REQUEST FOR QUOTES

Documentation Management and Workflow Solution

	Date	Time
Vendor's Electronic Question Due Date (See below note)	June 11, 2025	2:00 PM
Quote Submission Date (See below note)	July 17, 2025	2:00 PM

Dates are subject to change. All times contained in the RFQ refer to Eastern Time.
All changes will be reflected in Bid Amendments to the Request for Quotes posted on the Division of Investment's website.

RFQ Issued By:
State of New Jersey
Department of the Treasury
Division of Investment
50 West State Street, 9th Floor
Trenton, NJ 08608

Date: June 11, 2025

TABLE OF CONTENTS

ATTACHMENTS

1 INTRODUCTION AND SUMMARY

1.1 NEW JERSEY DIVISION OF INVESTMENT OVERVIEW

The State of New Jersey Department of the Treasury, Division of Investment ("DOI" or the "Division") was created by P.L. 1950, c. 270 (the "Act"), which became effective on July 1, 1950. The Act created the DOI and the State Investment Council ("SIC"). An important objective of the Act creating the DOI and the SIC was to centralize all functions relating to purchases, sales, or exchanges of securities for the State's diverse funds under experienced and professional management.

The role of the SIC is to formulate policies governing the investment of funds by the Director of DOI (the "Director"), and to consult with the Director with respect to the work of the Division. New regulations adopted by the Council are filed with the Office of Administrative Law and published in the New Jersey Register for public comment prior to adoption. Implementation of investment policies is vested in the Director.

The DOI invests the assets of seven different State pension funds: the Consolidated Police & Firemen's Pension Fund, the Police and Firemen's Retirement System of New Jersey, the Judicial Retirement System, the Prison Officers' Pension Fund, the Public Employees' Retirement System, the State Police Retirement System, and the Teachers' Pension & Annuity Fund (collectively referred to in this report as the "Pension Fund"). The net asset value of the Pension Fund assets managed by the Division totaled approximately $80 billion as of June 30, 2024. The Division also manages the State of New Jersey Cash Management Fund, Supplemental Annuity Collective Trust (a 403b plan), a portion of the NJBEST Fund (a 529 college savings plan) as well as several funds under the New Jersey State Employees Deferred Compensation Plan (a 457 plan).

1.2 DOI OBJECTIVES

To support the DOI's investment processes, we have initiated a project to evaluate document management and workflow software vendors. While the primary focus of the prospective solution would be to support private market and public market investment opportunity tracking and management processes, the DOI would like to assess a solution for the entire Division, including capital markets, private markets investment operations, compliance, legal and risk management.

1.3 MINIMUM REQUIREMENTS

The vendor and solution shall meet the following minimum requirements in order to proceed with responding to this RFQ:

- A minimum of 5 or more Institutional Investment Management clients installed on the proposed solution each with Assets Under Management (AUM) of $ 5 billion and above.
- Each active client must have 10 or more users on the proposed solution.
- The solution must be deployed as a cloud/SaaS offering.
- All data must be stored in a United States based data center.

1.4 DOI STATISTICS

The following are key statistics about DOI funds and the planned usage of the solution for determining usage patterns and cost estimates:

1. Estimated number of total users: **50-55 expected (65 in the Division to date)**
    - Frequent users (Read/Write privileges) – **50**
    - Occasional users (Read only) – **5**
    - Annual growth assumption – **users could increase by 10%**
2. Estimated number of contacts – **700+ (expected to increase into 1,000s in a year)**
3. Estimated number of events/workflow transactions (includes new investments, capital calls, other activities) – **2-3 capital calls per day; 10-20 new investments per year**

1.5 CONTRACTUAL TERMS; ORDER OF PRECEDENCE

The State of New Jersey Standard Terms and Conditions (Rev. 2/8/2024) and Waivered Contracts/Delegated Purchase Authority Supplement to the State of New Jersey Standard Terms and Conditions (Rev. 1/11/2022) (collectively, the "Standard Terms and Conditions" or "SSTCs") will apply to all Contracts made with the State. These terms are in addition to the terms

and conditions set forth in this RFQ and should be read in conjunction with them unless the RFQ specifically indicates otherwise. The Standard Terms and Conditions may be found as Attachment 1 of this RFQ, as well as at the link below:

https://www.nj.gov/treasury/purchase/forms/CombinedStateofNewJerseyStandardTermsandConditionsandWaiveredSupplement.pdf

The Contract awarded, and the entire agreement between the parties, as a result of this RFQ shall consist of: (1) the final RFQ (including any Bid Amendments), (2) the Standard Terms and Conditions, (3) the Bidder's responses to clarifications, if applicable, (4) the Bidder's Best and Final Offer, if applicable; (5) the Bidder's Quote; and (6) documents submitted by the Bidder that have been negotiated and accepted by the DOI. In the event of a conflict in the terms and conditions among the documents comprising this Contract, the order of precedence, for purposes of interpretation thereof, is listed from highest ranking to lowest ranking as noted above.

Any other terms or conditions not included in the documents described above shall not be incorporated into the Contract awarded. Any references to external documentation, including those documents referenced by a URL, including without limitation, technical reference manuals, technical support policies, copyright notices, additional license terms, etc., are subject to the terms and conditions of the RFQ and the Standard Terms and Conditions. In the event of any conflict between the terms of a document incorporated by reference and the terms and conditions of the RFQ and the Standard Terms and Conditions, the terms, and conditions of the RFQ and the Standard Terms and Conditions shall prevail.

2 PRE-QUOTE SUBMISSION INFORMATION

The Bidder assumes sole responsibility for the complete effort required in submitting a Quote and for reviewing the Quote submission requirements and the Scope of Work requirements.

2.1 QUESTION AND ANSWER PERIOD

The DOI will electronically accept questions and inquiries from all potential Bidders.

Questions should be directly tied to the RFQ and asked in consecutive order, from beginning to end, following the organization of the RFQ.

A Bidder shall submit questions only by email to DOI.RFP@treas.nj.gov. The DOI will not accept any question in person or by telephone concerning this RFQ. The due date for electronic questions and inquiries relating to this RFQ is indicated on the RFQ cover sheet. In the event that questions are posed by Bidders, answers to such questions will be issued by Bid Amendment. Any Bid Amendment will become part of this RFQ and part of any Contract awarded as a result of this RFQ. Addenda to this RFQ, if any, will be posted to the DOI's website.

2.2 QUESTIONS REGARDING THE STANDARD TERMS AND CONDITIONS

Questions regarding the Standard Terms and Conditions and exceptions to mandatory requirements should be posed during the Electronic Question and Answer period and should contain the Bidder's suggested changes and the reason(s) for the suggested change(s).

2.3 BID AMENDMENTS

In the event that it becomes necessary to clarify or revise this RFQ, such clarification or revision will be by Bid Amendment. Any Bid Amendment will become part of this RFQ and part of any Contract awarded. Bid Amendments will be posted on the DOI's website at DOI.RFP@treas.nj.gov. There are no designated dates for release of Bid Amendments. It is the sole responsibility of the Bidder to be knowledgeable of all Bid Amendments related to this RFQ.

3 QUOTE SUBMISSION REQUIREMENTS

3.1 QUOTE SUBMISSION

In order to be considered for award, the Quote must be received by the DOI by the required date and time indicated on the RFQ cover sheet. If the Quote submission deadline has been revised, the new Quote submission deadline shall be shown on the posted Bid Amendment.

Quotes not received prior to the Quote submission deadline shall be rejected.

The Bidder must submit the Quote electronically to the DOI at the following address: DOI.RFP@treas.nj.gov

Each Quote shall include one copy in "read only" PDF file format for review and one copy in an editable and "writable" PDF file format for redaction.

3.2 BIDDER RESPONSIBILITY

The Bidder assumes sole responsibility for the complete effort required in submitting a Quote in response to this RFQ. No special consideration will be given after Quotes are opened because of a Bidder's failure to be knowledgeable as to all of the requirements of this RFQ. The State assumes no responsibility and bears no liability for costs incurred by a Bidder in the preparation and submittal of a Quote in response to this RFQ or any pre-contract award costs incurred.

3.3 BIDDER ADDITIONAL TERMS SUBMITTED WITH THE QUOTE

A Bidder may submit additional terms as part of its Quote for consideration by the State. Additional terms are Bidder-proposed terms or conditions that do not conflict with the scope of work required in this RFQ, the terms and conditions of this RFQ, or the Standard Terms and Conditions. It is incumbent upon the Bidder to identify and remove its conflicting proposed terms and conditions prior to Quote submission.

3.4 QUOTE CONTENT

The Quote should be submitted with the attachments organized in following manner:

- Forms (see Section 3.5 of the RFQ)
- Technical Quote (see Section 6 of the RFQ)
- Pricing (see Section 9 of the RFQ)

A Bidder should not password protect any submitted documents. Use of URLs in a Quote should be kept to a minimum and shall not be used to satisfy any material term of an RFQ. If a preprinted or other document included as part of the Quote contains a URL, a printed copy of the information should be provided and will be considered as part of the Quote.

3.5 FORMS, REGISTRATIONS AND CERTIFICATIONS TO BE SUBMITTED WITH QUOTE

A Bidder is required to complete and submit the following forms, registrations, and certifications:

3.5.1 OWNERSHIP DISCLOSURE FORM

Pursuant to N.J.S.A. 52:25-24.2, in the event the Bidder is a corporation, partnership or limited liability company, the Bidder must disclose all 10% or greater owners by (a) completing and submitting the Ownership Disclosure Form with the Quote; (b) if the Bidder has submitted a signed and accurate Ownership Disclosure Form dated and received no more than six (6) months prior to the Quote submission deadline for this procurement, the DOI may rely upon that form; however, if there has been a change in ownership within the last six (6) months, a new Ownership Disclosure Form must be completed, signed and submitted with the Quote; or, (c) a Bidder with any direct or indirect parent entity which is publicly traded may submit the name and address of each publicly traded entity and the name and address of each person that holds a 10 percent or greater beneficial interest in the publicly traded entity as of the last annual filing with the federal Securities and Exchange Commission or the foreign equivalent, and, if there is any person that holds a 10 percent or greater beneficial interest, also shall submit links to the websites containing the last annual filings with the federal Securities and Exchange

Commission or the foreign equivalent and the relevant page numbers of the filings that contain the information on each person that holds a 10 percent or greater beneficial interest.

A Bidder's failure to submit the information required by N.J.S.A. 52:25-24.2 with its Quote will result in the rejection of the Quote as non-responsive and preclude the award of a Contract to said Bidder.

3.5.2 DISCLOSURE OF INVESTMENT ACTIVITIES IN IRAN FORM

The Bidder should submit the Disclosure of Investment Activities in Iran Form with its Quote to certify that, pursuant to N.J.S.A. 52:32-58, neither the Bidder, nor one (1) of its parents, subsidiaries, and/or affiliates (as defined in N.J.S.A. 52:32-56(e)(3)), is listed on the Department of the Treasury's List of Persons or Entities Engaging in Prohibited Investment Activities in Iran and that neither the Bidder, nor any of its parents, subsidiaries, and/or affiliates, is involved in any of the investment activities set forth in N.J.S.A. 52:32-56(f). If the Bidder is unable to so certify, the Bidder shall provide a detailed and precise description of such activities as directed on the form. If a Bidder does not submit the form with the Quote, the Bidder must comply within seven (7) business days of the State's request or the State may deem the Quote non-responsive.

3.5.3 DISCLOSURE OF INVESTIGATIONS AND OTHER ACTIONS INVOLVING BIDDER FORM

The Bidder should submit the Disclosure of Investigations and Other Actions Involving Bidder Form with its Quote to provide a detailed description of any investigation, litigation, including administrative complaints or other administrative proceedings, involving any public sector clients during the past five (5) years, including the nature and status of the investigation, and, for any litigation, the caption of the action, a brief description of the action, the date of inception, current status, and, if applicable, disposition. If a Bidder does not submit the form with the Quote, the Bidder must comply within seven (7) business days of the State's request or the State may deem the Quote non-responsive.

3.5.4 MACBRIDE PRINCIPLES FORM

The Bidder should submit the MacBride Principles Form with its Quote. Pursuant to N.J.S.A. 52:34-12.2, a Bidder is required to certify that it either has no ongoing business activities in Northern Ireland and does not maintain a physical presence therein or that it will take lawful steps in good faith to conduct any business operations it has in Northern Ireland in accordance with the MacBride principles of nondiscrimination in employment as set forth in N.J.S.A. 52:18A-89.5 and in conformance with the United Kingdom's Fair Employment (Northern Ireland) Act of 1989, and permit independent monitoring of their compliance with those principles. If a Bidder does not submit the form with the Quote, the Bidder must comply within seven (7) business days of the State's request or the State may deem the Quote non-responsive.

3.5.5 SOURCE DISCLOSURE FORM

The Bidder should submit a completed Source Disclosure Form with its Quote. Pursuant to N.J.S.A. 52:34-13.2, all Contracts primarily for services shall be performed within the United States. If a Bidder does not submit the form with the Quote, the Bidder must comply within seven (7) business days of the State's request or the State may deem the Quote non-responsive.

3.5.6 CONFIDENTIALITY/COMMITMENT TO DEFEND

Quotes can be released to the public in accordance with the New Jersey Open Public Records Act (OPRA), N.J.S.A. 47:1A-1 et seq., or the common law right to know.

The Bidder should submit a completed and signed Confidentiality /Commitment to Defend Form with the Quote. In the event that the Bidder does not submit the Confidentiality form with the Quote, the State reserves the right to request that the Bidder submit the form after Quote submission.

After the Quote submission deadline, all information submitted by a Bidder in response to a RFQ is considered public information notwithstanding any disclaimers to the contrary submitted by a Bidder. Proprietary, financial, security and confidential information may be exempt from public disclosure by OPRA and/or the common law when the Bidder has a good faith, legal/factual basis for such assertion.

When the RFQ contains a negotiation component, the Quote will not be subject to public disclosure until a notice of intent to award a Contract is announced.

As part of its Quote, a Bidder may request that portions of the Quote be exempt from public disclosure under OPRA and/or the common law. Bidder must provide a detailed statement clearly identifying those sections of the Quote that it claims are exempt from production, and the legal and factual basis that supports said exemption(s) as a matter of law. The State will not honor any attempts by a Bidder to designate its price sheet and/or the entire Quote as proprietary and/or confidential, and/or to claim copyright protection for its entire Quote. If the State does not agree with a Bidder's designation of proprietary and/or confidential information, the State will use commercially reasonable efforts to advise the Bidder. Copyright law does not prohibit access to a record which is otherwise available under OPRA.

The State reserves the right to make the determination as to what to disclose in response to an OPRA request. Any information that the State determines to be exempt from disclosure under OPRA will be redacted.

In the event of any challenge to the Bidder's assertion of confidentiality that is contrary to the State's determination of confidentiality, the Bidder shall be solely responsible for defending its designation, but in doing so, all costs and expenses associated therewith shall be the responsibility of the Bidder. The State assumes no such responsibility or liability.

In order not to delay consideration of the Quote or the State's response to a request for documents, the State requires that Bidder respond to any request regarding confidentiality markings within the timeframe designated in the State's correspondence regarding confidentiality. If no response is received by the designated date and time, the State will be permitted to release a copy of the Quote with the State making the determination regarding what may be proprietary or confidential.

3.5.7 SUBCONTRACTOR UTILIZATION PLAN

Bidders intending to use Subcontractor(s) shall list all subcontractors on the Subcontractor Utilization Plan form.

For a Quote that does NOT include the use of any Subcontractors, the Bidder is automatically certifying that, if selected for an award, the Bidder will be performing all work required by the Contract.

If it becomes necessary for the Contractor to substitute a Subcontractor, add a Subcontractor, or substitute its own staff for a Subcontractor, the Contractor will identify the proposed new Subcontractor or staff member(s) and the work to be performed. The Contractor shall forward a written request to substitute or add a Subcontractor or to substitute its own staff for a Subcontractor to the State Contract Manager for consideration. The Contractor must provide a completed Subcontractor Utilization Plan, a detailed justification documenting the necessity for the substitution or addition and resumes of its proposed replacement staff or of the proposed Subcontractor's management, supervisory, and other key personnel that demonstrate knowledge, ability, and experience relevant to that part of the work which the Subcontractor is to undertake. The qualifications and experience of the replacement(s) must equal or exceed those of similar personnel proposed by the Contractor in its Quote. The State Contract Manager will forward the request to the Director for approval.

NOTE: No substituted or additional Subcontractors are authorized to begin work until the Contractor has received written approval from the State.

3.5.8 PAY TO PLAY PROHIBITIONS

Pursuant to N.J.S.A. 19:44A-20.13 et seq. (P.L.2005, c.51, rev. P.L.2023, c.30), and Executive Order 333(2023), the State shall not enter into a Contract to procure services or any material, supplies or equipment, or to acquire, sell, or lease any land or building from any Business Entity, where the value of the transaction exceeds $17,500, if that Business Entity has solicited or made any contribution of money, or pledge of contribution, including in-kind contributions, to a Continuing Political Committee or to a candidate committee and/or election fund of any candidate for or holder of the public office of Governor of Lieutenant Governor during certain specified time periods.

Further, the Contractor is required, on a continuing basis, to report any contributions it makes during the term of the Contract, and any extension(s) thereof, at the time any such contribution is made.

Prior to awarding any Contract or agreement to any Business Entity pursuant to a non-fair and open process, the Business Entity proposed as the intended Contractor of the Contract shall submit the Two-Year Chapter 51/Executive Order 333 Vendor Certification and Disclosure of Political Contributions for Non-Fair and Open Contracts, certifying either that no contributions to a Continuing Political Committee or to a candidate committee or election fund of a gubematorial candidate

have been made by the Business Entity and reporting all qualifying contributions made by the Business Entity or any person or entity whose contributions are attributable to the Business Entity. The required form and instructions available for review on the Division's website at https://www.nj.gov/treasury/purchase/forms.shtml.

3.5.9 AFFIRMATIVE ACTION

The Bidder and its named subcontractors should submit, with the Quote, a copy of a New Jersey Certificate of Employee Information Report, or a copy of Federal Letter of Approval verifying it is operating under a federally approved or sanctioned Affirmative Action program. If the Contractor and/or its named subcontractors are not in possession of either a New Jersey Certificate of Employee Information Report or a Federal Letter of Approval, it/they must complete and submit the Affirmative Action Employee Information Report (AA-302). Information, instruction, and the application are available at: https://www.state.nj.us/treasury/contract_compliance/index.shtml. If a Bidder does not submit the form with the Quote, the Bidder must comply within seven (7) business days of the State's request or the State may deem the Quote non-responsive.

3.5.10 BUSINESS REGISTRATION

In accordance with N.J.S.A. 52:32-44(b), a Bidder and its named Subcontractors must have a valid Business Registration Certificate ("BRC") issued by the Department of the Treasury, Division of Revenue and Enterprise Services prior to the award of a Contract. A Bidder should verify its Business Registration Certification Active status on the "Maintain Terms and Categories" Tab within its profile in NJSTART. In the event of an issue with a Bidder's Business Registration Certification Active status, NJSTART provides a link to take corrective action.

3.5.11 CERTIFICATION OF NON-INVOLVEMENT IN PROHIBITED ACTIVITIES WITH RUSSIA OR BELARUS

The Bidder should submit the Certification of Non-Involvement in Prohibited Activities with Russia or Belarus Form with its Quote. Pursuant to P.L.2022, c. 3, a person or entity seeking to enter into or renew a contract for the provision of goods or services shall certify that it is not engaging in prohibited activities in Russia or Belarus as defined by P.L.2002, c. 3, sec. 1(e). If a Bidder does not submit the form with the Quote, the Bidder must comply within seven (7) business days of the State's request or the State may deem the Quote non-responsive.

3.5.12 STATE OF NEW JERSEY SECURITY DUE DILIGENCE THIRD-PARTY INFORMATION SECURITY QUESTIONNAIRE

The Bidder should complete and submit the State of New Jersey Security Due Diligence Third-Party Information Security Questionnaire (Questionnaire) with its Quote. If a Bidder does not submit the completed Questionnaire with the Quote, the Bidder must comply within seven (7) business days of the State's request or the State may deem the Quote non-responsive.

This Questionnaire is designed to provide the State with an overview of the Bidder's security and privacy controls to ensure that the Bidder will (1) meet the State of New Jersey's objectives as outlined and documented in the Statewide Information Security Manual; and (2) comply with the State's security requirements as outlined in *Section 6 – Data Security Requirements – Contractor Responsibility*. The State reserves the right to remove a Bidder from consideration of Contract award if the State determines that the Bidder's Questionnaire failed to sufficiently convey that the Bidder's security and privacy controls meet the State's requirements.

The State has executed a Confidentiality/Non-Disclosure Agreement which is attached to the Questionnaire. The Bidder should countersign the Confidentiality/Non-Disclosure Agreement and include it with its submitted Questionnaire. If a Bidder does not submit the signed Confidentiality/Non-Disclosure Agreement with the Questionnaire, the Bidder must comply within seven (7) business days of the State's request or the State may deem the Quote non-responsive. No amendments to Confidentiality/Non-Disclosure Agreement are permitted.

To the extent permissible under OPRA, the New Jersey common law right to know, and any other lawful document request or subpoena, the completed Questionnaire and supplemental documentation provided by the Bidder will be kept confidential and not shared with the public or other Bidders.

3.6 TECHNICAL QUOTE

The Bidder shall set forth its overall technical approach and plans to meet the requirements of the RFQ in a narrative format. This narrative shall demonstrate to the Evaluation Committee that the Bidder understands the objectives that the Contract is intended to meet, the nature of the required work, and the level of effort necessary to successfully complete the Contract. The narrative shall demonstrate that the Bidder's approach and plans to undertake and complete the Contract are appropriate to the tasks and subtasks involved.

Mere reiterations of RFQ tasks and subtasks are strongly discouraged, as they do not provide insight into the Bidder's approach to complete the Contract. The Bidder's response to this section shall demonstrate to the Evaluation Committee that the Bidder's detailed plans and approach proposed to complete the Scope of Work are realistic, attainable, and appropriate, and that the Bidder's Quote will lead to successful Contract completion.

As part of its Quote, the Bidder should include the following information:

3.6.1 EXECUTIVE SUMMARY

Provide an executive summary of not more than two pages identifying the firm's approach and plans to provide the requested services and substantiating why the firm is best qualified to provide the requested services.

3.6.2 VENDOR PROFILE

3.6.2.1 FIRM OVERVIEW

- Primary contact information.
- Company Name.
- Year founded.
- Country of incorporation.
- Location of firm – headquarters and all other offices.
- Size of firm (total staff, total staff dedicated to product, total staff by location).
- Main market (either geographical area or country).
- Public company or privately held.
- Parent company name, if applicable.
- Brief information on parent company, if applicable.
- Brief description of additional business lines or products, if applicable.
- Acquisitions, mergers, changes of ownership, name changes or other corporate events in the last three years, including any pending events.
- Percentage of your firm's annual revenue from the proposed solution.
- Provide an insight into the vision of your firm. Elaborate on current and future strategic partnerships and any organizational changes and firm wide initiatives.
- Provide information relating to the firm's organization, personnel, and experience, including, but not limited to, references, together with contact names and telephone numbers, evidencing the firm's qualifications, and capabilities to perform the services required by this RFQ.
- Provide the approximate number of technical staff supporting the product. Explain of any recent technical staff turnover.
- Is your company currently for sale or involved in any transaction to either acquire or be acquired or to merge with another organization, and/or has your company been involved in any such reorganization, acquisition, or merger within the past 3 years? If the answer is "yes" provide details. Include details of any significant third-party funding.
- Describe any major pending litigation or litigation settled (including a summary of the court findings) in the last two years.
- Provide details of any negative actions taken by other contracting entities against the firm in the course of performing contracts of a similar size and scope to the work required by this RFQ including, but not limited to, receipt of letters of potential default, default, cure notices, termination of services for cause, or other similar notifications/processes. Provide details, including any negative audits, reports, or findings by any governmental agency for which the firm is/was the Contractor on any contracts of similar scope.

3.6.2.2 SOLUTION OVERVIEW & CLIENT BASE

- Indicate the name of the product and any relevant modules.
- How long has it been in production?
- Describe how the product is offered in terms of core functionality and optional modules. Please include how the modules are integrated.
- Indicate the most current version of the software in production, and when it was generally made available. If there are separate release versions for each module, please include these.
- Describe the history and evolution of the product. If a third party is responsible for designing and building software, please name the third party, the nature of their relationship, and when the relationship was established.
- Indicate the total number of clients you have who are currently using the proposed product, the type of firm they are, and the country or region they are operating in.
- Please provide details of any past security breaches with your solution.
- Please provide a profile of your client base by client AUM.
- Provide the number of new and lost clients for each of the last 5 years, along with explanations for lost clients.
- Indicate how many implementations your firm currently has in the pipeline.
- Describe your firm's experience delivering similar solutions for companies similar in size and complexity to NJDOI.

3.6.2.3 PRODUCT PLANNING

- Provide a list of major functional enhancements planned in the next 18 months, with a brief description of each enhancement.
- Provide a list of major technology enhancements planned in the next 18 months, with a brief description of each enhancement.
- Provide a list of both major functional and technical enhancements over the last 2 years.
- Describe how pending enhancements are prioritized and communicated to your clients.
- Describe responsibilities for testing product enhancements (e.g., vendor versus client).
- Describe your firm's approach to Application Development (e.g., locations, onshore/offshore mix).
- Describe how clients can suggest and influence future product enhancements (e.g., advisory board, user group, periodic meetings with clients).

3.6.3 GENERAL DESCRIPTION OF PRODUCT

3.6.3.1 EASE OF USE

- What are the options for accessing software over the internet using PCs, iPads/tablets, and smart phones (IOS/Android)? What features of the software are restricted? What are the differences, if any, in the user interfaces?
- Explain the ability to work remotely offline and able to sync back up with the solution.
- Explain what is involved in configuring the user interface to NJDOI's needs, with respect to:
- Adding new fields;
- Re-arranging the layout; and/or
- Changing the presentation of existing fields.

3.6.3.2 SECURITY AND ACCESS

- Explain user authentication process.
- Explain the level of granularity of user access (by function or user interface, or entity, function, or data level) and role-based access.
- Explain your support for single or reduced sign-on. Explain the process by which your system can accept and use security credentials from another system. Does the application or service support SAML identity federation standards?
- Explain what apps the solution is registered with? Preference for Azure registered app.
- Does the application or service support multi-factor authentication?

- Does your organization work with third parties, such as IT service providers that have access to your information or systems? If yes, describe the due diligence, oversight and controls you exercise on work performed by the service providers.
- When storing or transmitting sensitive information does your organization use encryption? If yes, what type?
- Are your organization's systems and networks monitored for security events? Cyber-security prevention protocols?
- Will NJDOI's data be stored segregated from your other customer data?
- Explain your data backup protocols.
    i. NJDOI preference: Monthly backup of DOI data to the State of New Jersey's data warehouse.
- Are all web applications (internal and external, and including web administrative access to application) developed based on secure coding guidelines such as the Open Web Application Security Project guide (OWASP), WASC Threat Classification or CIS Top 20?
- Have your security program and technical controls been audited or certified against industry standards for example SOC2/ISO 27001?
- Have you completed CAIQ and SOC2 assessments? When? Provide details.
- When NJDOI terminates use in your software (end of life/end of tenure), how would NJDOI obtain its data? How do you show proof that the data has been deleted from your environment?

3.6.3.3 REPORTING

- Does the system come with an internal / proprietary reporting and dashboard tool?
- Can the system work with external reporting tools? What tools are being used at other implementations?
- Does the system support a WYSUWYG (What You See Is What You Get) approach while designing the reports and dashboards? Does the system provide formatting like Microsoft office products?
- What is the skill set required to develop new reports or dashboards? Can they be created by end users or business analysts? If yes, provide examples of complexity that require additional technical assistance.
- Explain the report distribution and related capabilities provided by the system.

3.6.4 DOCUMENT COLLECTION, STORAGE & RETRIEVAL

3.6.4.1 DOCUMENT COLLECTION

- Explain how the system collects documents from emails.
- Explain how the system can collect documents from third party portals (e.g. external manager portals, service provider portals)
- Can the system accept documents from a third-party document collection system?

3.6.4.2 DOCUMENT STORAGE

- Explain what is involved in defining custom document types, sub-types, characteristics, and tags into the system. Such as categorized sleeves (asset classes) for document organization.
- Can the system automatically tag the document based on some characteristic (i.e. document location, file name, source of document etc.). Explain other tagging options (based on document date author, email subject - for documents captured in emails, document content, etc.)?
- What level of auto-tagging can the system support based on content of data?
- Explain how your system handles version control of documents.
- Outline how a user can ensure he/she is accessing the most recent version of the document.
- Display your system's ability to alert a user if a duplicate version of a document is opened.
- Outline how a user can access historical versions of the same document.
- Outline the system's document archive / purge capabilities. Can users set up automated rules for archiving, purging, and setting expiry dates?
- Can a document be modified outside the system, after being defined to it? Explain what controls exist to prevent concurrent update of documents outside the system and within the system.
- Is there the ability to lock certain documents from being edited at all?

3.6.4.3 DOCUMENT RETRIEVAL

- Explain the document search capability. Include in your explanation, explain search based on document content (such as keywords) and document characteristics, tags, and metadata.
- Explain the system's workflow capabilities associated with documents.
- Can users use the system to search for documents by location (in a shared drive), without the document being defined to the system?

3.6.5 PROFILE MANAGEMENT

3.6.5.1 ENTITY PROFILES

- Explain how you can support entity profiles for GPs, investment managers, and investment advisors. Also need to create and maintain detailed profiles for each investment fund and vehicle. Is there a limit to the amount of information /reference data that can be kept on each of these entities?
- How does the solution uniquely identify each profile?
- Explain how contacts can be stored and maintained for these entities.
- Outline how you can establish organizational structured hierarchy and relationships between GP and investment manager entities and investment vehicles and funds.
- Can the solution include a "geography function" that allows for a search within a defined radius to identify investment fund managers in the area to schedule a meeting with?

3.6.5.2 PROFILE EDITING & COMMENTING

- Explain how to maintain profiles through dynamic editing with comment addition capability.

3.6.6 NOTES & MONITORING AND OTHER CRM RELATED FUNCTIONALITY

3.6.6.1 NOTE-TAKING FEATURES

- Explain how you can link notes to investment funds/vehicles and GPs.
- Is there a character limit for notes?
- Is there a dictate function available through mobile app/tablet?
- Is there a full screen note-box present on the screen when adding content of a note?
- Can you copy and paste into the note box content from another source such as a Word, Excel, or PowerPoint document?
- Can you create free form content using native word processing capability – changing fonts, bulleted lists, indentations, line spacing, colors, etc.?
- Does the system allow for notes to be stored as draft? Explain the workflow support that is provided in converting a draft note to final note.
- Explain how note templates are created and how you can create a note leveraging a note template.
- Can your system's bulk edit multiple notes? Explain how this is done.
- Show how a user can annotate or comment on a note created by another user both within the body of the note and in a separate comment section.
- Does your system have the ability to add charts, graphs, and tables?
- Does your system include a dictate function available through mobile app/tablet?

3.6.6.2 DOCUMENT ATTACHMENT

- Outline your support for adding documents to notes. Support uploading and downloading in multiple formats, including but not limited to; pdf, doc, docx, xls, xlsx, ppt, pptx, jpg, png, txt, vsd.
- Explain how to Link a Note created in your system to an external document (in client's shared drive).

3.6.6.3 NOTE DISTRIBUTION

- Explain functionality around automated email distribution of notes integrated with common email clients. Notes based on what they are associated with can apply business rules to then distribute those notes directly automatically to individuals or groups or individuals to read directly on the screen.

- Explain template creation with automated distribution to GPs or other parties to be filled out and returned.

3.6.6.4 AUTO-POPULATE NOTES

- Explain how organizational-level notes can show up as a shared note with all linked investment profiles related to that organization.

3.6.6.5 OTHER CRM FUNCTIONALITY

- Can the system support two-way integration with Outlook? Is the integration real time? Explain what this means from a user perspective for Calendar / meeting schedule, Email and Contact lists.
- Explain what is involved in configuring the system to display a list of meetings or appointments based on defined criteria (by Manager, Investment, Contact, Date, Geography, etc.).
- Does the system support a mail merge function? Explain how this works.
- Does the system allow users to create and store private views of the contacts and related data? Explain what is involved in this process.
- Can the system import contact, notes, and other information from another application? Explain what is involved in this process and what are the challenges / restrictions?

3.6.7 WORKFLOW PROCESS REQUIREMENTS

3.6.7.1 TRACK DISCRETE PROJECTS ACROSS VARIOUS TASKS

- Outline where project/new investment opportunity sits within the Approval cycle for Internal Investment Committee, Investment Policy Committee and State Investment Council meeting timelines as well as legal review through closing.
- Explain how a user can be assigned to a specific asset class, or manager type.
- Explain how tasks can be created and automatically or manually assigned to a user, along with notification of the assignment.
- Outline how the user can be notified of a task deadline for a task that is assigned to that specific user.
- Explain your system's ability for a user to view the status of a task within a specific workflow.
- Explain how a manager could be notified to review a piece of content or an annotated document.
- Can tasks be set up to recur on a user-defined schedule?
- Can creation of content be controlled by read/write permissions on a specific entity?

3.6.7.2 CONTINUOUS WORKFLOW MANAGEMENT

- Outline the Workflow process beginning with pipeline entry and tracks through checklist process with ability to click through each process to see detailed notes.
- Explain how to create custom notifications and alerts such as upcoming task deadline, availability of a document / investment for review or informative reasons only (method, message, frequency, escalation, etc.).
- Explain how to subscribe to projects, workflows, and receive notifications.
- Explain how an email delivered to a common mailbox can be a trigger for a workflow process – send notification to a user for action, alert another user for the need of a follow up action (e.g., Capital call request comes in, gets sent to a user for initial validation, sent to second user for approval and then to third user for payment).

3.6.7.3 SEGREGATION OF PROCESS

- Explain how the Investment team, ESG team as well as Legal and Compliance and Operations will be able to track investment workflow while also tracking where it sits within the department's own process.
- Explain the approval functionality. What can be automated? Do you have the ability to request approvals ad hoc?

- Can you lock down/disallow edits on certain investments after a particular stage is accomplished?

3.6.7.4 INVESTMENT FLOW – OPPORTUNITY MANAGEMENT

- Explain the ability to automatically collect unsolicited investment opportunities from managers and load into the solution.
- Explain how to manually add an investment opportunity and create documents related to the opportunity.
- Explain how your system allows users to compare the characteristics of multiple opportunities.
- Is there any limit on the number of relationships or characteristics that can be assigned to an opportunity?
- Describe the word processing capabilities while entering comments. Does the system allow for graphs and charts as part of comments, provide spell check capabilities, and date/timestamp all entries? Is there any limit on the amount of comments / notes that can be added to an opportunity?
- Explain what types of information can be tracked for investments in the solution such as economic terms of investments, including net and gross returns, MOIC, DPI, TVPI, etc.
- Explain ability to track Governance related items including ESG, MWBE and key terms of LPA, etc.
- Is information collected on an opportunity during the investment stage available to users after that opportunity has been converted to an investment? Explain if there are any constraints in this process.

3.6.7.5 INVESTMENT FLOW – TRACKING

- Explain how NJDOI can set up their own opportunity stages. Is there a limit on the number of stages that can be set up? Can the stages vary by opportunity characteristics (e.g. size of opportunity, investment type)?
- Can an opportunity be set up to automatically move from one stage to another? Can an opportunity be set up so the movement from one stage to another is a manual process?
- Explain the kinds of user alerts that are available during investment tracking (e.g. all workflow tasks are not complete prior to advancing to the next investment stage, investment has not moved from a stage for "n" days, etc.).
- Can authorized users add / modify comments on an investment at any stage? Can you configure the system so users cannot modify comments after a certain stage? Explain how this is done.

3.6.8 ADDITIONAL TECHNICAL REQUIREMENTS

3.6.8.1 COMPATIBILITY/INTEGRATION

- Describe the types of file formats that your solution is able to support.
- Describe the methods of integration that your solution is able to support (i.e. real-time/messaged based, batch, on demand, file based, API, web services).
- Describe your experience integrating your solution with your clients' proprietary applications, including the ability to initiate client's applications or create data for delivery to client applications from your UI.
- Please explain your integration with the following data providers that are in place today for your current clients and provide examples. If no integration exists with the data vendor, please explain how you would integrate.
    i. MS Office (Outlook, Excel, Word, etc.)
    ii. FactSet
    iii. Bloomberg
    iv. Caissa
    v. Burgiss
    vi. Preqin
    vii. Barra

3.6.8.2 DEPLOYMENT OPTIONS

- Outline the deployment and "go live" plan. Cloud deployment is required, no on-premise equipment or software.

3.6.8.3 SYSTEM SCABILITY, AVAILABILITY, AND PERFORMANCE

- What is the largest volume you process amongst your client installations (# of users, # of documents, # of entities, # of records per day, # of third parties, systems involved, etc.)?
- Explain results of volume and stress tests you have conducted on your product.

- Explain the high availability provisions in your architecture (parallel processing, redundancy, data replication, mirroring, etc.).
- Describe your Business Continuity and Disaster Recovery plans.

3.6.8.4 ARCHITECTURE & INFRASTRUCTURE

- Describe the system's overall technical architecture. (Please include a schematic of the system architecture).
- Describe the minimum hardware requirements.
- Describe the major system components and how they interact with each other.
- Describe the system's application and data architecture. (Please include how the system employs web services and the type of databases supported):
- Do you have multiple data center locations?
- Software Development technologies: languages and GUI presentation.
- Is open source utilized? If so, describe.

3.6.9 VENDOR SUPPORT & TRAINING

3.6.9.1 IMPLEMENTATION & CUSTOMER SUPPORT

- Describe the firm's implementation methodology. Please include a description of the typical system implementation phases, dependencies, and resources.
- Describe the average time frame for a new client to implement the product. Describe the factors that affect the time frame (modules implemented, # of users, # of templates).
- Describe your approach to converting historical data from a third-party Document Management system.
- Provide a sample / template implementation plan listing activities and tasks.
- Describe the typical resources required for implementation (including vendor, client resources, and any other third-party resources).
- Do you have a professional services organization to support your implementations?
- Do you have preferred implementation partners? If yes, describe the typical roles and responsibilities of implementation partners.
- Describe your client support model (e.g., dedicated support representative, centralized help desk, hours, locations, service levels, and training/certification programs).
- Describe the countries or regions your firm can support.
- Describe how the system can support a 24x7 global operation, including any updates that may require system downtime.
- Describe your system audit capabilities and maintenance procedures. (Please include the types of audit reports that are available to clients.)
- Describe your proof of concept capabilities.
- Explain the service level agreement model for:
    i. Support Availability Schedule;
    ii. Application Availability Uptime/Downtime commitments;
    iii. Response time commitments on servers;
    iv. Database Storage/Capacity commitments;
    v. System Resource Utilization (CPU) commitments; and
    vi. User Capacity and Scalability commitments.
- Outline how you track Service Level Agreement (SLA) performance metrics. What, if any, penalties or incentives do you support in your SLA's in the event the SLA is not met? Please provide examples.
- Explain how often you provide periodic status reports on SLA metrics, incident logs, and operating metrics.
- How do you facilitate the communication of Product Roadmaps to NJDOI staff?
- Please describe the services that you offer to support your clients in the development of additional systems integrations and/or configuration changes (post go-live).

3.6.9.2 TRAINING MATERIALS

- Outline how you provide comprehensive training materials and sessions for users at different levels using in-person, web-based and computer-based training methods.
- Do you assist with assessing, identifying, and documenting the business process implications to the firm with the new solution in place?

- Do you present a Knowledge Transfer Plan? Provide user manuals, current technical and business release notes.

3.6.10 ADDITIONAL CONSIDERATIONS

3.6.10.1 TESTING/DATA MIGRATION

- Outline your quality assurance test plan that details the strategy that will be used to verify and ensure that the solution meets its design specifications and other requirements.
- Explain the process for assisting with data migration from current systems (Microsoft SharePoint, Teams, Excel, Word, PDF, CSV, State Street Canoe and/or FTP for other document platforms) to the new DMS.
- Explain how you would perform Calendar upload/sharing and meeting invite sharing.

3.6.10.2 CONFIGURATION

- Explain how you assure configuration / customization meets DOI's specific needs and evolving workflows.
- Outline how you communicate whether any configuration falls outside of the core software offering and what that means to DOI.

3.6.10.3 SOFTWARE UPDATES

- Explain your software upgrade process. Include the level of effort required from a client's standpoint. What support, if any, do you provide for client's regression testing during an upgrade? Are clients forced to upgrade or do they have an option to remain on the current version?
    i. Preferred schedule: Coordinated regular updates and maintenance without significant downtime during the hours of 7:00 AM – 7:00 PM, Monday through Friday.
- Explain how development requests are submitted and prioritized.

3.7 ADDITIONAL DOCUMENT(S)

Bidder shall submit any documents that the Bidder will request that the DOI to execute with respect to this contract.

3.8 FINANCIAL CAPABILITY OF THE BIDDER

The Bidder should provide sufficient financial information to enable the State to assess the financial strength and creditworthiness of the Bidder and its ability to undertake and successfully complete the Contract. In order to provide the State with the ability to evaluate the Bidder's financial capacity and capability to undertake and successfully complete the Contract, the Bidder should submit the following:

A. For publicly traded companies the Bidder shall provide copies or the electronic location of the annual reports filed for the two most recent years; or
B. For privately held companies the Bidder shall provide the certified financial statement (audited or reviewed) in accordance with applicable standards by an independent Certified Public Accountant which include a balance sheet, income statement, and statement of cash flow, and all applicable notes for the most recent calendar year or the Bidder's most recent fiscal year.

If the information is not supplied with the Quote, the State may still require the Bidder to submit it. If the Bidder fails to comply with the request within seven (7) business days, the State may deem the Quote non-responsive.

A Bidder may designate specific financial information as not subject to disclosure when the Bidder has a good faith legal/factual basis for such assertion. The State reserves the right to make the determination to accept the assertion and shall so advise the Bidder.

4 SCOPE OF WORK

4.1 GENERAL REQUIREMENTS

4.1.1 EASE OF USE

- Solution shall have user-friendly interface, accessible over the internet.

Solution shall require minimal training with available training resources including onsite, web-based, and built-in application help functions.

4.1.2 SECURITY AND ACCESS

- Solution shall include role-based access controls, including read/write capabilities.
- Solution shall include audit trails and secure encryption methods.

4.1.3 CROSS-DEPARTMENTAL

- Solution shall meet diverse functional needs of various departments with customizable workflows.

4.2 DOCUMENTATION & STORAGE REMOVAL

4.2.1 DOCUMENT FILING SYSTEM

- Solution shall include categorized sleeves (e.g, asset classes, types of documents, etc.) for document organization.
- Solution shall include advanced search and filtering options.

4.2.2 SEARCH FUNCTIONALITY

- Solution shall provide efficient, quick, and accurate search results using keywords, tags, or metadata.
-
- Solution shall include a "geography function" that allows for a search within a defined radius to identify investment managers in the area to schedule a meeting with.

4.3 PROFILE MANAGEMENT

4.3.1 GENERAL PARTNER AND MANAGER PROFILES

- Solution shall maintain profiles with associated investment vehicles for General Partners, investment fund managers, and investment advisers.

4.3.2 INVESTMENT PROFILES

- Solution shall provide detailed profiles for each investment fund or vehicle.

4.3.3 PROFILE EDITING & COMMENTING

- Solution shall allow for dynamic editing with comment addition capability.
- Solution should allow a user to add documents to a profile.

4.4 NOTES & MONITORING

4.4.1 NOTE-TAKING FEATURES

- Solution shall provide linked notes to investment funds/vehicles and General Partners with adequate space and format support.
- .
- Solution should include a full screen note-box to add notes

4.4.2 DOCUMENT ATTACHMENT

- Solution shall include support for adding documents to notes and for uploading and downloading in multiple formats, including but not limited to: pdf, doc, docx, xls, xlsx, ppt, pptx, jpg, png, txt, vsd.

4.4.3 NOTE DISTRIBUTION

- Solution shall provide for automated email distribution of notes integrated with common email clients
-

4.4.4 AUTO-POPULATE NOTES

- Solution shall automatically populate organizational-level notes into linked investment profiles and/or as a meeting note.

4.5 WORKFLOW PROCESS REQUIREMENTS

4.5.1 TRACK DISCRETE PROJECTS ACROSS VARIOUS TASKS

- Solution should identify where project sits within the approval cycle for Internal Investment Committee, Investment Policy Committee and State Investment Council as well as legal review through closing.

4.5.2 CONTINUOUS WORKFLOW MANAGEMENT

- Solution should track the workflow process beginning with pipeline entry and continuing through checklist processes with the ability to click through each process to see detailed notes.
- Solution should have the ability to subscribe to projects, workflows, and receive notifications.

4.5.3 SEGREGATION OF PROCESS

- Solution should enable the Investment team, the ESG team as well as Legal and Compliance and Operations to track the investment workflow while also tracking where it sits within each department's own process.
- Solution should enable users to request approvals.
- Solution shall enable users to edit other's notes.

4.5.4 INVESTMENT DILIGENCE DOCUMENTATION

- Solution shall track economic terms of investments, including net and gross returns, MOIC, DPI, TVPI, etc.
- Solution shall track governance-related items including ESG, MWBE and compliance with key terms of LPA, etc.

4.6 ADDITIONAL TECHNICAL REQUIREMENTS

4.6.1 COMPATIBILITY

- Solution should integrate with existing systems and infrastructure, where applicable, and specifically with current DOI vendors including MS Office (Outlook, Excel, Word, etc.), FactSet, Bloomberg, Caissa, Burgiss, Preqin, and Barra.

4.6.2 DEPLOYMENT OPTIONS

- Solution shall be cloud-based, with no on-premise equipment or software required.

4.6.3 SCALABILITY

- Solution should scale easily with growing data and user base without performance loss.

4.7 VENDOR SUPPORT & TRAINING

4.7.1 CUSTOMER SUPPORT

- Solution shall provide service level agreement guarantees.

4.7.2 TRAINING MATERIALS

- Solution shall provide comprehensive training materials and sessions for users at different levels using in-person, web-based and computer-based training methods.

4.8 ADDITONAL CONSIDERATIONS

4.8.1 DATA MIGRATION

- Contractor shall assist with data migration from current systems (Microsoft SharePoint, Teams, Excel, Word, PDF, CSV) to the new DMS.
-

4.8.2 CUSTOMIZATION

- Solution should allow for configuration/customization to meet DOI's specific needs and evolving workflows.

4.8.3 SOFTWARE UPDATES

- Solution shall provide for coordinated regular updates and maintenance without significant downtime during the hours of 7:00 am – 7:00 pm eastern time, Monday through Friday.

4.8.4 MONTHLY DATA BACKUP

- Solution shall provide for monthly backup of DOI data to the State of New Jersey's data warehouse.

5 GENERAL CONTRACT TERMS

The Contractor shall have sole responsibility for the complete effort specified in this Contract. Payment will be made only to the Contractor. The Contractor is responsible for the professional quality, technical accuracy and timely completion and submission of all deliverables and other services required to be provided under this Contract. The Contractor shall, without additional compensation, correct or revise any errors, omissions, or other deficiencies in its deliverables and other services. The approval of deliverables furnished under this Contract shall not in any way relieve the Contractor of responsibility for the technical adequacy of its work. The review, approval, acceptance, or payment for any of the deliverables or services shall not be construed as a waiver of any rights that the State may have arising out of the Contractor's performance of this Contract.

5.1 CONTRACT TERM AND EXTENSION OPTION

The base term of this Contract shall be for a period of three (3) years.

This Contract may be extended up to two (2) years with no single extension exceeding one (1) year, by the mutual written consent of the Contractor and the State at the same terms, conditions, and pricing at the rates in effect in the last year of this Contract or rates more favorable to the State.

5.2 CONTRACT TRANSITION

In the event that a new Contract has not been awarded prior to the expiration date for this Contract, including any extensions exercised, and the State exercises this Contract transition, the Contractor shall continue this Contract under the same terms, conditions, and pricing until a new Contract can be completely operational. At no time shall this transition period extend more than 365 calendar days beyond the expiration date of this Contract, including any extensions exercised.

During the transition period, the Contractor will be required to continue and complete any previous tasks and statements of work agreed upon prior to the expiration date of the Contract.

5.3 OWNERSHIP OF MATERIAL

A. **State Data** – The State owns State Data. Contractor shall not obtain any right, title, or interest in any State Data, or information derived from or based on State Data. State Data provided to Contractor shall be delivered or returned to the State of New Jersey upon thirty (30) days' notice by the State or thirty (30) days after the expiration or termination of the Contract. Except as specifically required by the requirements of the RFQ, State Data shall not be disclosed, sold, assigned, leased, or otherwise disposed of to any person or entity other than the State unless specifically directed to do so in writing by the State Contract Manager.

B. **Work Product; Services** – The State owns all Deliverables developed for the State in the course of providing Services under the Contract, including but not limited to, all data, technical information, materials gathered, originated, developed, prepared, used or obtained in the performance of the Contract, including but not limited to all reports, surveys, plans, charts, literature, brochures, mailings, recordings (video and/or audio), pictures, drawings, analyses, graphic representations, print-outs, notes and memoranda, written procedures and documents, regardless of the state of completion, which are prepared for or are a result of the Services required under the Contract.

C. **Vendor Intellectual Property; Commercial off the Shelf Software (COTS) and Customized Software** – Contractor retains ownership of all Vendor Intellectual Property, and any modifications thereto and derivatives thereof, that the Contractor supplies to the State pursuant to the Contract, and grants the State a non-exclusive, royalty-free license to use Vendor Intellectual Property delivered to the State for the purposes contemplated by the Contract for the duration of the Contract including all extensions. In the event Contractor provides its standard license agreement terms with its Quote, such terms and conditions must comply with *RFQ Section 1.2 – Order of Precedence of Contractual Terms*.

D. **Third Party Intellectual Property** – Unless otherwise specified in the RFQ that the State, on its own, will acquire and obtain a license to Third Party Intellectual Property, Contractor shall secure on the State's behalf, in the name of the State and subject to the State's approval, a license to Third Party Intellectual Property sufficient to fulfill the business objectives, requirements and specifications identified in the Contract at no additional cost to the State beyond that in the Quote price. In the event Contractor is obligated to flow-down commercially standard third-party terms and conditions customarily provided to the public associated with Third Party Intellectual Property and such terms and conditions conflict with RFQ requirements, including the SSTC, the State will accept such terms and conditions with the exception of the following: indemnification, limitation of liability, choice of law, governing law, jurisdiction, and confidentiality. The RFQ including the SSTC shall prevail with respect to such conflicting terms and conditions. In addition, the State will not accept any provision requiring the State to indemnify a third party or to submit to arbitration. Such terms are considered void and of no effect. third party terms and conditions should be submitted with the Quote. If Contractor uses Third Party Intellectual Property, Contractor must indemnify the State for infringement claims with respect to the Third-Party Intellectual Property. Contractor agrees that its use of Third-Party Intellectual Property shall be consistent with the license for the Third-Party Intellectual Property, whether supplied by the Contractor, secured by the State as required by the RFQ, or otherwise supplied by the State.

E. **Work Product; Custom Software** – The State owns all Custom Software which shall be considered "work made for hire", i.e., the State, not the Contractor, subcontractor, or third party, shall have full and complete ownership of all such Custom Software. To the extent that any Custom Software may not, by operation of the law, be a "work made for hire" in accordance with the terms of the Contract, Contractor, subcontractor, or third party hereby assigns to the State, or Contractor shall cause to be assigned to the State, all right, title and interest in and to any such Custom Software and any copyright thereof, and the State shall have the right to obtain and hold in its own name any copyrights, registrations and any other proprietary rights that may be available.

F. **State Intellectual Property** – The State owns all State Intellectual Property provided to Contractor pursuant to the Contract. State Intellectual Property shall be delivered or returned to the State of New Jersey upon thirty (30) days' notice by the State or thirty (30) days after the expiration or termination of the Contract. The State grants Contractor a non-exclusive, royalty-free, license to use State Intellectual Property for the purposes contemplated by the Contract. Except as specifically required by the requirements of the RFQ, State Intellectual Property shall not be disclosed, sold, assigned, leased, or otherwise disposed of to any person or entity other than the State unless specifically directed to do so in writing by the State Contract Manager.

G. **No Rights** – Except as expressly set forth in the Contract, nothing in the Contract shall be construed as granting to or conferring upon Contractor any right, title, or interest in State Intellectual Property or any intellectual property that is now owned or licensed to or subsequently owned by or licensed by the State. Except as expressly set forth in the Contract, nothing in the Contract shall be construed as granting to or conferring upon the State any right, title, or interest in any Vendor Intellectual Property that is now owned or subsequently owned by Contractor. Except as expressly set forth in the Contract, nothing in the Contract shall be construed as granting to or conferring upon the State

any right, title, or interest in any Third-Party Intellectual Property that is now owned or subsequently owned by a third party.

5.4 SUBSTITUTION OF STAFF

If a Contractor needs to substitute any management, supervisory or key personnel, the Contractor shall identify the substitute personnel and the work to be performed. The Contractor must provide detailed justification documenting the necessity for the substitution. Resumes must be submitted for the individual(s) proposed as substitute(s) whom must have qualifications and experience equal to or better than the individual(s) originally proposed or currently assigned.

The Contractor shall forward a request to substitute staff to the State Contract Manager for consideration and approval. No substitute personnel are authorized to begin work until the Contractor has received written approval to proceed from the State Contract Manager.

5.5 ELECTRONIC PAYMENTS

With the award of this Contract, the successful Contractor will be required to receive its payments electronically. To receive payments via automatic deposit from the State of New Jersey, the Contractor must complete the EFT information within its NJSTART Vendor Profile. Please refer to the QRG entitled "Vendor Profile Management – Company Information and User Access" for instructions.

6 DATA SECURITY REQUIREMENTS

6.1 INFORMATION SECURITY PROGRAM MANAGEMENT

The Contractor shall establish and maintain a framework to provide assurance that information security strategies are aligned with and support the State's business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, in an effort to manage risk. Information security program management shall include, at a minimum, the following:

A. Establishment of a management structure with clear reporting paths and explicit responsibility for information security;
B. Creation, maintenance, and communication of information security policies, standards, procedures, and guidelines to include the control areas listed in sections below;
C. Development and maintenance of relationships with external organizations to stay abreast of current and emerging security issues and for assistance, when applicable; and independent review of the effectiveness of the Contractor's information security program.

6.2 COMPLIANCE

The Contractor shall develop and implement processes to ensure its compliance with all statutory, regulatory, contractual, and internal policy obligations applicable to this Contract. Examples include but are not limited to General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act of 1996 (HIPAA), IRS-1075. Contractor shall timely update its processes as applicable standards evolve.

A. Within ten (10) Calendar Days after award, the Contractor shall provide the State with contact information for the individual or individuals responsible for maintaining a control framework that captures statutory, regulatory, contractual, and policy requirements relevant to the organization's programs of work and information systems;
B. Throughout the solution development process, Contractor shall implement processes to ensure security assessments of information systems are conducted for all significant development and/or acquisitions, prior to information systems being placed into production; and
C. The Contractor shall also conduct periodic reviews of its information systems on a defined frequency for compliance with statutory, regulatory, and contractual requirements. The Contractor shall document the results of any such reviews.

6.3 PERSONNEL SECURITY

The Contractor shall implement processes to ensure all personnel having access to relevant State information have the appropriate background, skills, and training to perform their job responsibilities in a competent, professional, and secure manner. Workforce security controls shall include, at a minimum:

A. Position descriptions that include appropriate language regarding each role's security requirements;
B. To the extent permitted by law, employment screening checks are conducted and successfully passed for all personnel prior to beginning work or being granted access to information assets;
C. Rules of behavior are established and procedures are implemented to ensure personnel are aware of and understand usage policies applicable to information and information systems;
D. Access reviews are conducted upon personnel transfers and promotions to ensure access levels are appropriate;
E. Contractor disables system access for terminated personnel and collects all organization owned assets prior to the individual's departure; and
F. Procedures are implemented that ensure all personnel are aware of their duty to protect information assets and their responsibility to immediately report any suspected information security incidents.

6.4 SECURITY AWARENESS AND TRAINING

The Contractor shall provide periodic and on-going information security awareness and training to ensure personnel are aware of information security risks and threats, understand their responsibilities, and are aware of the statutory, regulatory, contractual, and policy requirements that are intended to protect information systems and State Confidential Information from a loss of confidentiality, integrity, availability, and privacy. Security awareness and training shall include, at a minimum:

A. Personnel are provided with security awareness training upon hire and at least annually, thereafter;
B. Security awareness training records are maintained as part of the personnel record;
C. Role-based security training is provided to personnel with respect to their duties or responsibilities (e.g., network and systems administrators require specific security training in accordance with their job functions); and
D. Individuals are provided with timely information regarding emerging threats, best practices, and new policies, laws, and regulations related to information security.

6.5 RISK MANAGEMENT

The Contractor shall establish requirements for the identification, assessment, and treatment of information security risks to operations, information, and/or information systems. Risk management requirements shall include, at a minimum:

A. An approach that categorizes systems and information based on their criticality and sensitivity;
B. An approach that ensures risks are identified, documented, and assigned to appropriate personnel for assessment and treatment;
C. Risk assessments shall be conducted throughout the lifecycles of information systems to identify, quantify, and prioritize risks against operational and control objectives and to design, implement, and exercise controls that provide reasonable assurance that security objectives will be met; and
D. A plan under which risks are mitigated to an acceptable level and remediation actions are prioritized based on risk criteria and timelines for remediation are established. Risk treatment may also include the acceptance or transfer of risk.

6.6 PRIVACY

If there is State Data associated with the Contract, this section is applicable.

A. Data Ownership. The State owns State Data. Contractor shall not obtain any right, title, or interest in any State Data, or information derived from or based on State Data.
B. Data usage, storage, and protection of Personal Data are subject to all applicable international, federal and state statutory and regulatory requirements, as amended from time to time, including, without limitation, those for HIPAA, Tax Information Security Guidelines for Federal, State, and Local Agencies (IRS Publication 1075), New Jersey State tax confidentiality statute, the New Jersey Privacy Notice found at NJ.gov, N.J.S.A. § 54:50-8, New Jersey Identity Theft Prevention Act, N.J.S.A. § 56:11-44 et. seq., the federal Drivers' Privacy Protection Act of

1994, Pub.L.103-322, and the confidentiality requirements of N.J.S.A. § 39:2-3.4. Contractor shall also conform to PCI DSS, where applicable.

C. Security: Contractor agrees to take appropriate administrative, technical, and physical safeguards reasonably designed to protect the security, privacy, confidentiality, and integrity of user information. Contractor shall ensure that State Data is secured and encrypted during transmission or at rest.

D. Data Transmission: The Contractor shall only transmit or exchange State Data with other parties when expressly requested in writing and permitted by and in accordance with requirements of the Contract or the State of New Jersey. The Contractor shall only transmit or exchange State Data with the State of New Jersey or other parties through secure means supported by current technologies.

E. Data Storage: All data provided by the State of New Jersey or State data obtained by the Contractor in the performance of the Contract must be stored, processed, and maintained solely in accordance with a project plan and system topology approved by the State Contract Manager. No State data shall be processed on or transferred to any device or storage medium including portable media, smart devices and/or USB devices, unless that device or storage medium has been approved in advance in writing by the State Contract Manager. The Contractor must not store or transfer State of New Jersey data outside of the United States.

F. Data Re-Use: All State Data shall be used expressly and solely for the purposes enumerated in the Contract Data shall not be distributed, repurposed, or shared across other applications, environments, or business units of the Contractor. No State Data shall be transmitted, exchanged, or otherwise passed to other contractors or interested parties except on a case-by-case basis as specifically agreed to in writing by the State Contract Manager.

G. Data Breach: In the event of any actual, probable or reasonably suspected Breach of Security, or any unauthorized access to or acquisition, use, loss, destruction, compromise, alteration or disclosure of any Personal Data, Contractor shall: (a) immediately notify the State of such Breach of Security, but in no event later than 24 hours after learning of such security breach; (b) designate a single individual employed by Contractor who shall be available to the State 24 hours per day, seven (7) days per week as a contact regarding Contractor's obligations under *Bid Solicitation Section 6.34 - Incident Response*; (c) not provide any other notification or provide any disclosure to the public regarding such Breach of Security without the prior written consent of the State, unless required to provide such notification or to make such disclosure pursuant to any applicable law, regulation, rule, order, court order, judgment, decree, ordinance, mandate or other request or requirement now or hereafter in effect, of any applicable governmental authority or law enforcement agency in any jurisdiction worldwide (in which case Contractor shall consult with the State and reasonably cooperate with the State to prevent any notification or disclosure concerning any Personal Data or Breach of Security); (d) assist the State in investigating, remedying and taking any other action the State deems necessary regarding any Breach of Security breach and any dispute, inquiry, or claim that concerns the Breach of Security; (e) follow all instructions provided by the State relating to the Personal Data affected or potentially affected by the Breach of Security; (f) take such actions as necessary to prevent future Breaches of Security; and (g) unless prohibited by an applicable statute or court order, notify the State of any third party legal process relating to any Breach of Security including, at a minimum, any legal process initiated by any governmental entity (foreign or domestic).

H. Minimum Necessary. Contractor shall ensure that State Data requested represents the minimum necessary information for the services as described in this Bid Solicitation and, unless otherwise agreed to in writing by the State, that only necessary individuals or entities who are familiar with and bound by the Contract will have access to the State Data in order to perform the work.

I. End of Contract Data Handling: Upon termination/expiration of this Contract the Contractor shall first return all State Data to the State in a usable format as defined in the Contract, or in an open standards machine-readable format if not. The Contractor shall then erase, destroy, and render unreadable all Contractor backup copies of State Data according to the standards enumerated in accordance with the State's most recent Media Protection policy, https://www.cyber.nj.gov/grants-and-resources/state-resources/statewide-information-security-manual-sismand certify in writing that these actions have been completed within 30 days after the termination/expiration of the Contract or within seven (7) days of the request of an agent of the State whichever should come first.

J. In the event of loss of any State Data or records where such loss is due to the intentional act, omission, or negligence of the Contractor or any of its subcontractors or agents, the Contractor shall be responsible for recreating such lost data in the manner and on the schedule set by the State Contract Manager. The Contractor shall ensure that all State Data is backed up and is recoverable by the Contractor. In accordance with prevailing federal or state law or regulations, the Contractor shall report the loss of State data.

6.7 ASSET MANAGEMENT

The Contractor shall implement administrative, technical, and physical controls necessary to safeguard information technology assets from threats to their confidentiality, integrity, or availability, whether internal or external, deliberate, or accidental. Asset management controls shall include at a minimum:

A. Information technology asset identification and inventory;
B. Assigning custodianship of assets; and
C. Restricting the use of non-authorized devices.

6.8 SECURITY CATEGORIZATION

The Contractor shall implement processes that classify information and categorize information systems throughout their lifecycles according to their sensitivity and criticality, along with the risks and impact in the event that there is a loss of confidentiality, integrity, availability, or breach of privacy. Information classification and system categorization includes labeling and handling requirements. Security categorization controls shall include the following, at a minimum:

A. Implementing a data protection policy;
B. Classifying data and information systems in accordance with their sensitivity and criticality;
C. Masking sensitive data that is displayed or printed; and
D. Implementing handling and labeling procedures.

6.9 MEDIA PROTECTION

The Contractor shall establish controls to ensure data and information, in all forms and mediums, are protected throughout their lifecycles based on their sensitivity, value, and criticality, and the impact that a loss of confidentiality, integrity, availability, and privacy would have on the Contractor, business partners, or individuals. Media protections shall include, at a minimum:

A. Media storage/access/transportation;
B. Maintenance of sensitive data inventories;
C. Application of cryptographic protections;
D. Restricting the use of portable storage devices;
E. Establishing records retention requirements in accordance with business objectives and statutory and regulatory obligations; and
F. Media disposal/sanitization.

6.10 CRYPOTGRAPHIC PROTECTIONS

The Contractor shall employ cryptographic safeguards to protect sensitive information in transmission, in use, and at rest, from a loss of confidentiality, unauthorized access, or disclosure. Cryptographic protections shall include at a minimum:

A. Using industry standard encryption algorithms;
B. Establishing requirements for encryption of data in transit;
C. Establishing requirements for encryption of data at rest; and
D. Implementing cryptographic key management processes and controls.

6.11 ACCESS MANAGEMENT

The Contractor shall establish security requirements and ensure appropriate mechanisms are provided for the control, administration, and tracking of access to, and the use of, the Contractor's information systems that contain or could be used to access State data. Access management plan shall include the following features:

A. Ensure the principle of least privilege is applied for specific duties and information systems (including specific functions, ports, protocols, and services), so processes operate at privilege levels no higher than necessary to accomplish required organizational missions and/or functions;
B. Implement account management processes for registration, updates, changes, and de-provisioning of system access;
C. Apply the principles of least privilege when provisioning access to organizational assets;

D. Provision access according to an individual's role and business requirements for such access;
E. Implement the concept of segregation of duties by disseminating tasks and associated privileges for specific sensitive duties among multiple people;
F. Conduct periodic reviews of access authorizations and controls.

6.12 IDENTITY AND AUTHENTICATION

The Contractor shall establish procedures and implement identification, authorization, and authentication controls to ensure only authorized individuals, systems, and processes can access the State's information and Contractor's information and information systems. Identity and authentication provide a level of assurance that individuals who log into a system are who they say they are. Identity and authentication controls shall include, at a minimum:

A. Establishing and managing unique identifiers (e.g., User-IDs) and secure authenticators (e.g., passwords, biometrics, personal identification numbers, etc.) to support nonrepudiation of activities by users or processes; and
B. Implementing multi-factor authentication (MFA) requirements for access to sensitive and critical systems, and for remote access to the Contractor's systems.

6.13 REMOTE ACESSS

The Contractor shall strictly control remote access to the Contractor's internal networks, systems, applications, and services. Appropriate authorizations and technical security controls shall be implemented prior to remote access being established. Remote access controls shall include at a minimum:

A. Establishing centralized management of the Contractor's remote access infrastructure;
B. Implementing technical security controls (e.g., encryption, multi-factor authentication, IP whitelisting, geo-fencing); and
C. Training users in regard to information security risks and best practices related remote access use.

In the event the Contractor shall be approved to utilize State-provided remote access connectivity to conduct work on systems, networks, and data repositories managed and hosted within the New Jersey Garden State Network (GSN) for State approved business, the Contractor shall collaborate with the State in accordance with State defined usage restrictions, configuration/connection requirements, and implementation guidance for remote access into the GSN.

6.14 SECURITY ENGINEERING AND ARCHITECTURE

The Contractor shall employ security engineering and architecture principles for all information technology assets, and such principles shall incorporate industry recognized leading security practices and sufficiently address applicable statutory and regulatory obligations. Applying security engineering and architecture principles shall include:

A. Implementing configuration standards that are consistent with industry-accepted system hardening standards and address known security vulnerabilities for all system components;
B. Establishing a defense in-depth security posture that includes layered technical, administrative, and physical controls;
C. Incorporating security requirements into the systems throughout their life cycles;
D. Delineating physical and logical security boundaries;
E. Tailoring security controls to meet organizational and operational needs;
F. Performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk;
G. Implementing controls and procedures to ensure critical systems fail-secure and fail-safe in known states; and
H. Ensuring information system clock synchronization.

6.15 CONFIGURATION MANAGEMENT

The Contractor shall ensure that baseline configuration settings are established and maintained in order to protect the confidentiality, integrity, and availability of all information technology assets. Secure configuration management shall include, at a minimum:

A. Hardening systems through baseline configurations; and
B. Configuring systems in accordance with the principle of least privilege to ensure processes operate at privilege levels no higher than necessary to accomplish required functions.

6.16 ENDPOINT SECURITY

The Contractor shall ensure that endpoint devices are properly configured, and measures are implemented to protect information and information systems from a loss of confidentiality, integrity, and availability. Endpoint security shall include, at a minimum:

A. Maintaining an accurate and updated inventory of endpoint devices;
B. Applying security categorizations and implementing appropriate and effective safeguards on endpoints;
C. Maintaining currency with operating system and software updates and patches;
D. Establishing physical and logical access controls;
E. Applying data protection measures (e.g., cryptographic protections);
F. Implementing anti-malware software, host-based firewalls, and port and device controls;
G. Implementing host intrusion detection and prevention systems (HIDS/HIPS) where applicable;
H. Restricting access and/or use of ports and I/O devices; and
I. Ensuring audit logging is implemented and logs are reviewed on a continuous basis.

6.17 ICS/SCADA/OT SECURITY

The Contractor shall implement controls and processes to ensure risks, including risks to human safety, are accounted for, and managed in the use of Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems and Operational Technologies (OT). ICS/SCADA/OT Security requires the application of all of the enumerated control areas in this Bid Solicitation, including, at a minimum:

A. Conducting risk assessments prior to implementation and throughout the lifecycles of ICS/SCADA/OT assets;
B. Developing policies and standards specific to ICS/SCADA/OT assets;
C. Ensuring the secure configuration of ICS/SCADA/OT assets;
D. Segmenting ICS/SCADA/OT networks from the rest of the Contractor's networks;
E. Ensuring least privilege and strong authentication controls are implemented;
F. Implementing redundant designs or failover capabilities to prevent business disruption or physical damage; and
G. Conducting regular maintenance on ICS/SCADA/OT systems.

6.18 INTERNET OF THINGS SECURITY

The Contractor shall implement controls and processes to ensure risks are accounted for and managed in the use of Internet of Things (IoT) devices including, but not limited to, physical devices, vehicles, appliances, and other items embedded with electronics, software, sensors, actuators, and network connectivity which enables these devices to connect and exchange data. IoT security shall include, at a minimum, the following:

A. Developing policies and standards specific to IoT assets;
B. Ensuring the secure configuration of IoT assets;
C. Conducting risk assessments prior to implementation and throughout the lifecycles of IoT assets;
D. Segmenting IoT networks from the rest of the Contractor's networks; and
E. Ensuring least privilege and strong authentication controls are implemented.

6.19 MOBILE DEVICE SECURITY

The Contractor shall establish administrative, technical, and physical security controls required to effectively manage the risks introduced by mobile devices used for organizational business purposes. Mobile device security shall include, at a minimum, the following:

A. Establishing requirements for authorization to use mobile devices for organizational business purposes;
B. Establishing Bring Your Own Device (BYOD) processes and restrictions;
C. Establishing physical and logical access controls;

D. Implementing network access restrictions for mobile devices;
E. Implementing mobile device management solutions to provide centralized management of mobile devices and to ensure technical security controls (e.g., encryption, authentication, remote-wipe, etc.) are implemented and updated as necessary;
F. Establishing approved application stores from which applications can be acquired;
G. Establishing lists approved applications that can be used; and
H. Training of mobile device users regarding security and safety.

6.20 NETWORK SECURITY

The Contractor shall implement defense-in-depth and least privilege strategies for securing the information technology networks that it operates. To ensure information technology resources are available to authorized network clients and protected from unauthorized access, the Contractor shall:

A. Include protection mechanisms for network communications and infrastructure (e.g., layered defenses, denial of service protection, encryption for data in transit, etc.);
B. Include protection mechanisms for network boundaries (e.g., limit network access points, implement firewalls, use Internet proxies, restrict split tunneling, etc.);
C. Control the flow of information (e.g., deny traffic by default/allow by exception, implement Access Control Lists, etc.); and
D. Control access to the Contractor's information systems (e.g., network segmentation, network intrusion detection and prevention systems, wireless restrictions, etc.).

6.21 CLOUD SECURITY

The Contractor shall establish security requirements that govern the use of private, public, and hybrid cloud environments to ensure risks associated with a potential loss of confidentiality, integrity, availability, and privacy are managed. This shall ensure, at a minimum, the following:

A. Security is accounted for in the acquisition and development of cloud services;
B. The design, configuration, and implementation of cloud-based applications, infrastructure and system-system interfaces are conducted in accordance with mutually agreed-upon service, security, and capacity-level expectations;
C. Security roles and responsibilities for the Contractor and the cloud provider are delineated and documented; and
D. Controls necessary to protect sensitive data in public cloud environments are implemented.

6.22 CHANGE MANAGEMENT

The Contractor shall establish controls required to ensure change is managed effectively. Changes are appropriately tested, validated, and documented before implementing any change on a production network. Change management provides the Contractor with the ability to handle changes in a controlled, predictable, and repeatable manner, and to identify, assess, and minimize the risks to operations and security. Change management controls shall include, at a minimum, the following:

A. Notifying all stakeholder of changes;
B. Conducting a security impact analysis and testing for changes prior to rollout; and
C. Verifying security functionality after the changes have been made.

6.23 MAINTENANCE

The Contractor shall implement processes and controls to ensure that information assets are properly maintained, thereby minimizing the risks from emerging information security threats and/or the potential loss of confidentiality, integrity, or availability due to system failures. Maintenance security shall include, at a minimum, the following:

A. Conducting scheduled and timely maintenance;
B. Ensuring individuals conducting maintenance operations are qualified and trustworthy; and
C. Vetting, escorting, and monitoring third-parties conducting maintenance operations on information technology assets.

6.24 THREAT MANAGEMENT

The Contractor shall establish effective communication protocols and processes to collect and disseminate actionable threat intelligence, thereby providing component units and individuals with the information necessary to effectively manage risk associated with new and emerging threats to the organization's information technology assets and operations. Threat management includes, at a minimum:

A. Developing, implementing, and governing processes and documentation to facilitate the implementation of a threat awareness policy, as well as associated standards, controls, and procedures.
B. Subscribing to and receiving relevant threat intelligence information from the US CERT, the organization's vendors, and other sources as appropriate.

6.25 VULNERABILITY AND PATCH MANAGEMENT

The Contractor shall implement proactive vulnerability identification, remediation, and patch management practices to minimize the risk of a loss of confidentiality, integrity, and availability of information system, networks, components, and applications. Vulnerability and patch management practices shall include, at a minimum, the following:

A. Prioritizing vulnerability scanning and remediation activities based on the criticality and security categorization of systems and information, and the risks associated with a loss of confidentiality, integrity, availability, and/or privacy;
B. Maintaining software and operating systems at the latest vendor-supported patch levels;
C. Conducting penetration testing and red team exercises; and
D. Employing qualified third-parties to periodically conduct independent vulnerability scanning, penetration testing, and red-team exercises.

6.26 CONTINUOUS MONITORING

The Contractor shall implement continuous monitoring practices to establish and maintain situational awareness regarding potential threats to the confidentiality, integrity, availability, privacy and safety of information and information systems through timely collection and review of security-related event logs. Continuous monitoring practices shall include, at a minimum, the following:

A. Centralizing the collection and monitoring of event logs;
B. Ensuring the content of audit records includes all relevant security event information;
C. Protecting of audit records from tampering; and
D. Detecting, investigating, and responding to incidents discovered through monitoring.

6.27 SYSTEM DEVELOPMENT AND ACQUISTION

The Contractor shall establish security requirements necessary to ensure that systems and application software programs developed by the Contractor or third-parties (e.g., vendors, contractors, etc.) perform as intended to maintain information confidentiality, integrity, and availability, and the privacy and safety of individuals. System development and acquisition security practices shall include, at a minimum, the following:

A. Secure coding;
B. Separation of development, testing, and operational environments;
C. Information input restrictions;
D. Input data validation;
E. Error handling;
F. Security testing throughout development;
G. Restrictions for access to program source code; and
H. Security training of software developers and system implementers.

6.28 PROJECT AND RESOURCE MANAGEMENT

The Contractor shall ensure that controls necessary to appropriately manage risks are accounted for and implemented throughout the System Development Life Cycle (SDLC). Project and resource management security practices shall include, at a minimum:

A. Defining and implementing security requirements;
B. Allocating resources required to protect systems and information; and
C. Ensuring security requirements are accounted for throughout the SDLC.

6.29 CAPACITY AND PERFORMANCE MANAGEMENT

The Contractor shall implement processes and controls necessary to protect against avoidable impacts to operations by proactively managing the capacity and performance of its critical technologies and supporting infrastructure. Capacity and performance management practices shall include, at a minimum, the following:

A. Ensuring the availability, quality, and adequate capacity of computing, storage, memory, and network resources are planned, prepared, and measured to deliver the required system performance and future capacity requirements; and
B. Implementing resource priority controls to prevent or limit Denial of Service (DoS) effectiveness.

6.30 THIRD PARTY MANAGEMENT

The Contractor shall implement processes and controls to ensure that risks associated with third-parties (e.g., vendors, contractors, business partners, etc.) providing information technology equipment, software, and/or services are minimized or avoided. Third party management processes and controls shall include, at a minimum:

A. Tailored acquisition strategies, contracting tools, and procurement methods for the purchase of systems, system components, or system service from suppliers;
B. Due diligence security reviews of suppliers and third parties with access to the Contractor's systems and sensitive information;
C. Third party interconnection security; and
D. Independent testing and security assessments of supplier technologies and supplier organizations.

6.31 PHYSICAL AND ENVIRONMENTAL SECURITY

The Contractor shall establish physical and environmental protection procedures that limit access to systems, equipment, and the respective operating environments, to only authorized individuals. The Contractor ensures appropriate environmental controls in facilities containing information systems and assets, to ensure sufficient environmental conditions exist to avoid preventable hardware failures and service interruptions. Physical and environmental controls shall include, at a minimum, the following:

A. Physical access controls (e.g., locks, security gates and guards, etc.);
B. Visitor controls;
C. Security monitoring and auditing of physical access;
D. Emergency shutoff;
E. Emergency power;
F. Emergency lighting;
G. Fire protection;
H. Temperature and humidity controls;
I. Water damage protection; and
J. Delivery and removal of information assets controls.

6.32 CONTINGENCY PLANNING

The Contractor shall develop, implement, test, and maintain a contingency plan to ensure continuity of operations for all information systems that deliver or support essential or critical business functions on behalf of the Contractor. The plan shall address the following:

A. Backup and recovery strategies;
B. Continuity of operations;
C. Disaster recovery; and
D. Crisis management.

6.33 INCIDENT RESPONSE

The Contractor shall maintain an information security incident response capability that includes adequate preparation, detection, analysis, containment, recovery, and reporting activities. Information security incident response activities shall include, at a minimum, the following:

A. Information security incident reporting awareness;
B. Incident response planning and handling;
C. Establishment of an incident response team;
D. Cybersecurity insurance;
E. Contracts with external incident response services specialists; and
F. Contacts with law enforcement cybersecurity units.

7 MODIFICATIONS TO THE STANDARD TERMS AND CONDITIONS

7.1 CONFIDENTIALITY

Section 5.23.E of the Standard Terms and Conditions is deleted in its entirety and replaced with the following:

"The State and the Contractor agree to hold the other's Confidential Information in confidence, using at least the same degree of care used to protect its own Confidential Information."

7.2 WAIVERED CONTRACTS SUPPLEMENT

Sections II.A through II.G of the Waivered Contracts Supplement to the State of New Jersey Standard Terms and Conditions are deleted.

Section III of the Waivered Contracts Supplement is not applicable to this Contract.

8 QUOTE EVALUATION AND AWARD

8.1 RECIPROCITY FOR JURISDICTIONAL BIDDER PREFERENCE

In accordance with N.J.S.A. 52:32-1.4, the State of New Jersey will invoke reciprocal action against an out-of-State Bidder whose state or locality maintains a preference practice for its in-state Bidders. The State of New Jersey will use the annual surveys compiled by the Council of State Governments, National Association of State Procurement Officials, or the National Institute of Governmental Purchasing or a State's statutes and regulations to identify States having preference laws, regulations, or practices and to invoke reciprocal actions. The State of New Jersey may obtain additional information as it deems appropriate to supplement the stated survey information.

A Bidder may submit information related to preference practices enacted for a State or Local entity outside the State of New Jersey. This information may be submitted in writing as part of the Quote response, including the name of the locality having the preference practice, as well as identification of the county and state, and should include a copy of the appropriate documentation, i.e., resolution, regulation, law, notice to Bidder, etc. It is the responsibility of the Bidder to provide documentation with the Quote or submit it to the DOI within five (5) business days after the deadline for Quote submission. Written evidence for a specific procurement that is not provided to the DOI within five (5) business days after the deadline for Quote submission may not be considered in the evaluation of that procurement, but may be retained and considered in the evaluation of subsequent procurements.

8.2 CLARIFICATION OF QUOTE

After the Quote submission deadline, unless requested by the State as noted below, Bidder contact with the DOI regarding this RFQ and the submitted Quote is not permitted. After the Quotes are reviewed, one (1), some or all of the Bidders may be asked to clarify inconsistent statements contained within the submitted Quote. A request for clarification may be made in order to resolve minor ambiguities, irregularities, informalities or clerical errors. Clarifications cannot correct any deficiencies or material omissions and cannot be used to revise or modify a Quote.

8.3 ORAL PRESENTATIONS AND DEMONSTRATIONS

After the Quotes are reviewed, one, some or all of the Bidders may be asked to give an oral presentation concerning its Quote. The State may request the Bidder to provide a demonstration of the Bidder's systems. A Bidder may not attend the oral presentations or demonstrations of another Bidder.

8.4 STATE'S RIGHT TO WAIVE IRREGULARITIES OR OMISSIONS

The State reserves the right to waive minor irregularities or omissions in a Quote. The State also reserves the right to waive a requirement that is not material, provided that:

- the requirement is not mandated by law;
- all of the otherwise responsive quotes failed to meet the requirement; and
- the failure to comply with the requirement does not materially affect the procurement or the State's interests associated with the procurement.

8.5 STATE'S RIGHT TO CHECK REFERENCES

The State may consult with clients of the Bidder during the evaluation of Quotes. Such consultation is intended to assist the State in making a Contract award that is most advantageous to the State.

8.6 EVALUATION CRITERIA

All Quotes will be reviewed to determine responsiveness. Non-responsive Quotes will be rejected without evaluation. Responsive Quotes will be evaluated by an Evaluation Committee. The following evaluation criteria categories, separate or combined in some manner, and not necessarily listed in order of significance, will be used to evaluate Quotes received in response to this RFQ:

A. The firm's approach and plans to perform the services required by the Scope of Services contained in this RFQ;
B. The firm's documented experience in successfully completing contracts of similar size and scope to the services required by this RFQ;
C. The qualifications and experience of the firm's personnel assigned to the engagement, with emphasis on documented experience in successfully completing work on contracts of similar size and scope to the services required by this RFQ; and
D. The overall ability of the firm to mobilize, undertake and successfully complete the contract.

8.7 QUOTE DISCREPANCIES

In evaluating Quotes, discrepancies between words and figures will be resolved in favor of words. Discrepancies between Unit Prices and totals of Unit Prices will be resolved in favor of Unit Prices. Discrepancies in the multiplication of units of work and Unit Prices will be resolved in favor of the Unit Prices. Discrepancies between the indicated total of multiplied Unit Prices and units of work and the actual total will be resolved in favor of the actual total. Discrepancies between the indicated sum of any column of figures and the correct sum thereof will be resolved in favor of the correct sum of the column of figures.

8.8 BEST AND FINAL OFFER (BAFO)

The DOI may invite one (1) Bidder or multiple Bidders to submit a Best and Final Offer (BAFO). Said invitation will establish the time and place for submission of the BAFO. Any BAFO that does not result in more advantageous pricing to the State will not be considered, and the State will evaluate the Bidder's most advantageous previously submitted pricing.

The DOI may conduct more than one (1) round of BAFO in order to attain the best value for the State.

BAFOs will be conducted only in those circumstances where it is deemed to be in the State's best interests and to maximize the State's ability to get the best value. Therefore, the Bidder is advised to submit its best technical and price Quote in response to this RFQ since the State may, after evaluation, make a Contract award based on the content of the initial submission.

8.9 NEGOTIATION

After evaluating Quotes, the DOI may enter into negotiations with one (1) Bidder or multiple Bidders. The primary purpose of negotiations is to maximize the State's ability to obtain the best value based on the mandatory requirements, evaluation criteria, and cost. Multiple rounds of negotiations may be conducted with one (1) Bidder or multiple Bidders. Negotiations will be structured by DOI to safeguard information and ensure that all Bidders are treated fairly.

Negotiations will be conducted only in those circumstances where it is deemed by the DOI to be in the State's best interests and to maximize the State's ability to get the best value. Therefore, the Bidder is advised to submit its best technical and price Quote in response to this RFQ since the State may, after evaluation, make a Contract award based on the content of the initial submission.

8.10 POOR PERFORMANCE

A Bidder with a history of performance problems may be bypassed for consideration of an award issued as a result of this RFQ. The following materials may be reviewed to determine Bidder performance:

A. Contract cancellations for cause pursuant to *State of New Jersey Standard Terms and Conditions Section 5.7(B)*;
B. Information contained in Vendor performance records;
C. Information obtained from audits or investigations conducted by a local, state, or federal agency of the Bidder's work experience;
D. Current licensure, registration, and/or certification status and relevant history thereof; or
E. Bidder's status or rating with established business/financial reporting services, as applicable.

Bidders should note that this list is not exhaustive.

8.11 RECOMMENDATION FOR AWARD

After the evaluation of the submitted Quotes is complete, the Evaluation Committee will recommend to the Director, the responsible Bidder whose Quote, conforming to this RFQ, is most advantageous to the State, price and other factors considered.

8.12 CONTRACT AWARD

Contract award(s) will be made with reasonable promptness by written notice to that responsible Bidder, whose Quote, conforming to this RFQ, is (are) most advantageous to the State, price, and other factors considered. Any or all Quotes may be rejected when the Director determines that it is in the State's best interest to do so. Notice of the state's intent to award shall be posted on the Division's website at DOI.RFP@treas.nj.gov.

9 PRICING

1. Given the statistics described in this questionnaire, please provide the total cost. Using the table below, please break down the total cost by one time implementation cost, ongoing and annual license, and support costs for the next 5 years. Year 1 costs would be for 65 users. For years 2-5, factor in the expected annual 10% increase in the user base.

Fee Type	Year 1	Year 2	Year 3	Extension Year 4	Extension Year 5
Annual Ongoing Charges					
Licensing					
Support					
Managed Service/Hosting					
Other (please add lines as needed)					
One-time charges		N/A	N/A	N/A	N/A
Implementation/Set-up		N/A	N/A	N/A	N/A
Other		N/A	N/A	N/A	N/A

2. What would be the increase in annual ongoing charges, if the number of users went up by 5 users? Indicate potential price increases for different user count ranges.
3. Describe pricing factors and licensing structure – including solution components (product modules, hosting services).
    a. If applicable, provide a % breakdown of annual ongoing charges, by module.
4. Outline license types and pricing differences for internal and external users.
5. Describe the licensing model in place for existing clients.
6. Describe implementation costs factors.
7. Describe on-going maintenance and support costs.

Failure to provide responses for pricing related questions above may deem a vendor's Quote non-responsive to the RFQ requirements.

10 GLOSSARY

Acceptance – The written confirmation by the Using Agency that Contractor has completed a Deliverable according to the specified requirements.

All-Inclusive Hourly Rate – An hourly rate comprised of all direct and indirect costs including, but not limited to: labor costs, overhead, fee or profit, clerical support, travel expenses, per diem, safety equipment, materials, supplies, managerial support and all documents, forms, and reproductions thereof. This rate also includes portal-to-portal expenses as well as per diem expenses such as food.

Best and Final Offer or BAFO – Pricing timely submitted by a Bidder upon invitation by the DOI after Quote opening, with or without prior discussion or negotiation.

Bid or RFQ – The documents which establish the bidding and Contract requirements and solicits Quotes to meet the needs of the Using Agencies as identified herein, and includes the RFQ, Standard Terms and Conditions (SSTC), State Price Sheet, Attachments, and Bid Amendments.

Bid Amendment – Written clarification or revision to this RFQ issued by the Division. Bid Amendments, if any, will be issued prior to Quote submission deadline.

Bidder – An entity offering a Quote in response to the RFQ.

Breach of Security – as defined by N.J.S.A. 56:8-161, means unauthorized access to electronic files, media, or data containing Personal Data that compromises the security, confidentiality, or integrity of Personal Data when access to the Personal Data has not been secured by encryption or by any other method or technology that renders the Personal Data unreadable or unusable. Good faith acquisition of Personal Data by an employee or agent of the Provider for a legitimate business purpose is not a Breach of Security, provided that the Personal Data is not used for purposes unrelated to the business or subject to further unauthorized disclosure.

Business Day – Any weekday, excluding Saturdays, Sundays, State legal holidays, and State-mandated closings unless otherwise indicated.

Calendar Day – Any day, including Saturdays, Sundays, State legal holidays, and State-mandated closings unless otherwise indicated.

Change Order – An amendment, alteration, or modification of the terms of a Contract between the State and the Contractor(s). A Change Order is not effective until it is signed and approved in writing by the Director or Deputy Director, Division of Purchase and Property.

Commercial off the Shelf Software or **COTS** - Software provided by Provider that is commercially available and that can be used with little or no modification.

Customized Software - COTS that is adapted or configured by Provider to meet specific requirements of the Authorized Purchaser that differ from the standard requirements of the base product. For the avoidance of doubt, "Customized Software" is not permitted to be sold to the State under the scope of this Contract.

Contract – The Contract consists of the Standard Terms and Conditions (SSTC), the RFQ, the responsive Quote submitted by a responsible Bidder as accepted by the State, the notice of award, any Best and Final Offer, any subsequent written document memorializing the agreement, any modifications to any of these documents approved by the State and any attachments, Bid Amendment or other supporting documents, or post-award documents including Change Orders agreed to by the State and the Contractor, in writing.

Contractor – The Bidder awarded a Contract resulting from this RFQ.

Deliverable – Goods, products, Services and Work Product that Contractor is required to deliver to the State under the Contract.

Discount – The standard price reduction applied by the Bidder to all items.

Division – The Division of Investment.

Evaluation Committee – A group of individuals or a Using Agency staff member assigned to review and evaluate Quotes submitted in response to this RFQ and recommend a Contract award.

Firm Fixed Price – A price that is all-inclusive of direct cost and indirect costs, including, but not limited to, direct labor costs, overhead, fee or profit, clerical support, equipment, materials, supplies, managerial (administrative) support, all documents, reports, forms, travel, reproduction, and any other costs.

Hardware – Includes computer equipment and any Software provided with the Hardware that is necessary for the Hardware to operate.

Internet of Things (IoT) - the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and network connectivity which enables these objects to connect and exchange data.

May – Denotes that which is permissible or recommended, not mandatory.

Mobile Device - means any device used by Provider that can move or transmit data, including but not limited to laptops, hard drives, and flash drives.

Must – Denotes that which is a mandatory requirement.

No Bid – The Bidder is not submitting a price Quote for an item on a price line.

No Charge – The Bidder will supply an item on a price line free of charge.

Non-Public Data - means data, other than Personal Data, that is not subject to distribution to the public as public information. Non-Public Data is data that is identified by the State as non-public information or otherwise deemed to be sensitive and confidential by the State because it contains information that is exempt by statute, ordinance, or administrative rule from access by the general public as public information.

Personal Data means –
"Personal Information" as defined in N.J.S.A. 56:8-161, means an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number,

(2) driver's license number or State identification card number or (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Dissociated data that, if linked would constitute Personal Information is Personal Information if the means to link the dissociated were accessed in connection with access to the dissociated data. Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state, or local government records, or widely distributed media; and/or

Data, either alone or in combination with other data, that includes information relating to an individual that identifies the person or entity by name, identifying number, mark or description that can be readily associated with a particular individual and which is not a public record, including but not limited to, Personally Identifiable Information (PII); government-issued identification numbers (e.g., Social Security, driver's license, passport); Protected Health Information (PHI) as that term is defined in the regulations adopted pursuant to the Health Insurance Portability and Accountability Act of 1996, P.L. No. 104-191 (1996) and found in 45 CFR Parts 160 to 164 and defined below; and Education Records, as that term is defined in the Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g.

Personally Identifiable Information or PII - as defined by the U.S. Department of Commerce, National Institute of Standards and Technology, means any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Project – The undertakings or services that are the subject of this RFQ.

Protected Health Information or **PHI** - has the same meaning as the term is defined in the regulations adopted pursuant to the Health Insurance Portability and Accountability Act of 1996, P.L. No. 104-191 (1996) and found in 45 CFR Parts 160 to 164 means Individually Identifiable Health Information (as defined below) transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer. The term "Individually Identifiable Health Information" has the same meaning as the term is defined in the regulations adopted pursuant to the Health Insurance Portability and Accountability Act of 1996, P.L. No. 104-191 (1996) and found in 45 CFR Parts 160 to 164 and means information that is a subset of Protected Health Information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Quote – Bidder's timely response to the RFQ including, but not limited to, technical Quote, price Quote including Best and Final Offer, any licenses, forms, certifications, clarifications, negotiated documents, and/or other documentation required by the RFQ.

Quote Submission Deadline - The date Quotes will be opened for evaluation and closed to further Quote submissions.

Request For Quotes (RFQ) – This series of documents, which establish the bidding and contract requirements and solicits Quotes to meet the needs of the Using Agencies as identified herein, and includes the RFQ, Standard Terms and Conditions (SSTC), price schedule, attachments, and Bid Amendments.

Security Incident - means the potential access by non-authorized person(s) to Personal Data or Non-Public Data that the Provider believes could reasonably result in the use, disclosure, or access or theft of State's unencrypted Personal Data or Non-Public Data within the possession or control of the Provider. A Security Incident may or may not turn into a Breach of Security.

Services – Includes, without limitation (i) Information Technology (IT) professional services, (ii) Software and Hardware-related services, including without limitation, installation, configuration, and training, and (iii) Software and Hardware maintenance and support and/or Software and Hardware technical support services.

Shall – Denotes that which is a mandatory requirement.

Should – Denotes that which is permissible or recommended, not mandatory.

Software - means, without limitation, computer programs, source codes, routines, or subroutines supplied by Provider, including operating software, programming aids, application programs, application programming interfaces and software products, and includes COTS, unless the context indicates otherwise.

Software as a Service or **SaaS** - means the capability provided to a purchaser to use the Provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through a thin client interface such as a Web browser (e.g., Web-based email) or a program interface. The purchaser does not manage or control the underlying cloud infrastructure, including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

State – The State of New Jersey.

State Confidential Information - shall consist of State Data and State Intellectual Property supplied by the State, any information or data gathered by the Contractor in fulfillment of the Contract and any analysis thereof (whether in fulfillment of the Contract or not);

State Contract Manager or SCM – The individual, responsible for the approval of all deliverables, i.e., tasks, sub-tasks, or other work elements in the Scope of Work. The SCM cannot direct or approve a Change Order.

State Data - means all data and metadata created or in any way originating with the State, and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the State, whether such data or output is stored on the State's hardware, the Provider's hardware or exists in any system owned, maintained or otherwise controlled by

the State or by the Provider. State Data includes Personal Data and Non-Public Data.

State Intellectual Property – Any intellectual property that is owned by the State. State Intellectual Property includes any derivative works and compilations of any State Intellectual Property.

State Price Sheet – the bidding document created by the State and attached to this RFQ on which the Bidder submits its Quote pricing as is referenced and described in the RFQ.

Subtasks – Detailed activities that comprise the actual performance of a task.

Subcontractor – An entity having an arrangement with a Contractor, whereby the Contractor uses the products and/or services of that entity to fulfill some of its obligations under its State Contract, while retaining full responsibility for the performance of all Contractor's obligations under the Contract, including payment to the Subcontractor. The Subcontractor has no legal relationship with the State, only with the Contractor.

Task – A discrete unit of work to be performed.

Third Party Intellectual Property – Any intellectual property owned by parties other than the State or Contractor and contained in or necessary for the use of the Deliverables. Third Party Intellectual Property includes COTS owned by Third Parties, and derivative works and compilations of any Third-Party Intellectual Property.

Unit Cost or Unit Price – All-inclusive, firm fixed price charged by the Bidder for a single unit identified on a price line.

Vendor – Either the Bidder or the Contractor.

Vendor Intellectual Property – Any intellectual property that is owned by Contractor and contained in or necessary for the use of the Deliverables or which the Contractor makes available for the State to use as part of the work under the Contract Vendor Intellectual Property includes COTS or Customized Software owned by Contractor, Contractor's technical documentation, and derivative works and compilations of any Vendor Intellectual Property.

Work Product – Every invention, modification, discovery, design, development, customization, configuration, improvement, process, Software program, work of authorship, documentation, formula, datum, technique, know how, secret, or intellectual property right whatsoever or any interest therein (whether patentable or not patentable or registerable under copyright or similar statutes or subject to analogous protection) that is specifically made, conceived, discovered, or reduced to practice by Contractor or Contractor's subcontractors or a third party engaged by Contractor or its subcontractor pursuant to the Contract Notwithstanding anything to the contrary in the preceding sentence, Work Product does not include State Intellectual Property, Vendor Intellectual Property or Third Party Intellectual Property.