



Request for Quotes

New Jersey Secure Choice Savings Program

Program Administrator Services

	Date	Time
Due Date For Questions	7/17/2023	5:00 PM
Submission Date	7/31/2023	5:00 PM

Dates are subject to change. All times contained in this Request for Quotes refer to Eastern Time. All changes will be reflected in Bid Amendments to the Request for Quotes posted on New Jersey Secure Choice Savings Program's website.

RFQ Issued By:

The New Jersey Secure Choice Savings Program Board

Date: June 15, 2023

TABLE OF CONTENTS

1.0	INTRODUCTION AND SUMMARY OF THE REQUEST FOR QUOTES	1
1.1	PURPOSE, INTENT AND BACKGROUND	1
1.2	ORDER OF PRECEDENCE OF CONTRACTUAL TERMS	1
2.0	PRE-QUOTE SUBMISSION INFORMATION	2
2.1	QUESTION AND ANSWER PERIOD	2
2.2	BID AMENDMENTS	2
3.0	QUOTE SUBMISSION REQUIREMENTS	3
3.1	QUOTE SUBMISSION	3
3.2	BIDDER RESPONSIBILITY	3
3.3	QUOTE CONTENT	3
3.4	FORMS, REGISTRATIONS AND CERTIFICATIONS TO BE SUBMITTED WITH QUOTE	3
3.4.1	OWNERSHIP DISCLOSURE FORM	3
3.4.2	DISCLOSURE OF INVESTMENT ACTIVITIES IN IRAN FORM	3
3.4.3	DISCLOSURE OF INVESTIGATIONS AND OTHER ACTIONS INVOLVING BIDDER FORM	3
3.4.4	MACBRIDE PRINCIPLES FORM	4
3.4.5	SERVICE PERFORMANCE WITHIN THE UNITED STATES	4
3.4.6	SUBCONTRACTOR UTILIZATION PLAN	4
3.4.7	PAY TO PLAY PROHIBITIONS	4
3.4.8	AFFIRMATIVE ACTION	5
3.4.9	STATE OF NEW JERSEY SECURITY DUE DILIGENCE THIRD-PARTY INFORMATION SECURITY QUESTIONNAIRES	5
3.4.10	BUSINESS REGISTRATION	5
3.4.11	CERTIFICATON REGARDING PROHIBITED ACTIVITIES WITH RUSSIA OR BELARUS	5
3.5	TECHNICAL QUOTE	5
3.5.1	MANAGEMENT OVERVIEW	5
3.5.1	CONTRACT MANAGEMENT AND COMMUNICATION WITH THE STATE CONTRACT MANAGER	6
3.5.3	REQUIRED PLANS	6
3.5.4	ORGANIZATIONAL EXPERIENCE	6
3.5.6	RESUMES	6
3.5.7	EXPERIENCE WITH CONTRACTS OF SIMILAR SIZE AND SCOPE	7
3.6	INSTRUCTIONS FOR THE SUBMISSION OF PRICING	7
4.0	SCOPE OF WORK	8
4.1	PROGRAM ADMINISTRATOR SERVICES - GENERAL PROGRAM-RELATED DUTIES AND PROVISIONS	8
4.2	PROGRAM TRUSTEE SERVICES - GENERAL PROGRAM-RELATED DUTIES AND PROVISIONS	8
4.3	WEB-BASED INDIVIDUAL RETIREMENT ACCOUNT (IRA) PLATFORM	8
4.4	PUBLIC SECURE CHOICE SAVINGS PROGRAM WEBSITE	8
4.5	RECORDKEEPING AND ADMINISTRATION	9
4.6	COMPLIANCE AND OVERSIGHT	10
4.7	REPORTS	10
4.8	MARKETING AND OUTREACH	10
4.9	CUSTOMER SERVICE	11
4.10	CLIENT SERVICES	12
5.0	GENERAL CONTRACT TERMS	13
5.1	CONTRACT TERM AND EXTENSION OPTION	13
5.2	CONTRACT TRANSITION	13
5.3	OWNERSHIP OF MATERIAL	13
5.4	ELECTRONIC PAYMENTS	14
5.5.1	NOTIFICATION OF LIQUIDATED DAMAGES	ERROR! BOOKMARK NOT DEFINED.
5.5.2	CONDITIONS FOR TERMINATION OF LIQUIDATED DAMAGES	ERROR! BOOKMARK NOT DEFINED.
5.5.3	SEVERABILITY OF INDIVIDUAL LIQUIDATED DAMAGES	ERROR! BOOKMARK NOT DEFINED.
5.5.4	WAIVER OF LIQUIDATED DAMAGES/LIQUIDATED DAMAGES NOT EXCLUSIVE REMEDY	ERROR! BOOKMARK NOT DEFINED.
5.5.6	PAYMENT OF LIQUIDATED DAMAGES	ERROR! BOOKMARK NOT DEFINED.
6.0	DATA SECURITY REQUIREMENTS – CONTRACTOR RESPONSIBILITY	15
6.1.	SECURITY PLAN	15

NOT

6.2.	INFORMATION SECURITY PROGRAM MANAGEMENT	15
6.3.	COMPLIANCE	15
6.4.	PERSONNEL SECURITY	15
6.5.	SECURITY AWARENESS AND TRAINING	16
6.6.	RISK MANAGEMENT	16
6.7.	PRIVACY	16
6.8.	ASSET MANAGEMENT	17
6.9.	SECURITY CATEGORIZATION	17
6.10.	MEDIA PROTECTION	18
6.11.	CRYPTOGRAPHIC PROTECTIONS	18
6.12.	ACCESS MANAGEMENT	18
6.13.	IDENTITY AND AUTHENTICATION	18
6.14.	REMOTE ACCESS	18
6.15.	SECURITY ENGINEERING AND ARCHITECTURE	19
6.16.	CONFIGURATION MANAGEMENT	19
6.17.	ENDPOINT SECURITY	19
6.18.	ICS/SCADA/OT SECURITY	19
6.19.	INTERNET OF THINGS SECURITY	20
6.20.	MOBILE DEVICE SECURITY	20
6.21.	NETWORK SECURITY	20
6.22.	CLOUD SECURITY	20
6.23.	CHANGE MANAGEMENT	21
6.24.	MAINTENANCE	21
6.25.	THREAT MANAGEMENT	21
6.26.	VULNERABILITY AND PATCH MANAGEMENT	21
6.27.	CONTINUOUS MONITORING	21
6.28.	SYSTEM DEVELOPMENT AND ACQUISITION	22
6.29.	PROJECT AND RESOURCE MANAGEMENT	22
6.30.	CAPACITY AND PERFORMANCE MANAGEMENT	22
6.31.	THIRD PARTY MANAGEMENT	22
6.32.	PHYSICAL AND ENVIRONMENTAL SECURITY	22
6.33.	CONTINGENCY PLANNING	23
6.34.	INCIDENT RESPONSE	23
6.35.	TAX RETURN DATA SECURITY	23
7.0	MODIFICATIONS TO THE STATE OF NEW JERSEY STANDARD TERMS AND CONDITIONS	26
7.1	INDEMNIFICATION	26
7.2	INSURANCE	27
7.2.1	PROFESSIONAL LIABILITY INSURANCE	27
7.2.2	CYBER BREACH INSURANCE	27
7.3	LIMITATION OF LIBAILITY OPTION	27
8.0	QUOTE EVALUATION AND AWARD	29
8.1	RECIPROCITY FOR JURISDICTIONAL BIDDER PREFERENCE	29
8.2	TIE QUOTES	29
8.3	STATE'S RIGHT TO INSPECT BIDDER'S FACILITIES	29
8.4	STATE'S RIGHT TO CHECK REFERENCES	29
8.5	EVALUATION CRITERIA	29
8.5.1	TECHNICAL EVALUATION CRITERIA	29
8.5.2	PRICE EVALUATION	29
8.6	QUOTE DISCREPANCIES	30
8.7	POOR PERFORMANCE	30
8.8	RECOMMENDATION FOR AWARD	30
8.9	CONTRACT AWARD	30
9.0	GLOSSARY	31

ATTACHMENT 1 – State of New Jersey Standard Terms and Conditions (9/1/2022)
ATTACHMENT 2 - State of New Jersey Security Due Diligence Third-Party Information Security Questionnaire

1.0 INTRODUCTION AND SUMMARY OF THE REQUEST FOR QUOTES

This Request for Quotes (RFQ) is issued by New Jersey Secure Choice Savings Program Board (“Board”).

1.1 PURPOSE, INTENT AND BACKGROUND

Governor Phil Murphy signed the New Jersey Secure Choice Act, [P.L. 2019, c. 56](#) (the “Act”), in March of 2019 to help private sector Employees save for their future in New Jersey (the “State”). The New Jersey Secure Choice Savings Program Board (the “Board”) is responsible for the start-up and administration of the New Jersey Secure Choice Savings Program (the “Program”), which is an automatic enrollment retirement savings program that allows private sector Employees to contribute, via payroll deductions, to an Individual Retirement Account (“IRA”) or Roth IRA (as defined under the Internal Revenue Code sections 408 and 408A, respectively).

The purpose of this RFQ is to solicit Quotes for qualified service providers who can provide Program Administration Services for the New Jersey Secure Choice Savings Program. The services sought shall include, but are not limited to: recordkeeping, trust services, participant service (e.g. call centers, web portals, reporting, statements and so on), employer support (e.g. call centers, web portals, and reporting) contributions processing, investment transaction processing, distribution processing and beneficiary tracking.

It is the intent of the State to award a Contract to that responsible Bidder whose quote conforming to this RFQ is most advantageous to the State of New Jersey (State), price and other factors considered. The State may award any or all price lines. The State, however, reserves the right to separately procure individual requirements that are the subject of the Contract during the Contract term, when in the sole discretion of the State doing so is deemed to be in the State’s best interest.

1.2 ORDER OF PRECEDENCE OF CONTRACTUAL TERMS

The Contract awarded, and the entire agreement between the parties, as a result of this RFQ shall consist of: (1) the final RFQ, (2) State of New Jersey Standard Terms and Conditions, and (3) the Quote. 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, listed from highest ranking to lowest ranking as noted above.

Any other terms or conditions not included with the Bidder’s Quote and accepted by the State, shall not be incorporated into the Contract awarded. Any references to external documentation, included 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 State of New Jersey Standard Terms and Conditions. In the event of any conflict between the terms of a document incorporated by reference, the terms and conditions of the RFQ and the State of New Jersey Standard Terms and Conditions shall prevail.

2.0 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 Board 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 to Executive Director Todd Hassler by email at: todd.hassler@scp.nj.gov. The Bidder should submit these questions with an email subject line titled: "NJ SCSP Program Admin RFP Questions".

The New Jersey Secure Choice Savings Program will not accept any question in person or by telephone concerning this RFQ. The cut-off 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 Addendum. Any Addendum to this RFQ 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 Secure Choice Savings Program's website.

2.2 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 with RFQ posted on New Jersey Secure Choice Savings Program's website. 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.

3.0 QUOTE SUBMISSION REQUIREMENTS

3.1 QUOTE SUBMISSION

In order to be considered for award, the Quote must be received by the Board by the required date and time indicated on the RFQ cover sheet. If the Quote opening deadline has been revised, the new Quote opening deadline shall be shown on the posted Bid Amendment. Quotes not received prior to the Quote opening deadline shall be rejected.

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 QUOTE CONTENT

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

- Forms
- Technical Quote
- State of New Jersey Security Due Diligence Third Party Information Security Questionnaire

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 the 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.

3.4 FORMS, REGISTRATIONS AND CERTIFICATIONS TO BE SUBMITTED WITH QUOTE

A Bidder is required to complete and submit the following forms.

3.4.1 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; or, (b) 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. N.J.S.A. 52:25-24.2.

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

3.4.2 DISCLOSURE OF INVESTMENT ACTIVITIES IN IRAN FORM

The Bidder should submit Disclosure of Investment Activities in Iran form 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 one (1) 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.

3.4.3 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.

3.4.4 MACBRIDE PRINCIPLES FORM

The Bidder should submit the MacBride Principles Form. 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.

3.4.5 SERVICE PERFORMANCE WITHIN THE UNITED STATES

The Bidder should submit a completed Source Disclosure Form. 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.

3.4.6 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.

3.4.7 PAY TO PLAY PROHIBITIONS

Pursuant to N.J.S.A. 19:44A-20.13 et seq. (P.L. 2005, c. 51, amended by P.L. 2023, c.30), 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 during the last four years that is determined by the Treasurer to be a conflict of interest.

Prior to awarding any Contract or agreement to any Business Entity pursuant to a fair and open process, as defined by N.J.S.A. 19:44A-20.23, the Business Entity proposed as the intended Contractor of the Contract shall submit the required forms / documents, certifying that either it has made no contributions, to a Continuing Political Committee during the last four years or reporting all contributions made by the Business Entity or any person or entity whose contributions are attributable to the Business Entity to a Continuing Political Committee in the last four years. Failure to submit the required forms will preclude award of a Contract under this Bid Solicitation.

3.4.8 AFFIRMATIVE ACTION

The intended Contractor and its named subcontractors must submit 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.

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

The Bidder shall complete and submit the State of New Jersey Security Due Diligence Third-Party Information Security Questionnaire (Questionnaire) with its Quote. 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 has executed a Confidentiality/Non-Disclosure Agreement which is attached to the Questionnaire. The Bidder must countersign the Confidentiality/Non-Disclosure Agreement and include it with its submitted Questionnaire. 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.

3.4.10 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.

3.4.11 CERTIFICATON REGARDING PROHIBITED ACTIVITIES WITH RUSSIA OR BELARUS

The Bidder should submit the Disclosure of Prohibited Activities in Russia / Belarus Form. 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 the Contractor is unable to so certify, the Contractor shall provide a detailed and precise description of such activities.

3.5 TECHNICAL QUOTE

The Bidder shall describe its approach and plans for accomplishing the work outlined in the Scope of Work. The Bidder must set forth its understanding of the requirements of this RFQ and its approach to successfully complete the Contract. The Bidder should include the level of detail it determines necessary to assist the Evaluation Committee in its review of the Bidder's Quote.

3.5.1 MANAGEMENT OVERVIEW

The Bidder shall set forth its overall technical approach and plans to meet the requirements of the RFQ in a narrative format. This narrative should 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 should 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 should 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.

3.5.1 CONTRACT MANAGEMENT AND COMMUNICATION WITH THE STATE CONTRACT MANAGER

The Bidder should describe its specific plans to manage, control and supervise the Contract to ensure satisfactory Contract completion of the Scope of Work. The description should include the Bidder's approach to communicate with the State Contract Manager including, but not limited to, status meetings, status reports, etc.

3.5.3 REQUIRED PLANS

The Bidder shall provide the following Plans and information with its submitted Quote:

- A. Implementation Plan - including a timeline for implementation and details for work to be completed each week and month.
- B. Roles and responsibilities matrix
- C. Communication strategy for Employers and Employees participating in the Program
- D. Risk mitigation strategy to avoid Program disruption and ensure continuity of the Contract work
- E. Training plan for Program staff
- F. Access control plan to ensure system access for Program staff
- G. Strategy, describing the post-implementation transition to the Bidders normative operations environment
- H. Contractor will establish, maintain, and comply with a privacy policy that is consistent with all applicable State, federal and industry requirements. Contractor will ensure its privacy policy complies with applicable federal or state laws or regulations.

3.5.4 ORGANIZATIONAL EXPERIENCE

- A. The Bidder shall include information relating to its organization, personnel, and experience, including, but not limited to, references, together with contact names and telephone numbers, evidencing the Bidder's qualifications, and capabilities to perform the services required by this RFQ. The Bidder should include the level of detail it determines necessary to assist the Evaluation Committee in its review of Bidder's Quote.

The Bidder should include an organization chart, with names showing management, supervisory and other key personnel (including Subcontractor management, supervisory, or other key personnel) to be assigned to the Contract.

- B. If the Bidder intends to use Subcontractors to, Bidder must indicate whether there is any relationship between the Bidder and the Subcontractor(s) identified. For example, please provide copies of the applicable affiliation agreement, Fee and/or Revenue Sharing Agreements.

3.5.6 RESUMES

Detailed resumes should be submitted for all management, supervisory, and key personnel to be assigned to the Contract. Resumes should emphasize relevant qualifications and experience of these individuals in successfully completing Contracts of a similar size and scope to those required by this RFQ. Resumes should include the following:

- A. The individual's previous experience in completing each similar Contract;
- B. Beginning and ending dates for each similar Contract;
- C. A description of the Contract demonstrating how the individual's work on the completed Contract relates to the individual's ability to contribute to successfully providing the services required by this RFQ; and
- D. With respect to each similar Contract, the name and address of each reference together with a person to contact for a reference check and a telephone number.

The Bidder should provide detailed resumes for each 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 designated to perform.

3.5.7 EXPERIENCE WITH CONTRACTS OF SIMILAR SIZE AND SCOPE

The Bidder should provide a comprehensive listing of contracts of similar size and scope that it has successfully completed, as evidence of the Bidder's ability to successfully complete services similar to those required by this RFQ. Emphasis should be placed on contracts that are similar in size and scope to the work required by this RFQ. A description of all such contracts should be included and should show how such contracts relate to the ability of the firm to complete the services required by this RFQ. For each such contract listed, the Bidder should provide two (2) names and telephone numbers of individuals for contracting party. Beginning and ending dates should also be given for each contract.

The Bidder must provide details of any negative actions taken by other contracting entities against them in the course of performing these projects including, but not limited to, receipt of letters of potential default, default, cure notices, termination of services for cause, or other similar notifications/processes. Additionally, the Bidder should provide details, including any negative audits, reports, or findings by any governmental agency for which the Bidder is/was the Contractor on any contracts of similar scope. In the event a Bidder neglects to include this information in its Quote, the Bidder's omission of necessary disclosure information may be cause for rejection of the Bidder's Quote by the State.

The Bidder should provide documented experience to demonstrate that each Subcontractor has successfully performed work on contracts of a similar size and scope to the work that the Subcontractor is designated to perform in the Bidder's Quote. The Bidder must provide a detailed description of services to be provided by each Subcontractor.

3.6 INSTRUCTIONS FOR THE SUBMISSION OF PRICING

The Contractor shall disclose its compensation plan through a detailed description of the total compensation arrangement that will be earned from the Program. This description shall include a summary of the total expected compensation per year, how and where compensation will be derived, and a description of the compensation arrangement that will provide the Program with the ability to calculate the compensation and make informed assessments concerning the prudence of the arrangements.

4.0 SCOPE OF WORK

In delivering the services under this section, the Contractor will exercise care, skill, prudence and diligence that a prudent man acting in a like capacity and familiar with such matters would use in the conduct of similar enterprise.

4.1 Program Administrator Services - General Program-Related Duties and Provisions

- A. Contractor may not engage an affiliate or a third-party (including an approved subcontractor) to do anything on its behalf that contractor is prohibited from doing directly under this Contract or the applicable law, rules, regulations, bulletins, and advisory opinions.
- B. At all times, Contractor shall utilize approved, qualified personnel to perform the services. Contractor shall be responsible for any economic detriment caused by Contractor's failure to use such personnel.
- C. Contractor shall have no right, or title to, or interest in the accounts, assets held in the accounts, program assets, or any program records.

4.2 Program Trustee Services - General Program-Related Duties and Provisions

Provide all trustee, fund administration, and fund accounting services necessary to support the investments, including, but not limited to, the following: custody, segregation of funds, cash management, banking services, and purchase and sale of underlying investment products to effectuate Participants' directions.

4.3 Web-based Individual Retirement Account (IRA) Platform

- A. Contractor shall provide a modern, accessible, secure online IRA platform that allows Employees and Employers to easily perform all aspects of plan/account set-up and management. The IRA platform shall:
 - i. Provide employers and employees with instructions and information regarding the facilitation of exemptions and enrollment for employers, and opt-out for employees.
 - ii. Allow employers to easily perform all necessary administrative tasks, including, but not limited to:
 - iii. Uploading and managing employee rosters and data;
 - iv. Inputting, changing, and otherwise managing payroll contributions for employees;
 - v. Integrating with payroll providers; and
 - vi. Designating authorized individuals to access the employer portal.
- B. Allow Employees to easily and reliably perform all self-service account management and maintenance, including, but not limited to the following:
 - i. Change investment elections;
 - ii. Change contribution levels;
 - iii. Transfer invested monies between portfolios;
 - iv. Request contributions and distributions (within program limits);
 - v. Update profile and demographic information;
 - vi. Change beneficiary designations/changes;
 - vii. Update passwords;
 - viii. View and download statements, confirmations, tax forms, and other pertinent documents; and
 - ix. View account information (i.e., account balances, historical transactions, earnings, and performance data).
- C. Provide a secure Employee and Employer portal for users to upload documents and other forms.
- D. Utilize technology which incorporates industry-standard security procedures in addition to having a recovery plan for contingencies such as data breaches.
- E. Be mobile device-compatible.
- F. Fully comply with Americans with Disabilities Act (ADA) laws, regulations, and standards, including compliance with the latest federal and state (as applicable) accessibility guidelines and applicable notification laws and regulations governing notices that must be given to employees concerning benefit eligibility.
- G. Be available to Program participants 24 hours a day, every day, with reasonable exceptions for pre-planned, pre-noticed maintenance down-time.

4.4 Public Secure Choice Savings Program Website

- A. Contractor shall provide a public-facing website specific to the Program and to its participants. The website shall provide all relevant program information to employers and employees and shall be mobile optimized, compatible with all major web browsers, and ADA compliant. Contractor’s responsibilities may include, but not be limited to the following:
 - i. Website design and build;
 - ii. Hosting and maintenance;
 - iii. Ongoing creation of site content including interactive features such as modeling tools and retirement calculators;
 - iv. Directing/linking users to pertinent actions (e.g., enrollment, login to employer and employee portals, etc.);
 - v. Developing and updating FAQs based on State feedback; and
 - vi. Hosting plan resources, forms, disclosures, and documents.
- B. Contractor shall make reasonable updates and changes to website design and content within five (5) business days of a change request from the State.
- C. Contractor, at the request of the State Contract Manager, will generate robust website and webpage reporting, including, by way of example and not limitation, details concerning traffic to specific webpages, account activity, user report generation, click-rates, time spent on pages, etc.

4.5 Recordkeeping and Administration

Contractor shall provide all recordkeeping and administrative services necessary to ensure the effective operation of the Program, in accordance with applicable federal and state laws and regulations. These services include, but are not limited to the following:

- A. Keeping secure and accurate records for each employer and employee account and for the Program as a whole.
- B. Collecting state administrative fees and remitting them to the program.
- C. Processing account enrollments and account closures (including handling any operations necessary following the death of a participant).
- D. Conducting comprehensive “know your customer” and Office of Foreign Assets Control screening during enrollment and on an ongoing basis, if required.
- E. Processing and recording the purchase, sale, and exchange of units in the program.
- F. Providing separate accounting for each participant including contributions, investment changes and distribution history, on a daily basis, providing all custodial, fund accounting, and banking services necessary to support the program’s operations, such as:
 - i. Custodianship of assets;
 - ii. Segregation of funds;
 - iii. Cash management;
 - iv. Automated clearing house (ACH) processing;
 - v. Net Asset Value calculation; and
 - vi. Assessing and remitting the Program fees within statutory limits.
- G. Administering a default provision (with a holding period or at a set dollar amount, and designated default portfolios) for employees who do not select investments.
- H. Processing contributions via ACH, payroll deduction, and check.
- I. Permitting Employees to contribute to multiple portfolios.
- J. Monitoring IRA contribution limits and preventing accounts from making excess contributions.
- K. Processing distributions via ACH and check.
- L. Enforcing hold times according to industry best practices, in order to prevent fraud and loss.
- M. Supporting decumulation strategies and options adopted by the Program.
- N. Processing IRA rollovers to and from qualified retirement plans.
- O. Supporting the use of all investment options selected by the Program.
- P. Creating all Program forms necessary for account set-up, maintenance and transacting (mirroring the enrollment and self-service functions available on the web-based IRA platform).
- Q. Handling all customer fulfillment requests for Program literature, forms, or other information.
- R. Managing a post office box or other central mailing address where participants can send in forms, documentation, or contributions.

- S. Processing all account transactions, forms, and other instructions accurately and in a timely manner.
- T. Providing quarterly account statements according to the participant's preferred method of receipt (paper mail or electronic delivery).
- U. Providing account confirmations and other correspondence to participants as necessary.
- V. Completing and distributing all required IRS tax forms (e.g., 1099-r and form 5498).
- W. Establishing a data exchange to intake information regarding eligible employers.
- X. Developing and distributing compliance notices to eligible employers.
- Y. Assisting the Program in administration of any current or future statutory grant programs to incentivize employer compliance.
- Z. Distributing Program disclosures as dictated by law and industry best practice, and as may be directed from time to time by Program staff.
- AA. Collaborating with other stakeholders, such as investment managers, banking institutions and payroll providers, as directed by the Program.

4.6 Compliance and Oversight

Contractor shall be responsible for ensuring the Program has proper legal structure, oversight, and compliance in accordance with all applicable federal and state laws and regulations. Contractor shall:

- A. Administer the Program as a fiduciary for Employers and Employees.
- B. Administer the Program and otherwise provide services in compliance with all relevant statutes, regulations, and industry best practices.
- C. Monitor for legal and regulatory changes that may affect the Program, and report any necessary compliance-related changes to Program.
- D. Prepare and distribute a Program disclosure statement and any supplements thereto, to Program participants.
- E. Prepare and distribute the required IRA disclosure documentation and custodial agreement and any supplements thereto, to Program Employers and/or Employees.
- F. Engage an independent third-party firm to prepare annual audited financial statements for the Program reporting monthly tracking metrics.
- G. Report to the Program immediately any identified fiduciary breach or possible violation of or failure to fully comply with applicable laws and regulations.
- H. Report to the Program immediately any operational failure that could result in financial impact to the participants, fiduciary breaches, or violation of law or regulations.
- I. Contractor shall be required to reimburse the Program for the costs of any fine(s), penalty(s) and/or taxes assessed to the Program which result from the Contractor's failure to perform in full accordance with its fiduciary duty, any applicable laws or regulations, or the industry standards.

4.7 Reports

- A. Contractor shall be responsible for generating and distributing reports regarding the Program, to Program personnel with approved access control, in accordance with applicable federal and state laws and regulations. These reports shall include, but not be limited to, the following:
 - i. Tracking metrics, which will be defined by the Program.
 - ii. Quarterly report: this report shall detail employer compliance, exemptions, enrollments, employee opt-out rates, contribution rates, investment options, customer service matters, call volumes, outcomes, and other relevant information.
 - iii. Ad-hoc report: this report shall consist of any requested, and available information.
 - iv. Annual report: this report shall consist of monthly and quarterly data, and any additional information as requested by the states.
 - v. Any other reports required by the Program.
- B. Program shall have access to the Employer and Employee data and be able to run any reports.
- C. The Contractor shall provide an annual report detailing the both direct and indirect compensation earned from the Program. The State Contract Manager, at his/her discretion, may request that the compensation earned be renegotiated with the Program.

4.8 Marketing and Outreach

- A. Contractor shall provide marketing and outreach services to the State in order to reach and educate the broadest audience. These services shall include, but are not limited to:
 - i. Supporting annual Marketing Plan development and execution;
 - ii. Collaborating with other stakeholders as directed by the Program;
 - iii. Utilize proper branding and work with the State to developing slogans for Program;
 - iv. Creating and producing promotional materials for the Program;
 - v. Creating and producing educational materials for Employers, Employees, and stakeholders;
 - vi. Supporting State efforts to develop a financial literacy curriculum designed to help Employers and Employees understand the Program and maximize the Program’s benefits;
 - vii. Delivering presentations and otherwise communicating with stakeholders, Employers, and Employees;
 - viii. Tracking and analyzing Program SEO and site analytics; and
 - ix. Assisting in the planning and execution of public launch events for the Program.
- B. Contractor shall also assist the Program with marketing and outreach efforts, which include the following:
 - i. Social media accounts and marketing campaigns;
 - ii. Digital and print marketing campaigns;
 - iii. Maintain proper branding and developing slogans for the Program;
 - iv. Creating and producing promotional materials for the Program; and
 - v. Working with any marketing firms the Program may retain.
- C. Contractor must obtain the prior written consent of the State prior to using their name, logo, seal, trademark or brand name on any program material or on any other advertising, publicity, or promotion material.
- D. Contractor shall must obtain the prior written consent of the Program prior to using any of the program data in a marketing program or campaign.
- E. Contractor shall must obtain the prior written consent of the Program prior to sharing or selling any of the Program data.

Contractor agrees that the Program may create marketing performance standards that are designed to evaluate Contractor’s marketing efforts and reach within the State, and that Contractor shall thereafter provide information, data, reports and such other materials as may be requested by the Program to understand and evaluate Contractor’s marketing efforts. Contractor agrees these marketing performance standards may include requirements that Contractor reach specific percentages of eligible participants (both employers and employees), as well as other stakeholders as identified by the Program, such as advocates, interest groups, partners, and providers.

Contractor shall provide the state with regular updates on:

- A. Marketing efforts;
- B. Marketing expenditures; and
- C. The results (effectiveness) of marketing efforts.

4.9 Customer Service

Contractor shall provide best-in-class customer service necessary to ensure efficient, supportive Program operation. Contractor shall perform all necessary customer service for the Program, as outlined in herein and as otherwise may be reasonably necessary to operate the Program. This includes, but is not limited to the following:

- A. Providing phone, email, and web-based chat support from 8:00 a.m. to 5:00 p.m., Monday through Friday, excluding State holidays.
- B. Providing callers with a voice messaging system during times that the call center is unavailable.
- C. Utilizing a customer authentication protocol to prevent unauthorized account access.
- D. Providing multilingual staff who can communicate at a minimum in English and Spanish.
- E. Providing training for all customer service representatives to ensure staff has ample knowledge of the Program.
- F. Adhering to customer service support standards mutually agreed upon by Program and Contractor during the implementation period.
- G. Establishing an escalation protocol, to be approved by the Program, for the quick resolution of customer complaints and difficult issues.

- H. Recording and regularly reviewing calls and emails with Employers and Account Holders for quality control purposes, and making such recordings available to the State upon request.
- I. Performing post-service satisfaction surveys and reporting results monthly to the State.
- J. All customer service representative shall be knowledgeable about the Program disclosure booklet, the Program materials, and Program policies and procedures.

4.10 Client Services

Contractor shall inform and consult with the State regarding the following:

- A. Contractor shall notify the State of any proposed changes to Key Personnel prior to implementing such changes. Contractor will notify the State in writing that changes have been made, within two calendar days after implementing such changes. In the event of any changes to Key Personnel, Contractor shall immediately designate interim Key Personnel reasonably acceptable to the State and, within six months, shall designate permanent Key Personnel.
- B. Program performance and operations.
- C. Attending meetings and providing program information, as requested.
- D. Being available via phone and/or email between the hours of 8:00 a.m. and 5:00 p.m., Monday through Friday, State holidays excluded.
- E. Providing Program files, records, documents and data to the State, that are in Contractor's possession and control, upon request.

5.0 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, services or commodities 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, goods 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 3 years.

This Contract may be extended up to maximum of three (3) 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 180 calendar days beyond the expiration date of this Contract, including any extensions exercised. During the transition period, the Contractor will be required to perform all work under the contract, and assist the Board transitioning the work to a new contract is required. Contract shall generate and deliver all records and/or reports, in the manner prescribed by the Board, to the new contractor.

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 1.4 – 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. The State’s license to Contractor is limited by the term of the Contract and the confidentiality obligations set forth in *RFQ Section 6 – Data Security Requirements – Contractor Responsibility*.
- 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 ELECTRONIC PAYMENTS

With the award of this Contract, the successful Contractor(s) will be required to receive its payment(s) electronically. In order to receive your payments via automatic deposit from the State of New Jersey, you must complete the EFT information within your [NJSTART](#) Vendor Profile. Please refer to the Quick Reference Guide entitled “Vendor Profile Management – Company Information and User Access” for instructions. The Quick Reference Guide is available on the [NJSTART Vendor Support Page](#).

6.0 DATA SECURITY REQUIREMENTS – CONTRACTOR RESPONSIBILITY

6.1. SECURITY PLAN

The Contractor shall submit a detailed Security Plan that addresses the Contractor's approach to meeting each applicable security requirement outlined below, to the State, no later than thirty (30) Calendar Days after the award of the Contract. The State approval of the Security Plan shall be set forth in writing. In the event that the State reasonably rejects the Security Plan after providing the Contractor an opportunity to cure, the Director may terminate the Contract pursuant to the SSTC.

6.2. 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
- D. Independent review of the effectiveness of the Contractor's information security program.

6.3. 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.

6.4. 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.

6.5. 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.

6.6. 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.

6.7. 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, N.J.S.A. 54:50-8, the New Jersey Privacy Notice found at NJ.gov 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 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.nj.gov/it/docs/ps/NJ_Statewide_Information_Security_Manual.pdf, and 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.

6.8. 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.

6.9. 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.

6.10.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.

6.11.CRYPTOGRAPHIC 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.

6.12.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.

6.13.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 provides 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.

6.14.REMOTE ACCESS

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.

6.15.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.

6.16.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.

6.17.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.

6.18.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.

6.19.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.

6.20.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.

6.21.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.).

6.22.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.

6.23.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.

6.24.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.

6.25.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.

6.26.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.

6.27.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.

6.28.SYSTEM DEVELOPMENT AND ACQUISITION

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.

6.29.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.

6.30.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.

6.31.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.

6.32.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.

6.33. 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.

6.34. 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.

6.35. TAX RETURN DATA SECURITY

A. PERFORMANCE

1. In performance of this Contract, the Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:
2. All work will be done under the supervision of the Contractor or the Contractor's employees;
3. Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract. Disclosure to anyone other than an officer or employee of the Contractor will be prohibited;
4. All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material;
5. The Contractor certifies that the data processed during the performance of this Contract will be completely purged from all data storage components of his or her computer facility, and the Contractor will retain no output at the time the work is completed. If immediate purging of all data storage

components is not possible, the Contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures;

6. Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used;
7. All computer systems receiving, processing, storing, or transmitting federal tax information must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to federal tax information.
8. No work involving federal tax information furnished under this Contract will be subcontracted without prior written approval of the IRS;
9. The Contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office; and
10. The agency will have the right to void this Contract if the Contractor fails to provide the safeguards described above.

B. CRIMINAL/CIVIL SANCTIONS

1. Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as \$5,000 or imprisonment for as long as five (5) years', or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than \$1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1;
2. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Contract. Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as \$1,000 or imprisonment for as long as one (1) year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for federal employees] in an amount equal to the sum of the greater of \$1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC section 7213A and 7431;
3. Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to Contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a Contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000; and

4. Granting a Contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain its authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, Contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and Exhibit 5, IRC Sec. 7213 Unauthorized Disclosure of Information). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. For both the initial certification and the annual certification, the Contractor should sign, either with ink or electronic signature, a confidentiality statement certifying its understanding of the security requirements.

C. INSPECTION

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the Contractor for inspection of the facilities and operations provided for the performance of any work under this Contract. On the basis of such inspection, specific measures may be required in cases where the Contractor is found to be noncompliant with Contract safeguards.

7.0 MODIFICATIONS TO THE STATE OF NEW JERSEY STANDARD TERMS AND CONDITIONS

7.1 INDEMNIFICATION

Section 4.1 of the State of New Jersey Standard Terms and Conditions is deleted in its entirety and replaced with the following:

4.1 INDEMNIFICATION

A. CONTRACTOR RESPONSIBILITIES - The Contractor's liability to the State and its employees in third party suits shall be as follows:

1. The Contractor shall indemnify, defend, and save harmless the State and its officers, agents, servants and employees, from and against any and all third-party claims, demands, suits, actions, recoveries, judgments and costs and expenses in connection therewith:
 - i. For or on account of the loss of life, tangible property (not including lost or damaged data) or injury or damage to the person, body or property (not including lost or damaged data) of any person or persons whatsoever, which shall arise from or result directly or indirectly from the work and/or products supplied under this Contract; and
 - ii. For or on account of the use of any patent, copyright, trademark, trade secret or other proprietary right of any copyrighted or uncopied composition, secret process, patented or unpatented invention, article or appliance ("Intellectual Property Rights") furnished or used in the performance of the contract; and
 - iii. For or on account of a Breach of Security resulting from Contractor's breach of its obligation to encrypt Personal Data or otherwise prevent its release or misuse; and
 - iv. The Contractor's indemnification and liability under Section 4.1(A)(1) is not limited by, but is in addition to the insurance obligations contained in Section 4.2 of the State Standard Terms and Conditions.
2. In the event of a claim or suit involving third-party Intellectual Property Rights, the Contractor, at its option, may: (1) procure for the State the legal right to continue the use of the product; (2) replace or modify the product to provide a non-infringing product that is the functional equivalent; or (3) refund the purchase price less a reasonable allowance for use that is agreed to by both parties. The State will: (1) promptly notify Contractor in writing of the claim or suit; (2) Contractor shall have control of the defense and settlement of any claim that is subject to Section 4.1(A)(1); provided, however, that the State must approve any settlement of the alleged claim, which approval shall not be unreasonably withheld. The State may observe the proceedings relating to the alleged claim and confer with the Contractor at its expense. Furthermore, neither Contractor nor any attorney engaged by Contractor shall defend the claim in the name of the State of New Jersey, nor purport to act as legal representative of the State of New Jersey, without having provided notice to the Director of the Division of Law in the Department of Law and Public Safety and to the Director of DPP. The State of New Jersey may, at its election and expense, assume its own defense and settlement.
3. Notwithstanding the foregoing, Contractor has no obligation or liability for any claim or suit concerning third-party Intellectual Property Rights arising from: (1) the State's unauthorized combination, operation, or use of a product supplied under this contract with any product, device, or software not supplied by Contractor; (2) the State's unauthorized alteration or modification of any product supplied under this contract; (3) the Contractor's compliance with the State's designs, specifications, requests, or instructions, provided that if the State provides Contractor with such designs, specifications, requests, or instructions, Contractor shall review same and advise if such designs, specifications, requests or instructions present potential issues of patent or copyright infringement and the State nonetheless directs the Contractor to proceed with one or more designs, specifications, requests or instructions that present potential issues of patent or copyright infringement; or (4) the State's failure to promptly implement a required update, use a new version of the product, or to make a change or modification to the product if requested in writing by Contractor.
4. Contractor will be relieved of its responsibilities under Subsection 4.1(A)(1)(i), (ii), and (iii) for any claims made by an unaffiliated third party that arise solely from the actions or omissions of the State, its officers, employees or agents.
5. This section states the entire obligation of Contractor and the exclusive remedy of the State, in respect of any infringement or alleged infringement of any Intellectual Property Rights. This indemnity obligation and remedy

are given to the State solely for its benefit and in lieu of, and Contractor disclaims, all warranties, conditions and other terms of non-infringement or title with respect to any product.

6. The provisions of this indemnification clause shall in no way limit the Contractor's obligations assumed in the Contract, nor shall they be construed to relieve the Contractor from any liability, nor preclude the State from taking any other actions available to it under any other provisions of the contract or otherwise at law or equity.
 7. The Contractor agrees that any approval by the State of the work performed and/or reports, plans or specifications provided by the Contractor shall not operate to limit the obligations of the Contractor assumed in the Contract.
 8. The State of New Jersey will not indemnify, defend or hold harmless the Contractor. The State will not pay or reimburse for claims absent compliance with Section 4.1(B) below and a determination by the State to pay the claim or a final order of a court of competent jurisdiction.
- B. STATE RESPONSIBILITIES - Subject to the New Jersey Tort Claims Act (N.J.S.A. 59:1-1 et seq.), the New Jersey Contractual Liability Act (N.J.S.A. 59:13-1 et seq.) and the appropriation and availability of funds, the State will be responsible for any cost or damage arising out of actions or inactions of the State, its employees or agents under Section 4.1(A)(1)(i), (ii), and (iii) which results in an unaffiliated third party claim. This is Contractor's exclusive remedy for these claims.

7.2 INSURANCE

7.2.1 PROFESSIONAL LIABILITY INSURANCE

Section 4.2 of the State of New Jersey Standard Terms and Conditions is supplemented with the following:

Professional Liability Insurance: The Contractor shall carry Errors and Omissions, Professional Liability Insurance, and/or Professional Liability Malpractice Insurance sufficient to protect the Contractor from any liability arising out the professional obligations performed pursuant to the requirements of this Contract. The insurance shall be in the amount of not less than \$1,000,000 or higher if appropriate per each occurrence and in such policy forms as shall be approved by the State. If the Contractor has claims-made coverage and subsequently changes carriers during the term of this Contract, it shall obtain from its new Errors and Omissions, Professional Liability Insurance, and/or Professional Malpractice Insurance carrier an endorsement for retroactive coverage.

7.2.2 CYBER BREACH INSURANCE

Section 4.2 of the State of New Jersey Standard Terms and Conditions supplemented with the following:

Cyber Breach Insurance: The Contractor shall carry Cyber Breach Insurance in sufficient to protect the Contractor from any liability arising out of its performance pursuant to the requirements of this Contract. The insurance shall be in an amount of not less than \$10,000,000 per each occurrence and in such policy forms as shall be approved by the State. The insurance shall at a minimum cover the following: Data loss, malware, ransomware and similar breaches to computers, servers and software; Protection against third-party claims; cost of notifying affected parties; cost of providing credit monitoring to affected parties; forensics; cost of public relations consultants; regulatory compliance costs; costs to pursue indemnity rights; costs to Data Breach and Credit Monitoring Services analyze the insured's legal response obligations; costs of defending lawsuits; judgments and settlements; regulatory response costs; costs of responding to regulatory investigations; and costs of settling regulatory claims.

7.3 LIMITATION OF LIABILITY OPTION

Section 4.3 is added to the State of New Jersey Standard Terms and Conditions:

4.3 LIMITATION OF LIABILITY

The Contractor's liability for actual, direct damages resulting from the Contractor's performance or non-performance of, or in any manner related to, the Contract for any and all third-party claims, shall be limited in the aggregate to 200% of the fees paid by the State during the previous twelve months to Contractor for the products or services giving rise to such damages. Notwithstanding the preceding sentence, in no event shall the limit of liability be less than \$1,000,000. This limitation of liability shall not apply to the following:

- i. The Contractor's indemnification obligations as described in Section 4.1; and
- ii. The Contractor's breach of its obligations of confidentiality described in this RFQ.

Notwithstanding the foregoing exclusions, where a Breach of Security is a direct result of Contractor's breach of its contractual obligation to encrypt Personal Data pursuant to this RFQ or otherwise prevent its release as reasonably determined by the State, the Contractor shall bear the costs associated with (1) the investigation and resolution of the Breach of Security; (2) notifications to individuals, regulators, or others required by federal and state laws or as otherwise agreed to; (3) a credit monitoring service required by state or federal law or as otherwise agreed to; (4) a website or a toll-free number and call center for affected individuals required by federal and state laws — all not to exceed the average per record, per person cost calculated for data breaches in the United States in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute for the public sector at the time of the Breach of Security; and (5) completing all corrective actions as reasonably determined by Contractor based on root cause of the Breach of Security. The Contractor shall not be liable for punitive, special, indirect, incidental, or consequential damages.

8.0 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 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 Board within five (5) business days after the deadline for Quote submission. Written evidence for a specific procurement that is not provided to the Board within five (5) business days of the public Quote submission date may not be considered in the evaluation of that procurement, but may be retained and considered in the evaluation of subsequent procurements.

8.2 TIE QUOTES

Tie Quotes will be awarded by the Director in accordance with N.J.A.C. 17:12-2.10.

8.3 STATE'S RIGHT TO INSPECT BIDDER'S FACILITIES

The State reserves the right to inspect the Bidder's establishment before making an award, for the purposes of ascertaining whether the Bidder has the necessary facilities for performing the Contract.

8.4 STATE'S RIGHT TO CHECK REFERENCES

The State may also 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.

8.5 EVALUATION CRITERIA

The following evaluation criteria categories, not necessarily listed in order of significance, will be used to evaluate Quotes received in response to this RFQ. The evaluation criteria categories may be used to develop more detailed evaluation criteria to be used in the evaluation process.

8.5.1 TECHNICAL EVALUATION CRITERIA

The following criteria will be used to evaluate and score Quotes received in response to this RFQ. Each criterion will be scored, and each score multiplied by a predetermined weight to develop the Technical Evaluation Score:

- A. Personnel: The qualifications and experience of the Bidder's management, supervisory, and key personnel assigned to the Contract, including the candidates recommended for each of the positions/roles required;
- B. Experience of firm: The Bidder's documented experience in successfully completing Contract of a similar size and scope in relation to the work required by this RFQ; and
- C. Ability of firm to complete the Scope of Work based on its Technical Quote: The Bidder's demonstration in the Quote that the Bidder understands the requirements of the Scope of Work and presents an approach that would permit successful performance of the technical requirements of the Contract.

8.5.2 PRICE EVALUATION

For evaluation purposes, Bidders will be ranked from lowest to highest according to the total Quote price located on the State-Supplied Price Sheet accompanying this RFQ.

8.6 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.

8.7 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.

8.8 RECOMMENDATION FOR AWARD

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

8.9 CONTRACT AWARD

The Contract award will be made with reasonable promptness by written notice to that responsible Bidder, whose Quote, conforming to this RFQ, is most advantageous to the State, price, and other factors considered.

9.0 GLOSSARY

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

Account Holder - Is a participating employee, non-participating employee, former employee and/or derivative account.

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.

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, State of New Jersey 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 opening.

Bid Opening Date – The date Quotes will be opened for evaluation and closed to further Quote submissions.

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 a 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.

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

Days After Receipt of Order (ARO) – The number of calendar days 'After Receipt of Order' in which the Board will receive the ordered materials and/or services.

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

Disabled Veterans' Business - means a business which has its principal place of business in the State, is independently owned and operated and at least 51% of which is owned and controlled by persons who are disabled veterans or a business which has its principal place of business in this State and has been officially verified by the United States Department of Veterans Affairs as a service disabled veteran-owned business for the purposes of department contracts pursuant to federal law. N.J.S.A. 52:32-31.2.

Disabled Veterans' Business Set-Aside Contract - means a Contract for goods, equipment, construction or services which is designated as a Contract with respect to which bids are invited and accepted only from disabled veterans' businesses, or a portion of a Contract when that portion has been so designated. N.J.S.A. 52:32-31.2.

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

Employee - "Means any individual who is 18 years of age or older, who lives in this State or is employed by an employer in this State, and whose wages are subject to withholding as provided in the "New Jersey Gross Income Tax Act," N.J.S.54A:1-1 et seq. For the purposes of this act, an employee who is co-employed by an employee leasing company or professional employer organization and a client company pursuant to an employee leasing agreement or professional employer agreement, as such terms are defined in section 1 of P.L.2001, c.260 (C.34:8-67), shall be treated as employed by the client company and not by the employee leasing company or professional employer organization." N.J.S.A. 43:23-14

Employer – “Means a person or entity engaged in a business, industry, profession, trade, or other enterprise in New Jersey, whether for profit or not for profit, that has at no time during the previous calendar year employed fewer than 25 employees in the State, has been in business at least two years, and has not offered a qualified retirement plan, including, but not limited to, a plan qualified under section 401(a), section 401(k), section 403(a), section 403(b), section 408(k), section 408(p), or section 457(b) of the Internal Revenue Code, or a plan sponsored by an employee leasing company or professional employer organization with which the employer has an employee leasing agreement or professional employer agreement as such terms are defined in section 1 of P.L.2001, c.260 (C. 34:8-67), in the preceding two years. “Employer” shall not mean the State, its political subdivisions, any office, department, division, bureau, board, commission or agency of the State or one of its political subdivisions, or any public body in the State.” N.J.S.A. 43:23-14

Evaluation Committee – A group of individuals or a Board 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.

Joint Venture – A business undertaking by two (2) or more entities to share risk and responsibility for a specific project.

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.

Percentage Discount or Markup - The percentage bid applied as a Markup or a Discount to a firm, fixed price contained within a price list/catalog.

Performance Security - means a guarantee, executed subsequent to award, in a form acceptable to the Division, that the successful bidder will complete the contract as agreed and that the State will be protected from loss in the event the contractor fails to complete the contract as agreed.

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 Opening Date - 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, State of NJ Standard Terms and Conditions (SSTC), price schedule, attachments, and Bid Amendments.

Retainage – The amount withheld from the Contractor payment that is retained and subsequently released upon satisfactory completion of performance milestones by the Contractor.

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.

Small Business – Pursuant to N.J.S.A. 52:32-19, N.J.A.C. 17:13-1.2, and N.J.A.C. 17:13-2.1, "small business" means a business that meets the requirements and definitions of "small business" and has applied for and been approved by the New Jersey Division of Revenue and Enterprise Services, Small Business Registration and M/WBE Certification Services Unit as (i) independently owned and operated, (ii) incorporated or registered in and has its principal place of business in the State of New Jersey; (iii) has 100 or fewer full-time employees; and has gross revenues falling in one (1) of the six (6) following categories:

For goods and services - (A) 0 to \$500,000 (Category I); (B) \$500,001 to \$5,000,000 (Category II); and (C) \$5,000,001 to \$12,000,000, or the applicable federal revenue standards established at 13 CFR 121.201, whichever is higher (Category III).

For construction services: (A) 0 to \$3,000,000 (Category IV); (B) gross revenues that do not exceed 50 percent of the applicable annual revenue standards established at 13 CFR 121.201 (Category V); and (C) gross revenues that do not exceed the applicable annual revenue standards established at CFR 121.201, (Category VI).

Small Business Set-Aside Contract – means (1) a Contract for goods, equipment, construction or services which is designated as a Contract with respect to which bids are invited and accepted only from small businesses, or (2) a portion of a Contract when that portion has been so designated." N.J.S.A. 52:32-19.

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.

Stakeholder(s) – shall include any State Department, or contracted service provider approved by the Program.

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-Supplied 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.

Using Agency[ies] – A State department or agency, a quasi-State governmental entity, or an Intrastate Cooperative Purchasing participant, authorized to purchase products and/or services under a Contract procured by the Division.

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.