Request for Quotes

State Integrated Recovery Operations and Management Systems (SIROMS)

	Date	Time
Due Date For Questions and RSVP for Optional Bidder Conference	**Wednesday, February 5, 2025**	2:00 PM
Optional Bidder Conference	**Week of February 10, 2025**	Specific Date & Time will be sent to Interested Bidders who RSVP
Submission Date	**Wednesday, February 19, 2025**	2:00 PM

Dates are subject to change. All times contained in the RFQ refer to Eastern Time.
All changes will be reflected in Bid Amendments to the Request for Quotes posted on Using Agency website.

RFQ Issued By:
State of New Jersey
Department of Community Affairs
101 South Broad Street
Trenton, NJ 08625

Date: January 22, 2025

TABLE OF CONTENTS

1 INTRODUCTION AND SUMMARY OF THE REQUEST FOR QUOTES

This Request for Quotes (RFQ) is issued by New Jersey Department of Community Affairs (NJDCA/Using Agency). The Contract will be awarded in the State of New Jersey's eProcurement system, ***NJSTART*** *(*www.njstart.gov*).* The awarded Contractor is advised to read through all Quick Reference Guides (QRGs) located on the NJSTART Vendor Support Page for information.

1.1 PURPOSE, INTENT, AND BACKGROUND

The purpose of this RFQ is to solicit Quotes from qualified Bidders with demonstrated experience in providing information technology ("IT") solutions for disaster recovery projects, which will allow the State to retain a Contractor to rapidly operate, manage, host, and maintain the existing state-owned Custom Software package known as State Integrated Recovery Operations and Management System (hereinafter referred to as "SIROMS" or the "System") as specified by NJDCA-Division of Disaster Recovery and Mitigation (DRM) program requirements and guidelines. The SIROMS environment is Custom Software created for the State of New Jersey and wholly owned by it.

It is the intent of the State to award a Contract to that responsible General Services Administration ("GSA") Bidder whose Quote, conforming to this RFQ is most advantageous to the State of New Jersey (State), price and other factors considered. The State will only consider Bidders who are on the GSA vendor list with the approved SIN #. The State may award any or all price lines. The State, however, reserves the right to separately procure individual requirements that are the subject of the Contract during the Contract term, when deemed to be in the State's best interest.

The NJDCA has years of experience overseeing housing recovery and mitigation efforts that started when Superstorm Sandy hit the State in 2012 and has developed a suite of software to support these efforts called the State's Integrated Recovery and Management Software (SIROMS).

DRM will continue its Superstorm Sandy work, particularly in the area of housing, infrastructure, and planning programs. Additionally, DRM manages multiple other Federal and State grants within the SIROMS environment, and will continue to expand its portfolio within SIROMS over the coming years.

Due to NJDCA's disaster recovery, resilience, and mitigation experience, the DRM is uniquely positioned to expand its role beyond Superstorm Sandy work. Accordingly, in February 2021, NJDCA officially changed the name of the Sandy Recovery Division (SRD) to the Division of Disaster Recovery and Mitigation, or DRM, to better reflect the NJDCA's mission of strengthening the State's long-term resilience against severe weather and catastrophic events.

The Governor's Office also appointed DRM as grant manager for the Coronavirus State Fiscal Recovery Fund (CSFRF) and the Coronavirus Capital Projects Fund (CPF), comprising more than $6.6 billion allocated to the State through the American Rescue Plan Act (ARPA). The CSFRF and CPF monies are directed to not only help address the COVID-19 public health emergency, but to facilitate a full economic recovery and to address economic inequities that the COVID-19 emergency exposed. DRM is responsible for overseeing the allocation of this funding and ensuring it meets all U.S. Treasury requirements.

DRM has initiated the planning of a new housing-related program in the wake of Hurricane Ida that contemplates using dollars from the FEMA Hazard Mitigation Grant Program (HMGP), in addition to the recent HUD award of over $228 million, to facilitate the State's recovery. DRM will be designing and administering additional infrastructure programs. Whether housing or infrastructure, all programs will have a mitigation or resiliency component.

The SIROMS environment is a fully functional IT solution that allows the State to manage its CDBG-DR Program to assist State residents. The SIROMS environment is Custom Software, created for the State of New Jersey and wholly owned by it. Please review Attachment 2 (SIROMS Technical Details) for additional information about the SIROMS environment.

SIROMS is a suite of software tools used throughout the Sandy grant to facilitate the financial management, grant management, federal reporting, document retention, and provides various administrative tools to the program.

1.2 ORDER OF PRECEDENCE OF CONTRACTUAL TERMS

The Contract awarded, and the entire agreement between the parties, as a result of this RFQ shall consist of: (1) the final RFQ, (2) State of New Jersey Standard Terms and Conditions, and (3) the Quote. In the event of a conflict in the terms and conditions among the documents comprising this Contract, the order of precedence is for purposes of interpretation thereof, listed from highest ranking to lowest ranking as noted above.

Any other terms or conditions, not included with the Bidder's Quote and accepted by the State, shall not be incorporated into the Contract awarded. Any references to external documentation, including those documents referenced by a URL, including without

limitation, technical reference manuals, technical support policies, copyright notices, additional license terms, etc., are subject to the terms and conditions of the RFQ and the State of New Jersey Standard Terms and Conditions. In the event of any conflict between the terms of a document incorporated by reference, the terms and conditions of the RFQ and the State of New Jersey Standard Terms and Conditions shall prevail.

2 PRE-QUOTE SUBMISSION INFORMATION

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

2.1 QUESTION AND ANSWER PERIOD

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

A. Questions should be directly tied to the RFQ and asked in consecutive order, from beginning to end, following the organization of the RFQ; and
B. A Bidder shall submit questions only to the Using Agency designee by email DRM.Solicitations@dca.nj.gov. The Using Agency will not accept any question in person or by telephone concerning this RFQ. The cut-off date for electronic questions and inquiries relating to this RFQ is indicated on the RFQ cover sheet. In the event that questions are posed by Bidders, answers to such questions will be issued by Addendum. Any Addendum to this RFQ will become part of this RFQ and part of any Contract awarded as a result of this RFQ. Addenda to this RFQ, if any, will be posted to the Using Agency's website.

2.2 OPTIONAL BIDDER CONFERENCE

After the Using Agency (DRM) has posted answers to the bidders' questions, DRM will host an optional Bidder Conference for interested bidders to learn more about the SIROMS software. The Bidder Conference will be held at the Using Agency address provided on the RFQ cover sheet.

Bidders interested in attending the optional Bidder Conference must email DRM.Solicitations@dca.nj.gov by the date indicated on the RFQ cover sheet for Bidder's Questions. The Using Agency will then reach out to the interested bidders with specific details pertaining to the optional Bidder Conference.

2.3 BID AMENDMENTS

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

3 QUOTE SUBMISSION REQUIREMENTS

3.1 QUOTE SUBMISSION

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

3.2 BIDDER RESPONSIBILITY

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

3.3 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 State of New Jersey Standard Terms and Conditions. Bidder proposed terms or conditions that conflict with those contained in the State of New Jersey Standard Terms and Conditions 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
- Attachment 3 - State Price Sheet
- Attachment 7 - State of New Jersey Security Due Diligence Third-Party Information Security Questionnaire

A Bidder should not password protect any submitted documents. Use of URLs in a Quote should be kept to a minimum and shall not be used to satisfy any material term of 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 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 State's request or the State may deem the Quote non-responsive.

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 Using Agency may rely upon that form; however, if there has been a change in ownership within the last six (6) months, a new Ownership Disclosure Form must be completed, signed and submitted with the Quote; or, (c) a Bidder with any direct or indirect parent entity which is publicly traded may submit the name and address of each publicly traded entity and the name and address of each person that holds a 10 percent or greater beneficial interest in the publicly traded entity as of the last annual filing with the federal Securities and Exchange Commission or the foreign equivalent, and, if there is any person that holds a 10 percent or greater beneficial interest, also shall submit links to the websites containing the last annual filings with the federal Securities and Exchange Commission or the foreign equivalent and the relevant page numbers of the filings that contain the information on each person that holds a 10 percent or greater beneficial interest. N.J.S.A. 52:25-24.2.

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

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 affiliates, is involved in any of the investment activities set forth in N.J.S.A. 52:32-56(f). If the Bidder is unable to so certify, the Bidder shall provide a detailed and precise description of such activities as directed on the form. If a Bidder does not submit the form with the Quote, the Bidder must comply within seven (7) business days of the State's request or the State may deem the Quote non-responsive.

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

3.5.5 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 State's request or the State may deem the Quote non-responsive.

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 State's request or the State may deem the Quote non-responsive.

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 State reserves the right to request that the Bidder submit the form after Quote submission.

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

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

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

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

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

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

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

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

3.5.8.1 SMALL BUSINESS AND/OR DISABLED VETERANS' BUSINESS SUBCONTRACTING SET-ASIDE CONTRACT

NOT APPLICABLE TO THIS PROCUREMENT.

3.5.9 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. The Campaign Contributions and Expenditure Reporting Act, 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). The Contract awarded as a result of this Bid Solicitation shall be considered non-fair and open and therefore subject to the political contribution disclosure required by Chapter 51 and Executive Order 333.

For Contracts Awarded to a Non-Fair and Open Process

Pursuant to Chapter 51 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, 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 Chapter51.pdf (nj.gov)

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, instruction and the application are available at https://www.state.nj.us/treasury/contract_compliance/index.shtml.

3.5.11 RESERVED

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

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

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

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

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

3.5.13 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 Bidder should verify its Business Registration Certification Active status on the "Maintain Terms and Categories" Tab within its profile in ***NJSTART***. In the event of an issue with a Bidder's Business Registration Certification Active status, ***NJSTART*** provides a link to take corrective action.

3.5.14 CERTIFICATION OF NON-INVOLVEMENT IN PROHIBITED ACTIVITIES IN RUSSIA OR BELARUS PURSUANT TO P.L.2022, C3

The Bidder should submit Certification of Non-Involvement in Prohibited Activities in Russia or Belarus Pursuant to N.J.S.A. § 52:32-60.1. Pursuant to P.L.2022, c.3, a person or entity seeking to enter into or renew a contract for the provision of goods or services shall certify that it is not Engaging in Prohibited Activities in Russia or Belarus as defined by P.L.2022, c.3, sec. 1(c). If the Contractor is unable to so certify, the Contractor shall provide a detailed and precise description of such activities.

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

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 Evaluation Committee in its review of the Bidder's Quote.

3.7 MANAGEMENT OVERVIEW

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

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

3.8 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 State Contract Manager including, but not limited to, status meetings, status reports, etc.

3.9 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.

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

3.10 MOBILIZATION PLAN

It is essential that the State have quick use of the functionality this Contract is to provide. Therefore, each Bidder shall include as part of its Quote a mobilization plan, beginning with the date of notification of Contract award and lasting no longer than 30 business days .

Such mobilization plan shall include the following elements:

A. A detailed timetable for the mobilization period of 30 business days. This timetable should be designed to demonstrate how the Bidder will have the personnel and equipment it needs to begin work on the Contract up and operational from the date of notification of award;
B. The Bidder's plan for the deployment and use of management, supervisory or other key personnel during the mobilization period. The plan should show all management, supervisory and key personnel that will be assigned to manage, supervise and monitor the Bidder's mobilization of the Contract within the 30 business day period. The Bidder should clearly identify management, supervisory or other key personnel that will be assigned only during the mobilization;
C. The Bidder's plan for recruitment of staff required to provide all services required by the RFQ on the Contract start date at the end of the mobilization period covering 30 business days. In the event the Bidder must hire management, supervisory and/or key personnel if awarded the Contract, the Bidder should include, as part of its recruitment plan, a plan to secure backup staff in the event personnel initially recruited need assistance or need to be replaced during the Contract term; and

D. The Bidder's plan for the purchase and distribution of equipment, inventory, supplies, materials, etc. that will be required to begin work on the Contract on the required start date.

3.11 ADDITIONAL PLANS

3.11.1 DISASTER RECOVERY PLAN

The Bidder shall submit a draft Disaster Recovery (DR) plan as part of the Quote, identifying locations and systems. The draft DR plan should demonstrate that the Bidder can continue to satisfy RFQ requirements to restore functionality and performance within 12-24 hours following an event where their primary hosting or business location is rendered unusable. Please see RFQ Section 4.5.1 for more information.

3.11.2 PERFORMANCE MANAGEMENT PLAN

The Bidder shall submit a draft Performance Management Plan in the Quote. This plan shall include both measurable hosted System performance and measurable Maintenance performance conducted by the Bidder staff. Please see RFQ Section 4.5.3 for more information.

At a minimum the Performance Management Plan shall describe how the Bidder shall meet the Service Metrics and Expected Service Levels set forth in the table below:

Service Metrics	Expected Service Level
Environment Metrics	
Fully Functional Infrastructure Uptime	99.7%
Fully Functional Applications Uptime	99.7%
Hosted System Responsiveness (Attachments)	Download and Upload 99% of attachments within 15 seconds
Hosted System Responsiveness (Actions)	99% of user actions compete within 2 seconds
Hosted System Responsiveness (Screens)	99% of screens load within 5 seconds
Help Desk Response (Via Telephone or In-Person)	
Response to Reported Helpdesk Issues: Defined as any issue which prevents a user from conducting their business as usual	Target Status Update: 30 Minutes Target Resolution or Workaround: 95% of the issues within 24 hours
Reporting Requests - Delivery	
New Report Request	20 Business Days
Scheduled Report Delivery	99% delivery within 1 hour of scheduled time
Scheduled Software Maintenance Request: Update to all effected reports	20 Business days of software release
Software Maintenance Requests(MR) – Response	
New Software Update	30 Business days

3.12 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.

3.13 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.

3.14 ORGANIZATION CHARTS

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

3.15 RESUMES

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

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

The Bidder should provide detailed resumes for each Subcontractor's management, supervisory, and other key personnel that demonstrate knowledge, ability, and experience relevant to that part of the work which the Subcontractor is designated to perform.

3.16 EXPERIENCE WITH CONTRACTS OF SIMILAR SIZE AND SCOPE

The Bidder should provide the three (3) most relevant 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 this necessary disclosure information may be cause for rejection of the Bidder's Quote by the State.

The Bidder should provide documented experience to demonstrate that each Subcontractor has successfully performed work on contracts of a similar size and scope to the work that the Subcontractor is designated to perform in the Bidder's Quote. A description of the Subcontractor's prior contracts should be included and should show how such contracts relate to the ability of the Subcontractor to complete the services it is designated to perform. The Bidder must provide a detailed description of services to be provided by each Subcontractor.

3.17 FINANCIAL CAPABILITY OF THE BIDDER

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

A. For publicly traded companies the Bidder 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, including a balance sheet, income statement, and statement of cash flow, and all applicable notes for the most recent calendar year or the Bidder's most recent fiscal year.

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

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

3.18 STATE-SUPPLIED PRICE SHEET INSTRUCTIONS

The Bidder must submit its pricing using the State-Supplied Price Sheet accompanying this RFQ as Attachment 3.

Any price changes including handwritten 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 pricing on the State-Supplied Price Sheet for each of the labor categories shown for Years One (1) through Four (4) and Optional Years Five (5) through (10), respectively. The Optional Years represent the Contract extension years if elected by the State after the Contract base term expires. Bidders shall submit an all-inclusive hourly rate for Labor Categories 1-3 and an annual rate for Hosting and Software Categories 4 and 5, respectively. A description of the Labor Categories can be found in Attachment 4. The Bidder shall not submit an estimate of the quantity of hours required to complete the work.

Failure to submit all information required will result in the proposal being disqualified.

3.18.1 DELIVERY TIME AND COSTS

Not applicable to this procurement.

3.18.2 CASH DISCOUNTS

The Bidder is encouraged to offer cash discounts based on expedited payment by the State. The State will make efforts to take advantage of discounts, but discounts will not be considered in determining the price rankings of Quotes. Should the Bidder choose to offer cash discounts, the following shall apply:

A. 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
B. 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.

3.18.4 USE OF "NO BID" VERSUS "NO CHARGE" ON THE STATE-SUPPLIED PRICE SHEET

All price lines must be filled out in accordance with the instructions above. If the Bidder is not submitting a price for an item on a price line, the Bidder must indicate "No Bid" on the State-Supplied Price Sheet accompanying this RFQ. If the Bidder will supply an item on a price line free of charge, the Bidder must indicate "No Charge" on the State-Supplied Price Sheet accompanying this RFQ. The use of any other identifier may result in the Bidder's Quote being deemed non-responsive.

4 SCOPE OF WORK

4.1 Business Objective

The business objective of this Contract is to maintain SIROMS and to support and assist with the implementation of the Action Plan and Action Plan Amendments to maintain disaster recovery services in a flexible, scalable, and efficient manner. The System provides to the State management and oversight capacity of the programs being used by other State Contractors and State Departments. The Contractor shall maintain and provide services for the full suite of IT services and platforms including but not limited to application software maintenance, production support, ACH processing, systems integration, database support, reporting, data warehouse support, disaster recovery, business support, helpdesk, website support, infrastructure support, hardware support, hosting, project management, and other IT related professional services as directed by the SCM for the System.

4.1.1 SUMMARY OF CONTRACT REQUIREMENTS

The Contractor shall maintain the greatest level of transparency within the limitations of State and Federal requirements. The Contractor shall:

A. Provide hosting, support, and maintenance for a full IT shared services platform including but not limited to application software maintenance, production support, electronic payment processing, systems integration, database support, reporting, data warehouse support, disaster recovery, business support, helpdesk, website support, infrastructure support, hardware support, hosting, project management, and other IT related professional services as directed by the SCM;
B. Host and maintain the System to efficiently implement and monitor the use of funds through the maintenance of a business process management system including tracking with application workflow and data management;
C. Maintain and enhance system and project controls, management, delivery, and oversight of disaster recovery projects;
D. Host and maintain a data warehouse where other authorized vendors and Departments will enter required fiscal, program, and performance data. The Contractor is responsible for providing a schedule of activities within 10 business days of Contract award that details how the Contractor assumes all responsibilities of the SIROMS System. The Contractor shall provide reporting accessible through Business Objects or a functional equivalent tool for reporting on project performance and effectiveness;
E. Maintain and enhance hosting infrastructure, system, and user support based upon the RFQ requirements and the RFQ Attachments, see Section 3.4.3 Hosting and Backup Services; and
F. The Contractor shall develop new functionality and enhancements to existing functionality as requested by the SCM.

Refer to Attachment 2 of this RFQ for details on existing SIROMS System, Infrastructure, Systems, Reporting and User Support.

4.2 Functional Requirements

4.2.1 CLOUD COMPUTING BUSINESS PROCESS MANAGEMENT (BPM) SYSTEMS

The Contractor shall maintain a full IT shared services platform including professional services and an IT operating environment with application development and technical and business process support. Services shall include Agile methodology to document the changes, create solutions, test, implement changes to business processes in support for fiscal, and IT processes training, maintenance, remediation of issues, consulting, software development, issue management, and other IT related professional services as directed by the SCM for the System. Data shall be captured in a format mutually agreed upon between the State and the Contractor that allows the State to obtain a monthly copy which shall comply with all applicable regulatory and reporting requirements contained in this RFQ, as directed by the SCM, or otherwise required by State or federal statutes or regulations.

The Contractor shall maintain the existing System and all its components including:

A. A process management engine designed to drive the progression of work in structured or unstructured processes or cases;
B. A graphical model-based environment for designing processes and supporting activities;
C. Capabilities to manage business rules to ensure regulatory and program compliance;
D. Content management capabilities to securely store files, electronic documents and images in compliance with the record retention requirements established in Section 4.4.6;
E. Internet role-based interaction portals that allow staff and the recipients of grant funds to interact with the applicable processes they are involved on;
F. Ability to link processes to the resources they control such as proposals, grant activities, the recipients of grant funds and fund disbursements;
G. Active analytics engine for monitoring performance in areas such as processes, resources, grant activities and fund balances;
H. Reporting to provide decision support for program stakeholders;
I. Exportable data in formats deemed acceptable to the State at its sole discretion, for Extract Transfer Load (ETL) processes and advanced analytics that are acceptable to the State;
J. Management and administration;

K. Interface with external systems such as other State agencies, authorities, contractors and banks;
L. Maintain, enhance, and update Systems and interfaces as identified by the SCM
M. Websites that support SIROMS data; and
N. Geographic Information System (GIS) maps that support SIROMS data.

4.2.2 INTERFACES

The Contractor shall exchange data between other data systems using Industry Standard techniques. The Contractor shall be responsible for maintaining interfaces approved by the SCM s but not limited to the following:

A. Treasury Interface
    1. A1 Interface – SIROMS to NJCFS – Transfer Funds request information; and
    2. A1 Inbound Interface – NJCFS to SIROMS – Transfer Funds disbursement information.

All interface jobs must run at-a-minimum once a day or as required by the SCM. The interface jobs shall check for data or files to interface. If there is no data or files to interface, the job will be considered run successfully. The Contractor is not responsible for errors, delays, or outages on the 3rd party's platform.

Interfaces may include databases such as SQL or Oracle or the functional equivalent to be approved in advance by the SCM.

4.2.3 HELPDESK

The Contractor shall provide a pre-configured helpdesk system for tracking and resolving issues involving the System end-user issues. Helpdesk services are billed at the labor rates Contractor submitted on the State-Supplied Price Sheet for the Junior Consultant labor category. This solution shall be web-based and allow end-users to create, track, and be notified of updates and resolution via email of submitted issues. The Contractor shall staff and maintain the helpdesk during State work days (Monday-Friday 8:00 a.m. – 5:00 p.m. excluding state holidays). The helpdesk shall provide incident management process, compliant with Infrastructure Technology Information Library ("ITIL") standards.

A. Helpdesk functions shall include, at a minimum:
    1. Registration;
    2. Resolution;
    3. Trend and root cause analysis; and
    4. Problem management.
B. There shall be monitoring and escalation procedures that allow classification and prioritization of any reported issue as an incident, service request, or information request. Requests shall be accepted by phone, email, or online web submission and shall include the following:
    1. End-user satisfaction with the quality of the helpdesk and other IT services shall be measured quarterly or as directed by the State and reported to the SCM at least twice each year. This report shall be a Contract deliverable. The report shall measure actual performance against expected services level as set forth in the Service Metrics Table found in Section 4.5.3;
    2. The helpdesk shall be staffed appropriately for agreed upon service levels and for the amount of user support projected to be required to support existing systems and maintain SLAs. The recommended labor categories are referenced in Attachment 4;
    3. The service desk expects 1 ticket per 5 Active System Users. The Contractor shall be able to scale helpdesk staff during critical outages, and after planned system upgrades or maintenance;
    4. The Contractor shall train the helpdesk staff to understand the business functions provided by the System and the business processes that they support. As support requests come from different parties, and some issues may be passed to subcontractors or other vendors or Departments, the Contractor shall document the support process in detail. The documentation shall indicate process flow, interface points, and interaction between the various groups involved in user support, incident management, and issue resolution;
    4. The Contractor shall maintain helpdesk software used for tracking issues identified by the State for resolution by the Contractor. System Users, State staff, and the Contractor shall be able to create tickets via the web-based interface. This shall provide a centralized system to manage changes, issues, development and implementation issues, quality control, user acceptance, and other trackable issues as referenced throughout this RFQ. The System shall organize the issues by category, (i.e. hardware, software, application errors, issue logs, functional flaws, etc.) to allow the Contractor and the SCM to efficiently prioritize and monitor issue resolution;
    5. The Contractor shall provide reporting and access to the helpdesk software in a manner that allows the State to verify work performed by the Contractor. The information available to the State shall include, but not be limited to: Requestor, assigned technician, request type/subtype/category/priority, requests and times/dates, tech responses and times/dates, subsequent correspondences and times/dates, resolutions and times/date. The State shall receive updated information weekly or as requested; and

6. The Contractor shall notify the appropriate System users of any outages or events effecting the System's functionality within 30 business minutes of the issue's report and updates every two (2) business hours there-after until resolved.

4.2.4 SYSTEM ADMINISTRATION

The Contractor shall:

A. Provide, maintain, and enhance a cloud-based system that is accessible through internet-based web browsers and mobile devices;
B. Procure, manage, and maintain such hardware, software, and network(s) capacity required to support the program operations within 30 business days or otherwise directed by SCM. Such costs will be tied to Categories 5 and 6 of the State Price Sheet
C. At the time the Contract ends or is terminated, turn over all hardware, software, applications and data purchased by the State for the Contractor to use in the management of this Contract to the State in the manner agreed to within Section 5. All licenses shall be purchased so that they may be transferred to the State, or transitioned to the new Contractor at the State's discretion, when the Contract ends or is terminated;
D. Manage and maintain an infrastructure for file management of critical documents;
E. Manage and maintain the following copies of the database, or as directed by the SCM:
    1. Production;
    2. Development – Refreshed once per month;
    3. Quality Assurance/User Testing – Refreshed once per month; and
    4. Reporting – Refreshed every 24 hours; and
F. Assure the IT Infrastructure performs and maintain Virtual Machines (VMs) within the hosted environment annually in addition to maintaining all other requirements within this RFQ.

4.2.5 DATA WAREHOUSE ENVIRONMENT

The Contractor shall:

A. Manage a data repository that is compatible with the State's enterprise data warehouse environment and structure that receives data from multiple programmatic systems;
B. Maintain Microsoft SQL Server Reporting Services (SSRS) or the functional equivalent of a report generating software system as the main reporting tool for the end-users, unless otherwise directed by the SCM; and
C. Make changes to the data environment as directed by the SCM.

4.2.6 TECHNICAL SERVICES

The Contractor shall:

A. Provide technical services for project management, business and technical requirements analysis and documentation, software development or configuration of the business process management system, testing, system maintenance, and training;
B. Develop and maintain documents that detail specific tasks, milestone dates and deliverables for each System Change Request (SCR) upon award;
C. Maintain a method of tracking level of effort and costs down to the work order/change request level;
D. Maintain and utilize a formal change management process to manage all changes to software and hardware environments;
E. Provide an annual assessment and training of industry technology trends, including Customizable Off The Shelf (COTS), solutions to the State; and
F. Ensure the System maintains complies with Federal, State financial practices, government accounting standards, and program requirements.

All SCRs necessary to maintain SIROMS are within the scope of this Contract. The State may initiate an SCR for any value at any time. An SCR requires the approval by the SCM. SCR scope costs will be invoiced based on the existing State Price Sheet labor categories.

4.2.7 IT PRACTICES, DATA SECURITY AND INTEGRITY

The Contractor shall:

A. Ensure the System complies with federal and New Jersey laws in regards to IT systems including but not limited to N.J.S.A 56:8-161 through N.J.S.A 56:8-166 regarding PII;
B. Use industry standard best practices for data integrity including regular backups, off site disaster recovery functionality and redundant systems;
C. Use industry standard best practices for encryption techniques such as use of Secure Sockets Layer ("SSL")\Transport Layer Security ("TLS") protocol for transmittal of data through the internet;

D. Use Industry Standard best practices for operation of data centers such as use of access controls, N+1capacity (100% capacity) for (Heating, Ventilation, Air Conditioning ("HVAC"), electrical, Uninterruptible Power Supply ("UPS") and generator facilities and dual instances for services such as power and internet connectivity; and
E. The Contractor shall:
    1. Provide a hosting environment for all module components that provide internal audit assurance and an external audit assurance through StateRAMP PMO or NIST SP 800-53 rev 5 moderate security baseline for the Contractor's Commercial Cloud infrastructure. The Contractor's hosting environment shall provide internal audit assurance of infrastructure compliance to NIST SP 800-53 rev 5 moderate security baseline for clients hosted either on-prem or within an AWS or Azure Commercial Cloud;
    2. Initiate testing and security compliance reporting as required by the State and Federal Government within 30 business days of Contract award; or
    3. Ensure all components of the SIROMS environment are hosted within a State managed environment (i.e. OIT-AWS).

4.2.8 FUNCTIONAL REQUIREMENTS

The following services will be billed at the labor rates submitted on the State Price Sheet. The Contractor shall:

A. Provide support, maintenance, upgrades, or enhancements as required;
B. Identify and document business requirements in order to assist the State in maintaining functionality and technical requirements for the Business Process Management (BPM) system and other applications which support the State Program;
C. Work with the State to modify business and technical requirements, implementation capabilities, and change system requirements based on business needs;
D. Make modifications that may be required based on the State's changing business needs. Updates to the application code shall include, but are not limited to:
    - Adding or updating modules;
    - Adding or updating reports;
    - Adding or updating interfaces;
    - Adding or editing existing code;
    - Creating or editing websites; and
    - Modification to software and database to accommodate business functionality for incoming programs/initiatives and to address any unanticipated State/federal mandates that result in minor software modifications; and
E. Make any necessary adjustments to the System based on feedback provided through the course of System use and that become necessary as a result of more sophisticated use and knowledge of the State's support systems.

4.3 TASKS AND DELIVERABLES

4.3.1 ROLE OF CONTRACTOR – STARTUP

The Contractor shall provide relevant personnel to obtain transitional training, access, and knowledge transfer from the State or current hosting/maintenance provider which shall be completed within 30 Business Days following Contract award. Transition will require the Contractor to cooperate with all parties necessary to facilitate the knowledge transfer including making the appropriate staff available for training and obtaining the necessary knowledge and skills required to host and maintain the SIROMS system in accordance with the requirements of this RFQ.

The Contractor is responsible for providing a schedule of activities within 10 business days of award that details how the Contractor assumes all responsibilities of the SIROMS System.

The Contractor shall assume all responsibilities pertaining to the hosting and maintenance of the SIROMS system within 40 business days.

4.3.2 CONTRACTOR STAFFING

The Contractor shall be responsible for staffing all positions under the Contract. These positions should be filled by a variety of staff found in Attachment 4 to support the requirements of this Contract.

During the Contract term the State and Contractor may work together to coordinate the hours of staffing positions.

The Contractor shall be responsible for recommending the final staff to fill positions under the Contract as part of its Quote. The State, however, shall be provided the opportunity to approve staff that the Contractor provided as part of its Quote and within the Contract term.

The Contractor shall require all staff that interface directly with the State to be on-site as directed by the SCM. This includes, but is not limited to, Project Manager, Business Analysts, Helpdesk Manager, and Helpdesk Analysts.

The functional responsibilities and the minimum criterion for education and experience for State approval to fill these positions under the Contract are described in Attachment 4. As required based on project needs, Contractor shall onboard new staff with the necessary skills and expertise within 30 business days of SCM notifying of the project request. Preferably, Contractor has access to a pool of staff "bench" resource that can be onboarded within the 30 day timeframe.

Contractor may, at the SCM's direction, provide Staff Augmentation, wherein the organization uses an outsourcing strategy to staff their project and meet submission deadlines successfully. This technique includes evaluating the current staff and determining additional proficiency. Staff augmentation is the utilization of outside personnel temporarily to augment an organization's capability and report on progress on a regular basis.

4.3.3 ROLE OF STATE TECHNICAL STAFF AND KNOWLEDGE TRANSFER

The State will make its best effort to ensure the following key team members are available as needed. The State may choose to consolidate the roles below:

- State Contract Manager ("SCM"): The SCM will be the primary point of contact for all communications between the State and the Contractor, and will be responsible for coordinating with the Contractor to conduct weekly status meetings and determine the priority of items to be addressed by the Contractor throughout the duration of the Contract;
- Business Subject Matter Expert ("SME"): The SME will work closely with both the Contractor's project manager, and the SCM, and will participate in joint application design sessions to define functional requirements for any new or enhanced system components. The SME will also support user acceptance testing of any new or enhanced system components;
- IT Project Manager: The State Project Manager will work with the SCM and SME ensuring that the Contractor receives clear direction on priorities of work to be performed and timelines associated with this Contract; and
- Systems Administrator: The State systems administrator will work with the IT Project Manager and is responsible for overseeing the Contractor's systems administration, infrastructure design and maintenance, communication on system outages, and quality of helpdesk support.

4.3.4 CONTRACT CLOSEOUT

Upon conclusion of the Contract, the Contractor shall comply with the closeout criteria below:

- The Contractor and the State shall conduct a closeout meeting, at which time the Contractor shall submit to the SCM a concluding status report indicating that all work and deliverables have been successfully completed according to the requirements defined;
- Upon the SCM's approval all documentation developed for the Contract shall be turned over to the State;
- Contractor must provide transitional support and training at the request of the State under the same terms and conditions until a new contract can be completely operational. A
- The Contractor shall supply to the State with administrative access to all systems, software, and transfer any licenses.

4.4 TECHNICAL ENVIRONMENT

4.4.1 STATE TECHNOLOGY REQUIREMENTS AND STANDARDS

The Contractor must participate in the New Jersey Office of Information Technology's System Architecture Review along with State Agency Staff: https://nj.gov/it/whatwedo/sar/

The Contractor shall develop a system that complies with the guidance of the NJ Statewide Information Security Manual: https: //www.nj.gov/it/docs/ps/NJ_Statewide_Information_Securi ty_Manual.pdf.

The Contractor shall comply with the NJ Web Presence Guidelines: https://www.tech.nj.gov/it/docs/NJ_Web_Presence_Guidelines.pdf.

The System's compliance with Web Content Accessibility Guidelines (WCAG) 2.0 Level AA, shall be verified using a commercially available software product certified for this purpose. In compliance with the 21st Century Integrated Digital Experience Act, user authentication shall leverage the state's shared Identity and Access Management (IAM) strategy. Options include:

a. The myNJ web access management system which is SAML 2.0 compliant and integrates with service providers that support SAML 2 Web Single Sign On
b. Microsoft Entra ID/Active Directory for employee-only applications

The Contractor shall fully support and participate in audits conducted upon the system or data contained within the System at the request of the State.

4.4.2 SYSTEM DESIGN

All System and application related documentation including infrastructure and architecture details shall be provided to the State upon request.

4.4.3 HOSTING AND BACKUP SERVICES

The SCM will identify and approve the hosting requirements and backup requirements of the SIROMS environment, including but not limited to, hosting within the State's cloud environment and/or hosting within the Contractor hosting environment. The Contractor shall be responsible for maintaining the hosting environment and working with all necessary parties to facilitate that maintenance.

Below are additional details pertaining Contractor hosting environment:

- For a Contractor-hosted cloud solution, the Contractor shall host the System in the Contractor's cloud and not only secure the physical and virtual application infrastructure utilizing the OIT, or SCM identified security requirements, but also control and secure physical and virtual access to the application hosting facilities, the racks supporting network infrastructure and processing server equipment, web, application and database servers;
- Contractor's hosting environment for all module components should provide internal audit assurance and an external audit assurance through StateRAMP PMO or NIST SP 800-53 rev 5 moderate security baseline for the Contractor's Commercial Cloud infrastructure. The Contractor's hosting environment should also provide internal audit assurance of infrastructure compliance to NIST SP 800-53 rev 5 moderate security baseline for clients hosted either on-prem or within an AWS or Azure Commercial Cloud;
- The Contractor may house non-production environments outside of the same Datacenter; however, all production data must reside within a secure environment identified in this RFQ. Production data must not reside in non-secured environments;
- If the Contractor is not FedRamp Moderate certified, the Contractor shall run a background check on all personnel who have physical access to the data centers which house SIROMS systems or data. The primary and backup data centers must be within the United States. An attestation of these requirements must be provided annually;
- Using a process approved by the SCM, the Contractor shall download and back up the State's data and systems nightly or as otherwise approved by the SCM; and
- The Contractor shall provide a copy of the State's stored data that is stored within the Contractor provided State System. Stored data shall be supplied in a database, unless otherwise directed by the SCM.

4.4.4 EXTRANET PLAN

The SIROMS environment does not use any communication links identified below. The State reserves the right to require use of these Extranet Options or to add additional interfaces as required.

Extranet uses:

- When an external 3rd party needs to initiate file transfers to a Garden State Network (GSN) Department or Agency;
- When information exchange between external parties needs to be secured or routed over a private connection; and
- When 3rd Parties want to build a private connection to an entity on the GSN, while avoiding the uncertainty of using the Internet as a medium.

Extranet Options:

The communication links between the State and the Contractor can be through a dedicated circuit or IPSEC tunnel over the Internet based upon the connectivity requirements and cost constraints.

The Contractor must work with DCA and OIT to establish an Extranet Partner relationship. The State and the Contractor will be required to follow the State's Extranet Policy and Procedure, and complete the application form, Memorandum of Understanding (MOU), operational form and security controls assessment checklist.

DCA, OIT, and external 3rd Party must agree on the Extranet service level the System will be utilizing for the connection, the cost of the connection, and who will be paying for the agreed upon services.

The communication links between the State of New Jersey and the Contractor can be through a MPLS cloud (preferred) or IPSEC tunnel over the Internet based upon the connectivity requirements and cost constraints.

The Contractor shall provide and maintain two (2) extranet communication links into the State of New Jersey. One of these links will be active and one will be a "hot" spare. The State of New Jersey and the Contractor will be required to follow the State's Extranet Policy and Procedure, and complete the application form, MOU, operational form and security controls assessment checklist.

4.4.5 TRANSMISSION OF FILES

The transmission of all files between the Contractor and the State system shall be transferred securely using the State file transfer methodology or otherwise directed by the SCM and OIT. The State will work with the Contractor in the implementation of the file transfer process. The secure file transfer shall meet the State and federal security guidelines and standards.

The State provides both synchronous and asynchronous file transfer methodologies.

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

Asynchronous:
1) The State's DataMotion is a supported option for non-automated or "ad-hoc" file exchange with State of New Jersey. A client license is required; and
2) The State's DataMotion-DataBridge is a supported option for automated file exchange with the State of New Jersey.

The Contractor shall test the file transfer with the State system on all file transfers prior to full implementation.

During the term of the Contract, the State may revise or change the file transfer method and/or format for the transmission of files to accommodate real time processing, and use case specific information and the Contractor shall be required to conform to all requirements. Reference:
NIST Special Publication 800-47 - Security Guide for Interconnecting Information Technology Systems (http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf)

4.4.6 AUTOMATED RECORDS MANAGEMENT/STORAGE SYSTEMS AND RELATED SERVICES
The State is required to comply with the Open Public Records Act (OPRA) which may be found at: http://www.state.nj.us/grc/laws/act/act.pdf and the New Jersey Administrative Code Title 5, Chapter 105 N.J.A.C. 5:105 (2008) which may be found at: http://www.state.nj.us/grc/home/rules/pdf/Promulgated_Regulations.pdf.

The Contractor shall be responsible for establishing a process to ensure that all requests made upon the Vendor {Contractor} for information that fall under OPRA are recorded and transmitted electronically to the SCM. OPRA requests will be processed by the State OPRA Custodian within DCA who will be responsible resolving same.

The Contractor shall work with the State to maintain DORES annual certifications.

The Contractor shall comply with the State's records retention schedule and with all State records storage policies, including but not limited to the short and long-term housing of physical documents and electronic images (i.e. paper documents, emails, correspondence, training material, and policy and procedures associated with the Program, etc.)

The requirements for the retention of records pertaining to Federal Grants, Record Series #0406- 0001 on the G100000 schedule can be found at the following website: http://www.nj.gov/treasury/revenue/rms/retentiondisposition.shtml

4.5 ASSESSMENTS/PLANS
The Contractor shall provide detailed plans as set forth below. The State may request revisions to these plans.

4.5.1 DISASTER RECOVERY PLAN
The Contractor shall submit the final version of their Disaster Recovery plan (DR Plan) 30 business days after Contract award. The DR Plan shall identify locations and systems. The DR Plan shall demonstrate that the Contractor can continue to satisfy RFQ requirements to restore functionality and performance within 12-24 hours following an event where their primary hosting or business location is rendered unusable. The plan must be reviewed, updated, and provided to the SCM annually.

The Contractor is responsible for testing the disaster recovery functionality against the plan annually and should coordinate with OIT and agency staff.

The State Contract Manager may require an independent review of the testing procedures. The results to be shared with the SCM. Testing will not occur more often than every two (2) years at a cost to the Contractor.

4.5.2 CONTINGENCY PLAN

The Contractor shall have a Contingency Plan identifying key personnel, organization units, and alternate sites with telecommunications and computers consistent with the security plan and disaster recovery plan noted above.

The plan shall be provided to the SCM within 30 business days after Contract award.

4.5.3 PERFORMANCE MANAGEMENT PLAN

The Contractor shall submit the final version of their Performance Management Plan 30 business days after Contract Award, and annually thereafter. This plan shall include both measurable hosted System performance and measurable Maintenance performance conducted by the Contractor staff but is not limited to:

The Contractor shall provide the performance testing results within 20 business days of a request by the State.

At a minimum the Performance Management Plan shall describe how the Contractor shall meet the Service Metrics and Expected Service Levels set forth in the table below:

Service Metrics	Expected Service Level
Environment Metrics	
Fully Functional Infrastructure Uptime	99.7%
Fully Functional Applications Uptime	99.7%
Hosted System Responsiveness (Attachments)	Download and Upload 99% of attachments within 15 seconds
Hosted System Responsiveness (Actions)	99% of user actions compete within 2 seconds
Hosted System Responsiveness (Screens)	99% of screens load within 5 seconds
Help Desk Response (Via Telephone or In-Person)	
Response to Reported Helpdesk Issues: Defined as any issue which prevents a user from conducting their business as usual	Target Status Update: 30 Minutes Target Resolution or Workaround: 95% of the issues within 24 hours
Reporting Requests - Delivery	
New Report Request	20 Business Days
Scheduled Report Delivery	99% delivery within 1 hour of scheduled time
Scheduled Software Maintenance Request: Update to all effected reports	20 Business days of software release
Software Maintenance requests(MR) – Response	
New Software Update	30 Business days

4.6 SOFTWARE ENVIRONMENT

The Contractor shall be able to run and support software the State uses to maintain the current environment which includes, but is not limited to, those listed below:

Software	Version	Expertise Required
Apache Camel	2.12.1 & 2.16.2	4 Years
MSFT SQL Svr R2	2008 R2 - 64 Bit	3 Years
OpenText (BPM)	9.4.2	5 Years
OpenText (ECM)	10.0.0.2645	5 Years
Amazon Web Services and Hosting	2024	1.5 Years
SAP BO	Enterprise 4.0	5 Years
Business Objects SDK	BO 4.0 FP3	3 Years
Microsoft Visual Studio	2013 & 2015	1 Year
Microsoft SQL Server	2008 R2	3 Years
Microsoft SSRS	2008	3 Years
Tableau	2021.3.3	3 Years

ArcGIS Web	2024	3 Years

Contractor shall procure any new software within 30 business days of identifying the project need

4.7 LIQUIDATED DAMAGES

The Division and the Contractor ("the Parties") agree that it would be extremely difficult to determine actual damages which the State will sustain as the result of the Contractor's failure to meet the performance requirements.

Any breach by the Contractor may prevent the DRM from complying with State and Federal regulatory or legal requirements; will adversely impact DRM's ability to administer and monitor these funds; and may lead to damages suffered by the State. Therefore, the Parties agree that the liquidated damages specified in **Table 1** below are reasonable estimates of the damages the State may sustain from the Contractor's performance deficiencies set forth within this section and are not to be construed as penalties.

Contractor is not liable for State outages or delays caused by the State or a third party outside of the Contractor's scope of the Contract.

4.7.1 PAYMENT OF LIQUIDATED DAMAGES

Once assessed, liquidated damages will be deducted from any funds owed to the Contractor by the State, and in the event the amount due the Contractor is not sufficient to satisfy the amount of the liquidated damages, the Contractor shall pay the balance to the State of New Jersey within 30 calendar days of written notification of the assessment. If the amount due is not paid in full, the balance will be deducted from subsequent payments to the Contractor.

4.7.2 NOTIFICATION OF LIQUIDATED DAMAGES

Upon determination that liquidated damages are to be assessed, the Director or the State Contract Manager will notify the Contractor of the assessment in writing. The availability of any period of cure will depend on the situation and will be in the sole discretion of the Director. The Director may, in the Director's sole discretion, elect to notify the Contractor that liquidated damages may be assessed so as to provide a warning, prior to assessing them in accordance with this section, but if the Director does not provide such a warning, the Director is not precluded from assessing liquidated damages in accordance with this Contract. Notwithstanding any provision of any RFQ to the contrary, should there be any conflict between this section and any other provision of the RFQ, this section shall supersede such section of the RFQ.

4.7.3 CONDITIONS FOR TERMINATION OF LIQUIDATED DAMAGES

The continued assessment of liquidated damages may be terminated at the sole discretion of the Director, only if all of the following conditions are met: A. The Contractor corrects the condition(s) for which liquidated damages were imposed; B. The Contractor notifies the State Contract Manager in writing that the condition(s) has (have) been corrected; and C. The Director reviews and approves in writing the recommendation of State Contract Manager.

Table 1 Liquidated Damages

Number	Topic	Description	Method of Assessing Damage Occurred	Liquidated Damages
1	Help Desk Response	During normal business hours/days, Contractor did not respond to Help Desk requests within one business day of the request as required in the Service Metrics Chart in Section 4.5.3 under "Help Desk Response."	Contractor did not respond to 95% of the Help Desk requests within 24 hours. "Respond" means either resolving the issue or escalating the issue to the development team. See row under "Help Desk Response" in the Service Metrics chart in Section 4.5.3	$1,000 per occurrence

4.7.4 WAIVER OF LIQUIDATED DAMAGES/LIQUIDATED DAMAGES NOT EXCLUSIVE REMEDY

The continued assessment of liquidated damages may be waived in writing at the sole discretion of the Director. The waiver of any liquidated damages due shall constitute a waiver only as to such assessment of liquidated damages and not a waiver of any future liquidated damage assessments. Failure to assess liquidated damages or to demand payment of liquidated damages within any period of time shall not constitute a waiver of such claim by the State.

4.7.5 SEVERABILITY OF INDIVIDUAL LIQUIDATED DAMAGES

If any portion of the liquidated damages provisions is determined to be unenforceable by a New Jersey court in one (1) or more applications, that portion remains in effect in all applications not determined to be invalid and is severable from the invalid applications. If any portion of the liquidated damages provisions is determined to be unenforceable, the other provision(s) shall remain in full force and effect.

4.8 INVOICING

4.8.1 INVOICING REQUIREMENTS

Upon contract award, the State shall go over the invoicing procedures with the Contractor. Contractor shall submit monthly invoices into the SIROMS system. Invoices shall include a cover sheet based on a prescribe format as instructed by the State along with supporting documentation. In the case of labor invoices such as Categories 1-4 on the State Price Sheet, Contractor shall submit accompanying timesheets to support the billable hours.

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 State may have arising out of the Contractor's performance of this Contract.

5.1 CONTRACT TERM AND EXTENSION OPTION

The base term of this Contract shall be for a period of four (4) years.

This Contract may be extended up to six (6) years with no single extension exceeding one (1) year, by the mutual written consent of the Contractor and the State at the same terms, conditions, and pricing at the rates in effect in the last year of this Contract or rates more favorable to the State.

5.2 CONTRACT TRANSITION

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

During the transition period, the Contractor will be required to perform the services under the same terms and conditions as the original Contract until the newly awarded contractor is fully operational.

5.3 PERFORMANCE SECURITY

NOT APPLICABLE TO THIS PROCUREMENT

5.4 OWNERSHIP OF MATERIAL

NOT APPLICABLE TO THIS PROCUREMENT

5.5 SUBSTITUTION OF STAFF

NOT APPLICABLE TO THIS PROCUREMENT

5.6 DELIVERY TIME AND COSTS

NOT APPLICABLE TO THIS PROCUREMENT

5.7 ELECTRONIC PAYMENTS

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

5.8 QUARTERLY SALES REPORTING AND SUPPLIER CONVENIENCE FEE

NOT APPLICABLE TO THIS PROCUREMENT.

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 State, no later than thirty (30) business days after the award of the Contract. The State approval of the Security Plan shall be set forth in writing. In the event that the State reasonably rejects the Security Plan after providing the Contractor an opportunity to cure, the Director may terminate the Contract pursuant to the SSTC.

6.2 INFORMATION SECURITY PROGRAM MANAGEMENT

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

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

6.3 COMPLIANCE

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

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

6.4 PERSONNEL SECURITY

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

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

6.5 SECURITY AWARENESS AND TRAINING

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

A. Personnel are provided with security awareness training upon hire and at least annually, thereafter;
B. Security awareness training records are maintained as part of the personnel record;
C. Role-based security training is provided to personnel with respect to their duties or responsibilities (e.g. network and systems administrators require specific security training in accordance with their job functions); and

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

6.6 RISK MANAGEMENT

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

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

6.7 PRIVACY

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

A. Data Ownership. The State owns State Data. Contractor shall not obtain any right, title, or interest in any State Data, or information derived from or based on State Data.
B. Data usage, storage, and protection of Personal Data are subject to all applicable international, federal and state statutory and regulatory requirements, as amended from time to time, including, without limitation, those for HIPAA, Tax Information Security Guidelines for Federal, State, and Local Agencies (IRS Publication 1075), New Jersey State tax confidentiality statute, the New Jersey Privacy Notice found at NJ.gov, N.J.S.A. § 54:50-8, New Jersey Identity Theft Prevention Act, N.J.S.A. § 56:11-44 et. seq., the federal Drivers' Privacy Protection Act of 1994, Pub.L.103-322, and the confidentiality requirements of N.J.S.A. § 39:2-3.4. Contractor shall also conform to PCI DSS, where applicable.
C. Security: Contractor agrees to take appropriate administrative, technical and physical safeguards reasonably designed to protect the security, privacy, confidentiality, and integrity of user information. Contractor shall ensure that State Data is secured and encrypted during transmission or at rest.
D. Data Transmission: The Contractor shall only transmit or exchange State Data with other parties when expressly requested in writing and permitted by and in accordance with requirements of the Contract or the State of New Jersey. The Contractor shall only transmit or exchange State Data with the State of New Jersey or other parties through secure means supported by current technologies.
E. Data Storage: All data provided by the State of New Jersey or State data obtained by the Contractor in the performance of the Contract must be stored, processed, and maintained solely in accordance with a project plan and system topology approved by the State Contract Manager. No State data shall be processed on or transferred to any device or storage medium including portable media, smart devices and/or USB devices, unless that device or storage medium has been approved in advance in writing by the State Contract Manager. The Contractor must not store or transfer State of New Jersey data outside of the United States.
F. Data Re-Use: All State Data shall be used expressly and solely for the purposes enumerated in the Contract Data shall not be distributed, repurposed or shared across other applications, environments, or business units of the Contractor. No State Data shall be transmitted, exchanged or otherwise passed to other contractors or interested parties except on a case-by-case basis as specifically agreed to in writing by the State Contract Manager.
G. Data Breach: In the event of any actual, probable or reasonably suspected Breach of Security, or any unauthorized access to or acquisition, use, loss, destruction, compromise, alteration or disclosure of any Personal Data, Contractor shall: (a) immediately notify the State of such Breach of Security, but in no event later than 24 hours after learning of such security breach; (b) designate a single individual employed by Contractor who shall be available to the State 24 hours per day, seven (7) days per week as a contact regarding Contractor's obligations under *Bid Solicitation Section 6.34 - Incident Response*; (c) not provide any other notification or provide any disclosure to the public regarding such Breach of Security without the prior written consent of the State, unless required to provide such notification or to make such disclosure pursuant to any applicable law, regulation, rule, order, court order, judgment, decree, ordinance, mandate or other request or requirement now or hereafter in effect, of any applicable governmental authority or law enforcement agency in any jurisdiction worldwide (in which case Contractor shall consult with the State and reasonably cooperate with the State to prevent any notification or disclosure concerning any Personal Data or Breach of Security); (d) assist the State in investigating, remedying and taking any other action the State deems necessary regarding any Breach of Security breach and any dispute, inquiry, or claim that concerns the Breach of Security; (e) follow all instructions provided by the State relating to the Personal Data affected or potentially affected by the Breach of Security; (f) take such actions as necessary to prevent future Breaches of Security; and (g) unless prohibited by an applicable statute or court order, notify the State of any third party legal process relating to any Breach of Security including, at a minimum, any legal process initiated by any governmental entity (foreign or domestic).

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

I. End of Contract Data Handling: Contractor shall continue transfer of State Data on a scheduled frequency agreed upon with the SCM, no less than a quarterly basis. Upon termination/expiration of this Contract, Contractor shall return any remaining State Data not already transferred to the State in a usable, readable, and non-proprietary format as defined in the Contract, or in an open standards machine-readable format if not. The Contractor shall then erase, destroy, and render unreadable all Contractor backup copies of State Data according to the standards enumerated in accordance with the State's most recent Media Protection policy, https://www.nj.gov/it/docs/ps/NJ_Statewide_Information_Security_Manual.pdf, and certify in writing that these actions have been completed within 30 days after the termination/expiration of the Contract or within seven (7) days of the request of an agent of the State whichever should come first.

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

6.8 ASSET MANAGEMENT

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

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

6.9 SECURITY CATEGORIZATION

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

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

6.10 MEDIA PROTECTION

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

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

6.11 CRYPTOGRAPHIC PROTECTIONS

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

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

6.12 ACCESS MANAGEMENT

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

A. Ensure the principle of least privilege is applied for specific duties and information systems (including specific functions, ports, protocols, and services), so processes operate at privilege levels no higher than necessary to accomplish required organizational missions and/or functions;
B. Implement account management processes for registration, updates, changes and de-provisioning of system access;
C. Apply the principles of least privilege when provisioning access to organizational assets;
D. Provision access according to an individual's role and business requirements for such access;
E. Implement the concept of segregation of duties by disseminating tasks and associated privileges for specific sensitive duties among multiple people;
F. Conduct periodic reviews of access authorizations and controls.

6.13 IDENTITY AND AUTHENTICATION

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

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

6.14 REMOTE ACCESS

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

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

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

6.15 SECURITY ENGINEERING AND ARCHITECTURE

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

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

6.16 CONFIGURATION MANAGEMENT

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

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

6.17 ENDPOINT SECURITY

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

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

6.18 ICS/SCADA/OT SECURITY

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

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

6.19 INTERNET OF THINGS SECURITY

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

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

6.20 MOBILE DEVICE SECURITY

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

A. Establishing requirements for authorization to use mobile devices for organizational business purposes;
B. Establishing Bring Your Own Device (BYOD) processes and restrictions;
C. Establishing physical and logical access controls;
D. Implementing network access restrictions for mobile devices;
E. Implementing mobile device management solutions to provide centralized management of mobile devices and to ensure technical security controls (e.g. encryption, authentication, remote-wipe, etc.) are implemented and updated as necessary;
F. Establishing approved application stores from which applications can be acquired;
G. Establishing lists approved applications that can be used; and
H. Training of mobile device users regarding security and safety.

6.21 NETWORK SECURITY

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

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

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

6.22 CLOUD SECURITY

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

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

6.23 CHANGE MANAGEMENT

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

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

6.24 MAINTENANCE

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

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

6.25 THREAT MANAGEMENT

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

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

6.26 VULNERABILITY AND PATCH MANAGEMENT

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

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

6.27 CONTINUOUS MONITORING

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

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

6.28 SYSTEM DEVELOPMENT AND ACQUISITION

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

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

6.29 PROJECT AND RESOURCE MANAGEMENT

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

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

6.30 CAPACITY AND PERFORMANCE MANAGEMENT

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

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

6.31 THIRD PARTY MANAGEMENT

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

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

6.32 PHYSICAL AND ENVIRONMENTAL SECURITY

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

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

J. Delivery and removal of information assets controls.

6.33 CONTINGENCY PLANNING

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

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

6.34 INCIDENT RESPONSE

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

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

6.35 TAX RETURN DATA SECURITY

A. PERFORMANCE

1. In performance of this Contract, the Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:
2. All work will be done under the supervision of the Contractor or the Contractor's employees;
3. Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Contract Information contained in such material will be treated as confidential and will not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract Disclosure to anyone other than an officer or employee of the Contractor will be prohibited;
4. All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output will be given the same level of protection as required for the source material;
5. The Contractor certifies that the data processed during the performance of this Contract will be completely purged from all data storage components of his or her computer facility, and the Contractor will retain no output at the time the work is completed. If immediate purging of all data storage components is not possible, the Contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures;
6. Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used;
7. All computer systems receiving, processing, storing, or transmitting federal tax information must meet the requirements defined in IRS Publication 1075. To meet functional and assurance requirements, the security features of the environment must provide for the managerial, operational, and technical controls. All security features must be available and activated to protect against unauthorized use of and access to federal tax information.
8. No work involving federal tax information furnished under this Contract will be subcontracted without prior written approval of the IRS;
9. The Contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office; and
10. The agency will have the right to void this Contract if the Contractor fails to provide the safeguards described above.

B. CRIMINAL/CIVIL SANCTIONS

1. Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as five (5) years', or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further

disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1;

2. Each officer or employee of any person to whom returns or return information is or may be disclosed shall be notified in writing by such person that any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Contract Information contained in such material shall be treated as confidential and shall not be divulged or made known in any manner to any person except as may be necessary in the performance of this Contract Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as one (1) year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for federal employees] in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC section 7213A and 7431;
3. Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to Contractors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a Contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000; and
4. Granting a Contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Contractors must maintain its authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, Contractors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and Exhibit 5, IRC Sec. 7213 Unauthorized Disclosure of Information). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. For both the initial certification and the annual certification, the Contractor should sign, either with ink or electronic signature, a confidentiality statement certifying its understanding of the security requirements.

C. INSPECTION

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

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

7.1 INDEMNIFICATION

Section 4.1 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.

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;

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.

7.2 INSURANCE

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

7.2.2 CYBER BREACH INSURANCE

Section 4.2 of the SSTC supplemented with the following:

Cyber Breach Insurance: The Contractor shall carry Cyber Breach Insurance in an amount 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 $5,000,000 or higher if appropriate per each occurrence and in such policy forms as shall be approved by the State. The insurance shall at a minimum cover the following: Data loss, malware, ransomware and similar breaches to computers, servers and software; Protection against third-party claims; cost of notifying affected parties; cost of providing credit monitoring to affected parties; forensics; cost of public relations consultants; regulatory compliance costs; costs to pursue indemnity rights; costs to Data Breach and Credit Monitoring Services analyze the insured's legal response obligations; costs of defending lawsuits; judgments and settlements; regulatory response costs; costs of responding to regulatory investigations; and costs of settling regulatory claims.

7.3 LIMITATION OF LIABLITY

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.

7.4 PERFORMANCE GUARANTEE OF CONTRACTOR

Section 5.11 of the SSTC is supplemented with the following:

H. Third-Party Hosting.

1. To the extent Contractor has the legal right to do so, Contractor agrees to assign or pass through to the State or otherwise make available for the benefit of the State, any manufacturer's or supplier's warranty applicable to any third-party software, hardware or equipment provided by Contractor. Contractor does not itself give or make any warranty of any kind with respect to third-party software, hardware or equipment.
2. In addition, the terms and conditions below apply to the hosting services provided by an independent commercial public cloud infrastructure company ("Third-Party Hosting Supplier") as part of the services provided under this Contract.
    a. The State acknowledges and agrees that the Contractor will be contracting with a Third-Party Hosting Supplier as a vendor to provide the cloud computing platform and tools ("TPHS Platform") as part of the services provided under this Contract. The State agrees that Third-Party Hosting Supplier shall not be deemed a "subcontractor" under this Contract. The State hereby consents to:
        i. the use of the Third Party Hosting Supplier; and
        ii. the storage of State Data in, and transfer of State Data into, the TPHS Platform in the United States.
    b. The State acknowledges that the Contractor's provision of and the State's use of the TPHS Platform is subject to the terms and Third-Party Hosting Supplier's access policy available at: https://s3.amazonaws.com/Reseller-Program-Legal-Documents/AWS+Access+Policy.pdf as it may be updated by the Third-Party Hosting Supplier from time to time, and as may be made available on any successor or related site designated by the Third Party Hosting Supplier in the event such use is not discontinued and permanently resolved within ten (10) days of the State being notified of such suspension.
    c. The State acknowledges that aspects of, or changes to, the functionality of the TPHS Platform is outside of Contractor's direct control. In the event the TPHS Platform experiences an availability, performance, or security failure, or State data is lost, corrupted, or destroyed, solely as a result of an outage, malfunction, unavailability of or change by third party hosting supplier to a TPHS Platform component, or Third-Party Hosting Supplier fault or negligence (a "failure"):
        i. The Contractor shall coordinate with the Third-Party Hosting Supplier and the State to monitor status on resolving any such issue, and Contractor shall work collaboratively with the State to develop a mutually agreeable resolution to address the impact of such failure;
        ii. To the extent Third-Party Hosting Supplier provides a credit/payment to Contractor as a result, Contractor shall apply such amount against amounts due to Contractor for the services; and
        iii. Contractor shall not be in breach of any of its obligations or be liable for service credits as a result of such failure.
        iv. The foregoing shall not relieve Contractor from responsibility for any other aspects of the services, such as the functionality of the hosted solution, or from responsibility for Contractor not having properly installed or configured any TPHS Platform components in accordance with the Contract. Notwithstanding anything to the contrary herein, all rights and remedies to which contractor is entitled in the event of a failure shall flow through to the State.
    d. State Items, once uploaded to the TPHS Platform, will be subject to security control measures found at: [https://aws.amazon.com/whitepapers/#security; the confidentiality and data security obligations set forth in this Contract will not apply to such State Items on the TPHS Platform. However, this shall not relieve the Contractor from responsibility for any other aspects of the services, including, without limitation, not having installed or configured any TPHS Platform components properly, nor shall it relieve Contractor of its data breach notification obligations herein. Contractor shall promptly notify the State of any unauthorized third-party access to any State Items.
        i. "State Items" means any State-provisioned application or other software provided to Contractor for installation or uploading onto the TPHS Platform as part of the services ("State Software") and any State-provisioned machine images, data, text, audio, video, images or other content that is provided to Contractor for installation or uploading onto the TPHS Platform as part of the services, or that the State or any of its end user (a) runs on any State Software hosted on the TPHS Platform; (b) uploads to any State Software hosted on the TPHS Platform; or (c) causes to interface with the TPHS Platform.
    e. The State's audit rights set forth in this Contract shall not extend to Third-Party Hosting Supplier's facilities, books, and records. In lieu of such audit rights, the State may review whatever documentation the Third-Party Hosting Supplier makes available to its customers and provides to the Contractor.

WARRANTY DISCLAIMER: THE WARRANTIES SET FORTH IN THE CONTRACT ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, AND VENDOR {CONTRACTOR} EXPRESSLY DISCLAIMS ALL OTHER WARRANTIES, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.

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

8.2 CLARIFICATION OF QUOTE

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

8.3 TIE QUOTES

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

8.4 STATE'S RIGHT TO INSPECT BIDDER'S FACILITIES

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

8.5 STATE'S RIGHT TO CHECK REFERENCES

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

8.6 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.

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.

PRICE EVALUATION

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

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

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

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

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

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

8.11 CONTRACT AWARD

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

The RFQ, including any addenda, Bidder quote, Bidder presentations, Bidder capability evaluations, written responses to inquiries, the Best and Final Offer (BAFO) and other documentation from the selected Bidder, which describes the solution, commitment, capabilities, and intent of the Bidder, shall become part of any Contract initiated by the State.

In no event shall a Bidder submit its own standard Contract terms and conditions as a response to this RFQ. Any such submission shall be null and void unless expressly agreed to in writing by the State. The proposed terms will be negotiated before a final Contract is entered. The inclusion of mandatory clauses is not negotiable.

8.12 NOTICE OF EO 125 AND EO 166; POSTING OF CONTRACT

The Contract resulting from this RFQ is subject to the requirements of Executive Order No. 125 (Christy 2013) as a Sandy funded Contract, and Executive Order 166 (Murphy 2020) as a COVID-19 funded Contract, respectively. Please see the Notice of Executive Order125 attached as Attachment 5, and the Notice of Executive Order 166 attached as Attachment 6.

9 GLOSSARY

9.1 CROSSWALK

NJSTART Term	Equivalent Statutory, Regulatory and/or Legacy Term
Bid/Bid Solicitation	Request For Proposal (RFQ)/Solicitation
Bid Amendment	Addendum
Change Order	Contract Amendment
Master Blanket Purchase Order (Blanket/Blanket P.O.)	Contract
Offer and Acceptance Page	Signatory Page
Quote	Proposal
Vendor	Bidder/Contractor

9.2 DEFINITIONS

Unless otherwise specified in this RFQ, the following definitions will be part of any Contract awarded, or order placed, as a result of this RFQ. Note that not all definitions included here apply to all RFQs.

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

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

Apparel - means any clothing, headwear, linens or fabric.

Apparel Contracts - include all purchases, rentals or other acquisition of apparel products by the State of New Jersey, including authorizations by the State of New Jersey for vendors to sell apparel products through cash allowances or vouchers issued by the State of New Jersey, and license agreements with a public body.

Apparel Production - includes the cutting and manufacturing of apparel products performed by the vendor or by any subcontractors, but not including the production of supplies or sundries such as buttons, zippers, and thread.

Approved Products – Those products that have been identified in RFQ as meeting Using Agency needs and confirmed as meeting product specifications.

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

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

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

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

Bid Security - means a guarantee, in a form acceptable to the Division, that the bidder, if selected, will accept the contract as bid; otherwise, the bidder or, as applicable, its guarantor will be liable for the amount of the loss suffered by the State, which loss may be partially or completely recovered by the State in exercising its rights against the instrument of bid security.

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

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

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

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

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

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

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

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

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

Cooperative Purchasing Program – The Division's intrastate program that provides procurement-related assistance to New Jersey local governmental entities and boards of education, State and county colleges and other public entities having statutory authority to utilize select State Contract s issued by the Division, pursuant to the provisions of N.J.S.A. 52:25-16.1 et seq.

Cooperative Purchasing Participants - These participants include quasi-State entities, counties, municipalities, school districts, volunteer fire departments, first aid squads, independent institutions of higher learning, County colleges, and State colleges

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

Dealer/Distributor – A Company authorized by a Bidder or Contractor as having the contractual ability to accept and fulfill orders and receive payments directly on behalf of the Contractor that is awarded a Contract. Any authorized Dealer/Distributor must agree to all terms and conditions contained within the RFQ and must agree to provide all products and services in accordance with the Contract specifications, terms, conditions and pricing.

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

Director – Director, Division of Purchase and Property, Department of the Treasury, who by statutory authority is the Chief Contracting Officer for the State of New Jersey; or the Director's designee.

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

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

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

Division – The Division of Purchase and Property.

Equivalent Products – Products offered other than those identified as an Approved Product in this RFQ that meet the specifications herein. Equivalent Products will be evaluated to ensure that they meet all technical, nutritional, and packaging specifications herein as part of the Quote evaluation process.

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

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

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

Internet of Things (IoT) - the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and network

connectivity which enables these objects to connect and exchange data.

Intrastate cooperative purchasing participants - refers to political subdivisions, volunteer fire departments and first aid squads, and independent institutions of higher education and school districts pursuant to N.J.S.A. 52:25-16.1 et seq., State and county colleges pursuant to N.J.S.A. 18A:64-60 and 18A:64A-25.9, quasi-State agencies and independent authorities pursuant to N.J.S.A. 52:27B-56.1, and other New Jersey public entities having statutory authority to utilize select State contracts issued by the Division

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

Life cycle assessment – The comprehensive examination of a product's environmental and economic aspects and potential impacts throughout its lifetime, including raw material extraction, transportation, manufacturing, use and disposal.

Life cycle cost – The amortized total cost of a product, including capital costs, installation costs, operating costs, maintenance costs, and disposal costs discounted over the lifetime of the product.

Master Blanket Purchase Order (Blanket/Blanket P.O.) – A Term Contract that allows repeated purchases from an awarded contract.

Materials in Solid Waste – Material found in the various components of the solid waste stream. General, solid waste has several components, such as municipal solid waste (MSW), construction and demolition debris (C&D), and nonhazardous industrial waste. Under RCRA Section 6002, EPA considers materials recovered from any component of the solid waste stream when designating items containing Recovered Materials.

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

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

Must – Denotes that which is a mandatory requirement.

Net Purchases - means the total gross purchases, less credits, taxes, regulatory fees and separately stated shipping charges not included in unit prices, made by Intrastate Cooperative Purchasing Participants, regardless of whether or not ***NJSTART*** is used as part of the purchase process.

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

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

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

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

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

Personal Data means –

"Personal Information" as defined in N.J.S.A. 56:8-161, means an individual's first name or first initial and last name linked with any one or more of the following data elements: (1) Social Security number, (2) driver's license number or State identification card number or (3) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. Dissociated data that, if linked would constitute Personal Information is Personal Information if the means to link the dissociated were accessed in connection with access to the dissociated data. Personal Information shall not include publicly available information that is lawfully made available to the general public from federal, state or local government records, or widely distributed media; and/or

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

Personally Identifiable Information or PII - as defined by the U.S. Department of Commerce, National Institute of Standards and Technology, means any information about an individual

maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

Post-Consumer Material – Material or finished product that has served its intended use and has been diverted or recovered from waste destined for disposal, having completed its life as a consumer item. Post-Consumer Materials are part of the broader category of Recovered Materials.

Pre-Consumer Material – Materials generated in manufacturing and converting processes, such as manufacturing scrap and trimmings/cuttings.

Price List/Catalog – A document published by a manufacturer, resellers, Dealers, or Distributors that typically contains product descriptions, a list of products with fixed prices to which a Bidder's percentage discount or markup bid is applied.

Procurement Bureau (Bureau) – The Division unit responsible for the preparation, advertisement, and issuance of RFQs, for the tabulation of Quotes and for recommending award(s) of Contract(s) to the Director and the Deputy Director.

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

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

Purchases - means the total gross purchases, less credits, taxes, regulatory fees and separately stated shipping charges not included in unit prices, made regardless of whether or not NJSTART is used as part of the purchase process.

Quasi-State Agency - is any agency, commission, board, authority or other such governmental entity which is established and is allocated to a State department or any bi-state governmental entity of which the State of New Jersey is a member, as defined in N.J.S.A. 52:27B-56.1, provided that any sale to any such bi-state governmental entity is for use solely within the State of New Jersey.

Quick Reference Guides (QRGs) – Informational documents which provide Vendors with step-by-step instructions to navigate the NJSTART eProcurement System. QRGs are available on the NJSTART Vendor Support Page.

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

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

Recovered Material – Waste material and byproduct that have been recovered or diverted from solid waste, but does not include materials and byproducts generated from, and commonly reused within, an original manufacturing process.

Recycling – The series of activities, including collection, separation, and processing, by which products or other materials are recovered from the solid waste stream for use in the form of raw materials in the manufacture of new products other than fuel for producing heat or power by combustion.

Recyclability – The ability of a product or material to be recovered from, or otherwise diverted from, the solid waste stream for the purpose of recycling.

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

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

Revision – A response to a BAFO request or a requested clarification of the Bidder's Quote.

RMAN – Recovered Materials Advisory Notices provide purchasing guidance and recommendations for Recovered and Post-Consumer Material content levels for designated items.

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

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

Shall – Denotes that which is a mandatory requirement.

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

Small Business – Pursuant to N.J.S.A. 52:32-19, N.J.A.C. 17:13-1.2, and N.J.A.C. 17:13-2.1, "small business" means a business that meets the requirements and definitions of "small business" and has applied for and been approved by the New Jersey Division of Revenue and Enterprise Services, Small Business Registration and M/WBE Certification Services Unit as (i) independently owned and operated, (ii) incorporated or registered in and has its principal place of business in the State of New Jersey; (iii) has 100 or fewer full-time employees; and has gross revenues falling in one (1) of the six (6) following categories:
For goods and services - (A) 0 to $500,000 (Category I); (B) $500,001 to $5,000,000 (Category II); and (C) $5,000,001 to $12,000,000, or the applicable federal revenue standards established at 13 CFR 121.201, whichever is higher (Category III).
For construction services: (A) 0 to $3,000,000 (Category IV); (B) gross revenues that do not exceed 50 percent of the applicable annual revenue standards established at 13 CFR 121.201 (Category V); and (C) gross revenues that do not exceed the applicable annual revenue standards established at CFR 121.201, (Category VI).

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

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

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

State – The State of New Jersey.

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

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

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

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

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

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

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

Task – A discrete unit of work to be performed.

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

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

US CERT – United States Computer Emergency Readiness Team.

USEPA – United States Environmental Protection Agency

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

Vendor – Either the Bidder or the Contractor.

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

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

9.3 CONTRACT SPECIFIC DEFINITIONS/ACRONYMS

Action Plan/Action Plan Amendments – The State submitted a CDBG-DR Action Plan, which is posted on DCA's website at the following link: http://www.renewjerseystronger.org/plans-reports/ The State's CDBG-DR Action Plan was approved by the United States Department of Housing and Urban Development (HUD) on April 29, 2013. This plan and its Amendments detail, among other things, how the State plans to manage and spend the total allocation across all grant.

Active System User – A unique user that can be identified by a unique SIROMS account and who logs in to the SIROMS system within the three (3) months prior to an annual maintenance extension. The user is required to have an active SIROMS account, and currently have access to the SIROMS system. Users that do not log in during a specified period are not considered "Active System User" for that period.

Agile - A set of values and principles for software development under which requirements and solutions evolve through the collaborative effort of self-organizing cross-functional teams. It advocates adaptive planning, evolutionary development, early delivery, and continuous improvement, and it encourages rapid and flexible response to change

American Rescue Plan Act (ARPA) – Passed in March 2021 (Public Law 117-2) and established the Coronavirus State and Local Fiscal Recovery Funds (CLSFRF) to provide state, local and Tribal governments with the resources needed to respond to the pandemic and its economic effects and to build a stronger, more equitable economy during the recovery.

Business Process Management (BPM) – A systematic approach to making an organization's workflow more effective, more efficient, and more capable of adapting to an ever-changing environment. A business process is an activity or set of activities that will accomplish a specific organizational goal.

Business Objects (BO) – SAP Business Objects (BO or BOBJ) is an enterprise software company, specializing in business intelligence and enterprise level reporting.

Community Development Block Grant (CDBG) Program – A flexible program within HUD that provides communities with resources to address a wide range of unique community development needs.

Community Development Block Grant – Disaster Recovery (CDBG-DR) – A program within HUD that provides flexible grants to help cities, counties, and States recover from presidentially declared disasters, especially in low-income areas, subject to availability of supplemental appropriations.

Coronavirus State Fiscal Recovery Fund (CSFRF) – A part of the American Rescue Plan Act that specifically delivers $195.3 billion to all 50 states and the District of Columbia to help turn the tide on the pandemic, address its economic fallout, and lay the foundation for a strong and equitable recovery.

Coronavirus Capital Projects Fund (CPF) – Provides $10 billion for states, territories and tribes to cover the costs of capital projects such as broadband infrastructure.

DCA – New Jersey Department of Community Affairs.

DEP – New Jersey Department of Environmental Protection

Departments – State agencies, authorities, divisions, or other instrumentalities of the State, as identified in the Action Plan or otherwise designated by the State.

DORES – New Jersey Division of Revenue and Enterprise Service.

ETL – Extract Transform Load used in Database management within reporting.

FTE – "Full Time Equivalent" or 40 hours of Contractor support per week totaling 2,040 hours per year. The rate must be comprised of all direct and indirect costs including, but not limited to: labor costs, overhead, fee or profit, clerical support, travel expenses, per diem, safety equipment, materials, supplies, managerial support and all documents, forms, and reproductions thereof.

FTP – File Transfer Protocol, is a standard network protocol used for the transfer of computer files from a server to a client using the Client–server model on a computer network.

FTPS – Extension to commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SLL) cryptographic protocols.

GSA - The General Services Administration.

Helpdesk – A point of contact that provides users the ability to gain assistance in troubleshooting problems related to hardware, software and network related issues.

HUD – U.S. Department of Housing and Urban Development.

Hurricane Ida ("Ida") – a deadly and extremely destructive Category 4 Atlantic hurricane in 2021 that became the second-most damaging and intense hurricane to make landfall in the U.S. state of Louisiana on record, behind Hurricane Katrina in 2005. The storm then traveled northeast as a tropical depression, causing flash flooding, tornadoes, and power outages, before exiting offshore. The storm inflicted nearly $65 billion in damage and killed 107 people (87 in the United States and 20 in Venezuela).

INCLL – Incentives for Landlords - a CDBG-DR funded program managed within SIROMS.

Industry Standard – A method or technique that is generally accepted as superior to alternatives because it produces results that are superior to those achieved by other means and has become the standard way of doing things within the industry.

IPSEC – Internet Protocol Security - Protocol Suite for Secure Internet Protocol communications - authenticates and encrypts each IP packet of a communication session.

Key Personnel – Are considered Project Manager, Business Analyst, Helpdesk Manager, and CDBG Specialist.

LHRP – Lead Hazard Reduction Program, a CDBG-DR funded program managed within SIROMS.

LMI – Low to Moderate Income homeowner's rebuilding program, a CDBG-DR funded program managed within SIROMS.

LRRP – Landlord Rental Repair Program, a CDBG-DR funded program managed within SIROMS.

MOU – Memorandum of Understanding, a bilateral or multilateral agreement between two (2) or more parties.

NIST Special Publications – National Institute of Standards and Technology (NIST) Computer/Cyber information security and guidelines, recommendations, and reference materials.

NJCFS – New Jersey Comprehensive Financial System

NJSTC – New Jersey Standard Terms and Conditions

Number (#) of Active System Users- A count of unique "Active System Users" that have logged into SIROMS during a specified period. A user will be counted once regardless of times they have been active. The SIROMS maintenance Vendor {Bidder(s)} user accounts are not counted towards the total number of active numbers.

Processor Core - The processing unit which receives instructions and performs calculations, or actions, based on those instructions.

QPR – Quarterly Performance Report as required of HUD grantees to detail their use of CDBG-DR funds.

RREM – Reconstruction, Rehabilitation, Elevation and Mitigation, a CDBG-DR funded program managed within SIROMS.

SAGE – System for Administering Grants Electronically

SCR – System Change Request

SFTP – Simple File Transfer Protocol is one of the two primary technologies for secure FTP networking.

SSL – Secure Socket Layer is the standard technology for establishing an encrypted link between a web server and web browser.

SQL – Structured Query Language is used to communicate with a database. According to ANSI (American National Standards Institute), it is the standard language for relational database management systems.

System – The servers, software, integrations, databases, data warehouses, and reports required to encompass the SIROMS environment.

Virtual Machine (VM) – A software computer that, like a physical computer, runs an operating system and applications. The virtual machine is comprised of a set of specification and configuration files and is backed by the physical resources of a host.