used.	
	Ability to apply Operating System, database, application server, and Third Party Component Security Patches within a reasonable period after Patch Release. Please specify periods as necessary.	38		There is no process for change, confoguration or patch management.	Change, configuration and patch management processes exist but they are not documented.	Change, configuration and patch management processes exist and they are well documented.	
	Ability to automate application patch installation process.	39		There is no process for change, configuration or patch management.	Automated, configuration and patch management processes exist but they are automated for only select systems identified in the vendor's evidence	Automated configuration and patch management processes exist and applies to database, application servers, third party components which are identified in the vendor's evidence	
	Ability to provide Notification of JEA and its customers within 24 hours of Security Vulnerability Discovery.	40		The provider does not speak to incident response handling.	The provider states that there is an incident response plan in place.	The provider specifies an incident response process and this process includes a notification process in the event of an incident within 24 hours of identification.	
	Firewall protection for Layers 3 through 7 of the OSI model, including stateful packet inspection of voice and video, if applicable.	41		The provider does not speak to firewall protection.	Firewall protection for Layers 3 through 7 of the OSI model is provided from a single vendor which logs events to a SIEM.	Firewall protection for Layers 3 through 7 of the OSI model is provided from multiple devices using multiple vendors which log events to a SIEM.	
	Intrusion detection/prevention.	42		The provider does not speak to Intrusion detection/prevention.	The provider implements an intrusion detection system which is currently subscribed for and receiving updates and logs events to a SIEM.	The provider implements an intrusion prevention system which is currently subscripbed for and receiving updates and logs events to a SIEM.	
WANT **uld like to have incorporated into the solution but are not required.** **e scored as part of the Evaluation Matrix for points.** **o Support these.**	Notification to JEA of security issues or vulnerabilities, and provide a timeline for resolution.	43		The provider does not speak to the communication of security issues or vulnerability notification.	The states they will notify JEA of security issues or vulnerabilities and provide a timeline for resolution.	The provider states they will notify JEA of security issues or vulnerabilities, provide a timeline for resolution and provide examples of notifications in the vendors evidence.	

Requirement Category	Item	Cloud Item #	Vendor NM/PM/FM Rating (See Next 3 Columns)	NM - "Not Met" Definition (0)	PM - "Partially Met" Definition (1)	FM - "Fully Met" Definition (2)	Vendor Evidence
Ability t nal security standards that JEA w ers provided in this section will b	Both synchronous and asynchronous message types.	44		Messages are only synchronous	Some messages are asynchronous others synchronous, and some both	All messages can be synchronous or asynchronous	
	Secured file transfer, based on industry standards.	45		No standards used for file transfer	Some standards used	All file transfers are based on industry standards (list standards used)	
	SOAP fault exceptions as provider or consumer of web services.	46		No fault exception handling	Some fault exceptions defined	All SOAP fault exceptions are defined	
	Use of both HTTPs and JMS transport protocols.	47		JMS and HTTPs no supported at all	Some JMS and/or Https supported	Both protocols fully supported	
	SOAP RPC and document binding's types.	48		No binding's types	Some binding types	All binding's types	
	WSDL v1.1 for all services provided or consumed by.	49		No WSDL support	Some WSDL supported services	All WSDL supported	

Requirement Category	Item	Cloud Item #	Vendor NM/PM/FM Rating (See Next 3 Columns)	NM - "Not Met" Definition (0)	PM - "Partially Met" Definition (1)	FM - "Fully Met" Definition (2)	Vendor Evidence
This section lists additio The answ	WS-I Basic Profile v1.1 for all services provided or consumed by.	50		The provider says nothing on data security standards.	The provider will comply with current security standards, but the standards are not specified, or the provider will enforce security measures at least as strong as the provider does for internal users.	The provider says it will comply with specific, emerging cloud security standards, and it agrees to certify compliance. The customer has the ability to exit the contract if there is a security breach resulting from provider negligence, or a contract breach.	
	JEA's target name space naming standards for all WSDL documents.	51		Name space standards not met	Some JEA standards met	Fully comply with standards	
	Both simple and complex data types for all WSDL documents.	52		Data types not supported	Some data types	All WSDL support simple and complex data types	
	Using JEA's common information models and common information model multispeak 5.0.	53		No common information model supported	Partial common information model (JEA or multispeak, or other utility accepted CIM)	All based on utility standard data model	
	Two-way SSL to ensure confidentiality of data in transit based on business requirements for all services provided or consumed by the system.	54		The provider says nothing on data security standards.	The provider offers a method to establish two-way SSL for some data in transit for somel services provided or consumed by the system which are identified in the vendor evidence.	The provider offers a method to establish two-way SSL for all data in transit for all services provided or consumed by the system.	
	Data loss prevention (DLP) is a strategy for making sure that end users do not send sensitive or critical information outside the corporate network. The term is also used to describe software products that help a network administrator control what data end users can transfer.	55		There is no DLP solution in place.	A DLP solution can be put in place if requested by the customer.	A DLP solution is standard in all contracts.	
	The ability to enable message-level integrity (XML digital signatures) controls based on business requirements for all	56		No message-level integrity	Some message-level integrity	Full message-level integrity	
	WSDL well-formed validation.	57		No support for WSDL	Some WDSL compliant services	Fully WSDL compliant	
	WSDL WS-I compliance validation.	58		No support for WSDL	Some WDSL compliant services	Fully WSDL compliant	
	Ability to import an XSD's and conforms to W3C standards for all WSDL documents.	59		No support for WSDL	Some WDSL compliant services	Fully WSDL compliant	
	Ability to use of standard SMTP Communications Protocols and Transports.	60		No support for SMTP	Some support	Fully compliant with SMTP protocol	
	Ability to support the ability to enable value, field, or message-level encryption based on business requirements for all services provided or consumed by the system.	61		No data encryption in place.	Partial data encryption in place.	Data encryption is in place for the level of data being protected.	
	Identity of the user invoking the service.	62		No Audit information is available	Identity of the user invoking the service is logged.	Identity of the user invoking the service is logged and logged to a SIEM.	
	Source IP address of the service requestor	63		No Audit information is available	Source IP address of the service requestor logging is in place.	Source IP address of the service requestor logging is in place and logged to a SIEM.	
	Date and time of the request	64		No Audit information is available	Date and time of request is logged.	Date and time of request is logged and logged to a SIEM.	
	The content of the message if this is a "command and control" operation.	65		No Audit information is available	command and control operations are logged.	command and control operations are logged and logged to a SIEM.	
	Ability to provide both a system and service identity to be used for coarse-grained and fine-grained authorization, respectively (when consuming a web service).	66		No Audit information is available	identity logging is in place.	Identity logging is in place and logged to a SIEM.	
	Audit logs shall be written in append mode to enable adding new audit events but disallowing previous events from modification.	67		No Audit information is available	Audit logs are written in append mode.	Audit logs are written in append mode and logged to a SIEM.	
	Ability to be authenticated at the user-level against the identity stored used by the system exposing the Web Services.	68		There is no authentication mechanism in place	There is single factor authentication in place	Authentication into the system requires multi factor authentication.	
	Ability to allow the security administrator to generate reports based on the service logs.	69		The provider does not speak to report generation.	Security administrators can generate reports based on service logs.	Security administrators can generate reports based on service logs and provide to customer upon request.	

Requirement Category	Item	Cloud Item #	Vendor NM/PM/FM Rating (See Next 3 Columns)	NM - "Not Met" Definition (0)	PM - "Partially Met" Definition (1)	FM - "Fully Met" Definition (2)	Vendor Evidence
	Customer audits allow the customer the right to oversee an audit of the service providers facilities and practices.	70		The provider says nothing about customer audits.	The provider will subject itself to a customer audit once a year.	The provider will subject itself to a customer audit at the customer's convenience.	
	Explain standard operating environment if its portable “interchangeable parts” between off-premise and on-premise applications. Show service level agreements with data transfer out of the cloud for SaaS.	71		The provider says nothing on data transfer.	Provider gives general information on portability.	Providers gives supporting documentation on details and best practices to port data between off-premise to on-premise and vice versa. Is the process seamless?	