Request For Quotes

Election Processing for the Police and Firemen's Retirement System of New Jersey

RFQ Issue Date:	**April 9, 2024**
Questions Due:	**April 22, 2024**
Time	**By 3:00 p.m. prevailing Eastern**
Quote Submission Due:	**May 2, 2024**
Time	**By 3:00 p.m. prevailing Eastern**

James A. Kompany
Chairman
Police and Firemen's Retirement System of New Jersey

1. Introduction and Summary of the Request for Quotes

This Request for Quotes (RFQ) is issued by the Police and Firemen's Retirement System of New Jersey (PFRSNJ). The Contract will be awarded through the PFRSNJ website: (https://www.nj.gov/pfrs/).

1.1 Purpose, Intent, and Background

The purpose of this RFQ is to solicit quotes ("Quotes") for the purpose of selecting a qualified contractor ("Contractor") to handle any or all Phases of the PFRSNJ trustee election process consistent with all statutory and regulatory requirements governing the election process, including but not limited to electronic delivery of the notice of election to employing locations (Phase I), verifying candidate nominations to assure compliance with the requisite number of valid PFRSNJ members (Phase II), printing of election packet materials, sorting (as described herein), mailing of election packets including postage (Phase III), and tabulation and certification of the results of the election (Phase IV).

It is the intent of the PFRSNJ to award one contract ("Contract") to that qualified bidder ("Bidder") whose Quote, conforming to this RFQ, is most advantageous to the PFRSNJ price and other factors considered. The PFRSNJ may award any or all price lines. The PFRSNJ, however, reserves the right to separately procure individual requirements that are the subject of the Contract during the Contract term, when determined to be in the PFRSNJ's best interest.

The State of New Jersey Standard Terms and Conditions and Waivered Contracts/Delegated Purchase Authority Supplement to the State of New Jersey Standard Terms and Conditions (SSTCs) included with this RFQ will apply to all Contracts made with the PFRSNJ. These terms are in addition to the terms and conditions set forth in this RFQ and should be read in conjunction with them unless the RFQ specifically indicates otherwise.

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) SSTCs, 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 PFRSNJ, shall not be incorporated into the Contract awarded. Any references to external documentation, including those documents referenced by a URL, such as without limitation, technical reference manuals, technical support policies, copyright notices, additional license terms, etc., are subject to the terms and conditions of this RFQ and the SSTCs. In the event of any conflict between the terms of a document incorporated by reference and the terms and conditions of the RFQ and the SSTCs, the RFQ and the SSTCs shall prevail.

2. Pre-Quote Submission Information

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

2.1 Question and Answer Period

The PFRSNJ will electronically accept questions and inquiries from all potential Bidders. Questions should be directly tied to the RFQ and asked in consecutive order, from beginning to end, following the organization of the RFQ; and each question should begin by referencing the RFQ page number and section number to which it relates.

A Bidder shall submit questions only to the PFRSNJ by email Courtney.Snedeker@pfrs.nj.gov. The PFRSNJ will not accept any questions in person or by telephone concerning this RFQ. The cut-off date for electronic questions and inquiries relating to this RFQ is indicated on the RFQ cover sheet. In the event that questions are posed by Bidders, answers to such questions will be issued by Addendum. Any Addendum to this RFQ will become part of this RFQ and part of any Contract awarded as a result of this RFQ. Addenda to this RFQ, if any, will be posted to the PFRSNJ website. https://www.nj.gov/pfrs/.

2.2 Bid Amendments

In the event that it becomes necessary to clarify or revise this RFQ, such clarification or revision will be by Bid Amendment. Any Bid Amendment will become part of this RFQ and part of any Contract awarded. Bid Amendments will be posted with the RFQ on the PFRSNJ website (https://www.nj.gov/pfrs/). There are no designated dates for release of Bid Amendments. It is the sole responsibility of the Bidder to be knowledgeable of all Bid Amendments related to this RFQ.

3. Quote Submission Requirements

3.1 Quote Submission

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

3.2 Bidder Responsibility

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

3.3 Bidder Additional Terms Submitted with the Quote

A Bidder may submit additional terms as part of its Quote. Additional terms are Bidder-proposed terms or conditions that do not conflict with the scope of work required in this RFQ, the terms and conditions of this RFQ, or the SSTCs. Bidder proposed terms or conditions that materially conflict with those contained the SSTCs will render a Quote non-responsive. It is incumbent upon the Bidder to identify and remove its conflicting proposed terms and conditions prior to Quote submission.

3.4 Quote Content

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

- Forms

- Technical Quote
- Price Quote

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

3.5 Forms, Registrations, and Certifications to be Submitted with Quote

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

3.5.1 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 PFRSNJ's request or the PFRSNJ may deem the Quote non-responsive. The Offer and Acceptance Page can be found in Attachment A1.

3.5.2 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 PFRSNJ 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 who holds a 10 percent or greater beneficial interest. N.J.S.A. 52:25-24.2. The Ownership Disclosure Form can be found in Attachment A2.

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 such Bidder.

3.5.3 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 affiliate, 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 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 PFRSNJ's request or the PFRSNJ may deem the Quote non-responsive. The Disclosure of Investment Activities in Iran form can be found in Attachment A3.

3.5.4 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 or 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 PFRSNJ's request or the PFRSNJ may deem the Quote non-responsive. The Disclosure of Investigations or Other Actions Involving Bidder Form can be found in Attachment A4.

3.5.5 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 PFRSNJ's request or the PFRSNJ may deem the Quote non-responsive. The MacBride Principles Form can be found in Attachment A5.

3.5.6 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 PFRSNJ's request or the PFRSNJ may deem the Quote non-responsive. The Source Disclosure Form can be found in Attachment A6.

3.5.7 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 PFRSNJ 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. The 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 such exemption(s) as a matter of law. The PFRSNJ 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 PFRSNJ does not agree with a Bidder's designation of proprietary and/or confidential information, the PFRSNJ 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 PFRSNJ reserves the right to make the determination as to what material(s) to disclose in response to an OPRA request. Any information that the PFRSNJ 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 PFRSNJ's determination of confidentiality, the Bidder shall be solely responsible for defending its designation, and in doing so, all costs and expenses associated therewith shall be the responsibility of the Bidder. The PFRSNJ assumes no such responsibility or liability.

In order not to delay consideration of the Quote or the PFRSNJ's response to a request for documents, the PFRSNJ requires that the Bidder respond to any request regarding confidentiality markings within the timeframe designated in the PFRSNJ's correspondence regarding confidentiality. If no response is received by the designated date and time, the PFRSNJ may release a copy of the Quote with the PFRSNJ making the determination regarding what material(s), if any, may be proprietary or confidential. The Confidentiality/Commitment to Defend Form can be found in Attachment A7.

3.5.8 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 shall 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 PFRSNJ 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. Any such request shall be subject to the approval of the PFRSNJ. The Subcontractor Utilization Plan Form can be found in Attachment A8.

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

3.5.9 Pay to Play Prohibitions

Pursuant to N.J.S.A. 19:44A-20.13 et seq. (P.L. 2005, c. 51), the PFRSNJ 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 the 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. The Two-Year Chapter 51/Executive Order 117 Vendor Certification and Disclosure of Political Contribution Form can be found in Attachment A9.

3.5.10 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, instructions, and the AA-302 application are available at:

https://www.state.nj.us/treasury/contract_compliance/index.shtml.

3.5.11 Executive Order 271

Pursuant to Public Law 205, Chapter 271, the Bidder must complete this Certification and Political Contribution Disclosure Form. This form must be completed at least ten (10) days prior to entering into a Contract for the services described in this RFQ. The Certification and Political Contribution Disclosure For Public Law 2005, Chapter 271 can be found in Attachment A10.

3.5.12 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 objectives as outlined and documented in the Statewide Information Security Manual; and (2) comply with the 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. The State of New Jersey Security Due Diligence Third-Party Information Security Questionnaire can be found in Attachment A11 .

3.5.13 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 copy of the current New Jersey Business Registration Certificate for the Bidder (and each subcontractor) must be submitted by the Bidder. Information and instructions for obtaining a BRC can be found at: https://www.nj.gov/treasury/revenue/gettingregistered.shtml.

3.5.14 Non Involvement in Prohibited Activities in Russia and Belarus

Pursuant to applicable state and federal law, a person or entity seeking to enter into or renew a contract with the PFRSNJ for the provision of goods or services shall certify that it is not identified on the U.S. Department of the Treasury's, Office of Foreign Assets Control's Consolidated Sanctions List. Accordingly, the Bidder shall submit an updated Certification of Non-Involvement in Prohibited Activities. The Certification of Non-Involvement in Prohibited Activities can be found in Attachment A12.

3.6 Technical Quote

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

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

demonstrate that the Bidder's approach and plans to undertake and complete the Contract are appropriate to the tasks and subtasks involved.

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

3.7 Contract Management

The Bidder should describe its specific plans to manage, control, and supervise the Contract to ensure satisfactory Contract completion according to the required schedule. The plan should include the Bidder's approach to communicate with the Contract Manager including, but not limited to, status meetings, status reports, etc.

3.8 Contract Schedule

The Bidder shall include a draft Contract schedule. If key dates are a part of this RFQ, the Bidder's schedule should incorporate such key dates and should identify the completion date for each task and sub-task required by the Scope of Work. Such schedule should also identify the associated deliverable item(s) to be submitted as evidence of completion of each task and/or subtask. See Attachment B for a sample election timeline ("Timeline") including sample key dates for an election. The Timeline for each election during the term of this Contract shall be created by the PFRSNJ and supplied to the Contractor on a case-by-case basis.

The Bidder should identify the Contract scheduling and control methodology to be used and should provide the rationale for choosing such methodology.

3.9 Organizational Experience

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

3.10 Location

The Bidder should include the address of where responsibility for managing the Contract will take place. The Bidder should include the telephone number and name of the individual to contact. The Bidder should also include the name and contact information for any of its employees working on the contract.

3.11 Experience with Contracts of Similar Size and Scope

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

numbers of individuals for contracting party. Beginning and ending dates should also be given for each contract.

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

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

3.12 Financial Capability of the Bidder

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

A. For publicly traded companies the Bidder should provide copies or the electronic location of the annual reports filed for the two most recent years; or

B. For privately held companies the Bidder should provide the certified financial statement (audited or reviewed) in accordance with applicable standards by an independent Certified Public Accountant which include a balance sheet, income statement, and statement of cash flow, and all applicable notes for the most recent calendar year or the Bidder's most recent fiscal year.

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

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

3.13 Price Quote

The Bidder must submit a price quote and attach it to this RFQ .

Any price changes including hand written revisions or "white-outs" must be initialed. Failure to initial price changes shall preclude a Contract award from being made to the Bidder pursuant to N.J.A.C. 17:12-2.2(a)(8).

The Bidder shall provide an all-inclusive rate for each task, within each Phase, described in the RFQ.

The PFRSNJ reserves the right to perform or arrange for the performance of all or part the work in Phases I and II. Submitting a quote for any line does not guarantee work or volume.

3.16 State of New Jersey Standard Terms and Conditions and Waivered Contracts/Delegated Purchasing Authority Supplement to the State of New Jersey Standard Terms and Conditions

The State of New Jersey Standard Terms and Conditions and Waivered Contracts/Delegated Purchasing Authority Supplement to the State of New Jersey Standard Terms and Conditions and the related Certification can be found in Attachment A13. The Bidder must submit a Certification Accepting the Standard Terms & Conditions.

3.17 Proof of Insurance

The Contractor is required to secure and maintain in force for the term of the contract insurance as provided in Section 4.2 of the State of New Jersey Standard Terms and Conditions and Waivered Contracts/Delegated Purchasing Authority Supplement to the State of New Jersey Standard Terms and Conditions. The Bidder must submit proof of insurance (ACORD form) as provided in the State of New Jersey Standard Terms and Conditions and Waivered Contracts/Delegated Purchasing Authority Supplement to the State of New Jersey Standard Terms and Conditions.

4. Scope of Work

The following is a list of general requirements for this Contractor and Request for Quotes. The Bidder shall have the ability to complete all four (4) Phases of each election as requested by the PFRSNJ.

The PFRSNJ reserves the right to temporarily or permanently move the performance of any Phase(s) during an election cycle in-house, if it is determined by the PFRSNJ to be in the PFRSNJ's best interests. The PFRSNJ will provide written notice a minimum of thirty (30) calendar days in advance of the commencement of a Phase if it is decided that the performance of a Phase will be performed in-house.

4.1 Phase I

The PFRSNJ reserves the right to complete all or part of Phase I in-house. Upon request, the Contractor shall complete the requirements listed under Phase I.

Phase I consists of:

A. For active police and firm member elections: Contractor electronically mails (emails) notice to the certifying officer or appropriate fiscal officer of each employing agency, together with instructions as to who is to receive the notices;

B. For retired member elections: Contractor mails notice to the member's last known mailing address; and

C. Contractor submits an invoice for payment of Phase I to be authorized by the PFRSNJ.

4.1.1 Printing and Mailing Electronic Notices

The PFRSNJ will provide an original form of a notice of election to the Contractor along with a certifying officer letter (for active police and fire only) at least nine (9) months prior to the expiration

of the term of the elected PFRSNJ trustee for active member-trustee positions and at least six (6) months prior to the expiration of a term of office for a retired member-trustee, or immediately upon the vacancy of a Board member.

For active PFRSNJ members the Contractor shall:

A. Receive all files created by the PFRSNJ which include employer name, address, certifying officer's name, telephone number, FAX number, internet address, pension location number, check distribution number (if any) and summary totals of the number of eligible voters at each employing agency;

B. Email election notices and certifying officer letter to each employing agency for distribution to eligible active PFRSNJ members;

C. Include in the certifying officer letter that the employing agency shall acknowledge proper distribution of the notice to its employees; and

D. Have an email address for an employing agency to acknowledge that an electronic copy was sent.

For retired PFRSNJ members the Contractor shall:

A. Receive all files provided by the PFRSNJ which include the retired member's last known mailing address; and
B. Mail the election notice to the last known mailing address of each of the retired members.

4.2 Phase II

The PFRSNJ reserves the right to complete all or part of Phase II in-house. Phase II consists of the nomination process of the election as well as the certification of the nominations.

4.2.1 Nomination Process

A member who is seeking the nomination to be a candidate for an elected position shall prepare a written letter of interest to the Board Secretary who will verify the eligibility of a member to be a candidate. If the member qualifies the Office of the Board Secretary will provide to the qualifying member instructions regarding the nomination process. Each eligible PFRSNJ member has the ability to nominate one (1) potential candidate for their respective member group (police members, fire members, and retired members).

Eligible active members shall have the ability to nominate only through an electronic secure website created by the Contractor.

Eligible retired members shall have the ability to nominate both through an electronic secure website created by the Contractor or by paper petition. The PFRSNJ will receive all paper petitions and forward those petitions to the Contractor for certification.

4.2.1.1 Electronic Nomination Process

The Contractor shall have a secure nominations website in which all listed members can access and submit their nomination choices. Each member shall be given customized secure access to the nomination website and have the ability to view all nominations that have been collected. The

Contractor shall give the PFRSNJ access to the secure nominations website to be able to view all potential candidates and their verifying signatures.

4.2.1.2 Paper Nomination Process

All paper nominations are sent to the PFRSNJ. The PFRSNJ will forward all paper nominations to the Contractor for certification within ten (10) weeks prior to the distribution of ballots. Each paper petition form shall require the candidate's name and employer, and the social security number or pensions membership number of each petitioner.

4.2.2 Validation of Nominations

The Contractor shall validate all electronic and paper nomination forms. Approximately ten (10) weeks prior to distribution of ballots, the PFRSNJ will ensure the Contractor is sent an internet transmission, CD, or secure email containing each PFRSNJ members name, social security number, membership number, and date of birth for the validation check. Each validation consists of the following steps that the Contractor shall perform:

A. Verify the petitioner's name and pension membership number, date of birth, and social security number with the database file provided to the Contractor. All of those results shall be electronically recorded on a secure website;

B. Validate all signatures to ensure the appropriate number of eligible active members has nominated the correct number of eligible candidates; and

C. Ensure that a minimum number of nominations are received: 500 for active police members who are eligible to vote for the position, 300 for active fire members who are eligible to vote for the position, and 100 for retired members who are eligible to vote for the position.

Upon completion of the verification process, the Contractor shall provide the PFRSNJ with a written report for each candidate of all validated petitioners names, membership numbers, and total number of nominations. The report shall include an exception list for all rejected nominations including the specific reason for the rejection. This report shall be sent via email to the PFRSNJ.

4.2.3 Candidate Selection (One (1) Candidate Only)

The PFRSNJ reserves the right to complete this step of the Phase in-house. The Contractor shall only complete this step upon request.

If only one (1) candidate receives the required nominations for a position, the candidate shall be deemed elected to the position without balloting. The PFRSNJ staff will notify the Board and the Board will announce there was no contest as only one candidate qualified.

4.3 Phase III

Phase III consists of the election balloting process and procedures. The PFRSNJ will ensure the Contractor is provided the member files that include member names, fund, member number, date of

birth, social security number, pension employer location number or payroll number, and check distribution number.

The Contractor shall:

A. Review all employer and member data the PFRSNJ will ensure is supplied;

B. Submit a sample election ballot output that the PFRSNJ will review;

C. Provide the PFRSNJ with a test of the electronic ballot procedures at least two (2) weeks prior to the distribution of the actual election packets. The PFRSNJ will proofread and make all edits to the test sample during this stage;

D. Print all election materials needed for distribution which include member's names, member's pension number (confidential and shall not be visible on the postage paid or on the self-sealed return mailer), location number, ballot control number, PIN number, and specified distribution code for sorting locations on the outside of potion of the mailer;

E. For active police or fire members:

i. Mail active police or fire member PFRSNJ election packets and transmittal letters to the certifying officers at each employing location, sorted and distributed as described in the method listed in this specification;
ii. Certify to the PFRSNJ that the distribution of all election materials to the certifying officer at each employing location has been completed;

F. For retired members:

i. Mail eligible retired member PFRSNJ election packets and instruction letters to each eligible retired voter;
ii. Certify to the PFRSNJ that the distribution of all election materials to retired members has been completed;

G. Follow-up at least twice (if necessary) with employing locations that have not emailed a response regarding the certification of distribution of election packets or have not cast votes from that location. The Contractor must provide the PFRSNJ with a mid-election report that will list the location names and numbers of all employers that have certified the distribution of election packets and a separate list of those location that have not certified the distribution of election packets. The results of the Contractor's follow-up must be included in the mid-election report;

H. Produce replacement election packets for lost or missing election packets upon request of the PFRSNJ;

I. For active police or fire members:

i. distribute all individual member election packets to the employing locations and sorted via first- class mail or an express mail service by the dates listed on the Timeline provided by the PFRSNJ to the Contractor. The boxes or packets to employers must clearly indicate on the outside packet that the materials contain important time sensitive Board of Trustee election materials and must be distributed immediately. The employer is responsible for the distribution of the active member election packets to the eligible member voters;

J. For retired members:

i. distribute to each eligible retired voter an election packet.

K. Each election packet (for both active and retired members) must contain the following:

1. The eligible member's name, pension membership number, pension location number (for active members only), ballot number, and personal identification number ("PIN"); and

2. The name of each candidate nominated including a biographical sketch listing the candidate's background and employer for active members or former employer for retired members; and

3. The closing date of the election; and

4. Instructions containing information on how to properly cast a vote through one (1) of the means listed below. This will include a notification that shall advise the member that mutilated ballots, illegible ballots, ballots with write-in votes, ballots with multiple votes for one (1) position, or ballots where it can not be determined for whom the member intended to vote shall be declared invalid and not considered in the final election count;

5. There will be instructions on how to use the member's personal identification number (PIN). The instructions must also provide members with a statement regarding the confidentiality, and security used by the Contractor to protect the election process against fraudulent and/or multiple voting; and

6. The election packet will provide a designated space for members to record a confirmation number, which will be provided to the member by the Contractor upon completion of an electronic vote. Informational data about the election process must be provided, including that the first vote cast by the member will be counted as the official vote and all subsequent votes will be rejected; the last date to cast a vote; and the candidate collecting the plurality of all eligible votes will be deemed the winner of the election, subject to final approval by the PFRSNJ Board of Trustees.

L. Allow two methods of voting for active police and fire members and three methods of voting for retired members:

1. Toll-free telephone voice retrieval system- electronic vote;

2. Secure Internet site (provided by the Contractor); and

3. For retired members only, paper ballot (using bar code system, postage-paid, self-sealed, return mailer).

M. A transmittal letter must be enclosed with every employer packet which will require the certifying officers of each employing location to electronically certify that the election packets were received and distributed to active employees, and all non-distributable ballots (i.e., employee transferred, terminated, or retired) are properly discarded by the certifying officer at the employing locations;

N. Monitor that each employing location electronically verifies that they have distributed the election packets in accordance with NJ State statutes and regulations;

O. Report the results to the PFRSNJ at the time of the mid-election report and final certification;

P. Conduct written follow-up with the employing location at least twice (as necessary), and record the results as mentioned above; and

Q. All misprints and over prints shall not be charged to the PFRSNJ.

For retired member ballots, the PFRSNJ Board of Trustees reserves the right to assess the percentage of returned votes after the conclusion of each election and determine based upon an analysis of the frequency of use of paper ballots versus the cost of providing paper ballots whether or not paper ballot should continue to be incorporated in the election packet in future elections. The Secretary shall notify the Contractor handling the next election of the Board's decision regarding the inclusion of the paper ballot in the initial election packet. If the Board determines paper ballots shall no longer be included in the initial election packet members who cannot cast an electronic ballot may contact the Contractor to request a paper ballot. Members shall provide the Contractor with their proper ballot and pension numbers and home address. Upon proper request by an eligible voter, Contractor shall mail a paper ballot to the voter's home address, together with instructions for casting the ballot, biographical information about the candidates, a postage-paid return envelope, and a notification that shall advise the member that mutilated ballots, illegible ballots, ballots with write-in votes, ballots with multiple votes for one (1) position, or ballots where it cannot be determined for whom the member intended to vote shall be declared invalid and not considered in the final election count.

4.4 Phase IV

Phase IV consists of the validation and certification of all election results. The Contractor must complete the following:

A. Validate votes cast by eligible PFRSNJ members. The members voting through electronic means (telephone and Internet) will be given a confirmation number by the Contractor upon completion of a valid electronic vote;

B. Provide bi-weekly updates to the PFRSNJ regarding the overall status of the election returns. A mid-election listing of any employer location for which no ballots have been received by Contractor. Additionally, the report must indicate which employing locations have and which have not acknowledged distribution of the election packets after the required Contractor follow-up. The list should include verification of the locations with votes cast in one (1) or more of the three (3) methods as denoted in Phase III;

C. Count all paper ballots (for retired members only);

D. Not count and/or validate all ballots that are incorrectly completed or mutilated;

E. Count only ballots received on time according to the deadlines shown in the Timeline;

F. Perform a tabulation of electronic votes and/or paper ballots; and

G. Report of the final certification of results by 4:00PM EST on the dates according to the Timeline and must contain the following information:

1. The parties to the Contract;

2. The service performed in connection with the Contract;

3. The date of the original distribution of election packets;

4. The total number of all election packets distributed;

5. Sample paper ballot;

6. The results of certifications collected from employing locations;

7. The total number of replacement packets mailed;

8. The total number of electronic votes, and paper ballots received;

9. The total number of electronic votes, and paper ballots rejected, and the corresponding reasons;

10. The time and date of the receipt deadline for all electronic votes, and paper ballots;

11. The results of votes cast for each candidate;

12. The total number of votes received from each employing location; and

13. Verification that the total number of electronic votes matches the number of confirmation numbers assigned.

All certified ballots must be sent to the PFRSNJ within thirty (30) calendar days following the certification of the results of the election. At least fifteen (15) physical copies of the certified election results must also be sent to the PFRSNJ.

4.5 Payment

Following the completion of each Phase of the PFRSNJ election process performed by the Contractor, the Contractor shall submit an invoice to the PFRSNJ. The Contractor shall be paid the applicable all-inclusive task rate following the completion of each Phase.

Payment for the voting Phase is dependent on the percentage of votes received. If over 60% of the vote is received, the Contractor will be paid at a higher rate according to the price quote.

The Contractor shall be paid for postage of all mailings at the applicable federal postage rate. The Contractor must notify the PFRSNJ at least thirty (30) days prior to a government-imposed increase on postage. The PFRSNJ will adjust all postage pricing to match the government-imposed increase on postage upon notification.

5. General Contract Terms

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

waiver of any rights that the PFRSNJ may have arising out of the Contractor's performance of this Contract.

5.1 Contract Term and Extension Option

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

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

5.2 Contract Transition

In the event that a new Contract has not been awarded prior to the expiration date for this Contract, including any extensions exercised, and the PFRSNJ exercises this Contract transition, the Contractor shall continue this Contract under the same terms, conditions, and pricing until a new Contract can be completely operational. At no time shall this transition period extend more than 180 calendar days beyond the expiration date of this Contract, including any extensions exercised.

6. Data Security Requirements- Contractor Responsibility

6.1 Security Plan

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

6.2 Information Security Program Management

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

A. Establishment of a management structure with clear reporting paths and explicit responsibility for information security;

B. Creation, maintenance, and communication of information security policies, standards, procedures, and guidelines to include the control areas listed in sections below;

C. Development and maintenance of relationships with external organizations to stay abreast of current and emerging security issues and for assistance, when applicable; and

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

6.3 Compliance

The Contractor shall develop and implement processes to ensure its compliance with all statutory, regulatory, contractual, and internal policy obligations applicable to this Contract. Examples include,

but are not limited to, General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act of 1996 (HIPAA), and IRS Publication 1075. The Contractor shall timely update its processes as applicable standards evolve.

A. Within ten (10) calendar days after award, the Contractor shall provide the PFRSNJ 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, the Contractor shall implement processes to ensure security assessments of information systems are conducted for all significant development and/or acquisitions, prior to information systems being placed into production; and

C. The Contractor shall also conduct periodic reviews of its information systems on a defined frequency for compliance with statutory, regulatory, and contractual requirements. The Contractor shall document the results of any such reviews.

6.4 Personnel Security

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

A. Position descriptions that include appropriate language regarding each role's security requirements;

B. To the extent permitted by law, employment screening checks are conducted and successfully passed for all personnel prior to beginning work or being granted access to information assets;

C. Rules of behavior are established and procedures are implemented to ensure personnel are aware of and understand usage policies applicable to information and information systems;

D. Access reviews are conducted upon personnel transfers and promotions to ensure access levels are appropriate;

E. Contractor disables system access for terminated personnel and collects all organization owned assets prior to the individual's departure; and

F. Procedures are implemented that ensure all personnel are aware of their duty to protect information assets and their responsibility to immediately report any suspected information security incidents.

6.5 Security Awareness and Training

The Contractor shall provide periodic and ongoing 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 PFRSNJ Confidential Information from a loss of confidentiality, integrity, availability, and privacy. Security awareness and training shall include, at a minimum:

A. Personnel are provided with security awareness training upon hire and at least annually, thereafter;

B. Security awareness training records are maintained as part of the personnel record;

C. Role-based security training is provided to personnel with respect to their duties or responsibilities (e.g. network and systems administrators require specific security training in accordance with their job functions); and

D. Individuals are provided with timely information regarding emerging threats, best practices, and new policies, laws, and regulations related to information security.

6.6 Risk Management

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

A. An approach that categorizes systems and information based on their criticality and sensitivity;

B. An approach that ensures risks are identified, documented and assigned to appropriate personnel for assessment and treatment;

C. Risk assessments shall be conducted throughout the lifecycles of information systems to identify, quantify, and prioritize risks against operational and control objectives and to design, implement, and exercise controls that provide reasonable assurance that security objectives will be met; and

D. A plan under which risks are mitigated to an acceptable level and remediation actions are prioritized based on risk criteria and timelines for remediation are established. Risk treatment may also include the acceptance or transfer of risk.

6.7 Privacy

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

A. Data Ownership. The PFRSNJ owns PFRSNJ Data. The Contractor shall not obtain any right, title, or interest in any PFRSNJ Data, or information derived from or based on PFRSNJ 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: The 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 PFRSNJ Data is secured and encrypted during transmission or at rest.

D. Data Transmission: The Contractor shall only transmit or exchange PFRSNJ 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 PFRSNJ Data with the PFRSNJ or other parties through secure means supported by current technologies.

E. Data Storage: All data provided by the PFRSNJ or PFRSNJ 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 Contract Manager. No PFRSNJ 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 Contract Manager. The Contractor must not store or transfer PFRSNJ Data outside of the United States.

F. Data Re-Use: All PFRSNJ 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 PFRSNJ 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 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, the Contractor shall: (a) notify the PFRSNJ 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 the Contractor who shall be available to the PFRSNJ twenty-four (24) hours per day, seven (7) days per week as a contact regarding the 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 PFRSNJ, 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 PFRSNJ and reasonably cooperate with the PFRSNJ to prevent any notification or disclosure concerning any Personal Data or Breach of Security); (d) assist the PFRSNJ in investigating, remedying and taking any other action the PFRSNJ 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 PFRSNJ 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 PFRSNJ 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: The Contractor shall ensure that PFRSNJ Data requested represents the minimum necessary information for the services as described in this RFQ and, unless otherwise agreed to in writing by the PFRSNJ, that only necessary individuals or entities who are familiar with and bound by the Contract will have access to the PFRSNJ 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 PFRSNJ Data to the PFRSNJ 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 PFRSNJ Data according to the standards enumerated in accordance with the State of New Jersey'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 PFRSNJ, whichever should come first.

J. In the event of loss of any PFRSNJ 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 Contract Manager. The Contractor shall ensure that all PFRSNJ 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 PFRSNJ Data.

6.8 Asset Management

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

A. Information technology asset identification and inventory;

B. Assigning custodianship of assets; and

C. Restricting the use of non-authorized devices.

6.9 Security Categorization

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

A. Implementing a data protection policy;

B. Classifying data and information systems in accordance with their sensitivity and criticality;

C. Masking sensitive data that is displayed or printed; and

D. Implementing handling and labeling procedures.

6.10 Media Protection

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

A. Media storage/access/transportation;

B. Maintenance of sensitive data inventories;

C. Application of cryptographic protections;

D. Restricting the use of portable storage devices;

E. Establishing records retention requirements in accordance with business objectives and statutory and regulatory obligations; and

F. Media disposal/sanitization.

6.11 Cryptographic Protections

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

A. Using industry standard encryption algorithms;

B. Establishing requirements for encryption of data in transit;

C. Establishing requirements for encryption of data at rest; and

D. Implementing cryptographic key management processes and controls.

6.12 Access Management

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

A. Ensure the principle of least privilege is applied for specific duties and information systems (including specific functions, ports, protocols, and services), so processes operate at privilege levels no higher than necessary to accomplish required organizational missions and/or functions;

B. Implement account management processes for registration, updates, changes and de-provisioning of system access;

C. Apply the principles of least privilege when provisioning access to organizational assets;

D. Provision access according to an individual's role and business requirements for such access;

E. Implement the concept of segregation of duties by disseminating tasks and associated privileges for specific sensitive duties among multiple people;

F. Conduct periodic reviews of access authorizations and controls.

6.13 Identity and Authentication

The Contractor shall establish procedures and implement identification, authorization, and authentication controls to ensure only authorized individuals, systems, and processes can access the PFRSNJ's information and the Contractor's information and information systems. Identity and

authentication provides a level of assurance that individuals who log into a system are who they say they are. Identity and authentication controls shall include, at a minimum:

A. Establishing and managing unique identifiers (e.g. User-IDs) and secure authenticators (e.g. passwords, biometrics, personal identification numbers, etc.) to support nonrepudiation of activities by users or processes; and

B. Implementing multi-factor authentication (MFA) requirements for access to sensitive and critical systems, and for remote access to the Contractor's systems.

6.14 Remote Access

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

A. Establishing centralized management of the Contractor's remote access infrastructure;

B. Implementing technical security controls (e.g. encryption, multi-factor authentication, IP whitelisting, geo-fencing); and

C. Training users in regard to information security risks and best practices related remote access use.

6.15 Security Engineering and Architecture

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

A. Implementing configuration standards that are consistent with industry-accepted system hardening standards and address known security vulnerabilities for all system components;

B. Establishing a defense in-depth security posture that includes layered technical, administrative, and physical controls;

C. Incorporating security requirements into the systems throughout their life cycles;

D. Delineating physical and logical security boundaries;

E. Tailoring security controls to meet organizational and operational needs;

F. Performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk;

G. Implementing controls and procedures to ensure critical systems fail-secure and fail-safe in known states; and

H. Ensuring information system clock synchronization.

6.16 Configuration Management

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

A. Hardening systems through baseline configurations; and

B. Configuring systems in accordance with the principle of least privilege to ensure processes operate at privilege levels no higher than necessary to accomplish required functions.

6.17 Endpoint Security

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

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

6.18 ICS/SCADA/OT Security

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

6.19 Internet of Things Security

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

A. Developing policies and standards specific to IoT assets;

B. Ensuring the secure configuration of IoT assets;

C. Conducting risk assessments prior to implementation and throughout the lifecycles of IoT assets;

D. Segmenting IoT networks from the rest of the Contractor's networks; and

E. Ensuring least privilege and strong authentication controls are implemented.

6.20 Mobile Device Security

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

A. Establishing requirements for authorization to use mobile devices for organizational business purposes;

B. Establishing Bring Your Own Device ("BYOD") processes and restrictions;

C. Establishing physical and logical access controls;

D. Implementing network access restrictions for mobile devices;

E. Implementing mobile device management solutions to provide centralized management of mobile devices and to ensure technical security controls (e.g. encryption, authentication, remote-wipe, etc.) are implemented and updated as necessary;

F. Establishing approved application stores from which applications can be acquired;

G. Establishing lists approved applications that can be used; and

H. Training of mobile device users regarding security and safety.

6.21 Network Security

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

A. Include protection mechanisms for network communications and infrastructure (e.g. layered defenses, denial of service protection, encryption for data in transit, etc.);

B. Include protection mechanisms for network boundaries (e.g. limit network access points, implement firewalls, use Internet proxies, restrict split tunneling, etc.);

C. Control the flow of information (e.g. deny traffic by default/allow by exception, implement Access Control Lists, etc.); and

D. Control access to the Contractor's information systems (e.g. network segmentation, network intrusion detection and prevention systems, wireless restrictions, etc.).

6.22 Cloud Security

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

A. Security is accounted for in the acquisition and development of cloud services;

B. The design, configuration, and implementation of cloud-based applications, infrastructure and system-system interfaces are conducted in accordance with mutually agreed-upon service, security, and capacity-level expectations;

C. Security roles and responsibilities for the Contractor and the cloud provider are delineated and documented; and

D. Controls necessary to protect sensitive data in public cloud environments are implemented.

6.23 Change Management

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

A. Notifying all stakeholder of changes;

B. Conducting a security impact analysis and testing for changes prior to rollout; and

C. Verifying security functionality after the changes have been made.

6.24 Maintenance

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

A. Conducting scheduled and timely maintenance;

B. Ensuring individuals conducting maintenance operations are qualified and trustworthy; and

C. Vetting, escorting and monitoring third-parties conducting maintenance operations on information technology assets.

6.25 Threat Management

The Contractor shall establish effective communication protocols and processes to collect and disseminate actionable threat intelligence, thereby providing component units and individuals with

the information necessary to effectively manage risk associated with new and emerging threats to the organization's information technology assets and operations. Threat management includes, at a minimum:

A. Developing, implementing, and governing processes and documentation to facilitate the implementation of a threat awareness policy, as well as associated standards, controls and procedures; and

B. Subscribing to and receiving relevant threat intelligence information from the US CERT, the organization's vendors, and other sources as appropriate.

6.26 Vulnerability and Patch Management

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

A. Prioritizing vulnerability scanning and remediation activities based on the criticality and security categorization of systems and information, and the risks associated with a loss of confidentiality, integrity, availability, and/or privacy;

B. Maintaining software and operating systems at the latest vendor-supported patch levels;

C. Conducting penetration testing and red team exercises; and

D. Employing qualified third-parties to periodically conduct Independent vulnerability scanning, penetration testing, and red-team exercises.

6.27 Continuous Monitoring

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

A. Centralizing the collection and monitoring of event logs;

B. Ensuring the content of audit records includes all relevant security event information;

C. Protecting of audit records from tampering; and

D. Detecting, investigating, and responding to incidents discovered through monitoring.

6.28 System Development and Acquisition

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

A. Secure coding;

B. Separation of development, testing, and operational environments;

C. Information input restrictions;

D. Input data validation;

E. Error handling;

F. Security testing throughout development;

G. Restrictions for access to program source code; and

H. Security training of software developers and system implementers.

6.29 Project and Resource Management

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

A. Defining and implementing security requirements;

B. Allocating resources required to protect systems and information; and

C. Ensuring security requirements are accounted for throughout the SDLC.

6.30 Capacity and Performance Management

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

A. Ensuring the availability, quality, and adequate capacity of 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.

6.31 Third Party Management

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

A. Tailored acquisition strategies, contracting tools, and procurement methods for the purchase of systems, system components, or system service from suppliers;

B. Due diligence security reviews of suppliers and third parties with access to the Contractor's systems and sensitive information;

C. Third party interconnection security; and

D. Independent testing and security assessments of supplier technologies and supplier organizations.

6.32 Physical and Environmental Security

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

A. Physical access controls (e.g. locks, security gates and guards, etc.);

B. Visitor controls;

C. Security monitoring and auditing of physical access;

D. Emergency shutoff;

E. Emergency power;

F. Emergency lighting;

G. Fire protection;

H. Temperature and humidity controls;

I. Water damage protection; and

J. Delivery and removal of information assets controls.

6.33 Contingency Planning

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

A. Backup and recovery strategies;

B. Continuity of operations;

C. Disaster recovery; and

D. Crisis management.

6.34 Incident Response

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

A. Information security incident reporting awareness;

B. Incident response planning and handling;

C. Establishment of an incident response team;

D. Cybersecurity insurance;

E. Contracts with external incident response services specialists; and

F. Contacts with law enforcement cybersecurity units.

7. Modifications to the State of New Jersey Standard Terms and Conditions

7.1 Executive Director of the Police and Firemen's Retirement System of New Jersey

Any and all references in the Standard Terms & Conditions to the "Director" or the "Director of the Division of Purchase and Property" shall be read as: the "Executive Director of the Police and Firemen's Retirement System of New Jersey."

7.2 Indemnification

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

4.1 INDEMNIFICATION

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

1. The Contractor shall indemnify, defend, and save harmless the State and its officers, agents, servants and employees, from and against any and all third party claims, demands, suits, actions, recoveries, judgments and costs and expenses in connection therewith:

i. For or on account of the loss of life, tangible property (not including lost or damaged data) or injury or damage to the person, body or property (not including lost or damaged data) of any person or persons whatsoever, which shall arise from or result directly or indirectly from the work and/or products supplied under this Contract; and

ii. For or on account of the use of any patent, copyright, trademark, trade secret or other proprietary right of any copyrighted or uncopyrighted composition, secret process, patented or unpatented invention, article or appliance ("Intellectual Property Rights") furnished or used in the performance of the contract; and

iii. For or on account of a Breach of Security resulting from Contractor's breach of its obligation to encrypt Personal Data or otherwise prevent its release or misuse; and

iv. The Contractor's indemnification and liability under Section 4.1(A)(1) is not limited by, but is in addition to the insurance obligations contained in Section 4.2 of the State Standard Terms and Conditions.

2. In the event of a claim or suit involving third-party Intellectual Property Rights, the Contractor, at its option, may: (1) procure for the State the legal right to continue the use of the product; (2) replace or modify the product to provide a non-infringing product that is the functional equivalent; or (3) refund the purchase price less a reasonable allowance for use that is agreed to by both parties. The State will: (1) promptly notify Contractor in writing of the claim or suit; (2) Contractor shall have control of the defense and settlement of any claim that is subject to Section 4.1(A)(1); provided, however, that the State must approve any settlement of the alleged claim, which approval shall not be unreasonably withheld. The State

may observe the proceedings relating to the alleged claim and confer with the Contractor at its expense. Furthermore, neither Contractor nor any attorney engaged by Contractor shall defend the claim in the name of the State of New Jersey, nor purport to act as legal representative of the State of New Jersey, without having provided notice to the PFRSNJ and the Director of the Division of Law in the Department of Law and Public Safety and to the Director of DPP. The State of New Jersey may, at its election and expense, assume its own defense and settlement.

3. Notwithstanding the foregoing, the Contractor has no obligation or liability for any claim or suit concerning third-party Intellectual Property Rights arising from: (1) the State's unauthorized combination, operation, or use of a product supplied under this contract with any product, device, or software not supplied by Contractor; (2) the State's unauthorized alteration or modification of any product supplied under this contract; (3) the Contractor's compliance with the State's designs, specifications, requests, or instructions, provided that if the State provides Contractor with such designs, specifications, requests, or instructions, Contractor shall review same and advise if such designs, specifications, requests or instructions present potential issues of patent or copyright infringement and the State nonetheless directs the Contractor to proceed with one or more designs, specifications, requests or instructions that present potential issues of patent or copyright infringement; or (4) the State's failure to promptly implement a required update, use a new version of the product, or to make a change or modification to the product if requested in writing by Contractor.

4. Contractor will be relieved of its responsibilities under Subsection 4.1(A)(1)(i), (ii), and (iii) for any claims made by an unaffiliated third party that arise solely from the actions or omissions of the State, its officers, employees or agents.

5. This section states the entire obligation of Contractor and the exclusive remedy of the State, in respect of any infringement or alleged infringement of any Intellectual Property Rights. This indemnity obligation and remedy are given to the State solely for its benefit and in lieu of, and Contractor disclaims, all warranties, conditions and other terms of non-infringement or title with respect to any product.

6. The provisions of this indemnification clause shall in no way limit the Contractor's obligations assumed in the Contract, nor shall they be construed to relieve the Contractor from any liability, nor preclude the State from taking any other actions available to it under any other provisions of the contract or otherwise at law or equity.

7. The Contractor agrees that any approval by the State of the work performed and/or reports, plans or specifications provided by the Contractor shall not operate to limit the obligations of the Contractor assumed in the Contract.

8. The State of New Jersey will not indemnify, defend or hold harmless the Contractor. The State will not pay or reimburse for claims absent compliance with Section 4.1(B) below and a determination by the State to pay the claim or a final order of a court of competent jurisdiction.

B. STATE RESPONSIBILITIES - Subject to the New Jersey Tort Claims Act (N.J.S.A. 59:1-1 et seq.), the New Jersey Contractual Liability Act (N.J.S.A. 59:13-1 et seq.) and the appropriation and availability of funds, the State will be responsible for any cost or damage arising out of

actions or inactions of the State, its employees or agents under Section 4.1(A)(1)(i), (ii), and (iii) which results in an unaffiliated third-party claim. This is the Contractor's exclusive remedy for these claims.

7.3 Insurance

7.3.1 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 per each occurrence and in such policy forms as shall be approved by the PFRSNJ. If the Contractor has claims-made coverage and subsequently changes carriers during the term of this Contract, it shall obtain from its new Errors and Omissions, Professional Liability Insurance, and/or Professional Malpractice Insurance carrier an endorsement for retroactive coverage.

7.3.2 Cyber Breach Insurance

Section 4.2 of the SSTC supplemented with the following:

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

Level of Risk	Data Breach and Privacy/Cyber Liability Minimum Insurance Coverage
Low	$2,000,000
Moderate	$5,000,000
High	$10,000,000

7.3.3 Limitation of Liability Options

Section 4.0 of the SSTC is supplemented with the following:

4.3 LIMITATION OF LIABILITY

A. The Contractor's liability for actual, direct damages resulting from the Contractor's performance or non-performance of, or in any manner related to, the Contract for any and all third party claims, shall be limited in the aggregate to 200% of the fees paid by the State during the previous twelve months to Contractor for the products or services giving rise to such damages.

Notwithstanding the preceding sentence, in no event shall the limit of liability be less than $1,000,000. This limitation of liability shall not apply to the following:

i. The Contractor's indemnification obligations as described in Section 4.1; and

ii. The Contractor's breach of its obligations of confidentiality described in this RFQ.

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

C. The Contractor shall not be liable for punitive, special, indirect, incidental, or consequential damages.

8. Quote Evaluation and Award

8.1 Reciprocity for Jurisdictional Bidder Preference

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

A Bidder may submit information related to preference practices enacted for a State or Local entity outside the State of New Jersey. This information may be submitted in writing as part of the Quote response, including 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 PFRSNJ within five (5) business days after the deadline for Quote submission. Written evidence for a specific procurement that is not provided to the PFRSNJ within five (5) business days of the public Quote submission date may not be considered in the evaluation of that procurement, but may be retained and considered in the evaluation of subsequent procurements.

8.2 Clarification of Quote

After the Quote Opening Date, unless requested by the PFRSNJ as noted below, Bidder contact with the PFRSNJ 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.

8.3 Tie Quotes

Tie Quotes will be awarded by the Executive Director of the Police and Firemen's Retirement System of New Jersey in accordance with governing law including but not limited to N.J.A.C. 17:12-2.10.

8.4 The PFRSNJ's Right to Inspect Bidder's Facilities

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

8.5 The PFRSNJ's Right to Check References

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

8.6 Evaluation Criteria

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

8.6.1 Technical Evaluation Criteria

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

A. Personnel: The qualifications and experience of the Bidder's management, supervisory, and key personnel assigned to the Contract, including the candidates recommended for each of the positions/roles required;

B. Experience of firm: The Bidder's documented experience in successfully completing Contract of a similar size and scope in relation to the work required by this RFQ; and

C. Ability of firm to complete the Scope of Work based on its Technical Quote: The Bidder's demonstration in the Quote that the Bidder understands the requirements of the Scope of Work and presents an approach that would permit successful performance of the technical requirements of the Contract.

8.6.2 Price Evaluation

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

8.7 Quote Discrepancies

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

8.8 Best and Final Offer (BAFO)

The PFRSNJ 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 PFRSNJ will not be considered, and the PFRSNJ will evaluate the Bidder's most advantageous previously submitted pricing.

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

BAFOs will be conducted only in those circumstances where it is deemed to be in the PFRSNJ's best interests and to maximize the PFRSNJ'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 PFRSNJ may, after evaluation, make a Contract award based on the content of the initial submission

If the PFRSNJ 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.

8.9 Poor Performance

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

A. Contract cancellations for cause pursuant to State of New Jersey Standard Terms and Conditions Section 5.7(B);

B. information contained in Vendor performance records;

C. information obtained from audits or investigations conducted by a local, state or federal agency of the Bidder's work experience;

D. current licensure, registration, and/or certification status and relevant history thereof; or

E. Bidder's status or rating with established business/financial reporting services, as applicable.

Bidders should note that this list is not exhaustive.

8.10 Recommendation for Award

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

8.11 Contract Award

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

ATTACHMENT A

REQUEST FOR QUOTES
ELECTION PROCESSING FOR THE POLICE AND FIREMENS RETIREMENT SYSTEM OF NEW JERSEY

ATTACHMENT A1

OFFER AND ACCEPTANCE PAGE

STATE OF NEW JERSEY
T E POLICE AND FIREMEN'S RETIREMENT SYSTEM OF NEW JERSEY
50 WEST STATE STREET, P.O. BOX 297 TRENTON, NEW JERSEY 08625-0297

BID SOLICITATION # AND TITLE: _____

TO THE STATE OF NEW JERSEY:

Name of Bidder/Contractor _____
Address _____
City, State, Zip Code _____
Phone Number _____
Fax Number _____
Email Address _____
FEIN _____
Print Name & Title of Authorized Representative _____

Signature Authorized Representative _____

By submitting a Quote the Bidder certifies and confirms that:

1. It has read, understands, and agrees to all terms, conditions, and specifications set forth in the Bid Solicitation and the State of New Jersey Standard Terms and Conditions and agrees to furnish the goods, products, and/or services in compliance with those terms;
2. It has complied, and will continue to comply, with all applicable laws and regulations governing the provision of State goods and services, including the New Jersey Conflicts of Interest Law, N.J.S.A. 52:13D-12 to 28;
3. The price(s) and amount of its Quote have been arrived at independently and without consultation, communication or agreement with any other Contractor/Bidder or any other party;
4. Neither the price(s) nor the amount of its Quote, and neither the approximate price(s) nor approximate amount of this Quote, have been disclosed to any other firm or person who is a Bidder or potential Bidder, and they will not be disclosed before the Quote submission;
5. No attempt has been made or will be made to induce any firm or person to refrain from bidding on this Contract, or to submit a Quote higher than this Quote, or to submit any intentionally high or noncompetitive Quote or other form of complementary Quote;
6. The Quote 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;
7. The Bidder, its affiliates, subsidiaries, officers, directors, and employees are not, to Bidder's knowledge, currently under investigation by any governmental agency for alleged conspiracy or collusion with respect to bidding on any Contract 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 Contract;
8. The Bidder's failure to meet any of the terms and conditions of the Contract shall constitute a breach and may result in suspension or debarment from further State bidding; and
9. A defaulting Contractor may also be liable, at the option of the State, for the difference between the Blanket P.O. price and the price bid by an alternate Vendor {Bidder} of the goods or services in addition to other remedies available.

ACCEPTANCE OF OFFER *(For State Use Only)*

The Offer above is hereby accepted and now constitutes a Contract with the State of New Jersey. The Contractor is now bound to sell the goods, products, or services in accordance with the terms of the Bid Solicitation and the State of New Jersey Standard Terms and Conditions. The Contractor shall not commence any work or provide any good, product, or service under this Contract until the Vendor Contractor complies with all requirements set forth in the Bid Solicitation and receives written notice to proceed.

Contract/Master Blanket Purchase Order Number _____

Award Date _____ Effective Date _____

State of New Jersey Authorized Signature _____

Print Name and Title _____

ATTACHMENT A2

OWNERSHIP DISCLOSURE FORM

STATE OF NEW JERSEY DEPARTMENT OF THE TREASURY
POLICE AND FIREMEN'S RETIREMENT SYSTEM OF NEW JERSEY
50 WEST STATE STREET, P.O. BOX 297 TRENTON, NEW JERSEY 08625-029

VENDOR NAME: _____

PURSUANT TO N.J.S.A. 52:25-24.2, ALL PARTIES ENTERING INTO A CONTRACT WITH THE STATE ARE REQUIRED TO PROVIDE A STATEMENT OF OWNERSHIP.
Please answer all questions and complete the information requested.

		YES	NO
1.	The vendor is a **Non-Profit Entity**; and therefore, no disclosure is necessary.	☐	☐
2.	The vendor is a **Sole Proprietor**; and therefore, no other disclosure is necessary. A Sole Proprietor is a person who owns an unincorporated business by himself or her-self. A limited liability company with a single member is not a Sole Proprietor.	☐	☐
3.	The vendor is a **corporation, partnership, or limited liability company** with individuals, partners, members, stockholders, corporations, partnerships, or limited liability companies owning a 10% or greater interest; and therefore, disclosure is necessary.	☐	☐

If you answered **YES** to Question 3, you must disclose the information requested in the space below:*
(a) the names and addresses of all stockholders in the corporation who own 10% or more of its stock, of any class;
(b) all individual partners in the partnership who own a 10% or greater interest therein; or,
(c) all members in the limited liability company who own a 10% or greater interest therein.

NAME			
ADDRESS			
ADDRESS			
CITY	STATE	ZIP	

NAME			
ADDRESS			
ADDRESS			
CITY	STATE	ZIP	

NAME			
ADDRESS			
ADDRESS			
CITY	STATE	ZIP	

NAME			
ADDRESS			
ADDRESS			
CITY	STATE	ZIP	

		YES	NO
4.	For each of the corporations, partnerships, or limited liability companies identified in response to Question #3 above, are there any individuals, partners, members, stockholders, corporations, partnerships, or limited liability companies owning a 10% or greater interest of those listed business entities?	☐	☐

If you answered **YES** to Question 4, you must disclose the information requested in the space below:*
(a) the names and addresses of all stockholders in the corporation who own 10% or more of its stock, of any class;
(b) all individual partners in the partnership who own a 10% or greater interest therein; or,
(c) all members in the limited liability company who own a 10% or greater interest therein. The disclosure(s) shall be continued until the names and addresses of every non-corporate stockholder, individual partner, and/or member a 10% or greater interest has been identified.

NAME			
ADDRESS			
ADDRESS			
CITY	STATE	ZIP	

NAME			
ADDRESS			
ADDRESS			
CITY	STATE	ZIP	

NAME			
ADDRESS			
ADDRESS			
CITY	STATE	ZIP	

NAME			
ADDRESS			
ADDRESS			
CITY	STATE	ZIP	

5. As an alternative to completing this form, a Vendor 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% 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% 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% or greater beneficial interest.*

_____

_____

_____

** Attach additional sheets if necessary*

ATTACHMENT A3

DISCLOSURE OF INVESTMENT ACTIVITIES IN IRAN FORM

STATE OF NEW JERSEY
T E POLICE AND FIREMEN'S RETIREMENT SYSTEM OF NEW JERSEY
50 WEST STATE STREET, P.O. BOX 297 TRENTON, NEW JERSEY 08625-0297

BID SOLICITATION # AND TITLE: _____

VENDOR NAME: _____

Pursuant to N.J.S.A. 52:32-57, et seq. (P.L. 2012, c.25 and P.L. 2021, c.4) any person or entity that submits a bid or proposal or otherwise proposes to enter into or renew a contract must certify that neither the person nor entity, nor any of its parents, subsidiaries, or affiliates, is identified on the New Jersey Department of the Treasury's Chapter 25 List as a person or entity engaged in investment activities in Iran. The Chapter 25 list is found on the Division's website at https://www.state.nj.us/treasury/purchase/pdf/Chapter25List.pdf. Vendors/Bidders must review this list prior to completing the below certification. If the Director of the Division of Purchase and Property finds a person or entity to be in violation of the law, s/he shall take action as may be appropriate and provided by law, rule or contract, including but not limited to, imposing sanctions, seeking compliance, recovering damages, declaring the party in default and seeking debarment or suspension of the party.

CHECK THE APPROPRIATE BOX

☐ I certify, pursuant to N.J.S.A. 52:32-57, et seq. (P.L. 2012, c.25 and P.L. 2021, c.4), that neither the Vendor/Bidder listed above nor any of its parents, subsidiaries, or affiliates is listed on the New Jersey Department of the Treasury's Chapter 25 List of entities determined to be engaged in prohibited activities in Iran.

OR

☐ I am unable to certify as above because the Vendor/Bidder and/or one or more of its parents, subsidiaries, or affiliates is listed on the New Jersey Department of the Treasury's Chapter 25 List. I will provide a detailed, accurate and precise description of the activities of the Vendor/Bidder, or one of its parents, subsidiaries or affiliates, has engaged in regarding investment activities in Iran by completing the information requested below.

Entity Engaged in Investment Activities _____
Relationship to Vendor/ Bidder _____
Description of Activities _____
_____
_____
Duration of Engagement _____
Anticipated Cessation Date _____

**Attach Additional Sheets If Necessary.*

CERTIFICATION

I, the undersigned, certify that I am authorized to execute this certification on behalf of the Vendor, that the foregoing information and any attachments hereto, to the best of my knowledge are true and complete. I acknowledge that the State of New Jersey is relying on the information contained herein, and that the Vendor is under a continuing obligation from the date of this certification through the completion of any contract(s) with the State to notify the State in writing of any changes to the information contained herein; that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification. If I do so, I may be subject to criminal prosecution under the law, and it will constitute a material breach of my contract(s) with the State, permitting the State to declare any contract(s) resulting from this certification void and unenforceable.

_____ _____
Signature Date

_____
Print Name and Title

ATTACHMENT A4

DISCLOSURE OF INVESTIGATIONS AND OTHER ACTIONS INVOLVING THE VENDOR FORM

STATE OF NEW JERSEY
DEPARTMENT OF THE TREASURY - POLICE AND FIREMEN'S RETIREMENT SYSTEM OF NEW JERSEY
50 WEST STATE STREET, P.O. BOX 297 TRENTON, NEW JERSEY 08625-0297

BID SOLICITATION # AND TITLE: ______________________________

VENDOR NAME: ______________________________

PART 1

PLEASE LIST ALL OFFICERS/DIRECTORS OF THE VENDOR BELOW.

NAME TITLE ADDRESS ADDRESS CITY STATE ZIP	NAME TITLE ADDRESS ADDRESS CITY STATE ZIP
NAME TITLE ADDRESS ADDRESS CITY STATE ZIP	NAME TITLE ADDRESS ADDRESS CITY STATE ZIP

**Attach Additional Sheets If Necessary.*

PART 2

PLEASE REFER TO THE PERSONS LISTED ABOVE AND/OR THE PERSONS AND/OR ENTITIES LISTED ON THE OWNERSHIP DISCLOSURE FORM WHEN ANSWERING THESE QUESTIONS.

. Has any person or entity listed on this form or its attachments ever been arrested, charged, indicted, or convicted in a criminal or disorderly persons matter by the State of New Jersey (or political subdivision thereof), or by any other state or the U.S. Government?

2. Has any person or entity listed on this form or its attachments ever been suspended, debarred or otherwise declared ineligible by any government agency from bidding or contracting to provide services, labor, materials or supplies?

. Are there currently any pending criminal matters or debarment proceedings in which the firm and/or its officers and/or managers are involved?

. Has any person or entity listed on this form or its attachments been denied any license, permit or similar authorization required to engage in the work applied for herein, or has any such license, permit or similar authorization been revoked by any agency of federal, state or local government?

5. Has any person or entity listed on this form or its attachments been involved as an adverse party to a public sector client in any civil litigation or administrative proceeding in the past five (5) years?

IF ANY OF T E ANSWERS TO ESTIONS -5 ARE YES , PLEASE PRO IDE T E RE ESTED INFORMATION IN PART .
IF ALL OF T E ANSWERS TO ESTIONS -5 ARE NO , NO F RT ER ACTION IS NEEDED PLEASE SI N AND DATE T E FORM.

PART 3

DESCRIPTION OF THE INVESTIGATION OR LITIGATION, ETC.

If you answered “YES” to any of questions 1 - 5 above, you must provide a detailed description of any investigation or litigation, including, but not limited to, administrative complaints or other administrative proceedings involving public sector clients during the past five (5) years. The description must include the nature and status of the investigation, and for any litigation, the caption a brief description of the action, the date of inception, current status, and if applicable, the disposition.

PERSON OR ENTITY NAME ______________________________
CONTACT NAME ______________ PHONE NUMBER ______________
CASE CAPTION ______________________________
INCEPTION OF THE INVESTIGATION ______________ CURRENT STATUS ______________
SUMMARY OF INVESTIGATION ______________________________

**Attach Additional Sheets If Necessary.*

CERTIFICATION

I, the undersigned, certify that I am authorized to execute this certification on behalf of the Vendor, that the foregoing information and any attachments hereto, to the best of my knowledge are true and complete. I acknowledge that the State of New Jersey is relying on the information contained herein, and that the Vendor is under a continuing obligation from the date of this certification through the completion of any contract(s) with the State to notify the State in writing of any changes to the information contained herein; that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification. If I do so, I may be subject to criminal prosecution under the law, and it will constitute a material breach of my contract(s) with the State, permitting the State to declare any contract(s) resulting from this certification void and unenforceable.

______________________________ ______________________________
Signature Date

____
Print Name and Title

ATTACHMENT A5

MACBRIDE PRINCIPLES FORM

STATE OF NEW JERSEY DEPARTMENT OF THE TREASURY
POLICE AND FIREMEN'S RETIREMENT SYSTEM OF NEW JERSEY
50 WEST STATE STREET, P.O. BOX 297 TRENTON, NEW JERSEY 08625-0297

BID SOLICITATION # AND TITLE: _____

VENDOR NAME: _____

P N J , Vendor/Bidder is required to provide a certification in compliance with the MacBride Principles and Northern Ireland Act of 1989. Vendor/Bidder must complete the certification below by checking one of the two options listed below and signing where indicated. If the E Director finds contractors to be in violation of the principles that are the subject of this law, he/she shall take such action as may be appropriate and provided by law, rule or contract, including but not limited to, imposing sanctions, seeking compliance, recovering damages, declaring the party in default and seeking debarment or suspension of the party.

I, the undersigned, on behalf the Vendor/Bidder, certify

CHECK THE APPROPRIATE BOX

☐ The Vendor/Bidder has no business operations in Northern Ireland; or

OR

☐ The Vendor/Bidder 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 section 2 of P.L. 1987, c. 177 (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.

CERTIFICATION

I, the undersigned, certify that I am authorized to execute this certification on behalf of the Vendor, that the foregoing information and any attachments hereto, to the best of my knowledge are true and complete. I acknowledge that the State of New Jersey is relying on the information contained herein, and that the Vendor is under a continuing obligation from the date of this certification through the completion of any contract(s) with the State to notify the State in writing of any changes to the information contained herein; that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification. If I do so, I may be subject to criminal prosecution under the law, and it will constitute a material breach of my contract(s) with the State, permitting the State to declare any contract(s) resulting from this certification void and unenforceable.

_____ _____
Signature Date

_____
Print Name and Title

ATTACHMENT A6

SOURCE DISCLOSURE FORM

STATE OF NEW JERSEY DEPARTMENT OF T E TREAS RY
POLICE AND FIREMEN'S RETIREMENT SYSTEM OF NEW JERSEY
50 WEST STATE STREET, P.O. BOX 297 TRENTON, NEW JERSEY 08625-0297

BID SOLICITATION # AND TITLE: _____

VENDOR NAME: _____

The Vendor/Bidder submits this Form in response to a Bid Solicitation issued by the P F R S N J , in accordance with the requirements of N.J.S.A. 52:34-13.2.

PART 1

☐ All services will be performed by the Contractor and Subcontractors in the United States. Skip Part 2.

☐ Services will be performed by the Contractor and/or Subcontractors outside of the United States. **Complete Part 2.**

PART 2

Where services will be performed outside of the United States, please list every country where services will be performed by the Contractor and all Subcontractors. If any of the services cannot be performed within the United States, the Contractor shall state, with specificity, the reasons why the services cannot be performed in the United States. The E Director of the P F R S N J will review this justification and if deemed sufficient, the E Director may seek the B T ' approval.

Name of Contractor / Sub-contractor	Performance Location by Country	Description of Service(s) to be Performed Outside of the United States *	Reason Why the Service(s) Cannot be Performed in the United States *

Attach additional sheets if necessary to describe which service(s), if any, will be performed outside of the U.S. and the reason(s) why the service(s) cannot be performed in the U.S.

Any changes to the information set forth in this Form during the term of any Contract awarded under the referenced Bid Solicitation or extension thereof shall be immediately reported by the Contractor to the E Director of the P F R S N J . If during the term of the Contract, the Contractor shifts the location of services outside the United States, without a prior written determination by the E Director, the Contractor shall be deemed in breach of Contract, and the Contract will be subject to termination for cause pursuant to the Standard Terms and Conditions P F R S N J .

CERTIFICATION

I, the undersigned, certify that I am authorized to execute this certification on behalf of the Vendor, that the foregoing information and any attachments hereto, to the best of my knowledge are true and complete. I acknowledge that the State of New Jersey is relying on the information contained herein, and that the Vendor is under a continuing obligation from the date of this certification through the completion of any contract(s) with the State to notify the State in writing of any changes to the information contained herein; that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification. If I do so, I may be subject to criminal prosecution under the law, and it will constitute a material breach of my contract(s) with the State, permitting the State to declare any contract(s) resulting from this certification void and unenforceable.

_____ _____

Signature Date

_____

Print Name and Title

ATTACHMENT A7

CONFIDENTIALITY AND COMMITMENT TO DEFEND

STATE OF NEW JERSEY
POLICE AND FIREMEN'S RETIREMENT SYSTEM OF NEW JERSEY
50 WEST STATE STREET, P.O. BOX 297 TRENTON, NEW JERSEY 08625-0297

BID SOLICITATION # & TITLE: _____

The Bid Solicitation advises Bidders (hereinafter "Company") that the submitted "Quotes can be released to the public pursuant to N.J.A.C. 17:12-1.2(b) and (c), or under the New Jersey Open Public Records Act (OPRA), N.J.S.A. 47:1A-1.1 et seq., or the common law right to know." In the event that the Division receives a request for documents related to above referenced Bid Solicitation, in accordance with its statutory obligations under the New Jersey Open Public Records Act and/or the common law right to know, it is the Division's intent to fulfill the request for records which may include a copy of the Company's Quote.

If Company objects to the disclosure of any portions of the Quote, the Company must advise the Division and must attach a detailed statement clearly identifying those sections of the Quote that Company claims are exempt from disclosure. In requesting any exemption, Company must identify the specific statutory or other legal justification for each requested exemption and the factual basis that supports said exemption. In addition, if Company requests any exemption to disclosure of the Quote based upon claims of confidential/proprietary information and trade secrets (setting forth the nature of the formula, process, pattern, device or compilation), in accordance with *Ingersoll-Rand Co. v. Ciavatta*, 110 N.J. 609 (1988), Company must also indicate the following with respect to the requested exemption:

(1) the extent to which the information is known outside the owner's business;
(2) the extent to which it is known by employees and others involved with your business;
(3) the extent of the measures taken by your firm to guard the secrecy of the information;
(4) the value of the information to your firm and your competitors;
(5) the amount of effort or money expended by your firm in developing the information; and
(6) the ease or difficulty with which the information could be properly acquired or duplicated by others.

Further, if the Quote includes any copyright notices, within five business days, the Division will be permitted to release a copy of the Quote document(s) unless Company serves the Division with an order from a court of competent jurisdiction precluding such release.

The State reserves the right to make the final determination as to what is and is not subject to public disclosure under OPRA and/or the common law right to know, and will advise the Company accordingly. Please note that the State will not honor any claim of confidential, proprietary, trade secret, and/or copyright material that is not supported by a specific statutory or legal justification provided by the Company. The State will not honor any attempts by the Company to designate the entire Quote as proprietary, confidential and/or to claim copyright protection for its entire Quote.

Accordingly, in order to assist the Division with the fulfillment of potential document requests, please select **one** of the following:

☐ The Company's Quote **does not include** any confidential, proprietary and/or trade secrets; and therefore, the Company does not request any redactions be made prior to the release of the documents.

OR

☐ The Company's Quote **does include** confidential, proprietary and/or trade secrets; and therefore, the Company requests that certain portions of the Quote be redacted prior to the release of the documents.

The requested redactions are set forth in the attached statement which specifically identifies the portions of the Quote by section, page number, paragraph and or line; and identifies the specific statutory or other legal reason for each requested exemption.

In the event of any challenge to the Company's assertion of confidential/proprietary information, the Company shall be solely responsible for defending its designation. Company agrees that it shall defend and cooperate in the defense of an action against the State of New Jersey arising from or related to the non-disclosure, due to the Company's request, of documents submitted to the State of New Jersey, and relating to a Quote submitted by the Company in response to the above referenced Bid Solicitation, which was the subject of a request for government records under the New Jersey Open Public Records Act, N.J.S.A. 47:1A-1 et seq. ("OPRA"), or the common law right to know. The Company further agrees to indemnify and hold harmless the State against any judgments, costs, or attorneys' fees assessed against the State in connection with any action arising from, or related to, the non-disclosure, due to the Company's request, of documents submitted to the State, which are the subject of a request for government records under OPRA.

The Company makes the forgoing agreement with the understanding that the State may immediately disclose any documents withheld without further notice if the Company ceases to cooperate in the defense of an action against the State arising from or related to the above described non-disclosure due to the Company's request, and will disclose such documents withheld if so ordered by a court of competent jurisdiction.

The undersigned certifies that s/he is duly authorized to make this commitment on behalf of the Company.

_____
Company Name

_____ _____
Signature Date

_____
Print Name and Title

DESCRIPTION OF VENDOR REQUESTED QUOTE REDACTIONS*				
Quote Section, Form or Document	**Page Number**	**Paragraph and/or line**	**Description of item to be redacted**	**Statutory or other legal reason for each requested exemption**

** Home address and/or unlisted telephone/cell phone numbers must be listed on this form if they are to be redacted.*

ATTACHMENT A8

SUBCONTRACTOR UTILIZATION FORM

STATE OF NEW JERSEY
POLICE AND FIREMEN'S RETIREMENT SYSTEM OF NEW JERSEY
50 WEST STATE STREET, P.O. BOX 297 TRENTON, NEW JERSEY 08625-0297

BID SOLICITATION # AND TITLE: ____________________

VENDOR NAME: ____________________

List All Businesses To Be Used As Subcontractors. Attach Additional Sheets If Necessary.
If the Bid Solicitation has subcontracting set-aside goals, and the Vendor has not achieved the goals,
Vendor must attach information documenting its good faith effort to achieve the goals.

SUBCONTRACTOR'S NAME: ____________________
ADDRESS: ____________________

PHONE NUMBER: ____________________ FEIN: ____________________
EMAIL: ____________________
ESTIMATED VALUE OF WORK TO BE SUBCONTRACTED: ____________________
DESCRIPTION OF WORK TO BE SUBCONTRACTED: ____________________

IS THE SUBCONTRACTOR IS A SMALL BUSINESS?

IF YES, SMALL BUSINESS CATEGORY:

IS THE SUBCONTRACTOR IS A DISABLED VETERAN-OWNED BUSINESS?

SUBCONTRACTOR'S NAME: ____________________
ADDRESS: ____________________

PHONE NUMBER: ____________________ FEIN: ____________________
EMAIL: ____________________
ESTIMATED VALUE OF WORK TO BE SUBCONTRACTED: ____________________
DESCRIPTION OF WORK TO BE SUBCONTRACTED: ____________________

IS THE SUBCONTRACTOR IS A SMALL BUSINESS?

IF YES, SMALL BUSINESS CATEGORY:

IS THE SUBCONTRACTOR IS A DISABLED VETERAN-OWNED BUSINESS?

SUBCONTRACTOR'S NAME: ____________________
ADDRESS: ____________________

PHONE NUMBER: ____________________ FEIN: ____________________
EMAIL: ____________________
ESTIMATED VALUE OF WORK TO BE SUBCONTRACTED: ____________________
DESCRIPTION OF WORK TO BE SUBCONTRACTED: ____________________

IS THE SUBCONTRACTOR IS A SMALL BUSINESS?

IF YES, SMALL BUSINESS CATEGORY:

IS THE SUBCONTRACTOR IS A DISABLED VETERAN-OWNED BUSINESS?

ATTACHMENT A9

INFORMATION AND INSTRUCTIONS
For Completing the "Two-Year Chapter 51/Executive Order 333 Vendor Certification and Disclosure of Political Contributions for Non-Fair and Open Contracts" Form

Background Information

New Jersey law insulates the negotiation and award of State contracts from political contributions that posed a risk of improper influence, purchase of access or the appearance thereof. P.L.2005, c.51, as amended by the Elections Transparency Act, P.L.2023, c.30, codified at N.J.S.A. 19:44A-20.13 to 20.25 ("Chapter 51") and Executive Order No. 333 (2023).

For Contracts Awarded Pursuant to a Fair and Open Process

Pursuant to P.L.2005, c.51, as amended by the Elections Transparency Act, P.L.2023, c.30, codified at N.J.S.A. 19:44A-20.13 to 20.25 ("Chapter 51"), and Executive Order No. 333 (2023), contracts awarded pursuant to a fair and open process do **not** require a certification or disclosure of any solicitation or contribution of money, or pledge of contribution, including in-kind contributions.

For Contracts Awarded Pursuant to a Non-Fair and Open Process

Pursuant to P.L.2005, c.51, as amended by the Elections Transparency Act, P.L.2023, c.30, codified at N.J.S.A. 19:44A-20.13 to 20.25 ("Chapter 51"), and Executive Order No. 333 (2023), the State shall not enter into a Contract to procure services or any material, supplies or equipment, or to acquire, sell, or lease any land or building from any Business Entity, where the value of the transaction exceeds $17,500, if that Business Entity has solicited or made any contribution of money, or pledge of contribution, including in-kind contributions, to a Continuing Political Committee or to a candidate committee and/or election fund of any candidate for or holder of the public office of Governor during certain specified time periods.

Definitions:

A "fair and open process" means, at a minimum, that the contract shall be: publicly advertised in newspapers or on the Internet website maintained by the public entity in sufficient time to give notice in advance of the contract; awarded under a process that provides for public solicitation of proposals or qualifications and awarded and disclosed under criteria established in writing by the public entity prior to the solicitation of proposals or qualifications; and publicly opened and announced when awarded. A contract awarded under a process that includes public bidding or competitive contracting pursuant to State contracts law shall constitute a fair and open process. N.J.S.A. 19:44A-20.23 (P.L.2005, c.51, rev. P.L.2023, c.30).

A "Continuing Political Committee" means any political organization (a) organized under section 527 of the Internal Revenue Code; and (b) consisting of any group of two or more persons acting jointly, or any corporation, partnership, or any other incorporated or unincorporated association, including a political club, political action committee, civic association or other organization, which in any calendar year contributes or expects to contribute at least $5,500 to the aid or promotion of the candidacy of an individual, or of the candidacies of individuals, for elective public office, or the passage or defeat of a public question or public questions, and which may be expected to make contributions toward such aid or promotion or passage or defeat during a subsequent election, provided that the group, corporation, partnership, association or other organization has been determined to be a continuing political committee by the New Jersey Election Law Enforcement Commission under N.J.S.A.19:44A-8(b)(8). A Continuing Political Committee does not include a "political party committee," a "legislative leadership committee," or an "independent expenditure committee," as defined in N.J.S.A. 19:44A-3.

Two-Year Certification Process

Upon approval by the State Chapter 51 Review Unit, the Certification and Disclosure of Political Contributions form **for Non-Fair and Open Contracts** is valid for a two (2) year period. Thus, if a Business Entity and/or vendor receives approval on January 1, 2022, the certification expiration date would be December 31, 2023. Any change in the Business Entity's ownership status and/or political contributions during the two-year period will require the submission of new Chapter 51 forms to the contracting State Agency. **Please note that it is the Business Entity's responsibility to file new forms with the State should these changes occur.**

State Agency Instructions

Prior to the awarding of a contract, the State Agency should first use NJSTART (https://www.njstart.gov/bso/) to check the status of a Business Entity's Chapter 51 certification before contacting the Review Unit's mailbox at CD134@treas.nj.gov. If the State Agency does not find any Chapter 51 Certification information in NJSTART and/or the Business Entity is not registered in NJSTART, then the State Agency should send an e-mail to CD134@treas.nj.gov to verify the certification status of the Business Entity. If the response is that the Business Entity is NOT within an approved two-year period, then forms must be obtained from the Business Entity and forwarded for review. If the response is that the Business Entity is within an approved two-year period, then the response so stating should be placed with the bid/contract documentation for the subject project.

Instructions for Completing the Form

"For State Use Only" box

This box/section should **only** be filled out by the contracting State agency.

The contracting State agency must check the box indicating whether this is a fair and open contract. Please note that if the answer is **YES,** the **Chapter 51 form is not required** and should not be submitted as per the Elections Transparency Act, P.L.2023, c.30, codified at N.J.S.A. 19:44A-20.13 to 20.25 ("Chapter 51") and Executive Order No. 333 (2023).

NOTE: Parts 1, 2 and 3 of the form should be filled out the Business Entity.

Part 1: BUSINESS ENTITY INFORMATION

Business Name – Enter the full legal name of the Business Entity, including trade name if applicable.

Address, City, State, Zip and Phone Number – Enter the Business Entity's street address, city, state, zip code and telephone number.

Vendor Email – Enter the Business Entity's primary email address.

Vendor FEIN – Please enter the Business Entity's Federal Employment Identification Number.

Business Type – Check the appropriate box that represents the Business Entity's type of business formation.

Listing of officers, shareholders, partners or members – Based on the box checked for the business type, provide the corresponding information. (A complete list must be provided.)

Part 2: DISCLOSURE OF CONTRIBUTIONS

Read the two (2) types of political contributions that require disclosure and, if applicable, provide the recipient's information.

Name of Recipient – Enter the full legal name of the recipient.

Address of Recipient – Enter the recipient's street address.

Date of Contribution – Indicate the date the contribution was given.

Amount of Contribution – Enter the dollar amount of the contribution.

Type of Contribution – Select the type of contribution from the examples given.

Contributor's Name – Enter the full name of the contributor.

Relationship of the Contributor to the Vendor – Indicate the relationship of the contributor to the Business Entity. (e.g., officer or shareholder of the company, partner, member, parent company of the vendor, subsidiary of the vendor, etc.)

NOTE: If form is being completed electronically, click "Add a Contribution" to enter additional contributions. Otherwise, please attach additional pages as necessary.

Check the box under the recipient information within Part 2 if no reportable contributions have been solicited or made by the Business Entity. **This box must be checked if there are no contributions to report.**

Part 3: CERTIFICATION

Check Box A if the representative completing the Certification and Disclosure form is doing so on behalf of the Business Entity and all individuals and/or entities whose contributions are attributable to the Business Entity. No additional Certification and Disclosure forms are required if BOX A is checked.

Check Box B if the representative completing the Certification and Disclosure form is doing so on behalf of the Business Entity and all individuals and/or entities whose contributions are attributable to the Business Entity with the exception of those individuals and/or entities that submit their own separate form. For example, the representative is not signing on behalf of the vice president of a corporation, but all others. The vice president completes a separate Certification and Disclosure form. **Additional Certification and Disclosure forms are required from those individuals and/or entities that the representative is not signing on behalf of and are included with the business entity's submittal.**

Check Box C if the representative completing the Certification and Disclosure form is doing so on behalf of the Business Entity only. Additional Certification and Disclosure forms are required from all individuals and/or entities whose contributions are attributable to the Business Entity and must be included with the Business Entity submittal.

Check Box D when a sole proprietor is completing the Certification and Disclosure form or when an individual or entity whose contributions are attributable to the Business Entity is completing a separate Certification and Disclosure form.

Read the five statements of certification prior to signing.

The representative authorized to complete the Certification and Disclosure form must sign and print her/his name, title or position and enter the date.

State Agency Procedure for Submitting Form(s)

The State Agency should submit the completed and signed Two-Year Vendor Certification and Disclosure forms either electronically to: cd134@treas.nj.gov or regular mail at: Chapter 51 Review Unit, P.O. Box 230, 33 West State Street, Trenton, NJ 08625-0230. Original forms should remain with the State Agency and copies should be sent to the Chapter 51 Review Unit.

Business Entity Procedure for Submitting Form(s)

- The Business Entity should return this form to the contracting State Agency.
- The Business Entity should also submit the Certification and Disclosure form directly to the Chapter 51 review Unit only when:
- The Business Entity is approaching its two-year certification expiration date and is seeking certification renewal;
- The Business Entity had a change in its ownership structure; OR
- The Business Entity made any contributions during the period in which its last two-year certification was in effect, or during the term of a contract with a State Agency.

Questions & Information

Questions regarding Public Law 2005, Chapter 51 (N.J.S.A. 19:44A-20.13) as amended by the Elections Transparency Act, P.L.2023, c.30, codified at N.J.S.A. 19:44A-20.13 to 20.25 ("Chapter 51") and Executive Order No. 333 (2023) or may be submitted electronically through the Division of Purchase and Property website at: https://www.state.nj.us/treas/purchase/eo333questions.shtml.

Reference materials and forms are posted on the Political Contributions Compliance website at: https://www.state.nj.us/treasury/purchase/execorder333.shtml.

State of New Jersey
Department of the Treasury

Two-Year Chapter 51 /Executive Order 333 Vendor Certification and
Disclosure of Political Contributions for Non-Fair and Open Contracts

FOR STATE USE ONLY

Solicitation, RFP, or Contract No._____ Award Amount_____

Is the contract being awarded pursuant to a "fair and open process" pursuant to P.L.2023, c.30? Yes ☐ No ☐

Description of Services _____

State Agency Name _____Contact Person _____

Phone Number _____Contact Email _____

☐ Check if the Contract / Agreement is Being Funded Using FHWA Funds

Please check if requesting recertification ☐

Part 1: Business Entity Information

Full Legal Business Name _____
(Including trade name if applicable)

Address _____

City _____ State _____Zip _____ Phone _____

Vendor Email_____ Vendor FEIN (SS# if sole proprietor/natural person)_____

Check off the business type and list below the required information for the type of business selected.
MUST BE COMPLETED IN FULL

- ☐ Corporation: LIST ALL OFFICERS and any 10% and greater shareholder (If the corporation only has one officer, please write "sole officer" after the officer's name.)
- ☐ Professional Corporation: LIST ALL OFFICERS and ALL SHAREHOLDERS
- ☐ Partnership: LIST ALL PARTNERS with any equity interest
- ☐ Limited Liability Company: LIST ALL MEMBERS with any equity interest
- ☐ Sole Proprietor

Note: "Officers" means President, Vice President with senior management responsibility, Secretary, Treasurer, Chief Executive Officer or Chief Financial Officer of a corporation, or any person routinely performing such functions for a corporation.

Also Note: "N/A will not be accepted as a valid response. Where applicable, indicate "None."

All Officers of a Corporation or PC	**10% and greater shareholders of a corporation or all shareholders of a PC**

All Equity partners of a Partnership	**All Equity members of a LLC**

If you need additional space for listing of Officers, Shareholders, Partners or Members, please attach separate page.

Part 2: Disclosure of Contributions by the Business Entity or any person or entity whose contributions are attributable to the Business Entity.

1. Report below all contributions solicited or made during the 4 years immediately preceding the commencement of negotiations or submission of a proposal to any:

Political organization organized under Section 527 of the Internal Revenue Code and which also meets the definition of a continuing political committee as defined in N.J.S.A. 19:44A-3(n).

2. Report below all contributions solicited or made during the 5 ½ years immediately preceding the commencement of negotiations or submission of a proposal to any:

Candidate Committee for or Election Fund of any Gubernatorial candidate.

Full Legal Name of Recipient _____

Address of Recipient _____

Date of Contribution _____ Amount of Contribution _____

Type of Contribution (i.e. currency, check, loan, in-kind) _____

Contributor Name _____

Relationship of Contributor to the Vendor _____

If this form is not being completed electronically, please attach additional contributions on separate page.

Remove Contribution

Click the "Add a Contribution" tab to enter additional contributions.

Full Legal Name of Recipient _____

Address of Recipient _____

Date of Contribution _____ Amount of Contribution _____

Type of Contribution (i.e. currency, check, loan, in-kind) _____

Contributor Name _____

Relationship of Contributor to the Vendor _____

If this form is not being completed electronically, please attach additional contributions on separate page.

Remove Contribution

Click the "Add a Contribution" tab to enter additional contributions.

Add a Contribution

☐ **Check this box only if no political contributions have been solicited or made by the business entity or any person or entity whose contributions are attributable to the business entity.**

Part 3: Certification (Check one box only)

(A) ☐ I am certifying on behalf of the business entity and all individuals and/or entities whose contributions are attributable to the business entity as listed on Page 1 under **Part 1: Vendor Information**.

(B) ☐ I am certifying on behalf of the business entity and all individuals and/or entities whose contributions are attributable to the business entity as listed on Page 1 under **Part 1: Vendor Information**, except for the individuals and/or entities who are submitting separate Certification and Disclosure forms which are included with this submittal.

(C) ☐ I am certifying on behalf of the business entity only; any remaining persons or entities whose contributions are attributable to the business entity (as listed on Page 1) have completed separate Certification and Disclosure forms which are included with this submittal.

(D) ☐ I am certifying as an individual or entity whose contributions are attributable to the business entity.

I hereby certify as follows:

1. **I have read the Information and Instructions accompanying this form prior to completing the certification on behalf of the business entity.**

2. **All reportable contributions made by or attributable to the business entity have been listed above.**

3. The business entity has not knowingly solicited or made any contribution of money, pledge of contribution, including in-kind contributions, that would bar the award of a contract to the business entity unless otherwise disclosed above:

a) Within the 18 months immediately preceding the commencement of negotiations or submission of a proposal for the contract or agreement to a candidate committee or election fund of any candidate for the public office of Governor or election fund of holder of public office of Governor.

b) During the term of office of the current Governor to a candidate committee or election fund of a holder of the public office of Governor.

c) Within the 18 months immediately preceding the last day of the sitting Governor's first term of office to a candidate committee or election fund of the incumbent Governor.

4. During the term During the term of the contract/agreement the business entity has a continuing responsibility to report, by submitting a new Certification and Disclosure form, any contribution it solicits or makes to any candidate committee or election fund of any candidate or holder of the public office of Governor.

The business entity further acknowledges that contributions solicited or made during the term of the contract/agreement may be determined to be a material breach of the contract/agreement.

5. During the two-year certification period the business entity will report any changes in its ownership structure (including the appointment of an officer within a corporation) by submitting a new Certification and Disclosure form indicating the new owner(s) and reporting said owner(s) contributions.

I certify that the foregoing statements in Parts 1, 2 and 3 are true. I am aware that if any of the statements are willfully false, I may be subject to punishment.

Signed Name _____ Print Name _____

Title/Position _____ Date _____

Procedure for Submitting Form(s)

The contracting State Agency should submit this form to the Chapter 51 Review Unit when it has been required as part of a contracting process. The contracting State Agency should submit a copy of the completed and signed form(s), to the Chapter 51 Unit and retain the original for their records.

The Business Entity should return this form to the contracting State Agency. The Business Entity can submit this form directly to the Chapter 51 Review Unit only when it:

- Is approaching its two-year certification expiration date and wishes to renew certification;
- Had a change in ownership structure; OR
- Made any contributions during the period in which its last two-year certification was in effect, or during the term of a contract with a State Agency.

Forms should be submitted either electronically to:cd134@treas.nj.gov **, or regular mail at: Chapter 51 Review Unit, P.O. Box 230, 33 West State Street, Trenton, NJ 08625.**

ATTACHMENT A10

STATE OF NEW JERSEY DEPARTMENT OF THE TREASURY
POLICE AND FIREMEN'S RETIREMENT SYSTEM OF NEW JERSEY
50 WEST STATE STREET, P.O. BOX 297 TRENTON, NEW JERSEY 08625-0297

VENDOR/BIDDER CERTIFICATION AND POLITICAL CONTRIBUTION DISCLOSURE FORM
PUBLIC LAW 2005, CHAPTER 271

CONTRACT #: _____ **VENDOR/BIDDER:** _____

At least ten (10) days prior to entering into the above-referenced Contract, the Vendor/Bidder must complete this Certification and Political Contribution Disclosure Form in accordance with the directions below and submit it to the State contact for the referenced Contract.

NOTE that the disclosure requirements under Public Law 2005, Chapter 271 are separate and different from the disclosure requirements under Public Law 2005, Chapter 51 (formerly Executive Order 134). Although no Vendor/Bidder will be precluded from entering into a contract by any information submitted on this form, a Vendor's/Bidder's failure to fully, accurately and truthfully complete this form and submit it to the appropriate State agency may result in the imposition of fines by the New Jersey Election Law Enforcement Commission.

DISCLOSURE

The following is the required Vendor/Bidder Disclosure of all Reportable Contributions made in the twelve (12) months prior to and including the date of signing of this Certification and Disclosure to: (i) any State, county, or municipal committee of a political party, legislative leadership committee, candidate committee of a candidate for, or holder of, a State elective office, or (ii) any entity that is also defined as a "continuing political committee" under N.J.S.A. 19:44A-3(n) and N.J.A.C. 19:25-1.

The Vendor/Bidder is required to disclose Reportable Contributions by: the Vendor/Bidder itself; all persons or other business entities owning or controlling more than 10% of the profits of the Vendor/Bidder or more than 10% of the stock of the Vendor/Bidder, if the Vendor/Bidder is a corporation for profit; a spouse or child living with a natural person that is a Vendor/Bidder; all of the principals, partners, officers or directors of the Vendor/Contractor and all of their spouses; any subsidiaries directly or indirectly controlled by the Vendor/Bidder; and any political organization organized under section 527 of the Internal Revenue Code that is directly or indirectly controlled by the Vendor/Bidder, other than a candidate committee, election fund, or political party committee.

"Reportable Contributions" are those contributions that are required to be reported by the recipient under the "New Jersey Campaign Contributions and Expenditures Reporting Act," P.L. 1973, c.83 (C.19:44A-1 et seq.), and implementing regulations set forth at N.J.A.C. 19:25-10.1 et seq. As of January 1, 2005, contributions in excess of $300 during a reporting period are deemed "reportable."

Name and Address of Committee to which a Reportable Contribution was made	**Date of Reportable Contribution**	**Amount of Reportable Contribution**	**Contributor's Name**
Indicate "NONE" if no Reportable Contribution was made.			
		$	
		$	
		$	
		$	
Attach additional sheets if necessary			

CERTIFICATION

I, the undersigned, certify that I am authorized to execute this certification on behalf of the Vendor/Bidder, that the foregoing information and any attachments hereto, to the best of my knowledge are true and complete. I acknowledge that the State of New Jersey is relying on the information contained herein, and that the Vendor/Bidder is under a continuing obligation from the date of this certification through the completion of any contract(s) with the State to notify the State in writing of any changes to the information contained herein; that I am aware that it is a criminal offense to make a false statement or misrepresentation in this certification. If I do so, I will be subject to criminal prosecution under the law, and it will constitute a material breach of **my** agreement(s) with the State, permitting the State to declare any contract(s) resulting from this certification void and unenforceable.

_____ _____
Signature **Date**

_____
Print Name and Title

ATTACHMENT A11

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

Bid Solicitation #: _____

For: _____

_____

Published by:
New Jersey Cybersecurity and Communications Integration Cell

TABLE OF CONTENTS

INTRODUCTION

The State of New Jersey's Third-Party Information Security Questionnaire is intended to ensure the security and privacy of State information systems and information, regardless of the location or the party responsible for providing the systems, applications, or services. The Questionnaire is aligned with the controls and security objectives as documented in the Statewide Information Security Manual (SISM) has which been derived from applicable State and federal laws; industry best practices including the National Institute of Standards and Technology (NIST) Cybersecurity Framework for Improving Critical Infrastructure; the Center for Internet Security (CIS) Top 20 Critical Security Controls; the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM); lessons learned; and other New Jersey State Government business and technology related considerations.

INSTRUCTIONS

All vendors, business partners, and other third-parties, collectively referred to as organizations in this document, are required to implement security and privacy controls that are commensurate with the criticality and sensitivity of the State of New Jersey information systems and information they develop, implement, provide, manage, host, or access. The Third-Party Information Security Questionnaire informs the State as to the degree to which the organization conforms to the State's information security requirements.

Organizations that:

a) Develop, implement, provide, manage, or host State of New Jersey major systems and applications;
b) Develop, implement, provide, manage, or host State of New Jersey general support systems; and/or
c) Have authorized access to State systems production environments, internal networks, and/or sensitive information

are required to complete and submit the Third-Party Information Security Questionnaire. By submitting a Third-Party Information Security Questionnaire to the NJCCIC, the submitting individual attests to its truth and accuracy to the best of their knowledge at the time the submission is made.

In some cases, the State may require additional clarifying information, documentation, and copies of certifications and attestations beyond what was initially provided by the submitting organization. A submission shall not be considered complete until the NJCCIC receives all necessary documentation and completes a Third-Party Information Security Risk Assessment Report.

Based on the overall risk rating as determined by the NJCCIC, the sponsoring Agency will determine if the risk rating is acceptable to proceed for the given engagement. Based on the criticality and/or sensitivity of the information system and information in scope, as well as the legal, regulatory, and/or contractual requirements, the State may require the submitting organization to implement additional risk mitigation controls prior to the award of any contract or agreement.

CONFIDENTIALITY OF THIRD-PARTY INFORMATION SECURITY QUESTIONNAIRE SUBMISSIONS

An uncompleted Third-Party Information Security Questionnaire is considered a public document. It may be disseminated via authorized channels and requires no confidentiality protections. A completed Third-Party Information Security Questionnaire along with all supporting documentation would inherently include administrative or technical information regarding computer hardware, software, and networks which, if disclosed would jeopardize computer security of the submitting organization and/or the State of New Jersey. As such, to the extent permitted by law, all non-public information submitted as part of a completed Third-Party Information Security Questionnaire, including but not limited to supporting documents, records, notes, written comments, reports, or analysis generated in or in the execution of a vendor's submission shall be treated and deemed as confidential and exempt from public disclosure under the State of New Jersey Open Public Records Act (N.J.S.A. 47:1A-1 et seq.) and the Domestic Security Preparedness Act P.L. 2001, c.246.

ABOUT THE NEW JERSEY CYBERSECURITY AND COMMUNICATIONS INTEGRATION CELL (NJCCIC)

The New Jersey Cybersecurity and Communications Integration Cell is a component organization within the New Jersey Office of Homeland Security and Preparedness (OHSP). The NJCCIC is comprised of OHSP, Office of Information Technology, and New Jersey State Police personnel working in concert to make New Jersey more resilient to cyber threats. As part of its portfolio of duties, the NJCCIC is responsible for conducting information security risk assessments of third parties with access to State of New Jersey information assets.

For more information about the NJCCIC, please visit www.cyber.nj.gov or contact us at njccic@cyber.nj.gov or 1.833.4-NJCCIC.

SECTION I – NJ STATE GOVERNMENT SPONSORING DEPARTMENT/AGENCY INFORMATION – FOR THE STATE OF NEW JERSEY

NJ STATE GOVERNMENT DEPARTMENT/AGENCY SPONSOR INFORMATION	
Sponsoring Department/Agency:	
First Name:	**Email Address:**
Last Name:	**Phone #:**
Title:	

NJ STATE GOVERNMENT DEPARTMENT/AGENCY INFORMATION SECURITY OFFICER	
First Name:	**Email Address:**
Last Name:	**Phone #:**
Title:	

NJ STATE GOVERNMENT DEPARTMENT/AGENCY PRIVACY OFFICER	
First Name:	**Email Address:**
Last Name:	**Phone #:**
Title:	

SECTION II – DATA ACCESS AND SECURITY CATEGORIZATION – FOR THE STATE OF NEW JERSEY

DATA ACCESS AND SECURITY CATEGORIZATION

Please select the data types that will be generated, accessed, processed, stored, and/or transmitted as part of your engagement with the State of New Jersey. For information on data types and security categorization please refer to Appendix A – Glossary.

Non-Sensitive Data		Sensitive Data	
Public Data:	☐	Personally Identifiable Information:	☐
		Criminal Justice Information:	☐
		Federal Tax Information:	☐
		Electronic Protected Health Information:	☐
		Social Security Administration Provided Information:	☐
		Cardholder and/or Sensitive Authentication Data:	☐
		Other Sensitive Information not listed above:	☐

If you selected Other Sensitive Information, please describe the information below:

SECTION III – THIRD-PARTY ORGANIZATION INFORMATION

THIRD-PARTY ORGANIZATION PROFILE	
Organization Name:	**State:**
Mailing Address:	**Zip/Postal Code:**
City:	**Country:** United States
Organization Website URL: https://	

SUBMITTER'S CONTACT INFORMATION	
First Name:	**Email Address:**
Last Name:	**Phone #:**
Title:	

THIRD-PARTY ORGANIZATION INFORMATION SECURITY OFFICER CONTACT INFORMATION	
First Name:	**Email Address:**
Last Name:	**Phone #:**

THIRD-PARTY INFORMATION SECURITY QUESTIONNAIRE
Date Submitted:

SECTION IV – THIRD-PARTY INFORMATION SECURITY PROGRAM

For each of the control areas below, please provide accurate responses as they apply to your information security program and the scope of the anticipated engagement with the State of New Jersey. You are required to provide answers for all controls and questions as it applies to the scope of your engagement with the State of New Jersey. For any of the control areas or supplemental information questions in which you answer "No" or "N/A" (Not Applicable) please provide additional information explaining your answers in the "Optional - Please provide any additional information" text field. Some control areas include supplemental questions and may require additional documentation to be submitted.

1.0 – INFORMATION SECURITY PROGRAM MANAGEMENT (PM)	
1.1 – The organization establishes and maintains 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, all in an effort to manage risk. Information security program management includes, at a minimum, the following: • Establishment of a management structure with clear reporting paths and explicit responsibility for information security; • Creation, maintenance, and communication of information security policies, standards, procedures, and guidelines to include the control areas listed below; • Development and maintenance of relationships with external organizations to stay abreast of current and emerging security issues and for assistance, when applicable; and • Independent review of the effectiveness of the organization's information security program.	No
Supplemental Information	
1.2 – Do you align your information security program following industry standard frameworks such as the NIST CSF, ISO 27001, CIS Top 20, CoBIT? If yes, please list which framework(s) you employ.	
1.3 – Describe the process you follow, and how frequently, to review and update your security program and safeguards?	
1.4 – If you employ an Exception Management Policy please document the processes for the submission, review, documentation, and the application of exceptions to compliance with established information security policies and standards.	
1.5 – Please detail your disciplinary or sanction policy established for personnel and contractors who have violated security policies and procedures?	
1.6 – Optional - Please provide any additional information relative to this control area.	

2.0 – COMPLIANCE (CP)

2.1 – The organization develops, implements, and governs processes to ensure compliance with all applicable statutory, regulatory, contractual, and internal policy obligations. Ensuring compliance includes, at a minimum:

- Statutory, Regulatory, and Contractual Compliance;
- Security controls oversight; and
- Periodically conducting security assessments.

No

Supplemental Information

2.2 – Indicate all third-party security audits, and subsequent last audit dates, conducted at your organization to ensure compliance with applicable laws, regulations and contractual requirements.

- ☐ CJIS
- ☐ IRS-1075
- ☐ FISMA
- ☐ SOC2
- ☐ PCI-DSS
- ☐ Social Security Admin.
- ☐ FedRAMP
- ☐ Other:

2.3 – Specify all compliance frameworks and standards your organization follows (e.g., GDPR, COBIT, ISO, etc.). Please provide documentation for all IT operational, security, and privacy-related standards, certifications, and/or regulations for which your organization or the intended product/system/application/service is compliant.

2.4 – Optional - Please provide any additional information relative to this control area.

3.0 – PERSONNEL SECURITY (PS)	
3.1 – The organization implements processes to ensure all personnel, with 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 include, at a minimum: • Position descriptions that include appropriate language regarding each role's security requirements; • 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 organization information assets; • Rules of behavior are established and procedures are implemented to ensure personnel are aware of and understand usage policies applicable to the organization's information and information systems; • Access reviews are conducted upon personnel transfers and promotions to ensure access levels are appropriate; • Disabling system access for terminated personnel and collecting all organization owned assets prior to the individual's departure; and • Procedures are implemented that ensure all personnel are aware of their duty to protect organizational information assets and their responsibility to immediately report any suspected information security incidents.	No
Supplemental Information	
3.2 – Please describe the screening and background checks you conduct for your workforce (personnel, contractors, and third-parties) that have access to sensitive information (e.g., CJI, FTI, PCI, etc.).	
3.3 – Are all personnel required to sign an Acceptable Use Policy (AUP)? If you answered yes, please submit a copy of the AUP. If no, please explain.	
3.4 – Describe the procedures the organization follows to govern changes in employment (transfers, promotions, etc.) and/or termination of staff.	
3.5 – Optional - Please provide any additional information relative to this control area.	

4.0 – SECURITY AWARENESS AND TRAINING (AW)	
4.1 – The organization provides 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 includes, at a minimum: • Personnel are provided with security awareness training upon hire and at least annually, thereafter; • Security awareness training records are maintained as part of the personnel record; • 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 • Individuals are provided with timely information regarding emerging threats, best practices, and new policies, laws, and regulations related to information security.	No
Supplemental Information	
4.2 – Describe the security awareness and training program you provide to personnel and contractors to ensure they are aware of information security risks and threats, understand their responsibilities, and are aware of the statutory and policy requirements. Is the training mandatory? How is training by personnel documented and tracked? How often is security awareness training conducted?	
4.3 – Optional - Please provide any additional information relative to this control area.	

5.0 – RISK MANAGEMENT (RM)

5.1 – The organization establishes 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:

No

- Categorizing systems and information based on their criticality and sensitivity;
- Ensuring risks are identified, documented and assigned to appropriate personnel for assessment and treatment;
- Ensuring risk assessments are 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
- Mitigating risks to an acceptable level and prioritizing remediation actions based on risk criteria and establishing timelines for remediation. Risk treatment may also include the acceptance or transfer of risk.

Supplemental Information

5.2 – Describe the risk management processes you employ that account for the identification, assessment, and treatment of risks that can adversely impact the confidentiality, integrity, and availability of the product/system/application/service. How often are these risk management processes performed?

5.3 – Describe how risks and risk mitigation efforts are evaluated and prioritized. Include details on how you document and verify the results of these risk mitigation processes?

5.4 – Optional - Please provide any additional information relative to this control area.

6.0 – PRIVACY (PR)

6.1 – The organization establishes appropriate processes and safeguards necessary to protect the personally identifiable information (PII) that the organization collects, stores, processes, uses, and transmits on behalf of the State of New Jersey. Privacy controls and processes include, but are not limited to:

No

- Ensuring only the minimum amount of PII necessary to carry out the business function, and in accordance with applicable laws and regulations, is collected and stored;
- Safeguarding PII through the implementation of administrative, physical, and technical controls (e.g., access controls, encryption and tokenization, etc.); and
- Securely deleting PII when no longer necessary for business or legal purposes.

Supplemental Information

6.2 – Describe your privacy program and detail how it maintains currency with evolving applicable privacy requirements. Please submit a copy of or provide a link to your privacy program.

6.3 – Optional - Please provide any additional information relative to this control area.

7.0 – ASSET MANAGEMENT (AM)

7.1 – The organization implements 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 include, but are not limited to:

No

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

Supplemental Information

7.2 – Optional - Please provide any additional information relative to this control area.

8.0 – SECURITY CATEGORIZATION (SC)

8.1 – The organization implements processes that classify information and categorize information systems throughout their lifecycles according to their sensitivity and criticality, along with the risks and impact should there be a loss of confidentiality, integrity, availability, or breach of privacy. Information classification and system categorization includes labeling and handling requirements. Security Categorization controls include, but are not limited to, the following: No

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

Supplemental Information

8.2 – Optional - Please provide any additional information relative to this control area.

9.0 – MEDIA AND CRYPTOGRAPHIC PROTECTION (DP)

9.1 – The organization establishes 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 organization, business partners, or individuals. Media protections include, but are not limited to: No

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

Supplemental Information

9.2 – Detail the mechanisms used to secure data at rest, data in transit, and data in use.

9.3 – Describe cryptographic standards and technologies employed to protect sensitive State of New Jersey data. Include details on the encryption or hashing algorithms used, key management processes, use of hardware or software key storage, key fragmentation, etc.

9.4 – Optional - Please provide any additional information relative to this control area.

10.0 – ACCESS MANAGEMENT, IDENTITY, AND AUTHENTICATION (AC)

10.1 – The organization establishes security requirements and ensures appropriate mechanisms are provided for the control, administration, and tracking of access to, and the use of, the organization's information systems. Access management includes, at a minimum:

No

- Ensuring 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;
- Implementing account management processes for registration, updates, changes, and de-provisioning of system access;
- Ensuring the principle of least privilege when provisioning access to organizational assets;
- Provisioning access according to an individual's role and business requirements for such access;
- Implementing the concept of segregation of duties by disseminating tasks and associated privileges for specific sensitive duties among multiple people;
- 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;
- Implementing multi-factor authentication (MFA) requirements for access to sensitive and critical systems, and for remote access to the organization's systems and information; and
- Conducting periodic reviews of access authorizations and controls.

Supplemental Information

10.2 – Describe your organization's processes and methods utilized for granting access, reviewing access, and documenting the review. Do you centrally manage access throughout the organization? Explain in detail.

10.3 – Detail your password and authentication policy and standards. Include minimum length, lockout, complexity, timeout period, password history, etc. How are these managed and enforced?

10.4 – Describe the process of controlling and monitoring the use of privileged and administrative accounts within your organization. Is Multi-Factor Authentication (MFA) required for privileged access? Do end-users have local administrator access?

10.5 – If personnel and/or contractors are provided with remote access to your organization's internal network, please describe the mechanisms used for authentication and authorization. Detail the use of MFA for remote access, if applicable.

10.6 – Optional - Please provide any additional information relative to this control area.

11.0 – SECURITY ENGINEERING AND ARCHITECTURE (SE)

11.1 – The organization employs security engineering and architecture principles for all information technology assets, such that they incorporate industry recognized leading security practices and address applicable statutory and regulatory obligations. Applying security engineering and architecture principles include, at a minimum:

No

- Implementing configuration standards that are consistent with industry-accepted system hardening standards and addressing known security vulnerabilities for all system components;
- Establishing a defense in-depth security posture that includes layered technical, administrative, and physical controls;
- Incorporating security requirements into the systems throughout their life cycles;
- Delineating physical and logical security boundaries;
- Tailoring security controls to meet organizational and operational needs;
- 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;
- Implementing controls and procedures to ensure critical systems fail-secure and fail-safe in known states; and
- Ensuring information system clock synchronization across the organization.

Supplemental Information

11.2 – Optional - Please provide any additional information relative to this control area.

12.0 – CONFIGURATION MANAGEMENT (CM)

12.1 – The organization ensures 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 includes, but is not limited to:

No

- Hardening systems through baseline configurations; and
- 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.

Supplemental Information

12.2 – Describe the processes employed to establish and maintain baseline security configuration settings across your organization. Industry standard configuration and hardening standards include, but are not limited to, CIS Benchmarks, DISA STIGs, and component vendor security configuration guides.

12.3 – Describe the processes and protective technologies employed to verify these security configuration settings are maintained and to detect any attempts to adversely impact the confidentiality, integrity, and availability of components or data in your organization. Protective technologies include, but are not limited to, firewalls, host and network intrusion detection/protection systems, file integrity monitoring, and anti-malware software.

12.4 – Optional - Please provide any additional information relative to this control area.

13.0 – ENDPOINT SECURITY (ES)

13.1 – The organization ensures that endpoint devices are properly configured, and measures are implemented to protect the organization's information and information systems from a loss of confidentiality, integrity, and availability. Endpoint security includes, at a minimum: No

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

Supplemental Information

13.2 – Describe the standard personnel issued device security configuration/features (Login Password, anti-malware, Full Disk Encryption, Administrative Privileges, Firewall, Auto-lock, etc.).

13.3 – Are all endpoints in or with access to the production environment centrally managed? Explain.

13.4 – Describe how you limit data exfiltration of sensitive data from endpoints in or with access to the production environment.

13.5 – Optional - Please provide any additional information relative to this control area.

14.0 – ICS/SCADA/OT SECURITY (OT)

14.1 – The organization implements 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 included here in this document, including, at a minimum:

No

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

Supplemental Information

14.2 – As applicable, list and describe any ICS/SCADA/OT systems used across your organization and detail how those systems are secured physically, administratively, and technically.

14.3 – Optional - Please provide any additional information relative to this control area.

15.0 – INTERNET OF THINGS SECURITY (IT)

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

No

- Developing policies and standards specific to IoT assets;
- Ensuring the secure configuration of IoT assets;
- Conducting risk assessments prior to implementation, and throughout the lifecycles of IoT assets;
- Segmenting IoT networks from the rest of the organization's networks; and
- Ensuring least privilege and strong authentication controls are implemented.

Supplemental Information

15.2 – As applicable, list and describe any IoT devices used across your organization and detail how those devices are secured physically, administratively, and technically. Include information on network segmentation, access and authentication, and security updates.

15.3 – Optional - Please provide any additional information relative to this control area.

16.0 – MOBILE DEVICE SECURITY (MD)

16.1 – The organization establishes administrative, technical, and physical security controls required to effectively manage the risks introduced by mobile devices used for organizational business purposes. Mobile device security includes, at a minimum:

No

- Establishing requirements for authorization to use mobile devices for organizational business purposes;
- Establishing Bring Your Own Device (BYOD) processes and restrictions;
- Establishing physical and logical access controls;
- Implementing network access restrictions for mobile devices;
- 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;
- Establishing approved application stores from which applications can be acquired;
- Establishing lists of approved applications that can be used; and
- Training of mobile device users regarding security and safety.

Supplemental Information
16.2 – Does your organization allow for BYOD devices to connect to your internal network? If so, how are BYOD managed so they do not introduce additional risks?
16.3 – Optional - Please provide any additional information relative to this control area.

17.0 – NETWORK SECURITY (NS)	
17.1 – The organization implements defense-in-depth and least privilege strategies for securing the information technology networks that they operate. To ensure information technology resources are available to authorized network clients and protected from unauthorized access, organizations must: • Include protection mechanisms for network communications and infrastructure (e.g., layered defenses, denial of service protection, encryption for data in transit, etc.); • Include protection mechanisms for network boundaries (e.g., limit network access points, implement firewalls, use Internet proxies, restrict split tunneling, etc.); • Control the flow of information (e.g., deny traffic by default/allow by exception, implement Access Control Lists, etc.); and • Control access to the organization's information systems (e.g., network segmentation, network intrusion detection and prevention systems, wireless restrictions, etc.).	No
Supplemental Information	
17.2 – Optional - Please provide any additional information relative to this control area.	

18.0 – CLOUD SECURITY (CL)	
18.1 – The organization establishes 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 includes, at a minimum: • Security is accounted for in the acquisition and development of cloud services; • The design, configuration, and implementation of cloud-based applications, infrastructure and system interfaces are conducted in accordance with mutually agreed-upon service, security, and capacity-level expectations; • Security roles and responsibilities for the organization and the cloud provider are delineated and documented; and • Controls necessary to protect sensitive data in public cloud environments are implemented.	No
Supplemental Information	
18.2 – Optional - Please provide any additional information relative to this control area.	

19.0 – CHANGE MANAGEMENT (CH)	
19.1 – The organization establishes controls required to ensure change is managed effectively. Organizations must ensure changes are appropriately tested, validated, and documented before implementing any change on a production network. Change management provides the organization 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 include, at a minimum: • Notifying all stakeholders of changes; • Conducting a security impact analysis for changes; and • Verifying security functionality after the changes have been made.	No
Supplemental Information	
19.2 – Describe the change control process as it relates to patches, hot-fixes, upgrades, and configuration changes within your organization. Include information on review of proposed changes. Include information on timelines used for testing, implementation, and emergency change control.	
19.3 – Optional - Please provide any additional information relative to this control area.	

20.0 – MAINTENANCE (MA)	
20.1 – The organization implements 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 includes, at a minimum: • Conducting scheduled and timely maintenance; • Ensuring individuals conducting maintenance operations are qualified and trustworthy; and • Vetting, escorting, and monitoring third-parties conducting maintenance operations on the organization's information technology assets.	No
Supplemental Information	
20.2 – Optional - Please provide any additional information relative to this control area.	

21.0 – THREAT MANAGEMENT (TM)	
21.1 – The organization establishes 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: • Developing, implementing, and governing processes and documentation to facilitate the implementation of a threat awareness policy, as well as associated standards, controls and procedures; and • Subscribing to and receiving relevant threat intelligence information from the US CERT, the organization's vendors, and other sources as appropriate.	No
Supplemental Information	
21.2 – List and describe the threat intelligence sources you subscribe to or follow in order to keep abreast of potential security vulnerabilities and threats.	
21.3 – Optional - Please provide any additional information relative to this control area.	

22.0 – VULNERABILITY AND PATCH MANAGEMENT (VU)	
22.1 – The organization implements 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 include, at a minimum: • Prioritizing vulnerability scanning and remediation activities based on the criticality and security categorization of the organization's systems and information, and the risks associated with a loss of confidentiality, integrity, availability, and/or privacy; • Maintaining software and operating systems at the latest vendor-supported patch levels; • Conducting penetration testing and red team exercises; and • Employing qualified third-parties to conduct Independent vulnerability scanning, penetration testing, and red-team exercises.	No

Supplemental Information
22.2 – Describe your network vulnerability scanning and penetration testing process. Who conducts your network penetration testing and vulnerability scans? Are these vulnerability scans and penetration tests both external and internal? How often are vulnerability scans and penetration tests conducted?
22.3 – Describe how patches and vulnerability remediation processes prioritized. How do you document and verify the results of these remediation efforts?
22.4 – As applicable, please provide details on the most recent Application Code Review or Penetration Testing Reports carried out by independent third parties.
22.5 – Optional - Please provide any additional information relative to this control area.

23.0 – CONTINUOUS MONITORING (CO)	
23.1 – The organization implements continuous monitoring practices to establish and maintain situational awareness regarding potential threats to the confidentiality, integrity, availability, privacy, and safety of the organization's information and information systems through timely collection and review of security-related event logs. Continuous monitoring practices include, at a minimum: • Centralizing the collection and monitoring of event logs; • Ensuring the content of audit records includes all relevant security event information; • Protection of audit records from tampering; and • Detecting, investigating, and responding to incidents discovered through monitoring.	No
Supplemental Information	
23.2 – Describe the processes and technologies used for monitoring, alerting on, and logging of application, system, network, and security events. Include information on retention of logs and how they are reviewed.	
23.3 – Optional - Please provide any additional information relative to this control area.	

24.0 – SYSTEM DEVELOPMENT AND ACQUISITION (SD)	
24.1 – The organization establishes security requirements necessary to ensure that systems and application software programs developed by the organization 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 include, at a minimum: • Secure coding; • Separation of development, testing and operational environments; • Information input restrictions; • Input data validation; • Error handling; • Security testing throughout development; • Restrictions for access to program source code; and • Security training of software developers and system implementers.	No
Supplemental Information	
24.2 – As applicable, describe your Software Development Lifecycle (SDLC) including developers' access to production data, systems, and applications; version control tools used; promotion from development to production, etc.	
24.3 – As applicable, describe the processes you use to ensure code is being developed securely. Include details of the types of code reviews and analysis (e.g., static and dynamic) performed and how threat modeling is incorporated into the design phase of development.	
24.4 – As applicable, describe how you monitor for vulnerabilities in dependencies and third-party libraries or code included in the product/system/application/service.	
24.5 – Describe how API security is maintained including storage of API keys and support for IP whitelisting for API access.	

24.6 – As applicable, for web applications that require authentication as part of the product/system/application/service you're providing, please describe how you authenticate users. If passwords are used, describe complexity requirements, and how passwords are protected. If SAML, SSO and/or MFA is supported, please describe the available options.
24.7 – As applicable, describe additional user authentication controls including, but not limited to, IP whitelisting and geofencing.
24.8 – As applicable, describe the protective technologies (Web Application Firewalls, Proxies, etc.) that you employ to mitigate web application security risks (e.g., SQLi, XSS, XSRF, etc.).
24.9 – As applicable, describe the training you provide to developers with respect to secure coding practices and system development life cycle.
24.10 – Optional - Please provide any additional information relative to this control area.

25.0 – PROJECT AND RESOURCE MANAGEMENT (PM)	
25.1 – The organization ensures 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 include, at a minimum: • Defining and implementing security requirements; • Allocating resources required to protect systems and information; and • Ensuring security requirements are accounted for throughout the SDLC.	No
Supplemental Information	
25.2 – Optional - Please provide any additional information relative to this control area.	

26.0 – CAPACITY AND PERFORMANCE MANAGEMENT (CA)	
26.1 – The organization implements 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 include, but are not limited to, at a minimum: • 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 • Implementing resource priority controls to prevent or limit Denial of Service (DoS) effectiveness.	No
Supplemental Information	
26.2 – As applicable, describe the processes and controls that are employed to ensure information systems scale appropriately and meet availability needs. Include information on DDoS protections, automated provisioning of resources, high-availability, etc.	
26.3 – Optional - Please provide any additional information relative to this control area.	

27.0 – THIRD-PARTY MANAGEMENT (TP)

27.1 – The organization implements 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 include, at a minimum:

No

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

Supplemental Information

27.2 – Describe the processes utilized to validate third-party service providers' compliance with applicable laws, regulations, and contractual requirements.

27.3 – Optional - Please provide any additional information relative to this control area.

28.0 – PHYSICAL AND ENVIRONMENTAL SECURITY (PE)

28.1 – The organization establishes physical and environmental protection procedures that limit access to systems, equipment, and the respective operating environments, to only authorized individuals. The organization 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 include, at a minimum:

No

- Physical access controls (e.g., locks, security gates and guards, etc.);
- Visitor controls;
- Security monitoring and auditing of physical access;
- Emergency shutoff;
- Emergency power;
- Emergency lighting;
- Fire protection;
- Temperature and humidity controls;
- Water damage protection; and
- Delivery and removal of information assets controls.

Supplemental Information

28.2 – Optional - Please provide any additional information relative to this control area.

29.0 – CONTINGENCY PLANNING (CT)	
29.1 – The organization develops, implements, tests, and maintains contingency plans to ensure continuity of operations for all information systems that deliver or support essential or critical business functions on behalf of the organization. Contingency planning includes, at a minimum: • Backup and recovery strategies; • Continuity of operations; • Disaster recovery; and • Crisis management.	No
Supplemental Information	
29.2 – Describe the processes and plans that are implemented to ensure continuity of operations for your organization.	
29.3 – Describe the data and system backup/recovery processes employed and how the security categorization of the information is maintained in backup media. How often are backups tested to verify media reliability and information integrity? What are the recovery point and recovery time objectives?	
29.4 – As applicable, if an alternate site(s) has been established for storage, processing, and communications functions as part of the organization's contingency plan, describe the processes and timelines for failing over. Is the alternate site considered Hot, Warm, or Cold? Explain how often fail-over processes are tested and how results are documented and reviewed.	
29.5 – Optional - Please provide any additional information relative to this control area.	

30.0 – INCIDENT RESPONSE (IR)	
30.1 – The organization maintains an information security incident response capability that includes adequate preparation, detection, analysis, containment, recovery, and reporting activities. Information security incident response activities include, at a minimum: • Information security incident reporting awareness; • Incident response planning and handling; • Establishment of an incident response team; • Cybersecurity insurance; • Contracts with external incident response services specialists; and • Contacts with law enforcement cybersecurity units.	No
Supplemental Information	
30.2 – Describe how your incident response plan is tested and how often tests are conducted.	
30.3 – Describe in detail any breaches of information security your organization experienced over the past five years. Describe how affected customers were notified by your organization, the timeframe of such notifications, and steps taken by your organization to prevent the breach from recurring.	
30.4 – If the organization has purchased cybersecurity liability insurance describe in detail the scope of the coverage.	
30.5 – Optional - Please provide any additional information relative to this control area.	

SECTION V – SUPPORTING DOCUMENTATION TO BE SUBMITTED

Please submit the following supporting documentation with this questionnaire:

- Copy of your organization's written information security policies and standards ☐
- Copy of your Privacy Policy ☐
- Independent information security audits and/or certifications (e.g., PCI-DSS, SOC2 Type II, ISO27001, FEDRAMP, FISMA certification). ☐
- If the service/application you are proposing relies on subcontractors that handle State data, including Cloud Service Providers (CSP) (e.g., Amazon, Salesforce, Microsoft, Google, etc.), please submit relevant security profiles/certifications for the subcontractors, including CSPs, being utilized. ☐
- Other relevant documentation, reports, information (please provide an explanation, as applicable). ☐

APPENDIX A – GLOSSARY

Access: Ability and means to communicate with or otherwise interact with a system, to use system resources to handle information, to gain knowledge of the information the system contains, or to control system components and functions.

Access Control: The process of granting or denying specific requests to obtain and use information and related information processing services; and enter specific physical facilities.

Access Management: A discipline that focuses on ensuring that only approved roles are able to create, read, update, or delete data through appropriate and controlled methods.

Administrative Safeguards: Administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect electronic health information and to manage the conduct of the covered entity's workforce in relation to protecting that information.

Alert: Notification that a specific attack has been directed at an organization's information systems.

Alternate Processing Site: Locations and infrastructures from which emergency or backup processes are executed, when the main premises are unavailable or destroyed.

Attack: An attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity.

Audit: Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Audit Log: A chronological record of system activities. Includes records of system access and operations performed in a given period.

Authenticate: To verify the identity of a user, user device, or other entity.

Authentication: The process of verifying the identity, or other attributes claimed by or assumed, of an entity (user, process, or device), or to verify the source and integrity of data.

Authorization: Access privileges granted to a user, program, or process, or the act of granting those privileges.

Availability: The property of being accessible and useable, upon demand, by an authorized entity.

Baseline Configuration: A set of specifications for a system, or Configuration Item (CI) within a system, that has been formally reviewed and agreed upon at a given point in time, which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.

Best Practice: A proven activity or process that has been successfully used by multiple enterprises.

Boundary Protection: Monitoring and control of communications at the external boundary of an information system to prevent and detect malicious and other unauthorized communication, through the use of boundary protection devices (e.g., proxies, gateways, routers, firewalls, guards, encrypted tunnels).

Boundary Protection Device: A device with appropriate mechanisms that:

(i) Facilitates the adjudication of different interconnected system security policies (e.g., controlling the flow of information into or out of an interconnected system); and/or
(ii) Provides information system boundary protection.

Bring Your Own Device (BYOD): Refers to the policy of permitting personnel and contractors to use personally owned or third-party owned mobile devices for organizational business purposes.

Business Continuity Plan (BCP): The documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.

Cardholder Data: At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date, and/or service code. See **Sensitive Authentication Data** for additional data elements that may be transmitted or processed (but not stored) as part of a payment transaction.

Change Control: A formal process used to ensure that a process, product, service, or technology component is modified only in accordance with agreed-upon rules. Many organizations have formal Change Control Boards that review and approve proposed modifications to technology infrastructures, systems, and applications. Data Governance programs often strive to extend the scope of change control to include additions, modifications, or deletions to data models and values for reference/master data.

Clear Text: Information that is not encrypted.

Cloud Computing: A model for enabling on-demand network access to a shared pool of configurable IT capabilities/resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. It allows users to access technology-based services from the network cloud without knowledge of, expertise with, or control over the technology infrastructure that supports them. This cloud model is composed of five essential characteristics (on-demand self-service, ubiquitous network access, location independent resource pooling, rapid elasticity, and measured service); three service delivery models (Cloud Software as a Service [SaaS], Cloud Platform as a Service [PaaS], and Cloud Infrastructure as a Service [IaaS]); and four models for enterprise access (Private cloud, Community cloud, Public cloud, and Hybrid cloud).

Cloud Service Provider: An entity that offers cloud-based platform, infrastructure, application, or storage services. Cloud service providers include internal entities, and external entities, such as Amazon, Microsoft, Salesforce, Google, and others.

Compensating Security Control: A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system.

Compromise: Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred.

Confidentiality: The property that sensitive information is not disclosed to unauthorized individuals, entities, or processes.

Configuration Management: A structured process of managing and controlling changes to hardware, software, firmware, communications, and documentation throughout the system development life cycle.

Contingency Plan: Management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. The Contingency Plan is the first plan used by the enterprise risk managers to determine what happened, why, and what to do. It may point to the Continuity of Operations Plan (COOP) or Disaster Recovery Plan for major disruptions.

Continuous Monitoring: The process implemented to maintain a current security status for individual information systems, or for the entire suite of information systems, on which the operational mission of the enterprise depends.

Control: A means of managing a risk or ensuring that an objective is achieved. Controls can be preventative, detective, or corrective and can be fully automated, procedural, or technology-assisted human-initiated activates. They can include actions, devices, procedures, techniques, or other measures.

Criminal Justice Information (CJI): The term used to refer to all FBI Criminal Justice Information Services (CJIS) provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to, data consisting of biometric, identity history, biographic, property, and case/incident history. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

(i) Biometric Data – Data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Biometric information used to identify individuals include fingerprints, palm prints, iris scans, and facial recognition data.

(ii) Identity History Data – Textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.

(iii) Biographic Data – Information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.

(iv) Property Data – Information about vehicles and property associated with crime when accompanied by any personally identifiable information (PII).

(v) Case/Incident History – Information about the history of criminal incidents.

Criticality: A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function.

Cryptographic Key: A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification.

Cryptography: The discipline that embodies the principles, means, and methods for the transformation of data in order to hide their semantic content, prevent their unauthorized use, or prevent their undetected modification.

Data: A subset of information in an electronic format that allows it to be retrieved or transmitted.

Data Privacy: The assurance that a person's or organization's personal and private information is not inappropriately disclosed. Ensuring Data Privacy requires Access Management, eSecurity, and other data protection efforts. (SOURCE: Data Governance Institute)

Data Security: Protection of data from unauthorized (accidental or intentional) modification, destruction, or disclosure.

Defense-in-Depth: Information security strategy integrating people, technology, and operation capabilities to establish variable barriers across multiple layers and dimensions of the organization.

Denial of Service (DoS): The prevention of authorized access to resources or the delaying of time-critical operations. Depending on the service provided, time-critical may be defined at milliseconds or hours.

Disaster Recovery Plan (DRP): A written plan for recovering one or more information systems at an alternate facility in response to a major hardware or software failure or destruction of facilities.

Distributed Denial of Service (DDoS): A Denial of Service technique that uses numerous hosts to perform the attack.

Electronic Protected Health Information (ePHI): Electronic Protected Health Information (PHI) consists of any information about health status, provision of health care, or payment for health care that can be linked to an individual. PHI refers to all "individually identifiable information" held or transmitted by State entities or its business associates in any form or media, whether paper, electronic or oral. "Individually identifiable health information" is information, including demographic data, that relates to:

(i) The individual's past, present, or future physical or mental health or condition;

(ii) The provision of health care to the individual;

(iii) The past, present, or future payment for the provision of health care to the individual; or

(iv) The individual's identity for which there is a reasonable basis to believe it can be used to identify the individual.

Embedded System: An embedded system is a computer system with a dedicated function within a larger mechanical or electrical system, often with real-time computing constraints. It is embedded as part of a complete device often including hardware and mechanical parts.

Embedded Technology: Specialized hardware and software that is wholly incorporated as part of a larger system or machine.

Encryption: The process of changing plaintext into ciphertext for the purpose of security or privacy.

Endpoint: Any device capable of being connected, either physically or wirelessly to a network, and accepts communications back and forth across the network. Endpoints include, but are not limited to, computers, servers, tablets, mobile devices, or any similar network enabled device.

Entity: Either a subject (an active element that operates on information or the system state) or an object (a passive element that contains or receives information).

Federal Tax Information (FTI): FTI consists of federal tax returns (and information derived from it) that is in the agency's possession or control, which is covered by the confidentiality protections of the Internal Revenue Code (IRC) and subject to the IRC 6103(p)(4) safeguarding requirements including IRS oversight, including:

(i) Return information received directly from the IRS or obtained through an authorized secondary source, such as Social Security Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), Centers for Medicare and Medicaid Services (CMS), or another entity acting on behalf of the IRS pursuant to the IRC 6103(p)(2)(B) Agreement; and

(ii) Any information created by the recipient that is derived from federal return information received from the IRS or obtained through a secondary source.

Firewall: A gateway that limits access between networks in accordance with local security policy.

General Support System: An interconnected set of information resources under the same direct management control that shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people, which provides support for a variety of users and/or applications. A general support system, for example, can be a:

(i) Local Area Network (including workstations, printers, and other assets that support an agency office or facility);
(ii) Backbone Network (e.g., Department/Agency-wide and/or statewide (GSN));
(iii) Department/Agency information processing center, including its operating system and utilities (e.g., server room); and/or
(iv) Shared information processing service facility (e.g., State, or other, colocation data center).

Governance: Ensures that stakeholder needs, conditions, and options are evaluated to determine balanced, agreed upon enterprise objectives; setting direction through prioritization and decision making; and monitoring performance and compliance with direction and objectives.

Identification: The process of verifying the identity of a user, process, or device, usually as a prerequisite for granting access to resources in an IT system.

Industrial Control System: An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems (SCADA) used to control geographically dispersed assets, as well as distributed control systems (DCS) and smaller control systems using programmable logic controllers to control localized processes.

Information: Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.

Information Asset: Any data, device, or other component of an information or communication system. Assets generally include hardware (e.g., servers, laptop and desktop computers, switches), software (e.g., commercial off the shelf and custom developed applications and support systems) and information. Assets may also be referred to as information resources or systems.

Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide the confidentiality, integrity, and availability of information.

Information Security Classification: A system of designating security categories for information based on the impact to the business mission from loss of information confidentiality, integrity or availability (also classification, information classification, security classification)

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange (PBX) systems, and environmental control systems.

Information Technology: The term information technology includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources.

Integrity: The property that sensitive data has not been modified or deleted in an unauthorized and undetected manner.

Internet: The single, interconnected, worldwide system of commercial, governmental, educational, and other computer networks that share:

(i) The protocol suite specified by the Internet Architecture Board (IAB); and

(ii) The name and address spaces managed by the Internet Corporation for Assigned Names and Numbers (ICANN).

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

Intrusion Detection Systems (IDS): Hardware or software product(s) that gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations).

Intrusion Prevention Systems (IPS): Hardware or software product(s) that monitors network and/or system activities for malicious activity. The main functions of intrusion prevention systems are to identify malicious activity, log information about this activity, attempt to block/stop it, and report it.

IT Governance: The leadership, organizational structures, and processes that ensure that the enterprise's IT sustains and extends the enterprise's strategies and objectives.

Key: A value used to control cryptographic operations, such as decryption, encryption, signature generation, or signature verification.

Least Functionality: The principle of least functionality states that only the minimum access necessary to perform an operation should be granted to a user, a process, or a program, and that access should be granted only for the minimum amount of time necessary.

Least Privilege: The principle that a security architecture should be designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function.

Major Applications and Systems: Any system or application that includes one or more of the following characteristics:

(i) Users in more than one State Department/Agency;

(ii) Costs exceeds $250,000 to develop and implement (including the cost of hardware, software, and contract personnel);

(iii) Any public facing web application; and/or

(iv) Any application that stores or processes sensitive information or is deemed critical to the operations of the agency.

Malicious Code: Software or firmware intended to perform an unauthorized process that will have an adverse impact on the confidentiality, integrity, or availability of information system(s). A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Malware: A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or to otherwise annoy or cause disruption to the victim.

Media Sanitization: A general term referring to the actions taken to render data, written on media, unrecoverable by both ordinary and extraordinary means.

Minor Application: An application, other than a major application, that requires attention to security due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of the information in the application. Minor applications are typically included as part of a general support system.

Mobile Code: Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient.

Multi-factor Authentication: Authentication using two or more factors to achieve authentication. Factors include:

(i) Something you know (e.g., password/PIN);

(ii) Something you have (e.g., cryptographic identification device, token); or

(iii) Something you are (e.g., biometric).

Nonrepudiation: Protection against an individual falsely denying having performed a particular action. Provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, or receiving a message.

Operational Technology: The use of computers to monitor or alter the physical state of a system, such as the control system for a power station or the control network for a rail system. The term is established to demonstrate the technological and functional differences between traditional IT systems and Industrial Control Systems environment.

Password: A string of characters (letters, numbers, and other symbols) used to authenticate an identity or to verify access authorization.

Patch: An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Patch Management: The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. These revisions are known as patches, hot fixes, and service packs.

Payment Card Industry (PCI) Data Security Standard (DSS) Information: PCI DSS applies to the transmission, storage, or processing of confidential credit card data. This data classification includes credit card magnetic stripe data, card verification values, payment account numbers, personally identification numbers, passwords, and card expiration dates.

Penetration Testing: A test methodology in which assessors, using all available documentation (e.g., system design, source code, manuals) and working under specific constraints, attempt to circumvent the security features of an information system.

Personal Information: New Jersey Revised Statutes § 56:8-161 (2013) defines Personal Information as an individual's first name (or first initial) and last name linked with any one or more of the following data elements: (1) Social Security number; (2) driver's license number or State identification card number; or (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.

Personally Identifiable Information (PII): NIST Special Publication (SP) 800-121 defines PII as any information about an individual maintained by an organization, including:

(i) Any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and

(ii) Any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Examples of PII include, but are not limited to, the following:

- Name, such as full name, maiden name, mother's maiden name, or alias;
- Personal identification number, such as social security number (SSN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number;
- Address information, such as street address or email address;
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or a smaller, well defined group of people;
- Telephone numbers, including mobile, business, and personal numbers;
- Personal characteristics, including photographic image (especially of the face or other distinguishing characteristics), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry);
- Information identifying personally owned property, such as vehicle registration number or title number and related information; and
- Information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

Personal Identification Number (PIN): A password consisting only of decimal digits.

Personal Information (PI): An individual's first name, or first initial, and last name linked with any one or more of the following data elements:

(i) Social Security number;

(ii) Driver's license number or State identification card number;

(iii) Account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; or

(iv) Dissociated data that, if linked, would constitute personal information is personal information if the means to link the dissociated data were accessed in connection with access to the dissociated data.

Phishing: A digital form of social engineering that uses authentic-looking—but bogus—emails to request information from users or direct them to a fake Web site that requests information.

Plaintext: Unencrypted information.

Portable Storage Device: An information system component that can be inserted into and removed from an information system, to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory).

Privacy: Freedom from unauthorized intrusion or disclosure of information about an individual or entity.

Privileged Account: An information system account with approved authorizations of a privileged user. (Source: CNSSI-4009; NIST SP 800-53)

Privileged User: A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Process: A structured set of activities designed to accomplish a specific objective.

Protocol: Set of rules and formats, semantic and syntactic, permitting information systems to exchange information.

Remediation: The act of correcting a vulnerability or eliminating a threat.

Remote Access: Access to an organizational information system by a user (or an information system acting on behalf of a user) communicating through an external network (e.g., the Internet).

Risk: The level of impact on organizational operations (including mission, function, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.

Risk Assessment: The process of identifying risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, and other organizations, arising through the operation of an information system. Part of risk management incorporates threat and vulnerability analyses and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

Risk Management: The process of managing risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes:

(i) Conducting a risk assessment;
(ii) Implementing risk mitigation strategy; and
(iii) Employing techniques and procedures for the continuous monitoring of the security of information system(s).

Risk Mitigation: Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

Risk Tolerance: The level of risk an entity is willing to assume in order to achieve a potential desired result.

Role-Based Access Control (RBAC): A model for controlling access to resources where permitted actions on resources are identified with roles rather than with individual subject identities.

Safeguards: Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

Sanitization: Process to remove information from media such that information recovery is not possible. It includes removing all labels, markings, and activity logs.

Scanning: Sending packets or requests to another system to gain information to be used in a subsequent attack.

Security: A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach.

Security Controls: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information.

Security Requirements: Requirements levied on an information system that are derived from applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, procedures, or organizational mission/business case(s) needs to ensure the confidentiality, integrity, and availability of the information being processed, stored, or transmitted.

Sensitive Authentication Data: Security-related information (including, but not limited to, card validation codes/values, full track data of the magnetic stripe or equivalent on a chip, PINs, and PIN blocks) used to authenticate cardholders and/or authorize payment card transactions.

Sensitive Data: Data that is private, personal, or proprietary and must be protected from unauthorized access.

Sensitive Personally Identifiable Information (SPII): Personal information that, if lost, compromised, or disclosed without authorization, could result in substantial harm, embarrassment, inconvenience, or unfairness to an individual.

Separation of Duties: Practice of dividing steps in a function among different individuals, so as to keep a single individual from being able to subvert the process.

Social Security Administration Provided Information: Information that is obtained from the Social Security Administration (SSA). This can include a Social Security number verification indicator or other PII data.

Stakeholder: Anyone who has a responsibility for, an expectation from, or some other interest in the enterprise.

Strong Cryptography: Cryptography based on industry-tested and accepted algorithms, along with key lengths that provide a minimum of 112-bits of effective key strength and proper key-management practices. Cryptography is a method to protect data and includes both encryption and hashing. Examples of industry-tested and accepted standards and algorithms include: AES (128 bits and higher), TDES/TDEA (triple-length keys), RSA (2048 bits and higher), ECC (224 bits and higher), and DSA/D-H (2048/224 bits and higher).

Strong Password: A minimum of eight characters using a combination of upper and lowercase letters, numbers and special characters.

Supervisory Control and Data Acquisition (SCADA): A control system architecture that uses computers, networked data communications, and graphical user interfaces for high-level process supervisory management, but uses other peripheral devices, such as programmable logic controllers and discrete PID controllers, to interface to the process plant or machinery.

Supply Chain: A system of organizations, people, activities, information, and resources, possibly international in scope that provides products or services to consumers.

System: A discrete set of information technologies (including computer hardware, software, databases, etc.) organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

System Development Life Cycle (SDLC): The scope of activities associated with a system, encompassing the system's initiation, development and acquisition, implementation, operation and maintenance, and ultimately its disposal that instigates another system initiation.

Third Party: Any entity that an organization does business with. This may include suppliers, vendors, contract manufacturers, business partners and affiliates, brokers, distributors, resellers, and agents. Third parties can be 'upstream' (suppliers and vendors), 'downstream' (distributors and re-sellers), as well as non-contractual parties.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorizedaccess, destruction, disclosure, modification of information, and/or denial of service.

Trustworthiness: The attribute of a person or organization that provides confidence to others of the qualifications, capabilities, and reliability of that entity to perform specific tasks and fulfill assigned responsibilities.

Unauthorized Access: Occurs when a user, legitimate or unauthorized, accesses a resource that the user is not permitted to use.

Unauthorized Disclosure: An event involving the exposure of information to entities not authorized access to the information.

User: An individual, or system process acting on behalf of an individual, authorized to access an information system.

User-ID: Unique symbol or character string used by an information system to identify a specific user.

Vulnerability: Weakness in an information system, system security procedure(s), internal controls, or implementation that could be exploited or triggered by a threat source.

Vulnerability Scan: An automated process to proactively identify security weaknesses in a network or individual system.

ATTACHMENT A12

Certification of Non-Involvement in Prohibited Activities

Contract Title: _____
Vendor Name: _____

I, the undersigned, certify on behalf of the above-identified Vendor[1] (see definition below), that I have reviewed the Consolidated Sanctions List promulgated by the U.S. Department of the Treasury Office of Foreign Assets Control, and having done so certify:

☐ A. That the Vendor is not identified on the U.S. Department of the Treasury Office of Foreign Assets Control's Consolidated Sanctions List.

☐ B. That I am unable to certify as to "A" above because the Vendor is identified on the U.S. Department of the Treasury Office of Foreign Assets Control's Consolidated Sanctions List.

☐ C. That I am unable to certify as to "A" above, because the Vendor, though not identified on the U.S. Department of the Treasury Office of Foreign Assets Control's Consolidated Sanctions List is engaged in activities prohibited by 117 P.L. 110, 136 Stat. 1159.
Description of prohibited activity (Attach additional sheets if necessary):

By: _____ _____
(signature) (date)

_____
(title)

[1] Vendor means: (1) a natural person, corporation, company, limited partnership, limited liability company, business association, sole proprietorship, joint venture, partnership, society, trust, or any other nongovernmental entity, organization, or group; (2) any government entity or instrumentality of a government, including a multilateral development institution, as defined in Section 1701(c)(3) of the International Financial Institutions Act, 22 U.S.C. 262r(c)(3); or (3) any parent, successor, subunit, direct or indirect subsidiary or entity under common ownership or control with, any entity described in paragraph (1) or (2); that enters into a contract with the PFRSNJ for the provision of goods and/or services.

ATTACHMENT A13

State of New Jersey Standard Terms and Conditions

(Revised February 8, 2024)

And

Waivered Contracts/Delegated Purchase Authority Supplement to the State of New Jersey Standard Terms and Conditions

(Revised January 11, 2022)

STATE OF NEW JERSEY
DEPARTMENT OF THE TREASURY - DIVISION OF PURCHASE AND PROPERTY
33 WEST STATE STREET, P.O. BOX 230 TRENTON, NEW JERSEY 08625-0230

1.0 STANDARD TERMS AND CONDITIONS APPLICABLE TO THE CONTRACT

The following terms and conditions shall apply to all contracts or purchase agreements made with the State of New Jersey. The State's terms and conditions shall prevail over any conflicts set forth in a Contractor's Quote or Proposal.

2.0 STATE LAW REQUIRING MANDATORY COMPLIANCE BY ALL CONTRACTORS

The statutes, laws, regulations or codes cited herein are available for review at the New Jersey State Library, 185 West State Street, Trenton, New Jersey 08625.

2.1 BUSINESS REGISTRATION

Pursuant to N.J.S.A. 52:32-44, the State is prohibited from entering into a contract with an entity unless the Contractor and each subcontractor named in the proposal have a valid Business Registration Certificate on file with the Division of Revenue and Enterprise Services. A subcontractor named in a bid or other proposal shall provide a copy of its business registration to the Contractor who shall provide it to the State.

The contractor shall maintain and submit to the State a list of subcontractors and their addresses that may be updated from time to time with the prior written consent of the Director of the Division of Purchase and Property (Director) during the course of contract performance. The contractor shall submit to the State a complete and accurate list of all subcontractors used and their addresses before final payment is made under the contract.

Pursuant to N.J.S.A. 54:49-4.1, a business organization that fails to provide a copy of a business registration, or that provides false business registration information, shall be liable for a penalty of $25 for each day of violation, not to exceed $50,000 for each business registration copy not properly provided under a contract with a contracting agency.

The contractor and any subcontractor providing goods or performing services under the contract, and each of their affiliates, shall, during the term of the contract, collect and remit to the Director of the Division of Taxation in the Department of the Treasury, the Use Tax due pursuant to the "Sales and Use Tax Act, P.L.1966, c.30 (N.J.S.A. 54:32B-1 et seq.) on all sales of tangible personal property delivered into the State. Any questions in this regard can be directed to the Division of Revenue at (609) 292-1730. Form NJ-REG can be filed online at http://www.state.nj.us/treasury/revenue/busregcert.shtml.

2.2 OWNERSHIP DISCLOSURE

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

A current completed Ownership Disclosure Form must be received prior to or accompany the submitted Quote. A Contractor's failure to submit the completed and signed form prior to or with its Quote will result in the Contractor being ineligible for a Contract award, unless the Division of Purchase and Property (Division) has on file 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. 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.

In the alternative, a Contractor 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.

2.3 DISCLOSURE OF INVESTMENT ACTIVITIES IN IRAN

Pursuant to N.J.S.A. 52:32-58, the Contractor must utilize this Disclosure of Investment Activities in Iran form to certify that neither the Contractor, 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 Contractor, 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 Contractor is unable to so certify, the Contractor shall provide a detailed and precise description of such activities as directed on the form. A Contractor's failure to submit the completed and signed form will preclude the award of a Contract to said Contractor.

2.4 ANTI-DISCRIMINATION

All parties to any contract with the State agree not to discriminate in employment and agree to abide by all anti-discrimination laws including those contained within N.J.S.A. 10:2-1 through N.J.S.A. 10:2-4, N.J.S.A. 10:5-1 et seq. and N.J.S.A. 10:5-31 through 10:5-38, and all rules and regulations issued thereunder are hereby incorporated by reference. The agreement to abide by the provisions of N.J.S.A. 10:5-31 through 10:5-38 include those provisions indicated for Goods, Professional Service and General Service Contracts (Exhibit A, attached) and Constructions Contracts (Exhibit B and Exhibit C - Executive Order 151 Requirements) as appropriate.

The contractor or subcontractor, where applicable, agrees to comply with any regulations promulgated by the Treasurer pursuant to N.J.S.A. 10:5-31 et seq., as amended and supplemented from time to time.

2.5 AFFIRMATIVE ACTION

In accordance with N.J.A.C. 17:27-1.1, prior to award, the Contractor and subcontractor 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. Contractors or subcontractors not in possession of either a New Jersey Certificate of Employee Information Report or a Federal Letter of Approval must complete the Affirmative Action Employee Information Report (AA-302) located on the web at https://www.state.nj.us/treasury/contract_compliance/.

2.6 AMERICANS WITH DISABILITIES ACT

The contractor must comply with all provisions of the Americans with Disabilities Act (ADA), P.L 101-336, in accordance with 42 U.S.C. 12101, et seq.

2.7 MACBRIDE PRINCIPLES

The Contractor must certify pursuant to N.J.S.A. 52:34-12.2 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.

2.8 PAY TO PLAY PROHIBITIONS

New Jersey law insulates the negotiation and award of State contracts from political contributions that pose a risk of improper influence, purchase of access or the appearance thereof. P.L.2005, c.51, as amended by the Elections Transparency Act, P.L.2023, c.30, codified at N.J.S.A. 19:44A-20.13 to 20.25 ("Chapter 51") and Executive Order 333 (2023).

Pursuant to N.J.S.A. 19:44A-20.13 et seq. (P.L.2005, c.51, rev. P.L.2023, c.30), a "fair and open process" means, at a minimum, that the contract shall be: publicly advertised in newspapers or on the Internet website maintained by the public entity in sufficient time to give notice in advance of the contract; awarded under a process that provides for public solicitation of proposals or qualifications and awarded and disclosed under criteria established in writing by the public entity prior to the solicitation of proposals or qualifications; and publicly opened and announced when awarded. A contract awarded under a process that includes public bidding or competitive contracting pursuant to State contracts law shall constitute a fair and open process. N.J.S.A. 19:44A-20.23. The agency conducting the procurement will need to determine whether the procurement meets the Election Transparency Act definition of a "fair and open process" and instruct vendors on the applicability of Chapter 51.

A. For Contracts Awarded Pursuant to a Fair and Open Process

Pursuant to P.L.2005, c.51, as amended by the Elections Transparency Act, P.L.2023, c.30, codified at N.J.S.A. 19:44A-20.13 to 20.25 ("Chapter 51"), and Executive Order No. 333 (2023), contracts awarded pursuant to a fair and open process do not require a certification or disclosure of any solicitation or contribution of money, or pledge of contribution, including in-kind contributions.

B. For Contracts Awarded Pursuant to a Non-Fair and Open Process

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

(1) Make or solicit a contribution in violation of the statute;
(2) Knowingly conceal or misrepresent a contribution given or received;
(3) Make or solicit contributions through intermediaries for the purpose of concealing or misrepresenting the source of the contribution;
(4) Make or solicit any contribution on the condition or with the agreement that it will be contributed to a campaign committee or any candidate of holder of the public office of Governor or Lieutenant Governor;
(5) Engage or employ a lobbyist or consultant with the intent or understanding that such lobbyist or consultant would make or solicit any contribution, which if made or solicited by the business entity itself, would subject that entity to the restrictions of the Legislation;
(6) Fund contributions made by third parties, including consultants, attorneys, family members, and employees;

(7) Engage in any exchange of contributions to circumvent the intent of the Legislation; or

(8) Directly or indirectly through or by any other person or means, do any act which would subject that entity to the restrictions of the Legislation.

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.

A "Continuing Political Committee" means any political organization (a) organized under section 527 of the Internal Revenue Code; and (b) consisting of any group of two or more persons acting jointly, or any corporation, partnership, or any other incorporated or unincorporated association, including a political club, political action committee, civic association or other organization, which in any calendar year contributes or expects to contribute at least $5,500 to the aid or promotion of the candidacy of an individual, or of the candidacies of individuals, for elective public office, or the passage or defeat of a public question or public questions, and which may be expected to make contributions toward such aid or promotion or passage or defeat during a subsequent election, provided that the group, corporation, partnership, association or other organization has been determined to be a Continuing Political Committee by the New Jersey Election Law Enforcement Commission under N.J.S.A.19:44A-8. A Continuing Political Committee does not include a "political party committee," a "legislative leadership committee," or an "independent expenditure committee," as defined in N.J.S.A. 19:44A-3.

Prior to awarding any Contract or agreement to any Business Entity pursuant to a non-fair and open process, the Business Entity proposed as the intended Contractor of the Contract shall submit the Two-Year Chapter 51 /Executive Order 333 Vendor Certification and Disclosure of Political Contributions for Non-Fair and Open Contracts, certifying either that no contributions to a Continuing Political Committee or to a candidate committee or election fund of a gubernatorial candidate have been made by the Business Entity and reporting all qualifying contributions made by the Business Entity or any person or entity whose contributions are attributable to the Business Entity. The required form and instructions, available for review on the Division's website at http://www.state.nj.us/treasury/purchase/forms/eo134/Chapter51.pdf.

2.9 POLITICAL CONTRIBUTION DISCLOSURE

The contractor is advised of its responsibility to file an annual disclosure statement on political contributions with the New Jersey Election Law Enforcement Commission (ELEC), pursuant to N.J.S.A. 19:44A-20.27 (P.L.2005, c.271, rev. P.L.2023, c.30) if in a calendar year the contractor receives one or more contracts valued at $50,000.00 or more. It is the contractor's responsibility to determine if filing is necessary. Failure to file can result in the imposition of penalties by ELEC. Additional information about this requirement is available from ELEC by calling 1(888)313-3532 or on the internet at http://www.elec.state.nj.us/.

2.10 STANDARDS PROHIBITING CONFLICTS OF INTEREST

The following prohibitions on contractor activities shall apply to all contracts or purchase agreements made with the State of New Jersey, pursuant to Executive Order No. 189 (1988).

A. No vendor shall pay, offer to pay, or agree to pay, either directly or indirectly, any fee, commission, compensation, gift, gratuity, or other thing of value of any kind to any State officer or employee or special State officer or employee, as defined by N.J.S.A. 52:13D-13b. and e., in the Department of the Treasury or any other agency with which such vendor transacts or offers or proposes to transact business, or to any member of the immediate family, as defined by N.J.S.A. 52:13D-13i., of any such officer or employee, or partnership, firm or corporation with which they are employed or associated, or in which such officer or employee has an interest within the meaning of N.J.S.A. 52:13D-13g;

B. The solicitation of any fee, commission, compensation, gift, gratuity or other thing of value by any State officer or employee or special State officer or employee from any State vendor shall be reported in writing forthwith by the vendor to the New Jersey Office of the Attorney General and the Executive Commission on Ethical Standards, now known as the State Ethics Commission;

C. No vendor may, directly or indirectly, undertake any private business, commercial or entrepreneurial relationship with, whether or not pursuant to employment, contract or other agreement, express or implied, or sell any interest in such vendor to, any State officer or employee or special State officer or employee having any duties or responsibilities in connection with the purchase, acquisition or sale of any property or services by or to any State agency or any instrumentality thereof, or with any person, firm or entity with which he/she is employed or associated or in which he/she has an interest within the meaning of N.J.S.A. 52:13D-13g. Any relationships subject to this provision shall be reported in writing forthwith to the Executive Commission on Ethical Standards, now known as the State Ethics Commission, which may grant a waiver of this restriction upon application of the State officer or employee or special State officer or employee upon a finding that the present or proposed relationship does not present the potential, actuality or appearance of a conflict of interest;

D. No vendor shall influence, or attempt to influence or cause to be influenced, any State officer or employee or special State officer or employee in his/her official capacity in any manner which might tend to impair the objectivity or independence of judgment of said officer or employee;

E. No vendor shall cause or influence, or attempt to cause or influence, any State officer or employee or special State officer or employee to use, or attempt to use, his/her official position to secure unwarranted privileges or advantages for the vendor or any other person; and

F. The provisions cited above in paragraphs 2.8A through 2.8E shall not be construed to prohibit a State officer or employee or Special State officer or employee from receiving gifts from or contracting with vendors under the same terms and conditions as are offered or

made available to members of the general public subject to any guidelines the Executive Commission on Ethical Standards, now known as the State Ethics Commission may promulgate under paragraph 3c of Executive Order No. 189.

2.11 NEW JERSEY BUSINESS ETHICS GUIDE CERTIFICATION

The Treasurer has established a business ethics guide to be followed by a Contractor in dealings with the State. The guide can be found at: https://www.nj.gov/treasury/purchase/pdf/BusinessEthicsGuide.pdf.

2.12 NOTICE TO ALL CONTRACTORS SET-OFF FOR STATE TAX NOTICE

Pursuant to N.J.S.A. 54:49-19, effective January 1, 1996, and notwithstanding any provision of the law to the contrary, whenever any taxpayer, partnership or S corporation under contract to provide goods or services or construction projects to the State of New Jersey or its agencies or instrumentalities, including the legislative and judicial branches of State government, is entitled to payment for those goods or services at the same time a taxpayer, partner or shareholder of that entity is indebted for any State tax, the Director of the Division of Taxation shall seek to set off that taxpayer's or shareholder's share of the payment due the taxpayer, partnership, or S corporation. The amount set off shall not allow for the deduction of any expenses or other deductions which might be attributable to the taxpayer, partner or shareholder subject to set-off under this act.

The Director of the Division of Taxation shall give notice to the set-off to the taxpayer and provide an opportunity for a hearing within 30 days of such notice under the procedures for protests established under R.S. 54:49-18. No requests for conference, protest, or subsequent appeal to the Tax Court from any protest under this section shall stay the collection of the indebtedness. Interest that may be payable by the State, pursuant to P.L.1987, c.184 (c.52:32-32 et seq.), to the taxpayer shall be stayed.

2.13 COMPLIANCE - LAWS

The contractor must comply with all local, State and Federal laws, rules and regulations applicable to this contract and to the goods delivered and/or services performed hereunder.

2.14 COMPLIANCE - STATE LAWS

It is agreed and understood that any contracts and/or orders placed as a result of [this proposal] shall be governed and construed and the rights and obligations of the parties hereto shall be determined in accordance with the laws of the State of New Jersey.

2.15 WARRANTY OF NO SOLICITATION ON COMMISSION OR CONTINGENT FEE BASIS

The contractor warrants that no person or selling agency has been employed or retained to solicit or secure the contract upon an agreement or understanding for a commission, percentage, brokerage or contingent fee, except bona fide employees or bona fide established commercial or selling agencies maintained by the contractor for the purpose of securing business. If a breach or violation of this section occurs, the State shall have the right to terminate the contract without liability or in its discretion to deduct from the contract price or consideration the full amount of such commission, percentage, brokerage or contingent fee.

2.16 DISCLOSURE OF INVESTIGATIONS AND OTHER ACTIONS

The Contractor should submit the Disclosure of Investigations and Other Actions Form which provides 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 Contractor does not submit the form with the Quote, the Contractor must comply within seven (7) business days of the State's request or the State may deem the Quote non-responsive.

2.17 DISCLOSURE OF PROHIBITED ACTIVITIES WITH RUSSIA OR BELARUS

Pursuant to N.J.S.A. 52:32-60.1 et seq. (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 identified on the list of persons or entities engaging in prohibited activities in Russia or Belarus. Consistent with the federal law, the list of persons and entities engaging in prohibited activities in Russia or Belarus shall consist of all persons and entities appearing on the list of Specially Designated Nationals and Blocked Persons promulgated by the Office of Foreign Assets Control (OFAC) on account of activity relating to Russia or Belarus.

3.0 STATE LAW REQUIRING MANDATORY COMPLIANCE BY CONTRACTORS UNDER CIRCUMSTANCES SET FORTH IN LAW OR BASED ON THE TYPE OF CONTRACT

3.1 COMPLIANCE - CODES

The contractor must comply with New Jersey Uniform Construction Code and the latest National Electrical Code 70®, B.O.C.A. Basic Building code, Occupational Safety and Health Administration and all applicable codes for this requirement. The contractor shall be responsible for securing and paying all necessary permits, where applicable.

3.2 PREVAILING WAGE ACT

The New Jersey Prevailing Wage Act, N.J.S.A. 34: 11-56.25 et seq. is hereby made part of every contract entered into on behalf of the State of New Jersey through the Division of Purchase and Property, except those contracts which are not within the contemplation of the Act. The Contractor 's signature on [the proposal] is his/her guarantee that neither he/she nor any subcontractors he/she might employ to perform the work covered by [the proposal] has been suspended or debarred by the Commissioner, Department of Labor and Workforce Development for violation of the provisions of the Prevailing Wage Act and/or the Public Works Contractor Registration Acts; the Contractor's signature on the proposal is also his/her guarantee that he/she and any subcontractors he/she might employ to perform the work covered by [the proposal] shall comply with

the provisions of the Prevailing Wage and Public Works Contractor Registration Acts, where required.

3.3 PUBLIC WORKS CONTRACTOR REGISTRATION ACT

The New Jersey Public Works Contractor Registration Act requires all contractors, subcontractors and lower tier subcontractor(s) who engage in any contract for public work as defined in N.J.S.A. 34:11-56.26 be first registered with the New Jersey Department of Labor and Workforce Development pursuant to N.J.S.A. 34:11-56.51. Any questions regarding the registration process should be directed to the Division of Wage and Hour Compliance.

3.4 PUBLIC WORKS CONTRACT - ADDITIONAL AFFIRMATIVE ACTION REQUIREMENTS

N.J.S.A. 10:2-1 requires that during the performance of this contract, the contractor must agree as follows:

A. In the hiring of persons for the performance of work under this contract or any subcontract hereunder, or for the procurement, manufacture, assembling or furnishing of any such materials, equipment, supplies or services to be acquired under this contract, no contractor, nor any person acting on behalf of such contractor or subcontractor, shall, by reason of race, creed, color, national origin, ancestry, marital status, gender identity or expression, affectional or sexual orientation or sex, discriminate against any person who is qualified and available to perform the work to which the employment relates;

B. No contractor, subcontractor, nor any person on his/her behalf shall, in any manner, discriminate against or intimidate any employee engaged in the performance of work under this contract or any subcontract hereunder, or engaged in the procurement, manufacture, assembling or furnishing of any such materials, equipment, supplies or services to be acquired under such contract, on account of race, creed, color, national origin, ancestry, marital status, gender identity or expression, affectional or sexual orientation or sex;

C. There may be deducted from the amount payable to the contractor by the contracting public agency, under this contract, a penalty of $50.00 for each person for each calendar day during which such person is discriminated against or intimidated in violation of the provisions of the contract; and

D. This contract may be canceled or terminated by the contracting public agency, and all money due or to become due hereunder may be forfeited, for any violation of this section of the contract occurring after notice to the contractor from the contracting public agency of any prior violation of this section of the contract.

N.J.S.A. 10:5-33 and N.J.A.C. 17:27-3.5 require that during the performance of this contract, the contractor must agree as follows:

A. The contractor or subcontractor, where applicable, will not discriminate against any employee or applicant for employment because of age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex. Except with respect to affectional or sexual orientation and gender identity or expression, the contractor will take affirmative action to ensure that such applicants are recruited and employed, and that employees are treated during employment, without regard to their age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex. Such action shall include, but not be limited to the following: employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the contracting officer setting forth the provisions of this nondiscrimination clause;

B. The contractor or subcontractor, where applicable will, in all solicitations or advertisements for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex;

C. The contractor or subcontractor where applicable, will send to each labor union or representative of workers with which it has a collective bargaining agreement or other contract or understanding, a notice, to be provided by the agency contracting officer, advising the labor union or workers' representative of the contractor's commitments under this act and shall post copies of the notice in conspicuous places available to employees and applicants for employment, N.J.A.C. 17:27-3.7 requires all contractors and subcontractors, if any, to further agree as follows:

   1. The contractor or subcontractor agrees to make good faith efforts to meet targeted county employment goals established in accordance with N.J.A.C. 17:27-5.2;
   2. The contractor or subcontractor agrees to inform in writing its appropriate recruitment agencies including, but not limited to, employment agencies, placement bureaus, colleges, universities, and labor unions, that it does not discriminate on the basis of age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex, and that it will discontinue the use of any recruitment agency which engages in direct or indirect discriminatory practices;
   3. The contractor or subcontractor agrees to revise any of its testing procedures, if necessary, to assure that all personnel testing conforms with the principles of job-related testing, as established by the statutes and court decisions of the State of New Jersey and as established by applicable Federal law and applicable Federal court decisions; and
   4. In conforming with the targeted employment goals, the contractor or subcontractor agrees to review all procedures relating to transfer, upgrading, downgrading and layoff to ensure that all such actions are taken without regard to age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex, consistent with the statutes and court decisions of the State of New Jersey, and applicable Federal law and applicable Federal court decisions.

3.5 BUILDING SERVICE

Pursuant to N.J.S.A. 34:11-56.58 et seq., in any contract for building services, as defined in N.J.S.A. 34:11-56.59, the employees of the contractor

or subcontractors shall be paid prevailing wage for building services rates, as defined in N.J.S.A. 34:11.56.59. The prevailing wage shall be adjusted annually during the term of the contract.

3.6 THE WORKER AND COMMUNITY RIGHT TO KNOW ACT

The provisions of N.J.S.A. 34:5A-1 et seq. which require the labeling of all containers of hazardous substances are applicable to this contract. Therefore, all goods offered for purchase to the State must be labeled by the contractor in compliance with the provisions of the statute.

3.7 SERVICE PERFORMANCE WITHIN U.S.

Under N.J.S.A. 52:34-13.2, all contracts primarily for services awarded by the Director shall be performed within the United States, except when the Director certifies in writing a finding that a required service cannot be provided by a contractor or subcontractor within the United States and the certification is approved by the State Treasurer.

A shift to performance of services outside the United States during the term of the contract shall be deemed a breach of contract. If, during the term of the contract, the contractor or subcontractor, proceeds to shift the performance of any of the services outside the United States, the contractor shall be deemed to be in breach of its contract, which contract shall be subject to termination for cause pursuant to Section 5.7(b) (1) of the Standard Terms and Conditions, unless previously approved by the Director and the Treasurer.

3.8 BUY AMERICAN

Pursuant to N.J.S.A. 52:32-1, if manufactured items or farm products will be provided under this contract to be used in a public work, they shall be manufactured or produced in the United States, whenever available, and the contractor shall be required to so certify.

3.9 DOMESTIC MATERIALS

Pursuant to N.J.S.A. 52:33-2 et seq., if the contract is for the construction, alteration or repair of any public work, the contractor and all subcontractors shall use only domestic materials in the performance of the work unless otherwise noted in the specifications.

3.10 DIANE B. ALLEN EQUAL PAY ACT

Pursuant to N.J.S.A. 34:11-56.14 and N.J.A.C. 12:10-1.1 et seq., a contractor performing "qualifying services" or "public work" to the State or any agency or instrumentality of the State shall provide the Commissioner of Labor and Workforce Development a report regarding the compensation and hours worked by employees categorized by gender, race, ethnicity, and job category. For more information and report templates see https://nj.gov/labor/equalpay/equalpay.html.

3.11 EMPLOYEE MISCLASSIFICATION

In accordance with Governor Murphy's Executive Order #25 and the Task Force's July 2019 Report, employers are required to properly classify their employees. Workers are presumed to be employees and not independent contractors, unless the employer can demonstrate all three factors of the "ABC Test" below:

A. Such individual has been and will continue to be free from control or direction of the performance of such service, but under his or her contract of service and in fact; and
B. Such service is either outside the usual course of business for which such service is performed, or that such service is performed outside of all places of business of the enterprise for which such service is performed; and
C. Such individual is customarily engaged in an independently established trade, occupation, profession or business.

This test has been adopted by New Jersey under its Wage & Hour, Wage Payment and Unemployment Insurance Laws to determine whether a worker is properly classified. Under N.J.S.A. 34:1A-1.17-1.19, the Department of Labor and Workforce Development has the authority to investigate potential violations of these laws and issue penalties and stop work order to employers found to be in violation of the laws.

3.12 CYBERSECURITY INCIDENT REPORTING REQUIREMENT

Pursuant to N.J.S.A. 52:17B-193.2 et seq. (P.L.2023, c.19), Contractors that have access to, or host the State's network(s), system(s), application(s), or information shall report Cybersecurity Incidents to the New Jersey Office of Homeland Security and Preparedness (NJ OHSP) at https://www.cyber.nj.gov/report/ within 72 hours of when the Contractor reasonably believes that a Cybersecurity Incident has occurred.

Consistent with N.J.S.A. 52:17B-193.2, "Cybersecurity Incident" means a malicious or suspicious event occurring on or conducted through a computer network that jeopardizes the integrity, confidentiality, or availability of an information system or the information the system processes, stores, or transmits.

Consistent with N.J.S.A. 52:17B-193.3(f), any Cybersecurity Incident notification submitted to the NJ OHSP shall be deemed confidential, non-public, and not subject to the provisions of P.L.1963, c.73 (C.47:1A-1 et seq.), commonly known as the New Jersey Open Public Records Act, as amended and supplemented, and may not be discoverable in any civil or criminal action or subject to subpoena, unless the subpoena is issued by the New Jersey State Legislature and deemed necessary for the purposes of legislative oversight.

This reporting required by N.J.S.A. 52:17B-193.2 et seq. (P.L.2023, c.19) to NJ OHSP is in addition to the Contractor's responsibility to report Security Incidents as may be set forth in Contract Scope of Work or the Waivered Contracts Supplement to the State of New Jersey Terms and

Conditions. If the Waivered Contracts Supplement is not made part of the contract and a notification period is not specified in the Contract Scope of Work, the Contractor shall give notice of the Cybersecurity Incident to the Using Agency as soon as practicable, but no less than one business day, after the Contractor reasonably believes that a Cyber Security Incident has occurred.

4.0 INDEMNIFICATION AND INSURANCE

4.1 INDEMNIFICATION

The contractor's liability to the State and its employees in third party suits shall be as follows:

A. Indemnification for Third Party Claims - The contractor shall assume all risk of and responsibility for, and agrees to indemnify, defend, and save harmless the State of New Jersey and its employees from and against any and all claims, demands, suits, actions, recoveries, judgments and costs and expenses in connection therewith which shall arise from or result directly or indirectly from the work and/or materials supplied under this contract, including liability of any nature or kind for or on account of the use of any copyrighted or uncopyrighted composition, secret process, patented or unpatented invention, article or appliance furnished or used in the performance of this contract;

B. The contractor's indemnification and liability under subsection (A) is not limited by, but is in addition to the insurance obligations contained in Section 4.2 of these Terms and Conditions; and

C. In the event of a patent and copyright claim or suit, the contractor, at its option, may: (1) procure for the State of New Jersey the legal right to continue the use of the product; (2) replace or modify the product to provide a non-infringing product that is the functional equivalent; or (3) refund the purchase price less a reasonable allowance for use that is agreed to by both parties.

4.2 INSURANCE

The contractor shall secure and maintain in force for the term of the contract insurance as provided herein. All required insurance shall be provided by insurance companies with an A-VIII or better rating by A.M. Best & Company. All policies must be endorsed to provide 30 days' written notice of cancellation or material change to the State of New Jersey at the address shown below. If the contractor's insurer cannot provide 30 days written notice, then it will become the obligation of the contractor to provide the same. The contractor shall provide the State with current certificates of insurance for all coverages and renewals thereof. Renewal certificates shall be provided within 30 days of the expiration of the insurance. The contractor shall not begin to provide services or goods to the State until evidence of the required insurance is provided. The certificates of insurance shall indicate the contract number or purchase order number and title of the contract in the Description of Operations box and shall list the State of New Jersey, Department of the Treasury, Division of Purchase & Property, Contract Compliance & Audit Unit, P.O. Box 236, Trenton, New Jersey 08625 in the Certificate Holder box. The certificates and any notice of cancelation shall be emailed to the State at: ccau.certificate@treas.nj.gov

The insurance to be provided by the contractor shall be as follows:

A. Occurrence Form Commercial General Liability Insurance or its equivalent: The minimum limit of liability shall be $1,000,000 per occurrence as a combined single limit for bodily injury and property damage. The above required Commercial General Liability Insurance policy or its equivalent shall name the State, its officers, and employees as "Additional Insureds" and include the blanket additional insured endorsement or its equivalent. The coverage to be provided under these policies shall be at least as broad as that provided by the standard basic Commercial General Liability Insurance occurrence coverage forms or its equivalent currently in use in the State of New Jersey, which shall not be circumscribed by any endorsement limiting the breadth of coverage;

B. Automobile Liability Insurance which shall be written to cover any automobile used by the insured. Limits of liability for bodily injury and property damage shall not be less than $1,000,000 per occurrence as a combined single limit. The State must be named as an "Additional Insured" and a blanket additional insured endorsement or its equivalent must be provided when the services being procured involve vehicle use on the State's behalf or on State controlled property;

C. Worker's Compensation Insurance applicable to the laws of the State of New Jersey and Employers Liability Insurance with limits not less than:

1. $1,000,000 BODILY INJURY, EACH OCCURRENCE;
2. $1,000,000 DISEASE EACH EMPLOYEE; and
3. $1,000,000 DISEASE AGGREGATE LIMIT.

This $1,000,000 amount may be raised when deemed necessary by the Director;

In the case of a contract entered into pursuant to N.J.S.A. 52:32-17 et seq., (small business set asides) the minimum amount of insurance coverage in subsections A, B, and B. above may be amended for certain commodities when deemed in the best interests of the State by the Director.

5.0 TERMS GOVERNING ALL CONTRACTS

5.1 CONTRACTOR IS INDEPENDENT CONTRACTOR

The contractor's status shall be that of any independent contractor and not as an employee of the State.

5.2 FORCE MAJEURE

Neither party will be liable to the other for any delay or inability to perform its obligations if such delay or inability arises from any act of God, fire,

natural disaster, act of war (declared or undeclared), act of terrorism (domestic or international), riot, civil disturbance, pandemic or other public health crisis (arising during the term of the contract) In the event of such a delay or inability to perform, the time for performance will be extended by an amount reasonable under the specific circumstances and mutually agreed-upon date sufficient to allow Vendor to perform the work delayed by the force majeure.

5.3 CONTRACT TERM AND EXTENSION OPTION

If, in the opinion of the Director, it is in the best interest of the State to extend a contract, the contractor shall be so notified of the Director's Intent at least 30 days prior to the expiration date of the existing contract. The contractor shall have 15 calendar days to respond to the Director's request to extend the term and period of performance of the contract. If the contractor agrees to the extension, all terms and conditions of the original contract shall apply unless more favorable terms for the State have been negotiated.

5.4 STATE'S OPTION TO REDUCE SCOPE OF WORK

The State has the option, in its sole discretion, to reduce the scope of work for any deliverable, task or subtask called for under this contract. In such an event, the Director shall provide to the contractor advance written notice of the change in scope of work and what the Director believes should be the corresponding adjusted contract price. Within five (5) business days of receipt of such written notice, if either is applicable:

A. If the contractor does not agree with the Director's proposed adjusted contract price, the contractor shall submit to the Director any additional information that the contractor believes impacts the adjusted contract price with a request that the Director reconsider the proposed adjusted contract price. The parties shall negotiate the adjusted contract price. If the parties are unable to agree on an adjusted contract price, the Director shall make a prompt decision taking all such information into account, and shall notify the contractor of the final adjusted contract price; and

B. If the contractor has undertaken any work effort toward a deliverable, task or subtask that is being changed or eliminated such that it would not be compensated under the adjusted contract, the contractor shall be compensated for such work effort according to the applicable portions of its price schedule and the contractor shall submit to the Director an itemization of the work effort already completed by deliverable, task or subtask within the scope of work, and any additional information the Director may request. The Director shall make a prompt decision taking all such information into account, and shall notify the contractor of the compensation to be paid for such work effort.

Any changes or modifications to the terms of this Contract shall be valid only when they have been reduced to writing and signed by the Contractor and the Director.

5.5 CHANGE IN LAW

If, after award, a change in applicable law or regulation occurs which affects the Contract, the parties may amend the Contract, whether including new work required by the change in law or to eliminate work no longer required by the change in law along with a commensurate price change. The parties shall negotiate the terms of the change in good faith, however if agreement is not possible after reasonable efforts, the Director shall make a prompt decision taking all relevant information into account, and shall notify the Contractor of the final adjusted scope of work and contract price.

5.6 SUSPENSION OF WORK

The State may, for valid reason, issue a stop order directing the contractor to suspend work under the contract for a specific time. The contractor shall be paid for goods ordered, goods delivered, or services requested and performed until the effective date of the stop order. The contractor shall resume work upon the date specified in the stop order, or upon such other date as the State Contract Manager may thereafter direct in writing. The period of suspension shall be deemed added to the contractor's approved schedule of performance.

5.7 TERMINATION OF CONTRACT

A. For Convenience:
Notwithstanding any provision or language in this contract to the contrary, the Director may terminate this contract at any time, in whole or in part, for the convenience of the State, upon no less than 30 days written notice to the contractor;

B. For Cause:
   1. Where a contractor fails to perform or comply with a contract or a portion thereof, and/or fails to comply with the complaints procedure in N.J.A.C. 17:12-4.2 et seq., the Director may terminate the contract, in whole or in part, upon ten (10) days' notice to the contractor with an opportunity to respond; and
   2. Where in the reasonable opinion of the Director, a contractor continues to perform a contract poorly as demonstrated by e.g., formal complaints, late delivery, poor performance of service, short-shipping, so that the Director is required to use the complaints procedure in N.J.A.C. 17:12-4.2 et seq., and there has been a failure on the part of the contractor to make progress towards ameliorating the issue(s) or problem(s) set forth in the complaint, the Director may terminate the contract, in whole or in part, upon ten (10) days' notice to the contractor with an opportunity to respond.

C. In cases of emergency the Director may shorten the time periods of notification and may dispense with an opportunity to respond; and

D. In the event of termination under this section, the contractor shall be compensated for work performed in accordance with the contract, up to the date of termination. Such compensation may be subject to adjustments.

5.8 SUBCONTRACTING

The Contractor may not subcontract other than as identified in the contractor's proposal without the prior written consent of the Director. Such

consent, if granted in part, shall not relieve the contractor of any of his/her responsibilities under the contract, nor shall it create privity of contract between the State and any subcontractor. If the contractor uses a subcontractor to fulfill any of its obligations, the contractor shall be responsible for the subcontractor's: (a) performance; (b) compliance with all of the terms and conditions of the contract; and (c) compliance with the requirements of all applicable laws. Nothing contained in any of the contract documents, shall be construed as creating any contractual relationship between any subcontractor and the State.

5.9 RESERVED

5.10 MERGERS, ACQUISITIONS AND ASSIGNMENTS

If, during the term of this contract, the contractor shall merge with or be acquired by another firm, the contractor shall give notice to the Director as soon as practicable and in no event longer than 30 days after said merger or acquisition. The contractor shall provide such documents as may be requested by the Director, which may include but need not be limited to the following: corporate resolutions prepared by the awarded contractor and new entity ratifying acceptance of the original contract, terms, conditions and prices; updated information including ownership disclosure and Federal Employer Identification Number. The documents must be submitted within 30 days of the request. Failure to do so may result in termination of the contract for cause.

If, at any time during the term of the contract, the contractor's partnership, limited liability company, limited liability partnership, professional corporation, or corporation shall dissolve, the Director must be so notified. All responsible parties of the dissolved business entity must submit to the Director in writing, the names of the parties proposed to perform the contract, and the names of the parties to whom payment should be made. No payment shall be made until all parties to the dissolved business entity submit the required documents to the Director.

The contractor may not assign its responsibilities under the contract, in whole or in part, without the prior written consent of the Director.

5.11 PERFORMANCE GUARANTEE OF CONTRACTOR

The contractor hereby certifies that:

A. The equipment offered is standard new equipment, and is the manufacturer's latest model in production, with parts regularly used for the type of equipment offered; that such parts are all in production and not likely to be discontinued; and that no attachment or part has been substituted or applied contrary to manufacturer's recommendations and standard practice;
B. All equipment supplied to the State and operated by electrical current is UL listed where applicable;
C. All new machines are to be guaranteed as fully operational for the period stated in the contract from time of written acceptance by the State. The contractor shall render prompt service without charge, regardless of geographic location;
D. Sufficient quantities of parts necessary for proper service to equipment shall be maintained at distribution points and service headquarters;
E. Trained mechanics are regularly employed to make necessary repairs to equipment in the territory from which the service request might emanate within a 48-hour period or within the time accepted as industry practice;
F. During the warranty period the contractor shall replace immediately any material which is rejected for failure to meet the requirements of the contract; and
G. All services rendered to the State shall be performed in strict and full accordance with the specifications stated in the contract. The contract shall not be considered complete until final approval by the State's using agency is rendered.

5.12 DELIVERY REQUIREMENTS

A. Deliveries shall be made at such time and in such quantities as ordered in strict accordance with conditions contained in the contract;
B. The contractor shall be responsible for the delivery of material in first class condition to the State's using agency or the purchaser under this contract and in accordance with good commercial practice;
C. Items delivered must be strictly in accordance with the contract; and
D. In the event delivery of goods or services is not made within the number of days stipulated or under the schedule defined in the contract, the using agency shall be authorized to obtain the material or service from any available source, the difference in price, if any, to be paid by the contractor.

5.13 APPLICABLE LAW AND JURISDICTION

This contract and any and all litigation arising therefrom or related thereto shall be governed by the applicable laws, regulations and rules of evidence of the State of New Jersey without reference to conflict of laws principles and shall be filed in the appropriate Division of the New Jersey Superior Court.

5.14 CONTRACT AMENDMENT

Except as provided herein, the contract may only be amended by written agreement of the State and the contractor.

5.15 MAINTENANCE OF RECORDS AND AUDITS

A. Pursuant to N.J.A.C. 17:44-2.2, the contractor shall maintain all documentation related to products, transactions or services under this contract for a period of five (5) years from the date of final payment. Such records shall be made available to the New Jersey Office of the State Comptroller upon request.
B. The State may request, receive, review, and audit copies of any and all records and documents related to a State contract at any time. The Contractor shall make a good faith effort to cooperate with the request and upon receipt of the request, the Contractor shall promptly provide

the requested records and documents free of charge in the time, place, and manner specified. Failure of the contractor to comply with the request or the audit may be used by the State to establish contract non-compliance, to take any action, or seek any remedy available under the contract, at law, or in equity.

5.16 ASSIGNMENT OF ANTITRUST CLAIM(S)

The contractor recognizes that in actual economic practice, overcharges resulting from antitrust violations are in fact usually borne by the ultimate purchaser. Therefore, and as consideration for executing this contract, the contractor, acting herein by and through its duly authorized agent, hereby conveys, sells, assigns, and transfers to the State of New Jersey, for itself and on behalf of its political subdivisions and public agencies, all right, title and interest to all claims and causes of action it may now or hereafter acquire under the antitrust laws of the United States or the State of New Jersey, relating to the particular goods and services purchased or acquired by the State of New Jersey or any of its political subdivisions or public agencies pursuant to this contract.

In connection with this assignment, the following are the express obligations of the contractor:

A. It shall take no action that will in any way diminish the value of the rights conveyed or assigned hereunder;
B. It shall advise the Attorney General of New Jersey:
    1. In advance of its intention to commence any action on its own behalf regarding any such claim or cause(s) of action; and
    2. Immediately upon becoming aware of the fact that an action has been commenced on its behalf by some other person(s) of the pendency of such action.
C. It shall notify the defendants in any antitrust suit of the within assignment at the earliest practicable opportunity after the contractor has initiated an action on its own behalf or becomes aware that such an action has been filed on its behalf by another person. A copy of such notice shall be sent to the Attorney General of New Jersey; and
D. It is understood and agreed that in the event any payment under any such claim or cause of action is made to the contractor, it shall promptly pay over to the State of New Jersey the allotted share thereof, if any, assigned to the State hereunder.

5.17 NEWS RELEASES

The Contractor is not permitted to issue news releases pertaining to any aspect of the services being provided under this Contract without the prior written consent of the Director.

5.18 ADVERTISING

The Contractor shall not use the State's name, seal, or logos as a part of any commercial advertising without first obtaining the prior written consent of the New Jersey Secretary of State. The Contractor shall not use a Department or Using Agency's name, seal, logos, images, or any data or results arising from this Contract as a part of any commercial advertising without first obtaining the prior written consent of the Department.

5.19 ORGAN DONATION

As required by N.J.S.A. 52:32-33.1, the State encourages the contractor to disseminate information relative to organ donation and to notify its employees, through information and materials or through an organ and tissue awareness program, of organ donation options. The information provided to employees should be prepared in collaboration with the organ procurement organizations designated pursuant to 42 U.S.C. 1320b-8 to serve in this State.

5.20 LICENSES AND PERMITS

The Contractor shall obtain and maintain in full force and effect all required licenses, permits, and authorizations necessary to perform this Contract. Notwithstanding the requirements of the Bid Solicitation, the Contractor shall supply the State Contract Manager with evidence of all such licenses, permits and authorizations. This evidence shall be submitted subsequent to this Contract award. All costs associated with any such licenses, permits, and authorizations must be considered by the Contractor in its Quote.

5.21 CLAIMS AND REMEDIES

A. All claims asserted against the State by the Contractor shall be subject to the New Jersey Tort Claims Act, N.J.S.A. 59:1-1, et seq., and/or the New Jersey Contractual Liability Act, N.J.S.A. 59:13-1, et seq.
B. Nothing in this Contract shall be construed to be a waiver by the State of any warranty, expressed or implied, of any remedy at law or equity, except as specifically and expressly stated in a writing executed by the Director.
C. In the event that the Contractor fails to comply with any material Contract requirements, the Director may take steps to terminate this Contract in accordance with the SSTC, authorize the delivery of Contract items by any available means, with the difference between the price paid and the defaulting Contractor's price either being deducted from any monies due the defaulting Contractor or being an obligation owed the State by the defaulting Contractor, as provided for in the State administrative code, or take any other action or seek any other remedies available at law or in equity.

5.22 ACCESSIBILITY COMPLIANCE

The Contractor acknowledges that the State may be required to comply with the accessibility standards of Section 508 of the Rehabilitation Act, 29 U.S.C. §794. The Contractor agrees that any information that it provides to the State in the form of a Voluntary Product Accessibility Template (VPAT) about the accessibility of the Software is accurate to a commercially reasonable standard and the Contractor agrees to provide the State with technical information available to support such VPAT documentation in the event that the State relied on any of Contractor's VPAT information to comply with the accessibility standards of Section 508 of the Rehabilitation Act, 29 U.S.C. §794. In addition, Contractor shall defend any claims

against the State that the Software does not meet the accessibility standards set forth in the VPAT provided by Provider in order to comply with the accessibility standards of Section 508 of the Rehabilitation Act, 29 U.S.C. §794 and will indemnify the State with regard to any claim made against the State with regard to any judgment or settlement resulting from those claims to the extent the Provider's Software provided under this Contract was not accessible in the same manner as or to the degree set forth in the Contractor's statements or information about accessibility as set forth in the then-current version of an applicable VPAT.

5.23 CONFIDENTIALITY

A. The obligations of the State under this provision are subject to the New Jersey Open Public Records Act ("OPRA"), N.J.S.A. 47:1A-1 et seq., the New Jersey common law right to know, and any other lawful document request or subpoena;

B. By virtue of this Contract, the parties may have access to information that is confidential to one another. The parties agree to disclose to each other only information that is required for the performance of their obligations under this Contract. Contractor's Confidential Information, to the extent not expressly prohibited by law, shall consist of all information clearly identified as confidential at the time of disclosure Vendor Intellectual Property ("Contractor Confidential Information"). Notwithstanding the previous sentence, the terms and pricing of this Contract are subject to disclosure under OPRA, the common law right to know, and any other lawful document request or subpoena;

C. The State's Confidential Information shall consist of all information or data contained in documents supplied by the State, any information or data gathered by the Contractor in fulfillment of the Contract and any analysis thereof (whether in fulfillment of the Contract or not);

D. A party's Confidential Information shall not include information that: (a) is or becomes a part of the public domain through no act or omission of the other party, except that if the information is personally identifying to a person or entity regardless of whether it has become part of the public domain through other means, the other party must maintain full efforts under the Contract to keep it confidential; (b) was in the other party's lawful possession prior to the disclosure and had not been obtained by the other party either directly or indirectly from the disclosing party; (c) is lawfully disclosed to the other party by a third party without restriction on the disclosure; or (d) is independently developed by the other party;

E. The State agrees to hold Contractor's Confidential Information in confidence, using at least the same degree of care used to protect its own Confidential Information;

F. In the event that the State receives a request for Contractor Confidential Information related to this Contract pursuant to a court order, subpoena, or other operation of law, the State agrees, if permitted by law, to provide Contractor with as much notice, in writing, as is reasonably practicable and the State's intended response to such order of law. Contractor shall take any action it deems appropriate to protect its documents and/or information;

G. In addition, in the event Contractor receives a request for State Confidential Information pursuant to a court order, subpoena, or other operation of law, Contractor shall, if permitted by law, provide the State with as much notice, in writing, as is reasonably practicable and Contractor's intended response to such order of law. The State shall take any action it deems appropriate to protect its documents and/or information; and

H. Notwithstanding the requirements of nondisclosure described in this Section, either party may release the other party's Confidential Information:
   (i) if directed to do so by a court or arbitrator of competent jurisdiction; or
   (ii) pursuant to a lawfully issued subpoena or other lawful document request:
      (a) in the case of the State, if the State determines the documents or information are subject to disclosure and Contractor does not exercise its rights as described in Section 5.23(F), or if Contractor is unsuccessful in defending its rights as described in Section 5.23(F); or
      (b) in the case of Contractor, if Contractor determines the documents or information are subject to disclosure and the State does not exercise its rights described in Section 5.23(G), or if the State is unsuccessful in defending its rights as described in Section 5.23(G).

6.0 TERMS RELATING TO PRICE AND PAYMENT

6.1 PRICE FLUCTUATION DURING CONTRACT

Unless otherwise agreed to in writing by the State, all prices quoted shall be firm through issuance of contract or purchase order and shall not be subject to increase during the period of the contract. In the event of a manufacturer's or contractor's price decrease during the contract period, the State shall receive the full benefit of such price reduction on any undelivered purchase order and on any subsequent order placed during the contract period. The Director must be notified, in writing, of any price reduction within five (5) days of the effective date. Failure to report price reductions may result in cancellation of contract for cause, pursuant to provision 5.7(b)1.

In an exceptional situation the State may consider a price adjustment. Requests for price adjustments must include justification and documentation.

6.2 TAX CHARGES

The State of New Jersey is exempt from State sales or use taxes and Federal excise taxes. Therefore, price quotations must not include such taxes. The State's Federal Excise Tax Exemption number is 22-75-0050K.

6.3 PAYMENT TO VENDORS

A. The using agency(ies) is (are) authorized to order and the contractor is authorized to ship only those items covered by the contract

resulting from the RFP. If a review of orders placed by the using agency(ies) reveals that goods and/or services other than that covered by the contract have been ordered and delivered, such delivery shall be a violation of the terms of the contract and may be considered by the Director as a basis to terminate the contract and/or not award the contractor a subsequent contract. The Director may take such steps as are necessary to have the items returned by the agency, regardless of the time between the date of delivery and discovery of the violation. In such event, the contractor shall reimburse the State the full purchase price;

B. The contractor must submit invoices to the using agency with supporting documentation evidencing that work or goods for which payment is sought has been satisfactorily completed or delivered. For commodity contracts, the invoice, together with the Bill of Lading, and/or other documentation to confirm shipment and receipt of contracted goods must be received by the using agency prior to payment. For contracts featuring services, invoices must reference the tasks or subtasks detailed in the Scope of Work and must be in strict accordance with the firm, fixed prices submitted for each task or subtask. When applicable, invoices should reference the appropriate task or subtask or price line number from the contractor's proposal. All invoices must be approved by the State Contract Manager or using agency before payment will be authorized;

C. In all time and materials contracts, the State Contract Manager or designee shall monitor and approve the hours of work and the work accomplished by contractor and shall document both the work and the approval. Payment shall not be made without such documentation. A form of timekeeping record that should be adapted as appropriate for the Scope of Work being performed can be found at www.nj.gov/treasury/purchase/forms/Vendor_Timesheet.xls; and

D. The contractor shall provide, on a monthly and cumulative basis, a breakdown in accordance with the budget submitted, of all monies paid to any small business, minority or woman-owned subcontractor(s). This breakdown shall be sent to the Office of Diversity and Inclusion.

E. The Contractor shall have sole responsibility for all payments due any Subcontractor

6.4 OPTIONAL PAYMENT METHOD: P-CARD

The State offers contractors the opportunity to be paid through the MasterCard procurement card (p-card). A contractor's acceptance and a State agency's use of the p-card are optional. P-card transactions do not require the submission of a contractor invoice; purchasing transactions using the p-card will usually result in payment to a contractor in three (3) days. A contractor should take note that there will be a transaction-processing fee for each p-card transaction. To participate, a contractor must be capable of accepting the MasterCard. Additional information can be obtained from banks or merchant service companies.

6.5 NEW JERSEY PROMPT PAYMENT ACT

The New Jersey Prompt Payment Act, N.J.S.A. 52:32-32 et seq., requires state agencies to pay for goods and services within 60 days of the agency's receipt of a properly executed State Payment Voucher or within 60 days of receipt and acceptance of goods and services, whichever is later. Properly executed performance security, when required, must be received by the State prior to processing any payments for goods and services accepted by state agencies. Interest will be paid on delinquent accounts at a rate established by the State Treasurer. Interest shall not be paid until it exceeds $5.00 per properly executed invoice. Cash discounts and other payment terms included as part of the original agreement are not affected by the Prompt Payment Act.

6.6 AVAILABILITY OF FUNDS

The State's obligation to make payment under this contract is contingent upon the availability of appropriated funds and receipt of revenues from which payment for contract purposes can be made. No legal liability on the part of the State for payment of any money shall arise unless and until funds are appropriated each fiscal year to the using agency by the State Legislature and made available through receipt of revenue.

7.0 TERMS RELATING TO ALL CONTRACTS FUNDED, IN WHOLE OR IN PART, BY FEDERAL FUNDS

The provisions set forth in this Section of the Standard Terms and Conditions apply to all contracts funded, in whole or in part, by Federal funds as required by 2 CFR 200.317.

7.1 CONTRACTING WITH SMALL AND MINORITY BUSINESSES, WOMEN'S BUSINESS ENTERPRISES, AND LABOR SURPLUS AREA FIRMS.

Pursuant to 2 CFR 200.321, the State must take all necessary affirmative steps to assure that minority businesses, women's business enterprises, and labor surplus area firms are used when possible. Accordingly, if subawards are to be made the Contractor shall:

(1) Include qualified small and minority businesses and women's business enterprises on solicitation lists;
(2) Assure that small and minority businesses, and women's business enterprises are solicited whenever they are potential sources;
(3) Divide total requirements, when economically feasible, into smaller tasks or quantities to permit maximum participation by small and minority businesses, and women's business enterprises;
(4) Establish delivery schedules, where the requirement permits, which encourage participation by small and minority businesses, and women's business enterprises; and,
(5) Use the services and assistance, as appropriate, of such organizations as the Small Business Administration and the Minority Business Development Agency of the Department of Commerce.

7.2 DOMESTIC PREFERENCE FOR PROCUREMENTS

Pursuant to 2 CFR 200.322, where appropriate, the State has a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United States (including but not limited to iron, aluminum, steel, cement, and other manufactured products). If subawards are to be made the Contractor shall include a preference for the purchase, acquisition, or use of goods, products, or materials produced in the United

States (including but not limited to iron, aluminum, steel, cement, and other manufactured products). For purposes of this section:

(1) "Produced in the United States" means, for iron and steel products, that all manufacturing processes, from the initial melting stage through the application of coatings, occurred in the United States.

(2) "Manufactured products" means items and construction materials composed in whole or in part of nonferrous metals such as aluminum; plastics and polymer-based products such as polyvinyl chloride pipe; aggregates such as concrete; glass, including optical fiber; and lumber.

7.3 PROCUREMENT OF RECOVERED MATERIALS

Where applicable, in the performance of contract, pursuant to 2 CFR 200.323, the contractor must comply with section 6002 of the Solid Waste Disposal Act, as amended by the Resource Conservation and Recovery Act. The requirements of Section 6002 include procuring only items designated in guidelines of the Environmental Protection Agency (EPA) at 40 CFR Part 247 that contain the highest percentage of recovered materials practicable, consistent with maintaining a satisfactory level of competition, where the purchase price of the item exceeds $ 10,000 or the value of the quantity acquired during the preceding fiscal year exceeded $10,000; procuring solid waste management services in a manner that maximizes energy and resource recovery; and establishing an affirmative procurement program for procurement of recovered materials identified in the EPA guidelines.

To the extent that the scope of work or specifications in the contract requires the contractor to provide recovered materials the scope of work or specifications are modified to require that as follows.

i. In the performance of this contract, the Contractor shall make maximum use of products containing recovered materials that are EPA-designated items unless the product cannot be acquired—
   1. Competitively within a timeframe providing for compliance with the contract performance schedule;
   2. Meeting contract performance requirements; or
   3. At a reasonable price.

ii. Information about this requirement, along with the list of EPA- designated items, is available at EPA's Comprehensive Procurement Guidelines web site, https://www.epa.gov/smm/comprehensive- procurement-guideline-cpg-program.

iii. The Contractor also agrees to comply with all other applicable requirements of Section 6002 of the Solid Waste Disposal Act."

7.4 EQUAL EMPLOYMENT OPPORTUNITY

Except as otherwise provided under 41 CFR Part 60, all contracts that meet the definition of "federally assisted construction contract" in 41 CFR Part 60-1.3 must include the equal opportunity clause provided under 41 CFR 60-1.4(b), in accordance with Executive Order 11246, "Equal Employment Opportunity" (30 FR 12319, 12935, 3 CFR Part, 1964-1965 Comp., p. 339), as amended by Executive Order 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and implementing regulations at 41 CFR part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor." See, 2 CFR Part 200, Appendix II, para. C.

During the performance of this contract, the contractor agrees as follows:

(1) The contractor will not discriminate against any employee or applicant for employment because of race, color, religion, sex, sexual orientation, gender identity, or national origin. The contractor will take affirmative action to ensure that applicants are employed, and that employees are treated during employment without regard to their race, color, religion, sex, sexual orientation, gender identity, or national origin. Such action shall include, but not be limited to the following:

Employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided setting forth the provisions of this nondiscrimination clause.

(2) The contractor will, in all solicitations or advertisements for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to race, color, religion, sex, sexual orientation, gender identity, or national origin.

(3) The contractor will not discharge or in any other manner discriminate against any employee or applicant for employment because such employee or applicant has inquired about, discussed, or disclosed the compensation of the employee or applicant or another employee or applicant. This provision shall not apply to instances in which an employee who has access to the compensation information of other employees or applicants as a part of such employee's essential job functions discloses the compensation of such other employees or applicants to individuals who do not otherwise have access to such information, unless such disclosure is in response to a formal complaint or charge, in furtherance of an investigation, proceeding, hearing, or action, including an investigation conducted by the employer, or is consistent with the contractor's legal duty to furnish information.

(4) The contractor will send to each labor union or representative of workers with which he/she has a collective bargaining agreement or other contract or understanding, a notice to be provided advising the said labor union or workers' representatives of the contractor's commitments under this section, and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

(5) The contractor will comply with all provisions of Executive Order 11246 of September 24, 1965, and of the rules, regulations, and relevant orders of the Secretary of Labor.

(6) The contractor will furnish all information and reports required by Executive Order 11246 of September 24, 1965, and by rules, regulations, and orders of the Secretary of Labor, or pursuant thereto, and will permit access to his/her books, records, and accounts by the administering agency and the Secretary of Labor for purposes of investigation to ascertain compliance with such rules,

regulations, and orders.

(7) In the event of the contractor's noncompliance with the nondiscrimination clauses of this contract or with any of the said rules, regulations, or orders, this contract may be canceled, terminated, or suspended in whole or in part and the contractor may be declared ineligible for further Government contracts or federally assisted construction contracts in accordance with procedures authorized in Executive Order 11246 of September 24, 1965, and such other sanctions may be imposed and remedies invoked as provided in Executive Order 11246 of September 24, 1965, or by rule, regulation, or order of the Secretary of Labor, or as otherwise provided by law.

(8) The contractor will include the portion of the sentence immediately preceding paragraph (1) and the provisions of paragraphs (1) through (8) in every subcontract or purchase order unless exempted by rules, regulations, or orders of the Secretary of Labor issued pursuant to section 204 of Executive Order 11246 of September 24, 1965, so that such provisions will be binding upon each subcontractor or vendor. The contractor will take such action with respect to any subcontract or purchase order as the administering agency may direct as a means of enforcing such provisions, including sanctions for noncompliance:

Provided, however, that in the event a contractor becomes involved in, or is threatened with, litigation with a subcontractor or vendor as a result of such direction by the administering agency, the contractor may request the United States to enter into such litigation to protect the interests of the United States.

The applicant further agrees that it will be bound by the above equal opportunity clause with respect to its own employment practices when it participates in federally assisted construction work: Provided, That if the applicant so participating is a State or local government, the above equal opportunity clause is not applicable to any agency, instrumentality or subdivision of such government which does not participate in work on or under the contract.

The applicant agrees that it will assist and cooperate actively with the administering agency and the Secretary of Labor in obtaining the compliance of contractors and subcontractors with the equal opportunity clause and the rules, regulations, and relevant orders of the Secretary of Labor, that it will furnish the administering agency and the Secretary of Labor such information as they may require for the supervision of such compliance, and that it will otherwise assist the administering agency in the discharge of the agency's primary responsibility for securing compliance.

The applicant further agrees that it will refrain from entering into any contract or contract modification subject to Executive Order 11246 of September 24, 1965, with a contractor debarred from, or who has not demonstrated eligibility for, Government contracts and federally assisted construction contracts pursuant to the Executive Order and will carry out such sanctions and penalties for violation of the equal opportunity clause as may be imposed upon contractors and subcontractors by the administering agency or the Secretary of Labor pursuant to Part II, Subpart D of the Executive Order. In addition, the applicant agrees that if it fails or refuses to comply with these undertakings, the administering agency may take any or all of the following actions: Cancel, terminate, or suspend in whole or in part this grant (contract, loan, insurance, guarantee); refrain from extending any further assistance to the applicant under the program with respect to which the failure or refund occurred until satisfactory assurance of future compliance has been received from such applicant; and refer the case to the Department of Justice for appropriate legal proceedings.

7.5 DAVIS-BACON ACT, 40 U.S.C. 3141-3148, AS AMENDED

When required by Federal program legislation, all prime construction contracts in excess of $ 2,000 shall be done in compliance with the Davis-Bacon Act (40 U.S.C. 3141- 3144, and 3146-3148) and the requirements of 29 C.F.R. pt. 5 as may be applicable. The contractor shall comply with 40 U.S.C. 3141-3144, and 3146-3148 and the requirements of 29 C.F.R. pt. 5 as applicable. Contractors are required to pay wages to laborers and mechanics at a rate not less than the prevailing wages specified in a wage determination made by the Secretary of Labor. Additionally, contractors are required to pay wages not less than once a week.

7.6 COPELAND ANTI-KICK-BACK ACT

Where applicable, the Contractor must comply with Copeland "Anti-Kickback" Act (40 U.S.C. 3145), as supplemented by Department of Labor regulations (29 CFR Part 3, "Contractors and Subcontractors on Public Building or Public Work Financed in Whole or in Part by Loans or Grants from the United States").

a. Contractor. The Contractor shall comply with 18 U.S.C. § 874, 40 U.S.C. § 3145, and the requirements of 29 C.F.R. pt. 3 as may be applicable, which are incorporated by reference into the OGS centralized contract.

b. Subcontracts. The Contractor or subcontractor shall insert in any subcontracts the clause above and such other clauses as FEMA may by appropriate instructions require, and also a clause requiring the subcontractors to include these clauses in any lower tier subcontracts. The prime contractor shall be responsible for the compliance by any subcontractor or lower tier subcontractor with all of these contract clauses.

c. Breach. A breach of the clauses above may be grounds for termination of the OGS centralized contract, and for debarment as a Contractor and subcontractor as provided in 29 C.F.R. § 5.12.

7.7 CONTRACT WORK HOURS AND SAFETY STANDARDS ACT, 40 U.S.C. 3701-3708

Where applicable, all contracts awarded by the non-Federal entity in excess of $ 100,000 that involve the employment of mechanics or laborers must comply with 40 U.S.C. 3702 and 3704, as supplemented by Department of Labor regulations (29 CFR Part 5).

(1) Overtime requirements. No contractor or subcontractor contracting for any part of the contract work which may require or involve the employment of laborers or mechanics shall require or permit any such laborer or mechanic in any workweek in which he or she is employed on such work to work in excess of forty hours in such workweek unless such laborer or mechanic receives compensation at a rate not less than one and one-half times the basic rate of pay for all hours worked in excess of forty hours in such workweek.

(2) Violation; liability for unpaid wages; liquidated damages. In the event of any violation of the clause set forth in paragraph (b)(1) of this section the contractor and any subcontractor responsible therefor shall be liable for the unpaid wages. In addition, such contractor and subcontractor shall be liable to the United States (in the case of work done under contract for the District of Columbia or a territory, to such District or to such territory), for liquidated damages. Such liquidated damages shall be computed with respect to each individual laborer or mechanic, including watchmen and guards, employed in violation of the clause set forth in paragraph (b)(1) of this section, in the sum of $27 for each calendar day on which such individual was required or permitted to work in excess of the standard workweek of forty hours without payment of the overtime wages required by the clause set forth in paragraph (b)(1) of this section.

(3) Withholding for unpaid wages and liquidated damages. The unauthorized user shall upon its own action or upon written request of an authorized representative of the Department of Labor withhold or cause to be withheld, from any moneys payable on account of work performed by the contractor or subcontractor under any such contract or any other Federal contract with the same prime contractor, or any other federally-assisted contract subject to the Contract Work Hours and Safety Standards Act, which is held by the same prime contractor, such sums as may be determined to be necessary to satisfy any liabilities of such contractor or subcontractor for unpaid wages and liquidated damages as provided in the clause set forth in paragraph (b)(2) of this section.

(4) Subcontracts. The contractor or subcontractor shall insert in any subcontracts the clauses set forth in paragraph (b)(1) through (4) of this section and also a clause requiring the subcontractors to include these clauses in any lower tier subcontracts. The prime contractor shall be responsible for compliance by any subcontractor or lower tier subcontractor with the clauses set forth in paragraphs (b)(1) through (4) of this section.

7.8 RIGHTS TO INVENTIONS MADE UNDER A CONTRACT OR AGREEMENT

If the Federal award meets the definition of "funding agreement" under 37 CFR § 401.2 (a) and the recipient or subrecipient wishes to enter into a contract with a small business firm or nonprofit organization regarding the substitution of parties, assignment or performance of experimental, developmental, or research work under that "funding agreement," the recipient or subrecipient must comply with the requirements of 37 CFR Part 401, "Rights to Inventions Made by Nonprofit Organizations and Small Business Firms Under Government Grants, Contracts and Cooperative Agreements," and any implementing regulations issued by the awarding agency.

7.9 CLEAN AIR ACT, 42 U.S.C. 7401-7671Q, AND THE FEDERAL WATER POLLUTION CONTROL ACT, 33 U.S.C. 1251-1387, AS AMENDED

Where applicable, Contract and subgrants of amounts in excess of $150,000, must comply with the following:

Clean Air Act

7.9.1.1 The contractor agrees to comply with all applicable standards, orders or regulations issued pursuant to the Clean Air Act, as amended, 42 U.S.C. § 7401 et seq.

7.9.1.2 The contractor agrees to report each violation to the Division of Purchase and Property and understands and agrees that the Division of Purchase and Property will, in turn, report each violation as required to assure notification to the Federal Emergency Management Agency, and the appropriate Environmental Protection Agency Regional Office.

7.9.1.3 The contractor agrees to include these requirements in each subcontract exceeding $150,000 financed in whole or in part with Federal assistance provided by FEMA.

Federal Water Pollution Control Act

1. The contractor agrees to comply with all applicable standards, orders, or regulations issued pursuant to the Federal Water Pollution Control Act, as amended, 33 U.S.C. 1251 et seq.
2. The contractor agrees to report each violation to the Division of Purchase and Property and understands and agrees that the Division of Purchase and Property will, in turn, report each violation as required to assure notification to the Federal Emergency Management Agency, and the appropriate Environmental Protection Agency Regional Office.
3. The contractor agrees to include these requirements in each subcontract exceeding $150,000 financed in whole or in part with Federal assistance provided by FEMA.

7.10 DEBARMENT AND SUSPENSION (EXECUTIVE ORDERS 12549 AND 12689)

(1) This contract is a covered transaction for purposes of 2 C.F.R. pt. 180 and 2 C.F.R. pt. 3000. As such, the contractor is required to verify that none of the contractor's principals (defined at 2 C.F.R. § 180.995) or its affiliates (defined at 2 C.F.R. § 180.905) are excluded (defined at 2 C.F.R. § 180.940) or disqualified (defined at 2 C.F.R. § 180.935).

(2) The contractor must comply with 2 C.F.R. pt. 180, subpart C and2 C.F.R. pt. 3000, subpart C, and must include a requirement to comply with these regulations in any lower tier covered transaction it enters into.

(3) This certification is a material representation of fact relied upon by the State or authorized user. If it is later determined that the contractor did not comply with 2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C, in addition to remedies available to the State or authorized user, the Federal Government may pursue available remedies, including but not limited to suspension and/or debarment.

(4) The bidder or proposer agrees to comply with the requirements of2 C.F.R. pt. 180, subpart C and 2 C.F.R. pt. 3000, subpart C while this offer is valid and throughout the period of any contract that may arise from this offer. The bidder or proposer further agrees to include a provision requiring such compliance in its lower tier covered transactions.

7.11 BYRD ANTI-LOBBYING AMENDMENT, 31 U.S.C. 1352

Contractors that apply or bid for an award exceeding $100,000 must file the required certification. Each tier certifies to the tier above that it will not and has not used Federal appropriated funds to pay any person or organization for influencing or attempting to influence an officer or employee

of any agency, a member of Congress, officer or employee of Congress, or an employee of a member of Congress in connection with obtaining any Federal contract, grant or any other award covered by 31 U.S.C. 1352. Each tier must also disclose any lobbying with non-Federal funds that takes place in connection with obtaining any Federal award. Such disclosures are forwarded from tier to tier up to the non-Federal award. Such disclosures are forwarded from tier to tier up to the recipient who in turn will forward the certification(s) to the awarding agency.

7.12 PROHIBITION ON CERTAIN TELECOMMUNICATIONS AND VIDEO SURVEILLANCE SERVICES OR EQUIPMENT

(a) Recipients and subrecipients are prohibited from obligating or expending loan or grant funds to:

(1) Procure or obtain;

(2) Extend or renew a contract to procure or obtain; or

(3) Enter into a contract (or extend or renew a contract) to procure or obtain equipment, services, or systems that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. As described in *Public Law 115–232*, section 889, covered telecommunications equipment is telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).

(i) For the purpose of public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).

(ii) Telecommunications or video surveillance services provided by such entities or using such equipment.

(iii) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.

EXHIBIT A - GOODS, GENERAL SERVICE AND PROFESSIONAL SERVICES CONTRACTS

MANDATORY EQUAL EMPLOYMENT OPPORTUNITY LANGUAGE
N.J.S.A. 10:5-31 et seq. (P.L.1975, c.127)
N.J.A.C. 17:27 et seq.

During the performance of this contract, the contractor agrees as follows:

The contractor or subcontractor, where applicable, will not discriminate against any employee or applicant for employment because of age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex. Except with respect to affectional or sexual orientation and gender identity or expression, the contractor will ensure that equal employment opportunity is afforded to such applicants in recruitment and employment, and that employees are treated during employment, without regard to their age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex. Such equal employment opportunity shall include, but not be limited to the following: employment, upgrading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the Public Agency Compliance Officer setting forth provisions of this nondiscrimination clause.

The contractor or subcontractor, where applicable will, in all solicitations or advertisements for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex.

The contractor or subcontractor will send to each labor union, with which it has a collective bargaining agreement, a notice, to be provided by the agency contracting officer, advising the labor union of the contractor's commitments under this chapter and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

The contractor or subcontractor, where applicable, agrees to comply with any regulations promulgated by the Treasurer pursuant to N.J.S.A. 10:5-31 et seq., as amended and supplemented from time to time and the Americans with Disabilities Act.

The contractor or subcontractor agrees to make good faith efforts to meet targeted county employment goals established in accordance with N.J.A.C. 17:27-5.2.

The contractor or subcontractor agrees to inform in writing its appropriate recruitment agencies including, but not limited to, employment agencies, placement bureaus, colleges, universities, and labor unions, that it does not discriminate on the basis of age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex, and that it will discontinue the use of any recruitment agency which engages in direct or indirect discriminatory practices.

The contractor or subcontractor agrees to revise any of its testing procedures, if necessary, to assure that all personnel testing conforms with the principles of job related testing, as established by the statutes and court decisions of the State of New Jersey and as established by applicable Federal law and applicable Federal court decisions.

In conforming with the targeted employment goals, the contractor or subcontractor agrees to review all procedures relating to transfer, upgrading, downgrading and layoff to ensure that all such actions are taken without regard to age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex, consistent with the statutes and court decisions of the State of New Jersey, and applicable Federal law and applicable Federal court decisions.

The contractor shall submit to the public agency, after notification of award but prior to execution of a goods and services contract, one of the following three documents:

- Letter of Federal Affirmative Action Plan Approval;
- Certificate of Employee Information Report; or
- Employee Information Report Form AA302 (electronically provided by the Division and distributed to the public agency through the Division's website at http://www.state.nj.us/treasury/contract_compliance).

The contractor and its subcontractors shall furnish such reports or other documents to the Division of Purchase an Property, CCAU, EEO Monitoring Program as may be requested by the office from time to time in order to carry out the purposes of these regulations, and public agencies shall furnish such information as may be requested by the Division of Purchase an Property, CCAU, EEO Monitoring Program for conducting a compliance investigation pursuant to N.J.A.C. 17:27-1 et seq.

EXHIBIT B - CONSTRUCTION CONTRACTS

MANDATORY EQUAL EMPLOYMENT OPPORTUNITY LANGUAGE
N.J.S.A. 10:5-31 et seq. (P.L.1975, c.127)
N.J.S.A. 10:5-39 et seq. (P.L.1983, c.197)
N.J.A.C. 17:27-1.1 et seq.

During the performance of this contract, the contractor agrees as follows:

The contractor or subcontractor, where applicable, will not discriminate against any employee or applicant for employment because of age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex. Except with respect to affectional or sexual orientation and gender identity or expression, the contractor will ensure that equal employment opportunity is afforded to such applicants in recruitment and employment, and that employees are treated during employment, without regard to their age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex. Such equal employment opportunity shall include, but not be limited to the following: employment, up grading, demotion, or transfer; recruitment or recruitment advertising; layoff or termination; rates of pay or other forms of compensation; and selection for training, including apprenticeship. The contractor agrees to post in conspicuous places, available to employees and applicants for employment, notices to be provided by the Public Agency Compliance Officer setting forth provisions of this nondiscrimination clause.

The contractor or subcontractor, where applicable will, in all solicitations or advertisements for employees placed by or on behalf of the contractor, state that all qualified applicants will receive consideration for employment without regard to age, race, creed, color, national origin, ancestry, marital status, affectional or sexual orientation, gender identity or expression, disability, nationality or sex.

N.J.S.A. 10:5-39 et seq. requires contractors, subcontractors, and permitted assignees performing construction, alteration, or repair of any building or public work in excess of $250,000 to guarantee equal employment opportunity to veterans.

The contractor or subcontractor will send to each labor union, with which it has a collective bargaining agreement, a notice, to be provided by the agency contracting officer, advising the labor union or workers' representative of the contractor's commitments under this act and shall post copies of the notice in conspicuous places available to employees and applicants for employment.

The contractor or subcontractor, where applicable, agrees to comply with any regulations promulgated by the Treasurer, pursuant to N.J.S.A. 10:5-31 et seq., as amended and supplemented from time to time and the Americans with Disabilities Act.

When hiring or scheduling workers in each construction trade, the contractor or subcontractor agrees to make good faith efforts to employ minority and women workers in each construction trade consistent with the targeted employment goal prescribed by N.J.A.C. 17:27-7.2; provided, however, that the Dept. of LWD, Construction EEO Monitoring Program may, in its discretion, exempt a contractor or subcontractor from compliance with the good faith procedures prescribed by the following provisions, A, B and C, as long as the Dept. of LWD, Construction EEO Monitoring Program is satisfied that the contractor or subcontractor is employing workers provided by a union which provides evidence, in accordance with standards prescribed by the Dept. of LWD, Construction EEO Monitoring Program, that its percentage of active "card carrying" members who are minority and women workers is equal to or greater than the targeted employment goal established in accordance with N.J.A.C. 17:27-7.2. The contractor or subcontractor agrees that a good faith effort shall include compliance with the following procedures:

(A) If the contractor or subcontractor has a referral agreement or arrangement with a union for a construction trade, the contractor or subcontractor shall, within three business days of the contract award, seek assurances from the union that it will cooperate with the contractor or subcontractor as it fulfills its affirmative action obligations under this contract and in accordance with the rules promulgated by the Treasurer pursuant to N.J.S.A. 10:5-31 et. seq., as supplemented and amended from time to time and the Americans with Disabilities Act. If the contractor or subcontractor is unable to obtain said assurances from the construction trade union at least five business days prior to the commencement of construction work, the contractor or subcontractor agrees to afford equal employment opportunities minority and women workers directly, consistent with this chapter. If the contractor's or subcontractor's prior experience with a construction trade union, regardless of whether the union has provided said assurances, indicates a significant possibility that the trade union will not refer sufficient minority and women workers consistent with affording equal employment opportunities as specified in this chapter, the contractor or subcontractor agrees to be prepared to provide such opportunities to minority and women workers directly, consistent with this chapter, by complying with the hiring or scheduling procedures prescribed under (B) below; and the contractor or subcontractor further agrees to take said action immediately if it determines that the union is not referring minority and women workers consistent with the equal employment opportunity goals set forth in this chapter.

(B) If good faith efforts to meet targeted employment goals have not or cannot be met for each construction trade by adhering to the procedures of (A) above, or if the contractor does not have a referral agreement or arrangement with a union for a construction trade, the contractor or subcontractor agrees to take the following actions:
  (1) To notify the public agency compliance officer, the Dept. of LWD, Construction EEO Monitoring Program, and minority and women referral organizations listed by the Division pursuant to N.J.A.C. 17:27-5.3, of its workforce needs, and request referral of minority and women workers;

(2) To notify any minority and women workers who have been listed with it as awaiting available vacancies;
(3) Prior to commencement of work, to request that the local construction trade union refer minority and women workers to fill job openings, provided the contractor or subcontractor has a referral agreement or arrangement with a union for the construction trade;
(4) To leave standing requests for additional referral to minority and women workers with the local construction trade union, provided the contractor or subcontractor has a referral agreement or arrangement with a union for the construction trade, the State Training and Employment Service and other approved referral sources in the area;
(5) If it is necessary to lay off some of the workers in a given trade on the construction site, layoffs shall be conducted in compliance with the equal employment opportunity and non- discrimination standards set forth in this regulation, as well as with applicable Federal and State court decisions;
(6) To adhere to the following procedure when minority and women workers apply or are referred to the contractor or subcontractor:
    (i) The contactor or subcontractor shall interview the referred minority or women worker.
    (ii) If said individuals have never previously received any document or certification signifying a level of qualification lower than that required in order to perform the work of the construction trade, the contractor or subcontractor shall in good faith determine the qualifications of such individuals. The contractor or subcontractor shall hire or schedule those individuals who satisfy appropriate qualification standards in conformity with the equal employment opportunity and non-discrimination principles set forth in this chapter. However, a contractor or subcontractor shall determine that the individual at least possesses the requisite skills, and experience recognized by a union, apprentice program or a referral agency, provided the referral agency is acceptable to the Dept. of LWD, Construction EEO Monitoring Program. If necessary, the contractor or subcontractor shall hire or schedule minority and women workers who qualify as trainees pursuant to these rules. All of the requirements, however, are limited by the provisions of (C) below.
    (iii) The name of any interested women or minority individual shall be maintained on a waiting list, and shall be considered for employment as described in (i) above, whenever vacancies occur. At the request of the Dept. of LWD, Construction EEO Monitoring Program, the contractor or subcontractor shall provide evidence of its good faith efforts to employ women and minorities from the list to fill vacancies.
    (iv) If, for any reason, said contractor or subcontractor determines that a minority individual or a woman is not qualified or if the individual qualifies as an advanced trainee or apprentice, the contractor or subcontractor shall inform the individual in writing of the reasons for the determination, maintain a copy of the determination in its files, and send a copy to the public agency compliance officer and to the Dept. of LWD, Construction EEO Monitoring Program.
(7) To keep a complete and accurate record of all requests made for the referral of workers in any trade covered by the contract, on forms made available by the Dept. of LWD, Construction EEO Monitoring Program and submitted promptly to the Dept. of LWD, Construction EEO Monitoring Program upon request.

(C) The contractor or subcontractor agrees that nothing contained in (B) above shall preclude the contractor or subcontractor from complying with the union hiring hall or apprenticeship policies in any applicable collective bargaining agreement or union hiring hall arrangement, and, where required by custom or agreement, it shall send journeymen and trainees to the union for referral, or to the apprenticeship program for admission, pursuant to such agreement or arrangement. However, where the practices of a union or apprenticeship program will result in the exclusion of minorities and women or the failure to refer minorities and women consistent with the targeted county employment goal, the contractor or subcontractor shall consider for employment persons referred pursuant to (B) above without regard to such agreement or arrangement; provided further, however, that the contractor or subcontractor shall not be required to employ women and minority advanced trainees and trainees in numbers which result in the employment of advanced trainees and trainees as a percentage of the total workforce for the construction trade, which percentage significantly exceeds the apprentice to journey worker ratio specified in the applicable collective bargaining agreement, or in the absence of a collective bargaining agreement, exceeds the ratio established by practice in the area for said construction trade. Also, the contractor or subcontractor agrees that, in implementing the procedures of (B) above, it shall, where applicable, employ minority and women workers residing within the geographical jurisdiction of the union.

After notification of award, but prior to signing a construction contract, the contractor shall submit to the public agency compliance officer and the Dept. of LWD, Construction EEO Monitoring Program an initial project workforce report (Form AA-201) electronically provided to the public agency by the Dept. of LWD, Construction EEO Monitoring Program, through its website, for distribution to and completion by the contractor, in accordance with N.J.A.C. 17:27-7.

The contractor also agrees to submit a copy of the Monthly Project Workforce Report once a month thereafter for the duration of this contract to the Dept. of LWD, Construction EEO Monitoring Program and to the public agency compliance officer.

The contractor agrees to cooperate with the public agency in the payment of budgeted funds, as is necessary, for on the job and/or off the job programs for outreach and training of minorities and women.

(D) The contractor and its subcontractors shall furnish such reports or other documents to the Dept. of LWD, Construction EEO Monitoring Program as may be requested by the Dept. of LWD, Construction EEO Monitoring Program from time to time in order to carry out the purposes of these regulations, and public agencies shall furnish such information as may be requested by the Dept. of LWD, Construction EEO Monitoring Program for conducting a compliance investigation pursuant to N.J.A.C. 17:27-1.1 et seq.

EXHIBIT C - EXECUTIVE ORDER NO. 151 REQUIREMENTS

It is the policy of the Division of Purchase and Property that its contracts should create a workforce that reflects the diversity of the State of New Jersey. Therefore, contractors engaged by the Division of Purchase and Property to perform under a construction contract shall put forth a good faith effort to engage in recruitment and employment practices that further the goal of fostering equal opportunities to minorities and women.

The contractor must demonstrate to the Division of Purchase and Property's satisfaction that a good faith effort was made to ensure that minorities and women have been afforded equal opportunity to gain employment under the Division of Purchase and Property's contract with the contractor. Payment may be withheld from a contractor's contract for failure to comply with these provisions.

Evidence of a "good faith effort" includes, but is not limited to:

1. The Contractor shall recruit prospective employees through the State Job bank website, managed by the Department of Labor and Workforce Development, available online at https://newjersey.usnlx.com/;
2. The Contractor shall keep specific records of its efforts, including records of all individuals interviewed and hired, including the specific numbers of minorities and women;
3. The Contractor shall actively solicit and shall provide the Division of Purchase and Property with proof of solicitations for employment, including but not limited to advertisements in general circulation media, professional service publications and electronic media; and
4. The Contractor shall provide evidence of efforts described at 2 above to the Division of Purchase and Property no less frequently than once every 12 months.
5. The Contractor shall comply with the requirements set forth at N.J.A.C. 17:27.

This language is in addition to and does not replace good faith efforts requirements for construction contracts required by N.J.A.C. 17:27-3.6, 3.7 and 3.8, also known as Exhibit B.

This Supplement to the above State of New Jersey Standard Terms and Conditions ("Supplement") shall apply to all contracts or purchase agreements made with the State of New Jersey ("State") pursuant to a State Using Agency's Delegated Purchase Authority ("DPA") or under N.J.S.A. 52:34-9 or -10 ("Waivered Contracts"). The terms in this Supplement are in addition to, or modify the State of New Jersey Standard Terms and Conditions (SSTCs) as applicable and noted below.

I. ADDITIONS TO THE STANDARD TERMS AND CONDITIONS FOR ALL WAIVERED AND DELEGATED PURCHASE AUTHORITY CONTRACTS

A. ORDER OF PRECEDENCE

The "Contract" shall consist of the following documents: (1) this Supplement; (2) the State of New Jersey Standard Terms and Conditions; (3) the agency's scope of work; and, (4) the Contractor's proposal including any attachments or documents incorporated by reference. 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.

B. NO ARBITRATION

Notwithstanding anything to the contrary in Contractor's Standard Form Agreement ("SFA") or Scope of Work ("SOW"), the State does not agree to binding arbitration.

C. NO AUTO-RENEWAL

Notwithstanding anything to the contrary in Contractor's SFA or SOW, the State does not agree to auto-renewal of any services, standard software maintenance, technical support or service fees.

II. ADDITIONS TO THE STANDARD TERMS AND CONDITIONS FOR WAIVERED CONTRACTS, AS APPLICABLE

A. STATE'S RIGHT TO INSPECT CONTRACTOR'S FACILITIES

The State reserves the right to inspect the contractor's establishment before making an award, for the purposes of ascertaining whether the contractor has the necessary facilities for performing the Contract. The State may also consult with clients of the contractor to assist the State in making a contract award that is most advantageous to the State.

B. STATE'S RIGHT TO REQUEST FURTHER INFORMATION

The Director reserves the right to request all information which may assist him or her in making a contract award, including factors necessary to evaluate the contractor's financial capabilities to perform the Contract. Further, the Director reserves the right to request a contractor to explain, in detail, how the proposal price was determined.

C. DELIVERY TIME AND COSTS

Unless otherwise noted elsewhere in the scope of work, all delivery times are 30 calendar days after receipt of order (ARO) and prices for items in proposals shall be submitted Freight On Board (F.O.B.) Destination (30 calendar days ARO/F.O.B.). The contractor shall assume all costs, liability and responsibility for the delivery of merchandise in good condition to the State's Using Agency or designated purchaser. Thirty calendar days ARO/F.O.B. does not cover "spotting" but does include delivery on the receiving platform of the Using Agency at any destination in the State of New Jersey unless otherwise specified. No additional charges will be allowed for any additional transportation costs resulting from partial shipments made at the contractor's convenience when a single shipment is ordered. The weights and measures of the State's Using Agency receiving the shipment shall govern.

D. COLLECT ON DELIVERY (C.O.D) TERMS

C.O.D. terms will not be accepted.

E. CASH DISCOUNTS

The contractor is encouraged to offer cash discounts based on expedited payment by the State. The State will make efforts to take advantage of discounts. Should the contractor choose to offer cash discounts the following shall apply:

1. Discount periods shall be calculated starting from the next business day after the Using Agency has accepted the goods or services, received a properly signed and executed invoice and, when required, a properly executed performance security, whichever is latest; and
2. The date on the check issued by the State in payment of that invoice shall be deemed the date of the State's response to that invoice.

F. PERFORMANCE SECURITY

If performance security is required, such security must be submitted with the bid in the amount listed in the scope of work. N.J.A.C. 17:12-2.5. Acceptable forms of performance security are as follows:

1. A properly executed individual or annual performance bond issued by an insurance or security company authorized to do business in the State of New Jersey,
2. A certified or cashier's check drawn to the order of "Treasurer, State of New Jersey," or
3. An irrevocable letter of credit issued by a federally insured financial institution and naming "Treasurer, State of New Jersey," as beneficiary.

The Performance Security must be submitted to the State within 30 days of the effective date of the Contract award and cover the period of the Contract and any extensions thereof. Failure to submit performance security may result in cancellation of the Contract for cause and nonpayment for work performed.

Although the performance bond is required for the full term of the Contract, the Director recognizes that the industry practice of sureties is to issue a one (1) year performance bond for goods and services contracts. Thus, the contractor is permitted to submit a one (1) year performance bond for the amount required under the Contract and, on each succeeding anniversary date of the Contract, provide a continuation or renewal certificate to evidence that the bond is in effect for the next year of the Contract. This procedure will remain in place for each year of the Contract thereafter until the termination of the Contract. Failure to provide such proof on the anniversary date of the Contract shall result in suspension of the Contract, and possibly, termination of the Contract.

For performance bonds based on a percentage of the total estimated Contract price. On each anniversary of the effective date of the Contract, the amount of the required performance bond, unless otherwise noted, is calculated by applying the established RFQ performance bond percentage to the outstanding balance of the estimated amount of the Contract price to be paid to the contractor.

In the event that the Contract price is increased by a Contract Amendment, the contractor may be required to provide, within 30 calendar days of the effective date of the Contract Amendment, performance bond coverage for the increase in Contract price. The required increase in the performance bond amount is calculated by applying the established bond percentage set forth above to the increase in Contract price. Failure to provide such proof to the Director of this required coverage may result in the suspension of payment to the contractor until such time the contractor complies with this requirement.

G. RETAINAGE

If retainage is required on the Contract as stated in the scope of work, the state and/or agency will retain the stated percentage or retainage from each invoice. Payment of retainage will be authorized after satisfactory completion and submission of all services, deliverables or work products by the contractor and acceptance by the agency of all services, deliverables or work products required by the Contract.

For ongoing contracts, the agency will retain the stated percentage of each invoice submitted. At the end of the three (3) month period after payment of each invoice, the agency will review the contractor's performance and if performance has been satisfactory, the agency will release the retainage for the preceding three (3) month period. Following the expiration of the Contract, retained fees will be released to the contractor after certification by the agency's project manager, if any, that all services have been satisfactorily performed.

H. AUDIT NOTICE AND DISPUTE RESOLUTION

To the extent the contractor's proposal or Standard Form Agreement permits the contractor to conduct periodic audits of the State's usage of the Contractor Intellectual Property provided thereunder, such provision is amended to include the following audit notice and dispute resolution process:

1. AUDIT NOTICE – Notwithstanding anything to the contrary in the contractor's proposal or Standard Form Agreement, in the event that the contractor seeks to exercise a right in its proposal or Standard Form Agreement to audit the State's use of Contractor Intellectual Property, the contractor shall deliver simultaneous written notice, no less than thirty days in advance of the audit start date (unless the contractor's notice provides a longer notice period), to the: Agency requesting the waiver contract.
2. The notice shall reference the specific audit provision(s) in the contractor's proposal or Standard Form Agreement being exercised and include copies of same, specify the means by which the contractor will conduct the audit, and shall require the audit to be conducted in accordance with generally accepted standards in the field of such audits.
3. AUDIT DISPUTE RESOLUTION -- If the State, in good faith, provides the contractor with written notice of an alleged error in the amount of underpaid fees due the contractor as a result of an audit (the "dispute"), then the parties will endeavor to resolve the dispute in accordance with this paragraph. Each party will appoint a Vice President, Assistant Director, or the equivalent (hereinafter referred to as "Representative") to discuss the dispute and no formal proceedings for the judicial resolution of such dispute, except for the seeking of equitable relief or those required to avoid non-compliance with the New Jersey Contractual Liability Act, N.J.S.A. 59:13-1 et seq., may begin until either such Representative concludes, after a good faith effort to resolve the dispute, that resolution through continued discussion is unlikely. In addition, the parties shall refrain from exercising any termination right related to the dispute being considered under this paragraph and shall continue to perform their respective obligations under the Contract while they endeavor to resolve the dispute under this paragraph.
4. STATE NOT LIABLE FOR AUDIT COSTS -- Notwithstanding anything to the contrary in the contractor's proposal or Standard Form Agreement, the State will not reimburse the contractor for any costs related to an audit.
5. NO AUDIT RIGHT CREATED -- In the event that the contractor's proposal or Standard Form Agreement does not permit audits of the State's usage of Contractor Intellectual Property, Section 5.19 of this Supplement shall not be interpreted to provide such an audit right.

III. ADDITIONS TO THE STANDARD TERMS AND CONDITIONS FOR PROFESSIONAL SERVICES CONTRACTS, AS APPLICABLE

A. INSURANCE FOR PROFESSIONAL SERVICES CONTRACTS

Section 4.2 Insurance 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 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.

B. LIMITATION OF LIABILITY FOR PROFESSIONAL SERVICES CONTRACTS

Section 4.0 Indemnification and Insurance of the SSTC is supplemented with the following:

4.3 LIMITATION OF LIABILITY

The Contractor's liability to the State for actual, direct damages resulting from the Contractor's performance or non-performance of, or in any manner related to this Contract, for any and all claims, shall be limited in the aggregate to 200% of the total value of this Contract. This limitation of liability shall not apply to the following:

A. The Contractor's obligation to indemnify the State of New Jersey and its employees from and against any claim, demand, loss, damage, or expense relating to bodily injury or the death of any person or damage to real property or tangible personal property, incurred from the work or materials supplied by the Contractor under this Contract caused by negligence or willful misconduct of the Contractor;
B. The Contractor's breach of its obligations of confidentiality; and
C. The Contractor's liability with respect to copyright indemnification.

The Contractor's indemnification obligation is not limited by but is in addition to the insurance obligations.

The Contractor shall not be liable for special, consequential, or incidental damages.

IV. ADDITIONS TO THE STANDARD TERMS AND CONDITIONS FOR ALL INFORMATION TECHNOLOGY CONTRACTS, AS APPLICABLE

A. DEFINITIONS

The following definitions shall apply to information technology contracts:

1. The term "Acceptance" means the written confirmation by an Agency that the contractor has completed a Deliverable according to the specified requirements.
2. As defined by N.J.S.A. 56:8-161, the term "Breach of Security" means unauthorized access to electronic files, media, or data containing Personal Data that compromises the security, confidentiality, or integrity of Personal Data when access to the Personal Data has not been secured by encryption or by any other method or technology that renders the Personal Data unreadable or unusable. Good faith acquisition of Personal Data by an employee or agent of the Provider for a legitimate business purpose is not a Breach of Security, provided that the Personal Data is not used for a purposes unrelated to the business or subject to further unauthorized disclosure.
3. The term "Contractor Intellectual Property" means any intellectual property that is owned by the contractor and contained in or necessary for the use of the Deliverables or which the contractor makes available for the State to use as part of the work under the Contract. Contractor Intellectual Property includes COTS or Customized Software owned by the contractor, the contractor's technical documentation, and derivative works and compilations of any Contractor Intellectual Property.
4. The term Commercial Off the Shelf Software ("COTS") means Software provided by the contractor that is intended for general use.
5. The term "Custom Software" means Software and Work Product that is developed by the contractor at the request of the Agency to meet the specific requirements of the Agency and is intended for its use.
6. The term "Customized Software" means COTS that is adapted by the contractor to meet specific requirements of the Agency that differ from the standard requirements of the base product.
7. The term "Deliverable" means the goods, products, Services and Work Product that the contractor is required to deliver to the State under the Contract;
8. The term "End User" means the user of the Provider's solution.
9. The terms "goods" and "products" shall be deemed to include, without limitation, Software and Hardware.
10. The term "Hardware" shall be deemed to include computer equipment and any Software provided with the Hardware that is necessary for the Hardware to operate.
11. The term "Information Technology Contract" shall mean, notwithstanding any definition in New Jersey Statutes, a Contract for one or more of the following: Hardware, Software, Services, telecommunication goods and services, and all related goods.
12. The term "Mobile Device" means any device used by Provider that can move or transmit data, including but not limited to laptops, hard drives, and flash drives.
13. The term "Non-Public Data" means data, other than Personal Data, that is not subject to distribution to the public as public information. Non-Public Data is data that is identified by the State as non-public information or otherwise deemed to be sensitive and confidential by the State because it contains information that is exempt by statute, ordinance or administrative rule from access by the general public as public information.
14. The term "Personal Data" means:
    a. "Personal Information" as defined in N.J.S.A. 56:8-161, means an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number, (2) driver's license number or State identification

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

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

15. The term "Personally Identifiable Information" or "PII," as defined by the U.S. Department of Commerce, National Institute of Standards and Technology, means any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information,
16. The term "Protected Health Information" or "PHI," has the same meaning as the term is defined in the regulations adopted pursuant to the Health Insurance Portability and Accountability Act of 1996, P.L. No. 104-191 (1996) and found in 45 CFR Parts 160 to 164 means Individually Identifiable Health Information (as defined below) transmitted by electronic media, maintained in electronic media, or transmitted or maintained in any other form or medium. PHI excludes education records covered by the Family Educational Rights and Privacy Act (FERPA), as amended, 20 U.S.C. 1232g, records described at 20 U.S.C. 1232g(a)(4)(B)(iv) and employment records held by a covered entity in its role as employer. The term "Individually Identifiable Health Information" has the same meaning as the term is defined in the regulations adopted pursuant to the Health Insurance Portability and Accountability Act of 1996, P.L. No. 104-191 (1996) and found in 45 CFR Parts 160 to 164 and means information that is a subset of Protected Health Information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer or health care clearinghouse; and (2) relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual; and (a) that identifies the individual; or (b) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.
17. The term "Recovery Time Objective" or "RTO," means the maximum tolerable length of time that the Provider's solution may be unavailable after a failure or disaster occurs.
18. The term "Security Incident" means the potential access by non-authorized person(s) to Personal Data or Non-Public Data that the Provider believes could reasonably result in the use, disclosure, or access or theft of State's unencrypted Personal Data or Non-Public Data within the possession or control of the Provider. A Security Incident may or may not turn into a Breach of Security.
19. The term "Service Level Agreement" or "SLA," means the document that is part of the Provider's SFA that typically includes (1) the technical service level performance promises, (i.e. metrics for performance and intervals for measure), (2) description of service quality, (3) identification of roles and responsibilities, (4) security responsibilities and notice requirements, (5) how disputes are discovered and addressed, and (6) any remedies for performance failures.
20. The terms "Services" shall be deemed to include, without limitation (i) Information Technology ("IT") professional services; (ii) Software and Hardware-related services, including without limitation, installation, configuration, and training and (iii) Software and Hardware maintenance and support and/or Software and Hardware technical support services.
21. The term "Software" means, without limitation, computer programs, source codes, routines, or subroutines supplied by the contractor, including operating software, programming aids, application programs, application programming interfaces and software products, and includes COTS, Customized Software and Custom Software, unless the context indicates otherwise.
22. The term "State Data" means all data and metadata created or in any way originating with the State, and all data that is the output of computer processing of or other electronic manipulation of any data that was created by or in any way originated with the State, whether such data or output is stored on the State's hardware, the Provider's hardware or exists in any system owned, maintained or otherwise controlled by the State or by the Provider. State Data includes Personal Data and Non-Public Data.
23. The term "State Intellectual Property" means any intellectual property that is owned by the State. State Intellectual Property includes any derivative works and compilations of any State Intellectual Property.
24. The term "Third Party Intellectual Property" means any intellectual property owned by parties other than the State or the contractor and contained in or necessary for the use of the Deliverables. Third Party Intellectual Property includes COTS owned by Third Parties, and derivative works and compilations of any Third Party Intellectual Property.
25. The term "Work Product" means every invention, modification, discovery, design, development, customization, configuration, improvement, process, Software program, work of authorship, documentation, formula, datum, technique, know how, secret, or intellectual property right whatsoever or any interest therein (whether patentable or not patentable or registerable under copyright or similar statutes or subject to analogous protection) that is specifically made, conceived, discovered, or reduced to practice by the contractor or the contractor's subcontractors or a third party engaged by the contractor or its subcontractor pursuant to the Contract. Notwithstanding anything to the contrary in the preceding sentence, Work Product does not include State Intellectual Property, Contractor Intellectual Property or Third Party Intellectual Property.

B. INDEMNIFICATION FOR STANDARD TECHNOLOGY CONTRACTS

Section 4.1 Indemnification of the SSTC is deleted in its entirety and replaced with the following:

4.1 INDEMNIFICATION

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

A. The Contractor shall assume all risk of and responsibility for, and agrees to indemnify, defend, and save harmless the State and its officers, agents, servants and employees, from and against any and all third party claims, demands, suits, actions, recoveries, judgments and costs and expenses in connection therewith:
   1. For or on account of the loss of life, property or injury or damage to the person, body or property of any person or persons whatsoever, which shall arise from or result directly or indirectly from the work and/or products supplied under this Contract or the order; and
   2. For or on account of the use of any patent, copyright, trademark, trade secret or other proprietary right of any copyrighted or uncopyrighted composition, secret process, patented or unpatented invention, article or appliance ("Intellectual Property Rights") furnished or used in the performance of this Contract; and
   3. The Contractor's indemnification and liability under subsection (A) is not limited by, but is in addition to the insurance obligations.

B. In the event of a claim or suit involving third-party Intellectual Property Rights, the Contractor, at its option, may:
   1. procure for the State the legal right to continue the use of the product;
   2. replace or modify the product to provide a non-infringing product that is the functional equivalent; or
   3. in the event that the Contractor cannot do (1) or (2) refund the purchase price less a reasonable allowance for use that is agreed to by both parties.

C. The State will:
   1. promptly notify Contractor in writing of the claim or suit;
   2. give Contractor shall have control of the defense and settlement of any claim that is subject to Section 4.1(a); provided; however, that the State must approve any settlement of the alleged claim, which approval shall not be unreasonably withheld. The State may observe the proceedings relating to the alleged claim and confer with the Contractor at its expense.

D. Notwithstanding the foregoing, Contractor has no obligation or liability for any claim or suit concerning third-party Intellectual Property Rights arising from:
   1. the State's unauthorized combination, operation, or use of a product supplied under this Contract with any product, device, or Software not supplied by Contractor;
   2. the State's unauthorized alteration or modification of any product supplied under this Contract;
   3. the Contractor's compliance with the State's designs, specifications, requests, or instructions, provided that if the State provides Contractor with such designs, specifications, requests, or instructions, Contractor reviews same and advises that such designs, specifications, requests or instructions present potential issues of patent or copyright infringement and the State nonetheless directs the Contractor to proceed with one (1) or more designs, specifications, requests or instructions that present potential issues of patent or copyright infringement; or
   4. the State's failure to promptly implement a required update or modification to the product provided by Contractor after the Contractor has given written notice to the State of a need for such an update or modification.

E. Contractor will be relieved of its responsibilities under Subsection 4.1(a)(i) and (ii) for any claims made by an unaffiliated third party that arise solely from the actions or omissions of the State, its officers, employees or agents.

F. Subject to the New Jersey Tort Claims Act (N.J.S.A. 59:1-1 et seq.), the New Jersey Contractual Liability Act (N.J.S.A. 59:13-1 et seq.) and the appropriation and availability of funds, the State will be responsible for any cost or damage arising out of actions or inactions of the State, its employees or agents under Subsection 4.1(a)(i) and (ii) which results in an unaffiliated third party claim. This is Contractor's exclusive remedy for these claims;

G. This section states the entire obligation of Contractor and its suppliers, and the exclusive remedy of the State, in respect of any infringement or alleged infringement of any Intellectual Property Rights. This indemnity obligation and remedy are given to the State solely for its benefit and in lieu of, and Contractor disclaims, all warranties, conditions and other terms of non-infringement or title with respect to any product; and

H. Furthermore, neither Contractor nor any attorney engaged by Contractor shall defend the claim in the name of the State of New Jersey or any Authorized Purchaser, nor purport to act as legal representative of the State of New Jersey or any Authorized Purchaser, without having provided notice to the Director of the Division of Law in the Department of Law and Public Safety and to the Director of the Division of Purchase and Property. The State of New Jersey may, at its election and expense, assume its own defense and settlement; and

I. The State of New Jersey will not indemnify, defend, pay or reimburse for claims or take similar actions on behalf of the Contractor.

C. INSURANCE FOR STANDARD TECHNOLOGY CONTRACTS

Section 4.2 Insurance 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 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.

D. LIMITATION OF LIABILITY FOR STANDARD TECHNOLOGY CONTRACTS

Section 4.0 Indemnification and Insurance of the SSTC is supplemented with the following:

4.3 LIMITATION OF LIABILITY

The Contractor's liability to the State for actual, direct damages resulting from the Contractor's performance or non-performance of, or in any manner related to this Contract, for any and all claims, shall be limited in the aggregate to 200% of the total value of this Contract. This limitation of liability shall not apply to the following:

A. The Contractor's obligation to indemnify the State of New Jersey and its employees from and against any claim, demand, loss, damage, or expense relating to bodily injury or the death of any person or damage to real property or tangible personal property, incurred from the work or materials supplied by the Contractor under this Contract caused by negligence or willful misconduct of the Contractor;

B. The Contractor's breach of its obligations of confidentiality; and

C. The Contractor's liability with respect to copyright indemnification.

The Contractor's indemnification obligation is not limited by but is in addition to the insurance obligations.

The Contractor shall not be liable for special, consequential, or incidental damages.

E. PERFORMANCE GUARANTEE OF THE CONTRACTOR

Section 5.11 Performance Guarantee of the Contractor of the SSTC is supplemented with the following:

1. COTS and Customized Software
   a. Unless the Contractor Standard Form Agreement provides greater coverage as determined by the State, in its sole discretion, the contractor warrants that COTS and Customized Software products licensed to the State shall operate in all material respects as described in the Solicitation and/or contractor technical documentation for ninety (90) days after Acceptance. The State shall notify the contractor of any COTS or Customized Software product deficiency within ninety (90) days after Acceptance. For a Contract requiring the delivery of COTS or Customized Software and Custom Software, a notice within one hundred eighty (180) days that describes a deficiency in functional terms without specifying whether the deficiency is with COTS, Customized Software or Custom Software shall be deemed a notice that triggers the warranty provisions in both Section 5.11(a) and 5.11(b) of this Supplement.
   b. Except for the portion of the contractor's COTS or Customized Software product that intentionally contains one or more of the following for the purpose of anti-virus protection, the contractor warrants that, at the time of delivery and installation of the COTS or Customized Software provided pursuant to the Contract, its product shall be free of what are commonly defined as viruses, backdoors, worms, spyware, malware and other malicious code that will hamper performance of the COTS or Customized Software, collect unlawful personally identifiable information on users, or prevent the COTS or Customized Software from performing as required under the Contract.
   c. In the event of any breach of this warranty, the contractor shall correct the product errors that caused the breach of warranty, or if the contractor cannot substantially correct such breach in a commercially reasonable manner, the State may end its usage and recover the fees paid to the contractor for the license and any unused, prepaid, technical support fees paid. Under no circumstances does this warranty provision limit the contractor's obligation in the event of a breach of confidentiality.
   d. The contractor does not warrant that COTS or Customized Software is error-free or that it will operate uninterrupted.
2. Custom Software
   a. Unless the Contractor Standard Form Agreement provides greater coverage, as determined by the State, in its sole discretion, the contractor warrants that Custom Software Deliverables shall operate in all material respects as described in the applicable specification documentation for one hundred and eighty (180) days after Acceptance. The State shall notify the contractor of any Custom Software deficiency within one hundred and eighty (180) days after Acceptance of the Custom Software Deliverable (the "Notice Period"). Where the contractor is providing multiple Custom Software Deliverables over the term of the Contract, the Notice Period shall begin to run after the Acceptance of the final Custom Software Deliverable under the Contract. At that time, the State may assert defect claims relating to any and all of the Custom Software Deliverables provided under the Contract; however, the State may also assert claims earlier, in its discretion, without waiving the Notice Period.
   b. For a Contract requiring the delivery of COTS or Customized Software and Custom Software, a notice within one hundred eighty (180) days that describes a deficiency in functional terms without specifying whether the deficiency is with COTS, Customized Software or Custom Software shall be deemed a notice that triggers the warranty provisions in both Section 5.11(a) and 5.11(b) of this Supplement.
   c. The contractor warrants that, at the time of Acceptance of the Custom Software Deliverable provided pursuant to the Contract, its product shall be free of what are commonly defined as viruses, backdoors, worms, spyware, malware and other malicious code that will hamper performance of the Custom Software, collect unlawful personally identifiable information on users, or prevent the Custom Software from performing as required under the Contract. Under no circumstances does this warranty provision limit the contractor's obligation in the event of a breach of confidentiality.
   d. In the event of any breach of this warranty, the contractor shall correct the Custom Software errors that caused the breach of warranty, or if the contractor cannot substantially correct such breach in a commercially reasonable manner, the State may

recover a portion of the fees paid to the contractor for the Custom Software with the uncorrected defect or in the event that the Custom Software is still deemed, by the State in its sole discretion, to be usable by the State even with the uncorrected defect, the State may recover a portion of the fees paid to the contractor for the Custom Software (up to the total amount of such charges for such Custom Software) to reflect any reduction in the value of the Custom Software Deliverable as a result of the uncorrected defect. Under no circumstances does this warranty provision limit the contractor's obligations in the event of a breach of confidentiality.

e. The contractor does not warrant that Custom Software is error-free or that it will operate uninterrupted.

3. IT Services
   a. Unless the Contractor Standard Form Agreement provides greater coverage, as determined by the State, in its sole discretion, the contractor warrants that all Services will be provided in a professional manner consistent with industry standards. The State shall notify the contractor of any Services warranty deficiencies within ninety (90) days from performance of the deficient Services.
   b. In the event of any breach of this warranty, the contractor shall re-perform the deficient Services, or if the contractor cannot substantially correct a breach in a commercially reasonable manner, the State may end the relevant Services and recover the fees paid to the contractor for the deficient Services.
4. Hardware
   a. Unless the Contractor Standard Form Agreement provides greater coverage, as determined by the State, in its sole discretion, the contractor warrants that the equipment offered is standard new equipment, and is the manufacturer's latest model in production, with parts regularly used for the type of equipment offered; that such parts are all in production and not likely to be discontinued; and that no attachment or part has been substituted or applied contrary to manufacturer's recommendations and standard practice.
   b. The contractor warrants that all equipment supplied to the State and operated by electrical current is UL listed where applicable.
   c. The contractor warrants that all new machines are to be guaranteed as fully operational for one (1) year from time of Acceptance by the State. For the avoidance of doubt, Acceptance with respect to Hardware in this subsection (d) shall occur no later than sixty (60) days after delivery, as evidenced by a signed delivery receipt. The contractor shall render prompt service without charge, regardless of geographic location.
   d. The contractor warrants that sufficient quantities of parts necessary for proper service to equipment shall be maintained at distribution points and service headquarters.
   e. The contractor warrants that trained mechanics are regularly employed to make necessary repairs to equipment in the territory from which the service request might emanate within a 48-hour period or within the time accepted as industry practice.
   f. The contractor warrants that all Software included with the Hardware shall perform substantially in accordance with specifications, for one (1) year from the time of Acceptance. The contractor warrants that Software media will be free from material defects in materials and workmanship for a period of one (1) year from the date of Acceptance.
   g. In the event of any breach of this warranty, the contractor shall promptly repair, replace or refund the purchase price of product rejected for failure to conform with the contractor's product specifications.

5. THE WARRANTIES SET FORTH HEREIN ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, AND THE CONTRACTOR EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.

V. ADDITIONS TO THE STANDARD TERMS AND CONDITIONS FOR ALL INFORMATION TECHNOLOGY CONTRACTS WHICH INCLUDE SOFTWARE AS A SERVICE (SAAS)/CLOUD SOLUTION, AS APPLICABLE

A. ADDITIONAL TERMS FOR A CONTRACTOR'S DATA PROTECTION OBLIGATIONS

1. Data Ownership: The State will own all right, title and interest in its State Data that is related to the services provided by this contract. The Provider shall not use or access State user accounts or State Data, except (i) in the course of data center operations, (ii) in response to service or technical issues, (iii) as required by the express terms of this contract, or (iv) at the State's written request.

   Provider shall not collect, access, or use State Data except as strictly necessary to provide its solution to the State. No information regarding the State's use of the solution may be disclosed, provided, rented or sold to any third party for any reason unless required by law or regulation or by an order of a court of competent jurisdiction. This obligation shall survive and extend beyond the term of this contract.

2. Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the Provider to ensure that there is no inappropriate or unauthorized use of State Data at any time. To this end, the Provider shall safeguard the confidentiality, integrity, and availability of State Data and comply with the following conditions:
   a. The Provider shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of Personal Data and Non-Public Data. Such security measures shall be in accordance with recognized good industry practice and not less stringent than the measures the Provider applies to its own Personal Data and Non-Public Data of similar kind.
   b. All Personal Data shall be encrypted at rest and in transit with controlled access. Provider is responsible for encryption of the Personal Data. The level of protection and encryption for all Personal Data shall be identified and made a part of this contract.

c. Provider shall encrypt all Non-Public Data at rest and in transit. The level of protection and encryption for all Non-Public Data shall be identified and made a part of this contract.
d. Personal Data shall not be stored on Mobile Devices. Where Mobile Devices are required for Provider to accomplish the work, the Provider shall ensure the Mobile Device is hard drive encrypted consistent with validated cryptography standards as referenced in FIPS 140-2, Security Requirements for Cryptographic Modules for all Personal Data.
e. At no time shall any data or processes, which either belongs to or are intended for the use of State or its officers, agents, or employees, be copied, disclosed, or retained by the Provider or any party related to the Provider for subsequent use in any capacity that does not include the State.

3. Data Location: Provider shall provide its services to State and its End Users solely from data centers in the U.S. Storage of State Data at rest shall be located solely in data centers in the U.S. Provider shall not allow its personnel or contractors to store State Data on Mobile Devices, including personal computers, except for devices that are used and kept within the physical structure of its U.S. data centers. Provider shall permit its personnel and contractors to access State Data remotely only as required to provide technical support or upon prior notice and approval. The Provider may provide technical user support on a seven-day by 24-hour basis, unless otherwise prohibited in this contract.

4. Security Incident and Breach of Security Responsibilities.
   a. Security Incident Reporting Requirements: Once Provider reasonably determines that a Security Incident occurred, the Provider shall report a Security Incident to the appropriate State identified contact within 24 hours by the agreed upon method as defined in the contract. Provider will provide the State regular updates and all available relevant information including a description of the incident and those measures taken by Provider in response to the Security Incident.
   b. Breach of Security Reporting Requirements: If the Provider confirms or reasonably believes that there has been a Breach of Security, the Provider shall (1) immediately notify the appropriate State identified contact by the agreed upon method within 24 hours, unless a shorter time is required by applicable law, (2) take commercially reasonable measures to address and investigate the Breach of Security in a timely manner and (3) cooperate with the State as reasonably requested by the State and/or law enforcement to investigate and resolve the Breach of Security. Provider will provide the State regular updates and all available information to assist the State with notification to law enforcement and third parties as required by applicable law, including a description of the Breach of Security and those measures taken by Provider in response to the Breach of Security.
   c. Incident Response: When commercially reasonable to do so, Provider may communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries (subject to preapproval by the State if Provider specifically identifies the State or State Data), and seeking external expertise as mutually agreed at the time, defined by law, or contained in the SLA. Discussing Security Incidents with the State should be handled on an urgent as needed basis, as part of Provider communication and mitigation processes as mutually agreed at the time, defined by law, or contained in the SLA.
   d. Following a Security Incident or Breach of Security, Provider shall promptly implement necessary remedial measures, if necessary, and document responsive actions taken related to the Security Incident or Breach of Security, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

5. Termination and Suspension of Service:
   a. In the event of termination of the contract, the Provider shall implement an orderly return of State Data in a mutually agreeable format and the subsequent secure disposal of State Data remaining in Provider's possession.
   b. Suspension of services: During any period of suspension, the Provider shall not take any action to intentionally erase any State Data.
   c. Unless otherwise stipulated, in the event of termination of any services, SLA, or this contract in its entirety, the Provider shall not take any action to intentionally erase any State Data for a period of:
      1) 10 business days after the effective date of termination, if the termination is in accordance with the expiration of the defined contract term;
      2) 30 business days after the effective date of termination, if the termination is for convenience; or
      3) 60 business days after the effective date of termination, if the termination is for cause.

      After such period, the Provider shall have no obligation to maintain or provide any State Data and shall thereafter, unless legally prohibited, delete all State Data in its systems or otherwise in its possession or under its control in accordance with subsection (e) below.

   d. Post-Termination Assistance: The State shall be entitled to any post-termination assistance with respect to the services unless a unique data retrieval arrangement has been established as part of the contract.

   e. Secure Data Disposal: When requested by the State, the provider shall destroy all requested data in all of its forms, including but not limited to: disk, CD/DVD, backup tape, and paper. Data shall be permanently deleted and shall not be recoverable, according to National Institute of Standards and Technology (NIST) approved methods and certificates of destruction shall be provided to the State.

6. Background Checks: The Provider shall conduct criminal background checks and not utilize any staff, including sub-contractors, to fulfill the obligations of the contract who has been convicted of any crime of dishonesty, including but not limited to criminal fraud, or otherwise convicted of any felony or any misdemeanor offense for which incarceration for up to 1 year is an authorized penalty. The Provider shall promote and maintain an awareness of the importance of securing the State's Data among the Provider's employees and agents.

7. Access to security logs and other reports: The Provider shall provide logs and reports to the State in a format as specified in the contract and agreed to by both the Provider and the State. Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all State Data related to this contract, including but not limited to data, file management, transactions, or tools used to provide, manage, secure, or analyze the State's Data. The Provider shall maintain the reports and logs for the contract term and for two (2) years after the conclusion of the term, and shall provide them to the State in the course of a State audit or upon written request from the State.

8. Service Level Audit: The Provider shall allow the State to audit conformance to the contract terms. The State may perform this audit or contract with a third party at its discretion, at the State's expense.

9. Data Center Audit: The Provider shall have an independent third party audit of its data center(s) performed at least annually at their own expense, and provide the audit report to the State upon request.

10. Change Control and Advance Notice: The Provider shall give advance notice to the State of any upgrades (e.g. major upgrades, minor upgrades, system changes) that may impact service availability and performance. Said notice shall be provided at least thirty days in advance of the upgrade, unless otherwise agreed in the SLA.

11. Security: The Provider shall disclose its non-proprietary security processes and technical limitations to the State by completing the State's Security Controls Checklist or equivalent system security document, available upon request from the Office of Information Technology, as updated from time to time, such that adequate protection and flexibility can be attained between the State and the Provider.

12. Non-disclosure and Separation of Duties: The Provider shall enforce separation of job duties, require commercially reasonable non-disclosure agreements, and limit staff knowledge of State Data to that which is absolutely needed to perform job duties.

13. Import and Export of Data: The State shall have the ability to import or export data in piecemeal or in entirety at its discretion without interference from the Provider. This includes the ability for the State to import or export data to/from other Providers.

14. Responsibilities and Uptime Guarantee: The Provider shall be responsible for the acquisition and operation of all hardware, software, and network support related to the services being provided. The technical and professional activities required for establishing, managing, and maintaining the environment are the responsibilities of the Provider. The system shall be available 24 hours per day, 365 days per year (with agreed-upon maintenance downtime), and Provider shall provide service to the State as defined in the Service Level Agreement.

15. Right to Remove Individuals: The State shall have the right at any time to require that the Provider remove from interaction with the State any Provider representative who the State believes is detrimental to its working relationship with the Provider. The State will provide the Provider with notice of its determination, and the reasons it requests the removal. If the State signifies that a potential security violation exists with respect to the request, the Provider shall immediately remove such individual. The Provider shall not assign the person to any aspect of the contract or future work orders without the State's consent.

    Business Continuity and Disaster Recovery: The Provider shall provide a business continuity and disaster recovery plan upon request and ensure that the State's Recovery Time Objective (RTO) is met. The RTO shall be defined in the SLA.

B. INDEMNIFICATION FOR SAAS

Section 4.1 Indemnification of the SSTC is deleted in its entirety and replaced with the following;

4.1 INDEMNIFICATION

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

1. The Contractor shall indemnify, defend, and save harmless the State and its officers, agents, servants and employees, from and against any and all third party claims, demands, suits, actions, recoveries, judgments and costs and expenses in connection therewith:
    i. For or on account of the loss of life, tangible property (not including lost or damaged data) or injury or damage to the person, body or property (not including lost or damaged data) of any person or persons whatsoever, which shall arise from or result directly or indirectly from the work and/or products supplied under this Contract; and
    ii. For or on account of the use of any patent, copyright, trademark, trade secret or other proprietary right of any copyrighted or uncopyrighted composition, secret process, patented or unpatented invention, article or appliance

("Intellectual Property Rights") furnished or used in the performance of the contract; and

iii. For or on account of a Breach of Security resulting from Contractor's breach of its obligation to encrypt Personal Data or otherwise prevent its release or misuse; and

iv. The Contractor's indemnification and liability under Section 4.1(A)(1) is not limited by, but is in addition to the insurance obligations contained in Section 4.2 of the State Standard Terms and Conditions.

2. In the event of a claim or suit involving third-party Intellectual Property Rights, the Contractor, at its option, may: (1) procure for the State the legal right to continue the use of the product; (2) replace or modify the product to provide a non-infringing product that is the functional equivalent; or (3) refund the purchase price less a reasonable allowance for use that is agreed to by both parties. The State will: (1) promptly notify Contractor in writing of the claim or suit; (2) Contractor shall have control of the defense and settlement of any claim that is subject to Section 4.1(A)(1); provided, however, that the State must approve any settlement of the alleged claim, which approval shall not be unreasonably withheld. The State may observe the proceedings relating to the alleged claim and confer with the Contractor at its expense. Furthermore, neither Contractor nor any attorney engaged by Contractor shall defend the claim in the name of the State of New Jersey, nor purport to act as legal representative of the State of New Jersey, without having provided notice to the Director of the Division of Law in the Department of Law and Public Safety and to the Director of DPP. The State of New Jersey may, at its election and expense, assume its own defense and settlement.
3. Notwithstanding the foregoing, Contractor has no obligation or liability for any claim or suit concerning third-party Intellectual Property Rights arising from: (1) the State's unauthorized combination, operation, or use of a product supplied under this contract with any product, device, or software not supplied by Contractor; (2) the State's unauthorized alteration or modification of any product supplied under this contract; (3) the Contractor's compliance with the State's designs, specifications, requests, or instructions, provided that if the State provides Contractor with such designs, specifications, requests, or instructions, Contractor shall review same and advise if such designs, specifications, requests or instructions present potential issues of patent or copyright infringement and the State nonetheless directs the Contractor to proceed with one or more designs, specifications, requests or instructions that present potential issues of patent or copyright infringement; or (4) the State's failure to promptly implement a required update, use a new version of the product, or to make a change or modification to the product if requested in writing by Contractor.
4. Contractor will be relieved of its responsibilities under Subsection 4.1(A)(1)(i), (ii), and (iii) for any claims made by an unaffiliated third party that arise solely from the actions or omissions of the State, its officers, employees or agents.
5. This section states the entire obligation of Contractor and the exclusive remedy of the State, in respect of any infringement or alleged infringement of any Intellectual Property Rights. This indemnity obligation and remedy are given to the State solely for its benefit and in lieu of, and Contractor disclaims, all warranties, conditions and other terms of non-infringement or title with respect to any product.
6. The provisions of this indemnification clause shall in no way limit the Contractor's obligations assumed in the Contract, nor shall they be construed to relieve the Contractor from any liability, nor preclude the State from taking any other actions available to it under any other provisions of the contract or otherwise at law or equity.
7. The Contractor agrees that any approval by the State of the work performed and/or reports, plans or specifications provided by the Contractor shall not operate to limit the obligations of the Contractor assumed in the Contract.
8. The State of New Jersey will not indemnify, defend or hold harmless the Contractor. The State will not pay or reimburse for claims absent compliance with Section 4.1(B) below and a determination by the State to pay the claim or a final order of a court of competent jurisdiction.

B. STATE RESPONSIBILITIES - Subject to the New Jersey Tort Claims Act (N.J.S.A. 59:1-1 et seq.), the New Jersey Contractual Liability Act (N.J.S.A. 59:13-1 et seq.) and the appropriation and availability of funds, the State will be responsible for any cost or damage arising out of actions or inactions of the State, its employees or agents under Section 4.1(A)(1)(i), (ii), and (iii) which results in an unaffiliated third party claim. This is Contractor's exclusive remedy for these claims.

B. INSURANCE FOR SAAS

Section 4.2 Insurance of the SSTC is supplemented with the following:

1. 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 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.

2. Cyber Breach Insurance

   The Contractor shall carry Cyber Breach Insurance in sufficient to protect the Contractor from any liability arising out of its performance pursuant to the requirements of this Contract. The insurance shall be in an amount of not less than $2,000,000 in such policy forms as shall be approved by the State. The insurance shall at a minimum cover the following: Data loss, ransomware and similar breaches to computers, servers and software; Protection against third-party claims; cost of notifying affected parties; cost of providing credit monitoring to affected parties; forensics; cost of public relations consultants; regulatory compliance costs; costs to pursue indemnity rights; costs to Data Breach and Credit Monitoring Services analyze the insured's legal response obligations; costs of defending

lawsuits; judgments and settlements; regulatory response costs; costs of responding to regulatory investigations; and costs of settling regulatory claims.

C. LIMITATION OF LIABILITY FOR SAAS

Section 4.0 Indemnification and Insurance of the SSTC is supplemented with the following:

4.3 LIMITATION OF LIABILITY

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

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

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

B. The Contractor shall not be liable for punitive, special, indirect, incidental, or consequential damages.

State of New Jersey Standard Terms and Conditions and Waivered Contracts/Delegated Purchase Authority
Supplement to the State of New Jersey Standard Terms and Conditions
(Revised February 8, 2024)

I HEREBY ACCEPT THE TERMS AND CONDITIONS OF THIS CONTRACT

Signature

Date

Print Name and Title

Print Name of Contractor

ATTACHMENT B
SAMPLE PFRSNJ ELECTION TIMELINE

PFRSNJ ELECTION TIMELINE
Fire Position Commencing February 2023

March 25, 2022	Electronic Notice Sent to PFRS employers.
March 25 – May 20, 2022	Members write to the PFRSNJ staff requesting to be candidates and to request nominating instructions.
June 24, 2022	Vendor closes the nominations website and stops accepting nominations from candidates.
June 27 – July 1, 2022	Vendor verifies petition information and determines those who qualify for election.
July 5, 2022	Notify winners and losers of nomination. Sole winners are automatically elected.

IF MORE THAN ONE CANDIDATE QUALIFIES AND AN ELECTION IS NECESSARY

July 15, 2022	Candidate names selected for position on ballot. Final information emailed to vendor.
August 15, 2022	Sample ballot and envelope submitted by vendor to the PFRSNJ staff.
August 22, 2022	PFRSNJ staff approves final ballot.
August 29 – September 2, 2022	Vendor prints election packets & prepares for mailing to locations.
On or about September 12, 2022	Vendor mails all ballots to employers.
September 12 – November 10, 2022	Completed ballots returned to the vendor (voting ends).
November 14 - 16, 2022	Ballots counted.
November 18, 2022	Vendor completes final tabulation.
November 21, 2022	Vendor submits official results to the PFRSNJ Board Secretary.
December 12, 2022	PFRSNJ Board of Trustees certifies official results at its December meeting.
February 1, 2023	Fire elected position term begins.