Request for Proposals
Unemployment Cost Management Services
For the State of New Jersey

Issuer: State of New Jersey
Department of the Treasury
Division of Pensions and Benefits

Date of Issue: Monday, October 3, 2022
Questions Due: Friday, October 14, 2022
Proposal Submission Deadline: October 28, 2022 at 3:00 pm eastern standard time

1.1 PURPOSE AND INTENT

This Bid Solicitation {RFP} is issued by the Division of Pension and Benefits (DPB) Department of the Treasury. The purpose of this Bid Solicitation {RFP} is to solicit Quotes {Proposals} for a firm to manage the State's Unemployment Cost Management Services, which administers to workers employed by the State.

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 Condition. 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 Condition shall prevail.

1.3 BACKGROUND

Pursuant to N.J.A.C. 17:1-9.6, a Vendor {Contractor} will be designated to develop and maintain a program to monitor and control the cost of Unemployment Insurance (UI) to the State. The program is administered to all workers employed by the State covered by the New Jersey Unemployment Compensation Laws and paid by the Centralized Payroll Unit, covered employees of the various State colleges and universities, and employees of the Palisades Interstate Park Commission. The program will be designed to incorporate in its procedures all the reporting requirements of an employer as specified by the New Jersey Unemployment Compensation Laws and those controls and practices deemed necessary to minimize the cost of UI to the State.

The objectives of the Unemployment Cost Management Services are:

a. To consolidate under one (1) designated Vendor {Contractor} the reporting requirements as prescribed by the State's Unemployment Compensation Laws for each of the State's employing units and subunits; and

b. To develop and maintain procedures and controls to monitor and minimize the cost of UI to the State.

1.3.1 SUMMARY INFORMATION

The following chart (Volume of Activity from Fiscal Years 2019-2022) provides a history of the size and structure of the State workforce and the volume of activity under this Blanket P.O. {Contract} from fiscal years 2019-2022:

a. Claims Processed – This total reflects all claim forms processed by the Vendor {Contractor} during the reporting period specified;

b. Claims Protested – The number of claims that were challenged or protested by the Vendor {Contractor} during the specified period;

c. Covered Employees – The total number of State employees eligible for unemployment benefits;

d. Hearings – The number of hearing that occurred either as a result of the employer's appeal or the claimant's appeal during the specified period; and

e. Appeals – The number of appeals filed during the specified period.

Volume of Activity from Fiscal Years 2019-2022				
Dates	7/1/2018-6/30/2019	7/1/2019-6/30/2020	7/1/2020-6/30/2021	7/1/2021-06/30/2022
Centralized Payroll Covered Employees	67,091	66,144	64,473	63,072
Other Employers Covered Employees	43,092	42,519	40,014	40,283
Total Covered Employees	110,183	108,663	104,487	103,355
Total Benefit Charges Received	$ 13,735,238	$ 34,049,364	$ 596,264,748	$ 13,607,598
Claims Processed	1,910	4,345	43,354	4,647
Separations Received	445	650	3,677	724
Claims Protested	71	1,937	35,934	1,786
Hearings Scheduled	228	224	109	153
Appeals Filed	39	28	87	25

1.4 KEY EVENTS

1.4.1 ELECTRONIC QUESTION AND ANSWER PERIOD

The Division will electronically accept questions and inquiries from all potential Vendors {Bidders} via email to both Danielle.Tuccillo@Treas.NJ.Gov and Robert.Petroni@Treas.NJ.Gov

a. Questions should be directly tied to the Bid Solicitation {RFP} and asked in consecutive order, from beginning to end, following the organization of the Bid Solicitation {RFP}; and

b. Each question should begin by referencing the Bid Solicitation {RFP} page number and section number to which it relates.

The cut-off date for electronic questions and inquiries relating to this Bid Solicitation {RFP} is indicated on the Bid Solicitation {RFP} cover sheet. In the event that questions are posed by Vendors {Bidders}, answers to such questions will be issued by Bid Amendment {Addendum}.

1.4.1.1 EXCEPTIONS TO THE STATE OF NJ STANDARD TERMS AND CONDITIONS (SSTC)

Questions regarding the SSTC and exceptions to mandatory requirements must be posed during this Electronic Question and Answer period and shall contain the Vendor's {Bidder's} suggested changes and the reason(s) for the suggested changes.

1.4.2 SUBMISSION OF QUOTES {PROPOSALS}

In order to be considered for award, the Quote {Proposal} must be received by the Procurement Bureau of the Division at the appropriate location by the required time. Vendors {Bidders} shall submit a Quote {Proposal} either electronically or via hard copy.

Hard copy Quote {Proposal} must be submitted to the physical location noted below:

RICARDO ARCE STATE CONTRACT MANAGER
ACCOUNTING SERVICES – 7TH FLOOR
DIVISION OF PENSIONS AND BENEFITS
DEPARTMENT OF THE TREASURY
P.O. BOX 295
TRENTON, NJ 08625-0295
HAND DELIVER TO: 50 W. STATE STREET, TRENTON, NJ 08608

1.4.3 DEADLINE FOR SUBMISSION OF PROPOSALS:

In order to be considered, a proposal must arrive at the Department of the Treasury no later than the Proposal Submission Deadline indicated on the cover sheet of this RFP.

ANY PROPOSAL RECEIVED AFTER THE PROPOSAL SUBMISSION DEADLINE WILL BE REJECTED.

Bidders using U.S. Postal Service regular or express mail services should allow additional time since the U.S. Postal Service does not deliver directly to Department of the Treasury

1.4.4 BIDDER RESPONSIBILITY:

The bidder assumes sole responsibility for the complete effort required in submitting a proposal in response to the RFP. It is the sole responsibility of the bidder to be knowledgeable as to all of the requirements of this RFP. No special consideration will be given after proposals are received because of a bidder's failure to be knowledgeable as to such requirements. 1.3.4 Cost Liability: The State and the Board assume no responsibility and bear no liability for costs incurred by any bidder in the preparation and submittal of a proposal in response to this RFP

1.4.5 FORMS, REGISTRATIONS AND CERTIFICATIONS TO BE SUBMITTED WITH QUOTE:

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

I. OFFER AND ACCEPTANCE PAGE

The Bidder should complete and submit the Offer and Acceptance Page with the Quote. The Offer and Acceptance Page must be signed by an authorized representative of the Bidder. 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.

II. OWNERSHIP DISCLOSURE FORM

Pursuant to N.J.S.A. 52:25-24.2, in the event the Bidder is a corporation, partnership or limited liability company, the Bidder must disclose all 10% or greater owners by (a) completing and submitting the Ownership Disclosure Form with the Quote; (b) if the Bidder has submitted a

signed and accurate Ownership Disclosure Form dated and received no more than six (6) months prior to the Quote submission deadline for this procurement, the Using Agency may rely upon that form; however, if there has been a change in ownership within the last six (6) months, a new Ownership Disclosure Form must be completed, signed and submitted with the Quote; or, (c) a Bidder with any direct or indirect parent entity which is publicly traded may submit the name and address of each publicly traded entity and the name and address of each person that holds a 10 percent or greater beneficial interest in the publicly traded entity as of the last annual filing with the federal Securities and Exchange Commission or the foreign equivalent, and, if there is any person that holds a 10 percent or greater beneficial interest, also shall submit links to the websites containing the last annual filings with the federal Securities and Exchange Commission or the foreign equivalent and the relevant page numbers of the filings that contain the information on each person that holds a 10 percent or greater beneficial interest. 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.

III. 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.

IV. 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.

V. 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.

VI. 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.

VII. CONFIDENTIALITY/COMMITMENT TO DEFEND

Pursuant to the New Jersey Open Public Records Act (OPRA), N.J.S.A. 47:1A-1 et seq., or the common law right to know, Quotes can be released to the public in accordance with N.J.A.C. 17:12-1.2(b) and (c).

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

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

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

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

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

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

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

VIII. 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.

IX. PAY TO PLAY PROHIBITIONS

Pursuant to N.J.S.A. 19:44A-20.13 et seq. (P.L. 2005, c. 51), 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 candidate committee and/or election fund of any candidate for or holder of the public office of Governor or Lieutenant Governor, to any State, county, municipal political party committee, or to any legislative leadership committee during certain specified time periods.

Prior to awarding any Contract or agreement to any Business Entity, the Business Entity proposed as the intended Contractor of the Contract shall submit the Two-Year Chapter 51/Executive Order 117 Vendor Certification and Disclosure of Political Contributions form, certifying that no contributions prohibited by either Chapter 51 or Executive Order No. 117 have been made by the Business Entity and reporting all qualifying contributions made by the Business Entity or any person or entity whose contributions are attributable to the Business Entity. Failure to submit the required forms will preclude award of a Contract under this RFQ.

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

X. 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.

XI. 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.

XII. 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.

1.1.6 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.

If you certify that the bidder is engaged in activities prohibited by P.L. 2022, c. 3, the bidder shall have 90 days to cease engaging in any prohibited activities and on or before the 90th day after this certification, shall provide an updated certification. If the bidder does not provide the updated certification or at that time cannot certify on behalf of the entity that it is not engaged in prohibited activities, the State shall not award the business entity any contracts, renew any contracts, and shall be required to terminate any contract(s) the business entity holds with the State that were issued on or after the effective date of P.L. 2022, c. 3.

2.0 SCOPE OF WORK

The Vendor {Contractor} shall manage Unemployment Cost Management Services for all workers employed by the State and covered by the State's Unemployment Compensation Laws and paid by the State Centralized Payroll Unit, covered employees of the various State colleges and universities, and employees of the Palisades Interstate Park Commission. This includes, but is not limited to:

a. Collecting and storing wage and separation information for covered employees;
b. Responding to requests for wage and separation information from the NJ Department of Labor and Workforce Development (DLWD);

c. Reviewing eligibility and monetary determinations against available wage and separation information;
d. Protesting incorrect or questionable determinations on the State's behalf and filing appeals on the employer's behalf when a protested claim is settled in favor of the claimant;
e. Providing guidance and expertise to employers involved in a disputed claim;
f. Providing guidance and representation to employers at hearings; and
g. Maintaining procedures and controls to minimize Unemployment Insurance (UI) costs.
h. Project Management section outlined in the link should be adhered to by the Vendor http://www.nj.gov/it/docs/vendors/ProjectManagementAppendix.pdf

2.1 CONTRACTOR REQUIREMENTS

The Vendor {Contractor} shall perform the following services in the management of the Unemployment Cost Management Services program:

2.1.1 BEGINNING CONTRACT TRANSITION PERIOD

From the date of Blanket P.O. {Contract} award, the Vendor {Contractor} shall have 45 days to establish its offices and processes and transition the program from the previous Vendor {Contractor}.

The Vendor {Contractor} shall be required to perform the following activities:

a. Submit required authorization forms with the DLWD to act as the employer representative for the State;
b. Establish operating procedures with the DLWD;
c. Prepare and distribute announcement and instructional notices to the various employing agency contacts; and
d. Establish procedures for obtaining wage and separation information from the employing agencies.

Periodic meetings shall be scheduled with the State Contract Manager (SCM) and DLWD representatives during this period to provide status updates. The Vendor {Contractor} shall assume full responsibility for all Blanket P.O. {Contract} requirements on the 46th day of the Blanket P.O. {Contract} or the first business day thereafter.

2.1.2 COLLECTION OF WAGE AND SEPARATION INFORMATION

The Vendor {Contractor} shall establish procedures with the various employers to collect and store wage and separation information for covered employees. The Vendor {Contractor} shall meet or exceed the State's minimum system requirements for electronic file transmissions of this Bid Specification {RFP}, in regard to the wage data provided by the State's Centralized Payroll Unit. The Vendor {Contractor} shall provide a fixed-length file format for all data transmissions.

2.1.2.1 COOPERATIVE PURCHASING PARTNERS

State universities and colleges may send wage files to the Vendor {Contractor} by connecting to the Vendor's {Contractor's} server and transferring the files using Secure File Transfer Protocol. Currently Rutgers University is the only State university or college sending wage files. The Vendor {Contractor} shall work with the State universities and colleges to establish a wage

transmission procedure that is secure and ensures the use of leading encryption standards in order to protect confidential employee data.

On request of the SCM, the Vendor {Contractor} shall work with the other participating employers to establish wage reporting procedures. Over the course of the Blanket P.O. {Contract} period, efforts will be made by the SCM to encourage other participating employers to provide wage data to the Vendor {Contractor}.

2.1.3 RETRIEVAL INFORMATION PROCESS

The State shall provide basic separation data to the Vendor {Contractor} as terminations occur for employees on the State's Centralized Payroll. The information shall be sent electronically and shall include the former employee's name, social security number, employer payroll location number, job title, last day of work, first day of work and separation code. There are currently 146 contact persons representing 376 different State agency groups (including the State colleges and universities) each with its own unique payroll location number. The SCM will provide a listing of the various human resource representatives and their contact information to the Vendor {Contractor} upon Blanket P.O. {Contract} award.

The Vendor {Contractor} shall have an automated retrieval system in place for collecting separation information. Designated employer representatives shall be provided with access to the Vendor's {Contractor's} data retrieval system. The Vendor's {Contractor's} data retrieval process must be secure and protect personal and confidential employee data.

The Vendor {Contractor} shall store all data in a manner that permits a timely response to requests from the Division of Unemployment Insurance for wage and separation information. All responses shall be provided within ten (10) calendar days of the mailing date shown on the request form received from the Division of Unemployment Insurance.

2.1.4 REPORTING OF WAGE AND SEPARATION INFORMATION

The Vendor {Contractor} shall respond to wage information requests from the Division of Unemployment Insurance when the DLWD's Wage Record System employee database does not contain specific data required to determine a claimant's eligibility for unemployment benefits. The Vendor {Contractor} shall respond and provide specific information in the following cases:

a. When wage data is required on a weekly instead of a quarterly basis;
b. When a wage dispute exists, or when wage data is missing from the database;
c. When an alternative base year period must be used to determine monetary eligibility for benefits; or
d. When a claim is subject to a quality audit under the BAM program.

Wage requests will be sent to the Vendor {Contractor} on Form BC-2 - Request for Wage and Separation Information.

The Vendor {Contractor} shall respond to requests for separation information from the Division of Unemployment Insurance in the following cases:

a. When a claimant's job separation is for a reason other than a lack of work;

b. When a separation is due to a temporary layoff and the claimant has a definite date of recall;
c. When a claimant received wages for a period after his/her last day of work (e.g., vacation pay, severance pay, payment in lieu of notice, etc.);
d. When the claimant's employment by the State was for his/her "lag" period only;
e. When an employee reopens a claim for unemployment benefits; or
f. When the claimant is receiving a pension.

Requests for separation information and notices of monetary determinations and benefit charges will be sent to the Vendor {Contractor} by the DLWD via UI Separation Information Data and Exchange System (SIDES). The Vendor {Contractor} shall be a participating member in UI SIDES.

All payroll information shall be treated as confidential and shall be used only for the purpose of carrying out the terms of this Blanket P.O. {Contract}. The Vendor {Contractor} shall adhere to the requirements specified by Section 5.9 of this Bid Specification {RFP}, and all other applicable sections of this Bid Specification {RFP}, when dealing with confidential information.

2.1.5 CLAIMS VERIFICATION

The Vendor {Contractor} shall:

a. Review all monetary determinations reported on Form BC-3E- Notice to Employers of Monetary Determination verifying the State's potential liability against payroll information to ensure accuracy of the determination;
b. Review all non-monetary determinations to ensure that all separation issues have been properly adjudicated;
c. In consultation with State human resources personnel, protest incorrect or questionable determination to the Division of Unemployment Insurance; and
d. Subject to the decision of the employing Using Agency, file appeals against those determinations in cases where the Division of Unemployment Insurance disagrees with the protest.

2.1.6 HEARINGS

On request, the Vendor {Contractor} shall serve as the employer representative when a hearing has been scheduled to settle a protested claim, as well as provide advice and assistance to the claimant's former employer in all cases in which the former employer has agreed that an appeal should be filed or in which a former employee claimant files an appeal. Such advice and guidance shall include:

a. Researching background and facts;
b. Reviewing with the former employer the facts, issues, hearing procedure, instruction of witnesses, and required documentation;
c. Attendance at hearings to provide assistance to the employer representatives. The Vendor {Contractor} shall attend a hearing via teleconference or virtually; and
d. Reviewing decisions to provide recommendations as to further appropriate actions.

In accordance with legislation which was signed into law in September of 2010, §§3-9 - C.43:21-6.2 to 43:21-6.8, Registration of authorized agents in connection with claims for unemployment benefits; application and fees; registration number; cessation of representation, the Vendor {Contractor} shall have an authorized agent registration number to represent the State in matters/hearings regarding UI benefits and taxes.

2.1.7 INFORMATION AND RECORDS

The Vendor {Contractor} shall maintain computerized records based on payroll, separation, or other information provided by the State, or developed in the course of managing this program, to provide the basis for:

a. Responding to wage information requests;
b. Responding to claims notices;
c. Providing to the State all required reports; and
d. Identifying problems with respect to specific employing units, such as but not limited to, separation information, failure to appear at hearing, employment policies, or frequent errors.

2.1.8 EDUCATIONAL AND TRAINING ACTIVITIES

The Vendor {Contractor} shall provide, with the approval of the SCM, educational and instructional materials to personnel/payroll representatives at each employing Using Agency, covering the following:

a. Basic understanding of Unemployment Compensation Laws, including coverage, eligibility, taxable wages, use and significance of payroll and separation information, familiarity with associated forms, claims processing, and the hearing process;
b. Preparation and distribution of procedural instructions to all employing units;
c. Effects of hiring and personnel policies on unemployment compensation experience;
d. Working arrangements between employing units and the Vendor {Contractor}; and
e. Any other information deemed by the Vendor {Contractor} or SCM to be pertinent and appropriate.

2.1.9 **CLAIMS MONITORING AND CONTROL**

The Vendor {Contractor} shall maintain a system of controls, initiated upon the filing of a claim and notification of the initial determination, which shall monitor claims to insure proper handling and appropriate action at each step in the process. The Vendor {Contractor} shall verify liability or charges, the matching of claims and separation notices, and ensure that any benefit credits or adjustment to charges as a result of protests or appeals are properly awarded.

2.1.10 **REPORTS**

a. The Vendor {Contractor} shall have an on-line reporting system that the SCM can access to retrieve and download reports which summarize in a comprehensive fashion, claims activity, benefit charges, and relevant statistical and financial data required in order to make informative decisions relating to the cost of unemployment compensation to the State. The Vendor's {Contractor's} on-line reporting system shall have the capability to produce, at a minimum, the following reports that the SCM can access on demand for any specified time period (last week, last month, last year, or any designated timeframe) and must be updated on a daily basis:

b. A report summarizing claims filed, by employing agency, and the disposition of such claims. The report shall include the following: a listing of claimants, the reason for separation, whether the claim is protestable, potential total liability, actual charges to date, and charges removed or suspended;

c. A report summarizing unemployment claims activity in total and by employing agency. Furthermore, the report shall include the following: the number of claims received, potential liability, current period charges, responses received to requests for separation information, breakdown of claims and separations by type (e.g. quits, discharges, and/or layoffs), number and outcome of claims protested, percentage of claims protested, and the number and outcome of hearings;

d. A report summarizing program cost savings, including savings derived from favorable protests, favorable decisions at hearings, and discovery of erroneous charges; and

e. A compliance report that identifies employing agencies that have failed to provide separation information in a timely fashion and other information necessary to determine whether a claim should be protested or an appeal sought. The report shall summarize the number of times requested data was received late or not received and the estimated value of lost savings.

The Vendor's {Contractor's} on-line reporting system shall be updated on a daily basis to reflect the claims activity occurring through the close of business on the previous day.

2.1.11 **MEETINGS**

The Vendor {Contractor} shall attend in person meetings held at the discretion of the SCM. These meetings shall occur at least once per year in order to review the most recent reports for the month or quarter in order to identify problem areas and to plan for the necessary corrective action to be taken by the Vendor {Contractor} or the DPB.

Furthermore, the Vendor {Contractor} shall attend telephone status meetings held at the discretion of the SCM.

2.1.12 **INVESTIGATIONS**

The Vendor {Contractor} shall fully cooperate with the State in the investigation and prosecution of any potentially fraudulent claims.

2.2 **ENDING BLANKET P.O. {CONTRACT} TRANSITION PERIOD**

The Vendor {Contractor} shall cooperate with a successor Vendor {Contractor} and provide all information as needed during Blanket P.O. {Contract} transition to the successor Vendor {Contractor}.

2.2.1 TRANSMISSION OF FILES

The State of New Jersey supports multiple methods for data transfers internally within the Garden State Network or external to an extranet or business partner. The transmission of all files between the contractor and the State system must be transferred securely using the State file transfer methodology. The State will work with the contractor in the implementation of the file transfer process. The secure file transfer must meet the state and federal security guidelines and standards.

The State of New Jersey provides both asynchronous and synchronous file transfer methodologies.

Synchronous:

1) Connect:Direct Secure + is a supported option for file exchange with the State of New Jersey IBM mainframe.
2) FTPS over SSL (Explicit – port 21) is a supported option for file exchange for connections originating from the State of New Jersey IBM Mainframe. Must support RFC2228.
3) SFTP (FTP over SSHv2 or greater) is a supported option for file exchange with State of New Jersey distributed servers (non-IBM Mainframe).

Asynchronous:

1) The State of New Jersey's MOVEit Cloud is a supported option for non-automated or "ad-hoc" file exchange with State of New Jersey.
2) The State of New Jersey's MOVEit Cloud Automation is a supported option for automated file exchange with the State of New Jersey.

The contractor will be required to test the file transfer with the State system on all file transfers prior to full implementation.

During the life of the contract, the State may revise or change the file transfer method and/or format for the transmission of files to accommodate real time processing, and use case specific information and the contractor shall be required to conform to all requirements.

Reference:

NIST Special Publication 800-47 - Security Guide for Interconnecting Information Technology Systems (https://csrc.nist.gov/publications/detail/sp/800-47/rev-1/final)

2.2.2 HARD COPY SUBMISSION

If the Vendor {Bidder} is submitting a hard copy Quote {Proposal}, the Vendor {Bidder} must submit the following:

a. One (1) complete Quote {Proposal}, comprising all volumes and including original, physical signature, clearly marked as the "ORIGINAL" Quote {Proposal}.

b. **Six (6) complete and exact ELECTRONIC copies** of the original Quote {Proposal} in PDF file format on disc (CD or DVD). These should be cover to cover copies, and should not be password protected. **THE PRICE SCHEDULE (VOLUME 3) SHALL NOT BE INCLUDED ON THIS DISC.**

c. **One (1) complete and exact ELECTRONIC copy** of the original price schedule (Volume 3) in a Microsoft Excel file format on disc (CD or DVD) for redaction. These should be cover to cover copies, and should not be password protected.

Copies are necessary in the evaluation of the Quote {Proposal} and for record retention purposes. A Vendor {Bidder} failing to provide the requested number of copies will be charged the cost incurred by the State in producing the requested number of copies. The Vendor {Bidder} should make and retain a copy of its Quote {Proposal}.

2.3 QUOTE {PROPOSAL} CONTENT

The Quote {Proposal} should be submitted in three (3) volumes with the content of each volume as indicated below.

Volume 1

Section 1 - Forms

Note: In general, Volume 1 applies to hard copy submissions; however, there may be instances where Bid Solicitation {RFP} specific forms are required through electronic submission as well.

Volume 2

Section 2 - Technical Quote {Proposal}

Section 3 - Organizational Support and Experience

Section 3A - Any other miscellaneous documents to be included by the Vendor {Bidder}

Volume 3

Section 4 – Price Schedule

Note: Vendors {Bidders} submitting Quotes {Proposals} must complete its Price Schedule (Volume 3) as an attachment using the State-supplied price sheet/schedule(s) accompanying this Bid Solicitation {RFP}. The Vendor {Bidder} must enter a Unit Cost of $1.00 for each price line item. The Vendor {Bidder} is instructed to do so only as a mechanism to comply with Bid Solicitation {RFP} and prevent all pricing from being publicly displayed. In the event that a Vendor {Bidder} to submit a Quote {Proposal} uploads a price sheet/schedule attachment instead of entering a Unit Cost of $1.00 as instructed, the price sheet/schedule attachment will govern.

3. DATA SECURITY REQUIREMENTS – CONTRACTOR RESPONSIBILITY

b. 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's 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 State may terminate the Contract pursuant to the SSTC.

c. 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.

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.

d. 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.

e. 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.

f. PRIVACY

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

A. Data Ownership. The State owns State Data. Contractor shall not obtain any right, title, or interest in any State Data, or information derived from or based on State Data.
B. Data usage, storage, and protection of Personal Data are subject to all applicable international, federal and state statutory and regulatory requirements, as amended from time to time, including, without limitation, those for HIPAA, Tax Information Security Guidelines for Federal, State, and Local Agencies (IRS Publication 1075), New Jersey State tax confidentiality statute, the New Jersey Privacy Notice found at NJ.gov, N.J.S.A. § 54:50-8, New Jersey Identity Theft Prevention Act, N.J.S.A. § 56:11-44 et. seq., the federal Drivers' Privacy Protection Act of 1994, Pub.L.103-322, and the confidentiality requirements of N.J.S.A. § 39:2-3.4. Contractor shall also conform to PCI DSS, where applicable.
C. Security: Contractor agrees to take appropriate administrative, technical and physical safeguards reasonably designed to protect the security, privacy, confidentiality, and integrity of user information. Contractor shall ensure that State Data is secured and encrypted during transmission or at rest.
D. Data Transmission: The Contractor shall only transmit or exchange State Data with other parties when expressly requested in writing and permitted by and in accordance with requirements of the Contract or the State of New Jersey. The Contractor shall only transmit or exchange State Data with the State of New Jersey or other parties through secure means supported by current technologies.
E. Data Storage: All data provided by the State of New Jersey or State data obtained by the Contractor in the performance of the Contract must be stored, processed, and maintained solely in accordance with a project plan and system topology approved by the State Contract Manager. No State data shall be processed on or transferred to any device or storage medium including portable media, smart devices and/or USB devices, unless that device or storage medium has been approved in advance in writing by the State Contract

Manager. The Contractor must not store or transfer State of New Jersey data outside of the United States.

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

G. Data Breach: In the event of any actual, probable or reasonably suspected Breach of Security, or any unauthorized access to or acquisition, use, loss, destruction, compromise, alteration or disclosure of any Personal Data, Contractor shall: (a) notify the State immediately of such Breach of Security, but in no event later than 24 hours after 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 *RFQ Section 6.11 - 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 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 RFQ 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 back up 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 calendar days after the termination/expiration of the Contract or within seven (7) business days of the request of an agent of the State whichever should come first.

J. In the event of loss of any State Data 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.

g. 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.

h. 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.

i. 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.

j. PROJECT AND RESOURCE MANAGEMENT

The Contractor shall ensure that controls necessary to appropriately manage risks are accounted for and implemented throughout the term of the Contract 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 term.

k. 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.

l. 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.

1.1 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 State may terminate the Contract pursuant to the SSTC.

m. 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.

n. 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.

o. 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.

p. 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.

q. 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.

r. PRIVACY

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

A. Data Ownership. The State owns State Data. Contractor shall not obtain any right, title, or interest in any State Data, or information derived from or based on State Data.
B. Data usage, storage, and protection of Personal Data are subject to all applicable international, federal and state statutory and regulatory requirements, as amended from time to time, including, without limitation, those for HIPAA, Tax Information Security Guidelines for Federal, State, and Local Agencies (IRS Publication 1075), New Jersey State tax confidentiality statute, the New Jersey Privacy Notice found at NJ.gov, N.J.S.A. § 54:50-8, New Jersey Identity Theft Prevention Act, N.J.S.A. § 56:11-44 et. seq., the federal Drivers' Privacy Protection Act of 1994, Pub.L.103-322, and the confidentiality requirements of N.J.S.A. § 39:2-3.4. Contractor shall also conform to PCI DSS, where applicable.
C. Security: Contractor agrees to take appropriate administrative, technical and physical safeguards reasonably designed to protect the security, privacy, confidentiality, and integrity of user information. Contractor shall ensure that State Data is secured and encrypted during transmission or at rest.
D. Data Transmission: The Contractor shall only transmit or exchange State Data with other parties when expressly requested in writing and permitted by and in accordance with requirements of the Contract or the State of New Jersey. The Contractor shall only transmit or exchange State Data with the State of New Jersey or other parties through secure means supported by current technologies.
E. Data Storage: All data provided by the State of New Jersey or State data obtained by the Contractor in the performance of the Contract must be stored, processed, and maintained solely in accordance with a project plan and system topology approved by the State Contract Manager. No State data shall be processed on or transferred to any device or storage medium including portable media, smart devices and/or USB devices, unless that device or storage medium has been approved in advance in writing by the State Contract

Manager. The Contractor must not store or transfer State of New Jersey data outside of the United States.

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

G. Data Breach: In the event of any actual, probable or reasonably suspected Breach of Security, or any unauthorized access to or acquisition, use, loss, destruction, compromise, alteration or disclosure of any Personal Data, Contractor shall: (a) notify the State immediately of such Breach of Security, but in no event later than 24 hours after 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 *RFQ 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 RFQ 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.

s. 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.

t. 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.

u. 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.

v. 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.

w. 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.

x. 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.

y. 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.

z. 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.

aa. 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.

bb. 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.

cc. 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 RFQ, 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.

dd. 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. 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.

ee. 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.

ff. 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.).

gg. 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.

hh. 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.

ii. 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.

jj. 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.

kk. 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.

ll. 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.

mm. 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.

nn. 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.

oo. 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 compute, 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.

pp. 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.

qq. 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.

rr. 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.

ss. 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.

2.3.1.1 **OFFER AND ACCEPTANCE PAGE {SIGNATORY PAGE}**

The Vendor {Bidder} shall complete, including signature of an authorized representative of the Vendor {Bidder}, and submit the Offer and Acceptance Page {Signatory Page} accompanying this Bid Solicitation {RFP}. If the Vendor {Bidder} is a limited partnership, the Offer and Acceptance Page {Signatory Page} must be signed by a general partner. All information requested must be submitted. If the Vendor {Bidder} is a joint venture, the Offer and Acceptance Page {Signatory Page} must be signed by a principal of each party to the joint venture. Failure to comply will result in rejection of the Quote {Proposal}.

2.3.1.1.1 **MACBRIDE PRINCIPLES CERTIFICATION**

The Vendor {Bidder} must certify pursuant to N.J.S.A. 52:34-12.2 that it is in compliance 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 its compliance with those principles. See Section 2.5 of the SSTC and N.J.S.A. 52:34-12.2 for additional information about the MacBride principles.

By signing the Bid Solicitation {RFP} Offer and Acceptance Page {Signatory Page}, the Vendor {Bidder} is automatically certifying that either:

a. The Vendor {Bidder} has no operations in Northern Ireland; or

b. The Vendor {Bidder} has business operations in Northern Ireland and is committed to compliance with the MacBride principles.

A Vendor {Bidder} electing not to certify to the MacBride Principles must nonetheless sign the Bid Solicitation {RFP} Offer and Acceptance Page {Signatory Page} AND must include, as part of its Quote {Proposal}, a statement indicating its refusal to comply with the provisions of this Act.

2.3.1.1.2 **NO SUBCONTRACTOR CERTIFICATION**

For a Quote {Proposal} that does NOT include the use of any Subcontractors, by signing the Bid Solicitation {RFP} Offer and Acceptance Page {Signatory Page}, the Vendor {Bidder} is *automatically* certifying that:

a. In the event the award is granted to the Vendor's {Bidder's} firm and the Vendor {Bidder} later determines at any time during the term of the Blanket P.O. {Contract} to engage Subcontractors to provide certain goods and/or services, pursuant to Section 5.8 of the SSTC, the Vendor {Bidder} shall submit a Subcontractor Utilization Plan form for approval to the Division in advance of any such engagement of Subcontractors; and

b. If the Blanket P.O. {Contract} is a small business subcontracting set-aside, the Vendor {Bidder} certifies that in engaging Subcontractors, it shall make a good faith effort to achieve the subcontracting set-aside goals, and shall attach to the Subcontractor Utilization Plan documentation of such efforts in accordance with N.J.A.C. 17:13-4 *et seq*.

2.3.1.1.3 **NON-COLLUSION**

By submitting a Quote {Proposal} and signing the Bid Solicitation {RFP} Offer and Acceptance Page {Signatory Page}, the Vendor {Bidder} certifies as follows:

a. The price(s) and amount of its Quote {Proposal} have been arrived at independently and without consultation, communication or agreement with any other Vendor {Contractor, Bidder} or any other party;

b. Neither the price(s) nor the amount of its Quote {Proposal}, and neither the approximate price(s) nor approximate amount of this Quote {Proposal}, have been disclosed to any other firm or person who is a Vendor {Bidder} or potential Vendor {Bidder}, and they will not be disclosed before the Quote {Proposal} submission;

c. No attempt has been made or will be made to induce any firm or person to refrain from bidding on this Blanket P.O. {Contract}, or to submit a Quote {Proposal} higher than this Quote {Proposal}, or to submit any intentionally high or noncompetitive Quote {Proposal} or other form of complementary Quote {Proposal};

d. The Quote {Proposal} of the firm is made in good faith and not pursuant to any agreement or discussion with, or inducement from, any firm or person to submit a complementary or other noncompetitive Quote {Proposal}; and

e. The Vendor {Bidder}, its affiliates, subsidiaries, officers, directors, and employees are not currently under investigation by any governmental agency and have not in the last five (5) years been convicted or found liable for any act prohibited by state or federal law in any jurisdiction, involving conspiracy or collusion with respect to bidding on any public contract.

2.3.1.1.4 **NEW JERSEY BUSINESS ETHICS GUIDE CERTIFICATION**

The Treasurer has established a business ethics guide to be followed by Vendors {Bidders/Contractors} in its dealings with the State. The guide provides further information about compliance with Section 2.7 of the SSTC. The guide can be found at:

http://www.state.nj.us/treasury/purchase/ethics_guide.shtml

By signing the Bid Solicitation {RFP} Offer and Acceptance Page {Signatory Page}, the Vendor {Bidder} is automatically certifying that it has complied with all applicable laws and regulations governing the provision of State goods and services, including the Conflicts of Interest Law, N.J.S.A. 52:13D-12 to -28.

2.3.1.2 **NJ STANDARD BID SOLICITATION {RFP} FORMS REQUIRED WITH THE QUOTE {PROPOSAL}**

Vendor's {Bidder's} failure to complete, sign and submit the forms in Section 4.4.1.2 shall be cause to reject its Quote {Proposal} as non-responsive.

2.3.1.2.1 **OWNERSHIP DISCLOSURE FORM**

Pursuant to N.J.S.A. 52:25-24.2, in the event the Vendor {Bidder} is a corporation, limited liability company or partnership, the Vendor {Bidder} must complete an Ownership Disclosure Form.

A current completed Ownership Disclosure Form must be received prior to or accompany the submitted Quote {Proposal}. A Vendor's {Bidder's} failure to submit the completed and signed form with its Quote {Proposal} will result in the rejection of the Quote {Proposal} as non-responsive and preclude the award of a Blanket P.O. {Contract} to said Vendor {Bidder} unless the Division has on file a signed and accurate Ownership Disclosure Form dated and received no more than six (6) months prior to the Quote {Proposal} submission deadline for this procurement. If any ownership change has occurred within the last six (6) months, a new Ownership Disclosure Form must be completed, signed and submitted with the Quote {Proposal}.

2.3.1.2.2 **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.

4. PROFESSIONAL LIABILITY INSURANCE

Section 4.2 of the SSTC 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.

5. QUOTE EVALUATION AND AWARD

tt. 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 Using Agency within five (5) business days after the deadline for Quote submission. Written evidence for a specific procurement that is not provided to the Using Agency 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.

uu. CLARIFICATION OF QUOTE

After the Quote Opening Date, unless requested by the State as noted below, Bidder contact with the Using Agency regarding this RFQ and the submitted Quote is not permitted. After the Quotes are reviewed, one (1), some or all of the Bidders may be asked to clarify inconsistent statement contained within the submitted Quote.

vv. TIE QUOTES

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

ww. 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.

xx. 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.

yy. 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.

I. 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.

II. 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.

zz. 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.

aaa. BEST AND FINAL OFFER (BAFO)

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

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

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

If the Using Agency contemplates BAFOs, Quote prices will not be publicly read at the Quote opening. Only the name and address of each Bidder will be publicly announced at the Quote opening.

bbb. 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.

ccc. RECOMMENDATION FOR AWARD

After the evaluation of the submitted Quotes is complete, the Using Agency will recommend to the Director of the Division of Purchase and Property for award, the responsible Bidder(s) whose Quote, conforming to this RFQ, is most advantageous to the State, price and other factors considered.

ddd. CONTRACT AWARD

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