State of New Jersey
DEPARTMENT OF BANKING AND INSURANCE
20 WEST STATE ST
TRENTON, NJ 08625-0325

PHIL MURPHY
Governor

SHEILA OLIVER
Lt. Governor

MARLENE CARIDE
Commissioner

Request for Proposal

for

The Development of a Technology Platform and Consumer Assistance Center for New Jersey's State Based Health Exchange

Solicitation Number: DOBI 2019-001

August 15, 2019

Event	Date
Request for Proposal Release	August 15, 2019
Deadline for Questions and Inquiries from Potential Bidders	August 22, 2019 5:00 PM EST
Deadline for Proposal Submission	September 20, 2019 5:00pm EST

DOBI Procurement Contact:
Thomas Gallagher
dobi.purchasing@dobi.nj.gov

Table of Contents

1.0 INFORMATION FOR BIDDERS 5

1.1 PURPOSE AND INTENT 5
1.2 BACKGROUND 6

1.2.1 HEALTH EXCHANGE PROJECT MANAGEMENT OFFICE 6
1.2.2 CASELOAD 7
1.2.3 FUNDING 8

1.3 KEY EVENTS 8

1.3.1 ELECTRONIC QUESTION AND ANSWER PERIOD 8
1.3.2 SUBMISSION OF PROPOSAL 8

1.4 ADDITIONAL INFORMATION 9

1.4.1 ADDENDA: REVISIONS TO THIS RFP 9
1.4.2 BIDDER RESPONSIBILITY 9
1.4.3 COST LIABILITY 9
1.4.4 CONTENTS OF PROPOSAL 9
1.4.5 PROPOSAL SUBMISSION DATE AND TIME 10
1.4.6 PRICE ALTERATION IN HARD COPY PROPOSALS 10
1.4.7 JOINT VENTURE 10
1.4.8 STATE REQUIREMENTS 11

2.0 DEFINITIONS PROCUREMENT 12

2.1 DEFINITIONS/ACRONYMS HEALTH EXCHANGE 13

3.0 SCOPE OF WORK (SOW) 16

3.1 PROJECT OVERVIEW AND OBJECTIVES 16
3.2 PART 1 – TECHNOLOGY PLATFORM FOR STATE BASED EXCHANGE 16

3.2.1 DETAILED REQUIREMENTS FOR COORDINATED AND INTEGRATED INSURANCE AFFORDABILITY PROGRAM ELIGIBILITY AND ENROLLMENT IN THE PART 1 TECHNOLOGY PLATFORM. 18

3.3 CONSTRAINTS TO PART 1 – TECHNOLOGY PLATFORM FOR STATE BASED EXCHANGE 20
3.4 PART 1 TIMELINE, ACTIVITIES, AND DELIVERABLES 21

3.4.1 TECHNOLOGY PLATFORM PHASE ONE 21
3.4.2 TECHNOLOGY PLATFORM PHASE TWO 24
3.4.3 TECHNOLOGY PLATFORM PHASE THREE: M&O 25
3.4.4 TECHNOLOGY PLATFORM ENHANCED PLAN 25

3.5 PART 2 - CONSUMER ASSISTANCE CENTER 26
3.6 CONSTRAINTS TO PART II – CONSUMER ASSISTANCE CENTER IMPLEMENTATION 27
3.7 PART 2 TIMELINE, ACTIVITIES, AND DELIVERABLES 27

3.7.1 CONSUMER ASSISTANCE CENTER PHASE ONE: IMPLEMENTATION 27
3.7.2 CONSUMER ASSISTANCE CENTER PHASE TWO: CONSUMER ASSISTANCE TRANSITION. 29
3.7.3 CONSUMER ASSISTANCE CENTER PHASE THREE: OPERATIONS. 29

3.8 PROJECT SUPPORT 29
3.9 TECHNICAL REQUIREMENTS - ASSESSMENTS AND PLANS 30

3.9.1 SECURITY PLAN 30
3.9.2 INFORMATION SECURITY PROGRAM MANAGEMENT 30
3.9.3 COMPLIANCE 30
3.9.4 PERSONNEL SECURITY 31
3.9.6 RISK MANAGEMENT 32
3.9.7 PRIVACY 32
3.9.8 ASSET MANAGEMENT 34
3.9.9 SECURITY CATEGORIZATION 34
3.9.10 MEDIA PROTECTION 34
3.9.11 CRYPTOGRAPHIC PROTECTIONS 35

3.9.12 ACCESS MANAGEMENT 35
3.9.13 IDENTITY AND AUTHENTICATION 36
3.9.14 REMOTE ACCESS 36
3.9.15 CONFIGURATION MANAGEMENT 37
3.9.16 ENDPOINT SECURITY 37
3.9.17 ICS/SCADA/OT SECURITY 38
3.9.18 INTERNET OF THINGS SECURITY 38
3.9.19 MOBILE DEVICE SECURITY 38
3.9.20 NETWORK SECURITY 39
3.9.21 CLOUD SECURITY 39
3.9.22 CHANGE MANAGEMENT 40
3.9.23 MAINTENANCE 40
3.9.24 THREAT MANAGEMENT 40
3.9.25 VULNERABILITY AND PATCH MANAGEMENT 40
3.9.26 CONTINUOUS MONITORING 41
3.9.27 SYSTEM DEVELOPMENT AND ACQUISITION 41
3.9.28 PROJECT AND RESOURCE MANAGEMENT 42
3.9.29 CAPACITY AND PERFORMANCE MANAGEMENT 42
3.9.30 THIRD PARTY MANAGEMENT 42
3.9.31 PHYSICAL AND ENVIRONMENTAL SECURITY 42
3.9.32 CONTINGENCY PLANNING 43
3.9.33 INCIDENT RESPONSE 43

4.0 PROPOSAL PREPARATION AND SUBMISSION 45

4.1 GENERAL 45
4.2 PROPOSAL CONTENTS 45

4.2.1 DETAILED PROPOSAL REQUIREMENTS FOR SECTION 3.2 PART 1 – TECHNOLOGY PLATFORM FOR STATE BASED EXCHANGE 46
4.2.2 DETAILED PROPOSAL REQUIREMENTS FOR PART 2 – CONSUMER ASSISTANCE 47
4.2.3 PROJECT PLAN AND CONTRACT SCHEDULE 48
4.2.4 ORGANIZATIONAL SUPPORT AND EXPERIENCE 48

4.3 SUBCONTRACTOR UTILIZATION PLAN 49
4.4 PRICE SCHEDULE/SHEETS 49

4.4.1 HOURLY RATE SCHEDULE FOR CHANGE ORDERS 49

4.5 TECHNOLOGY PROJECT PLAN (TPP) 50

4.5.1 PLANS REQUIRED BY BID SOLICITATION SECTION 3.18 SECURITY PLAN AND STANDARDS 50

4.6 NON-COLLUSION 51

5.0 SPECIAL TERMS AND CONDITIONS 51

5.1 PRECEDENCE 51
5.2 CHANGE IN LAW 52
5.3 DATA CONFIDENTIALITY 52
5.4 NEWS RELEASES 53
5.5 ADDITIONAL WORK AND/OR PROJECTS 53
5.6 CONTRACT TERM AND EXTENSION OPTIONS 54
5.7 CONTRACT AMENDMENT 54
5.8 LIQUIDATED DAMAGES 54

5.8.1 NOTIFICATION OF LIQUIDATED DAMAGES 55
5.8.2 CONDITIONS FOR TERMINATION OF LIQUIDATED DAMAGES 55
5.8.3 SEVERABILITY OF INDIVIDUAL LIQUIDATED DAMAGES 55
5.8.4 WAIVER OF LIQUIDATED DAMAGES/LIQUIDATED DAMAGES NOT EXCLUSIVE REMEDY 55
5.8.5 PAYMENT OF LIQUIDATED DAMAGES 55

5.9 RETAINAGE 56
5.10 SERVICE LEVEL AGREEMENTS 56

5.10.1 VENDOR WARRENTS THAT IT SHALL MAINTAIN THE SYSTEM AND HOSTING SERVICES, IN WHOLE AND IN PART, TO MEET THE SERVICE LEVEL AGREEMENTS. 56
5.11 DATA SECURITY STANDARDS 56
5.12 FEDERAL TAX INFORMATON SECURITY (TAX INFORMATION SECURITY GUIDELINES FOR FEDERAL, STATE, AND LOCAL AGENCIES (IRS PUBLICATION 1075)) 57
6.0 PROPOSAL EVALUATION 61
6.1 RIGHT TO WAIVE 61
6.2 STATE'S RIGHT OF FINAL PROPOSAL ACCEPTANCE 61
6.3 STATE'S RIGHT TO INSPECT BIDDER'S FACILITIES 61
6.4 STATE'S RIGHT TO REQUEST FURTHER INFORMATION 62
6.5 PROPOSAL EVALUATION COMMITTEE 62
6.6 ORAL PRESENTATION AND/OR CLARIFICATION OF PROPOSAL 62
6.7 EVALUATION CRITERIA 62
6.7.1 TECHNICAL EVALUATION CRITERIA 62
6.7.2 BIDDER'S PRICE SCHEDULE 63
6.7.3 PROPOSAL DISCREPANCIES 63
6.7.4 EVALUATION OF THE PROPOSALS 63
6.8 NEGOTIATION AND BEST AND FINAL OFFER (BAFO) 63
6.9 COMPLAINTS 64
7.0 CONTRACT ADMINISTRATION 65
7.1 STATE CONTRACT MANAGER 65
7.1.1 SCM RESPONSIBILITIES 65

EXHIBITS

Exhibit 1 – P.L 2019 c. 141 Exchange Law
https://www.njleg.state.nj.us/2018/Bills/PL19/141_.PDF

Exhibit 2 – The State of NJ Standard Terms and Conditions (4/15/19)
https://www.state.nj.us/treasury/purchase/forms/StandardTermsandConditions.pdf

Exhibit 3 – Waivered Contracts Supplement to The State of New Jersey Standard Terms and Conditions (6/14/2018)
https://www.state.nj.us/treasury/purchase/forms/Waiver%20Supplement%20to%20Standard%20Terms%20and%20Conditions.pdf

Exhibit 4 – Service Level Agreements and Liquidated Damages

Exhibit 5 – Price Sheet

Exhibit 6 – State of New Jersey Security Due Diligence Third Party Information Security Questionnaire

1.0 INFORMATION FOR BIDDERS

1.1 PURPOSE AND INTENT

The intent of this Request for Proposal (RFP) is guided by P.L. 2019, Chapter 141, signed by Governor Philip D. Murphy on June 28, 2019, ("the Exchange law") *(See Exhibit 1)* https://www.njleg.state.nj.us/2018/Bills/PL19/141_.PDF

This RFP is intended to award one or more contracts for the development of a State based Health Exchange, including a technology platform and consumer assistance center, to the responsible Bidder(s) whose proposal(s), conforming to this RFP, is most advantageous to the State, price and other factors considered.

The New Jersey Department of Banking and Insurance ("DOBI") is seeking proposals from qualified vendors to provide: A hosted integrated online health insurance exchange technology platform **(Part 1)** and an associated consumer assistance center **(Part 2)** to support DOBI's anticipated operation of a State Based Exchange (SBE). DOBI desires a Vendor(s) with direct experience supporting an SBE, but any relevant experience supporting an ACA-compliant exchange will be considered; the proposed solutions should be capable of concurrently supporting each of the described functions, and should have supported all of the functions for a single SBE within a single Plan Year.

Part 1 – the integrated online health insurance exchange technology platform is further divided into three phases: (1) design, development, and implementation (DDI); (2) transition towards operation as an SBE (Transition); and (3) autonomous, ongoing maintenance and operations as an SBE (M&O). Phases one and two are further divided into distinct stages.

Part 2 – the consumer assistance center is divided into three phases: (1) implementation of the consumer assistance center (Implementation); (2) transition support and consumer assistance during Plan Year 2020 OEP (Consumer Assistance Transition); and (3) autonomous, ongoing maintenance and operations of the consumer assistance center (M&O). Phases one and two are further divided into distinct stages.

The State may award one or more contracts in conjunction with this RFP, as determined in the best interest of the State.

The State of NJ Standard Terms and Conditions (4/15/19), and Waivered Contracts Supplement to The State of New Jersey Standard Terms and Conditions (6/14/18) will apply to the contract(s) awarded under this RFP *(See Exhibit 2 and Exhibit 3)* https://www.state.nj.us/treasury/purchase/forms/StandardTermsandConditions.pdf; https://www.state.nj.us/treasury/purchase/forms/Waiver%20Supplement%20to%20Standard%20Terms%20and%20Conditions.pdf

These terms are in addition to the terms and conditions set forth in this RFP and should be read in conjunction with them unless the RFP specifically indicates otherwise.

1.2 BACKGROUND

Currently the State of New Jersey's health exchange is the Federally-Facilitated Marketplace (FFM). Thus, eligibility, enrollment, consumer assistance, plan certification, in-person assister training, and broker certification functions are carried out by the FFM. For many years, the State has been an effective rate review state and therefore has performed rate review in the individual and small group markets. Recently, the State has assumed a greater role in marketing, outreach, and plan management. Additionally, the Governor signed, P.L. 2018 Chapter 31, which replaced the federal individual mandate with an individual state mandate.

The Governor also signed the Exchange law on June 28, 2019 which, among other things, authorizes DOBI to establish a State-based exchange and assess premiums in the individual market to fund a variety of costs associated with the exchange and stabilizing the individual market.

The State has submitted declaration letters to CMS to transition to a State-based exchange on the federal platform (SBE-FP) for plan year 2020 and to a State-based exchange (SBE) for plan year 2021, subject to approval by the Centers for Medicare and Medicaid Services (CMS), a division of the United States Department of Health and Human Services (HHS). The letters designate the Commissioner of the New Jersey Department of Banking and Insurance (DOBI), Marlene Caride, as the State's point of contact. On August 1, 2019, DOBI submitted blueprints to CMS, to become a SBE-FP for plan year 2020 and to become a SBE for plan year 2021.

New Jersey currently has three carriers offering plans on the FFM, and one additional carrier offering plans exclusively off-exchange. There are twenty-five (25) total medical individual market Qualified Health Plans (QHPs) in 2019. Additionally, there are thirty-one dental (31) QHPs in the 2019 individual market.

Given the limited scope of SHOP utilization, it is DOBI's intent for the current Small Business Options Health Plan (SHOP) enrollment model, which utilizes the Direct Enrollment (DE) pathway, to continue, subject to CMS approval.

1.2.1 HEALTH EXCHANGE PROJECT MANAGEMENT OFFICE

DOBI will create a Health Exchange Project Management Office (HEPMO) for this project, anticipated to consist of Department staff members and contracted project management support staff. The HEPMO, under the direction of the State Contract Manager (SCM), will be responsible for the following project functions:

- Initial coordination of communications between Vendor(s) and the SBE's external stakeholders, including points of contact and communications protocols.
- Review, management, and approval of the project plans and control structures developed by the technology Vendor and the consumer assistance Vendor.
- Approval of deliverables for SOW Part One and SOW Part Two (approval of deliverables shall not be considered a waiver of defects in performance).

If separate Vendors are selected for SOW Part One and SOW Part Two the HEPMO shall also be responsible for the following functions:

- Initial coordination of communications between technology Vendor and consumer assistance Vendor, including points of contact and communications protocols.

- Scheduling and facilitation of joint Vendor meetings as necessary to ensure the successful integration of the consumer assistance center with the technology platform.

Vendor(s), in coordination with the HEPMO, shall be responsible for:

- Development and execution of project plans and control structures within each SOW (subject to HEPMO approval). Project plans and control structures shall be developed in accordance with a recognized project management standard.
- Scheduling and facilitation of recurring status meetings throughout Phases One and Two of each SOW.

DOBI intends to separately procure for HEPMO services. The Vendor(s) awarded the contract(s) resulting from this RFP shall not be the Vendor awarded the contract for the HEPMO and vice versa.

1.2.2 CASELOAD

The following tables represent New Jersey's application, plan selection, and enrollment metrics for Plan Year 2019 OEP source: CMS' 2019 OEP Snapshot Public Use File)

Plan Year 2019 Applications for QHP Coverage

Number of Submitted Applications	Individuals Applying for Coverage on Submitted Applications	Individuals Determined Eligible to Enroll in a Marketplace Plan	Individuals Determined Eligible to Enroll, with Financial Assistance	Individuals Determined or Assessed Eligible for Medicaid / CHIP by the Marketplace
233,555	350,333	297,384	215,354	52,431

Plan Year 2019 Plan Selections

Total Number of Consumers Who Have Selected a Marketplace Plan	New Consumers	Total Reenrollees	Active Reenrollees	Automatic Reenrollees
255,246	62,232	193,014	136,899	56,115

Additional enrollment information can be found using the New Jersey Individual Health Coverage Program Board Enrollment Data – https://www.state.nj.us/dobi/division_insurance/ihcseh/ihcsehenroll.html

Proposed solutions for SOW Part One and SOW Part Two shall provide the capacity to service at least a 20% increase in caseload versus the Plan Year 2019 figures.

By way of additional background, DHS has indicated that annually a best estimate of 200,000 NJ FamilyCare applications may transfer to the SBE.

1.2.3 FUNDING

DOBI is a State Department authorized under P.L.2019, c.141 to establish and fund the SBE. Under that law, the Commissioner may apply a monthly assessment to each individual health benefits plan sold in the individual market for the purpose of supporting the exchange through initial start-up costs associated with establishment of the exchange, exchange operations, outreach, enrollment, and other means of supporting the exchange, including any efforts that can increase market stabilization and that may result in a net benefit to policyholders. The assessment may be applied at a rate of up to 1 percent of the total monthly premium charged by a carrier for each health benefits plan during any period that the State is on a SBE-FP and 3.5 percent during any period that the State is on a SBE. The law also provides that the Commissioner has the discretion to adjust this rate up to 4 percent to ensure that the SBE is fully funded.

For the 2020 plan year, DOBI has advised carriers that a 1 percent assessment on premiums will be applied as the State transitions to an SBE-FP. DOBI intends, pursuant to the Exchange law, to notify carriers of the assessment rate for the 2021 plan year at least 20 days prior to the date the carriers are required to file rates with DOBI.

Nominal unallocated portions of the SBE-FP assessment may be available for the project initially, however, per the price sheet accompanying this RFP (See *Exhibit 5*), no payment will be made to the Vendor(s) until each individual stage has been completed and approved by the SCM. No additional funding streams, such as grant awards or New Jersey State General Fund Appropriations, are available to fund this project.

1.3 KEY EVENTS

1.3.1 ELECTRONIC QUESTION AND ANSWER PERIOD

DOBI will electronically accept questions and inquiries from all potential bidders through e-mails: dobi.purchasing@dobi.nj.gov

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

- Each question should begin by referencing the RFP page number and section number to which it relates.

Note: Questions regarding the State of NJ Standard Terms and Conditions and exceptions to mandatory requirements must be posed during this Electronic Question and Answer period and should contain the Bidder's suggested changes.

A bidder's only contact is to be with DOBI, Division of Procurement Office concerning this RFP.

The cut-off date for electronic questions and inquiries relating to this RFP is 5:00pm EST on August 22, 2019.

1.3.2 SUBMISSION OF PROPOSAL

In order to be considered for an award, complete proposals shall be sent to dobi.purchasing@dobi.nj.gov

Complete Proposal(s) must be received by 5:00pm EST on September 20, 2019.

Please note that the above email address cannot receive more than 23 MB in one email. If the proposal(s) are larger than 23MB, please plan accordingly and submit via multiple emails. All emails must be received by 5:00pm EST on September 20, 2019.

1.4 ADDITIONAL INFORMATION

1.4.1 ADDENDA: REVISIONS TO THIS RFP

In the event that it becomes necessary to clarify or revise this RFP, such clarification or revision will be by addendum. Any addendum to this RFP will become part of this RFP and part of any contract awarded as a result of this RFP.

ALL RFP ADDENDA WILL BE ISSUED BY DOBI

There are no designated dates for release of addenda. Therefore, bidders should check DOBI website at https://www.state.nj.us/dobi/financial/index.htm on a daily basis from time of RFP issuance through the proposal submission opening. Bidders can also request to receive the addenda on an ongoing basis via email by contacting dobi.purchasing@dobi.nj.gov .

It is the sole responsibility of the Bidder to be knowledgeable of all addenda related to this procurement.

1.4.2 BIDDER RESPONSIBILITY

The Bidder assumes sole responsibility for the complete effort required in submitting a proposal in response to this RFP. No special consideration will be given after proposals are opened because of a Bidder's failure to be knowledgeable as to all of the requirements of this RFP.

1.4.3 COST LIABILITY

The State assumes no responsibility and bears no liability for costs incurred by a bidder in the preparation and submittal of a proposal in response to this RFP.

1.4.4 CONTENTS OF PROPOSAL

Your proposal can be released to the public during the protest period established pursuant to N.J.A.C. 17:12-3.3, under the New Jersey Open Public Records Act, N.J.S.A. 47:1A-1 et seq. (OPRA), or the common law right to know. As provided in N.J.A.C. 17:12-1.2(b):

Subsequent to the proposal submission opening, all information submitted by Bidders in response to a solicitation is considered public information, notwithstanding any disclaimers to the contrary submitted by a bidder, except as may be exempted from public disclosure by OPRA and the common law.

Bidder must submit both a clean and a redacted version (redacting both personally identifiable information and proprietary and/or confidential information) of their proposal. A bidder may designate specific information as not subject to disclosure pursuant to the exceptions to OPRA

found at N.J.S.A. 47:1A-1.1, when the Bidder has a good faith legal and or factual basis for such assertion. The State reserves the right to make the determination as to what is proprietary or confidential and will advise the Bidder accordingly. The location in the proposal of any such designation should be clearly stated in a cover letter. **The State will not honor any attempt by a bidder to designate its entire proposal as proprietary, confidential and/or to claim copyright protection for its entire proposal.** In the event of any challenge to the Bidder's assertion of confidentiality with which the State does not concur, the Bidder shall be solely responsible for defending its designation.

1.4.5 PROPOSAL SUBMISSION DATE AND TIME

In order to be considered for an award, complete proposals shall be sent to dobi.purchasing@dobi.nj.gov

Complete Proposal(s) must be received by 5:00pm EST on September 20, 2019.

Please note that the above email address cannot receive more than 23 MB in one email. If the proposal(s) are larger than 23MB, please plan accordingly and submit via multiple emails. All emails must be received by 5:00pm EST on September 20, 2019.

A Bidder shall submit via email one (1) clean and one (1) redacted copy of its proposal as outlined above.

All information concerning the proposals submitted may be publicly announced and those proposals, except for information appropriately designated as proprietary and/or confidential, shall be available for inspection and copying. In those cases where negotiation is contemplated, only the names and addresses of the Bidders submitting proposals will be announced and the contents of the proposals shall remain proprietary and/or confidential until the award.

1.4.6 PRICE ALTERATION IN HARD COPY PROPOSALS

Proposal prices must be typed or written in ink. Any price change (including "white-outs") must be initialed. Failure to initial price changes shall preclude a contract award from being made to the Bidder.

1.4.7 JOINT VENTURE

If a joint venture is submitting a proposal, the agreement between the parties relating to such joint venture should be submitted with the joint venture's proposal. Authorized signatories from each party comprising the joint venture must sign the proposal. A separate Ownership Disclosure Form, Disclosure of Investigations and Actions Involving Bidder form, Disclosure of Investment Activities in Iran form, and Affirmative Action Employee Information Report must be supplied for each party to a joint venture. NOTE: Each party comprising the joint venture must also possess 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.

1.4.8 STATE REQUIREMENTS

The successful Vendor or Vendors will be required to complete and submit the following forms and documentation as set forth below. The forms are also available in electronic format at the following link.
https://www.nj.gov/treasury/purchase/forms.shtml

FORMS REQUIRED FOR ALL PROPOSAL SUBMISSIONS AT TIME OF PROPOSAL SUBMISSION	FORMS AVAILABLE
Offer and Acceptance (Signatory Page)	PDF (240 kB)
Disclosure of Investigations and Other Actions Involving Bidder	PDF (1 MB)
Disclosure of Investment Activities in Iran	PDF (1.73 MB)
Ownership Disclosure	PDF (1.61 MB)
Chapter 271 Vendor Certification and Political Contribution Disclosure Form (not to be confused with the Chapter 51 form below)	PDF (31 KB)
Source Disclosure	PDF (67 KB)
Subcontractor Utilization Plan	PDF (144 KB)
MacBride Principles	PDF (75 KB)

FORMS and DOCUMENTATION REQUIRED FOR CONTRACT AWARD	
Two-Year Ch 51/Executive Order 117 Vendor Certification and Disclosure of Political Contributions (Instructions included)	PDF (1.83 MB)
Ch 51/Executive Order 117 Q & A	PDF (98 kB)
Chapter 51/E0 117 Summary	PDF (98 kB)
Business Registration Certificate issued by the Department of the Treasury, Division of Revenue and Enterprise Services Instructions for obtaining a business registration certificate may be found at https://www.nj.gov/treasury/revenue/busregcert.shtml	
FORMS REQUIRED PRIOR TO CONTRACT EXECUTION	
Affirmative Action Employee Information Report *Corresponding Instructions & EEO Language (Form AA302)	PDF (274 KB) PDF (1.87 MB)

2.0 DEFINITIONS PROCUREMENT

The following definitions will be part of any contract awarded or order placed as result of this RFP.

Addendum – Written clarification or revision to this RFP issued by DOBI.

All-Inclusive Hourly Rate – An hourly rate comprised of all direct and indirect costs including, but not limited to: 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.

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

Bidder – An individual or business entity submitting a proposal in response to this RFP.

Commissioner – The Commissioner of the New Jersey Department of Banking and Insurance.

Contract – This RFP, any addendum to this RFP, and the Bidder's proposal submitted in response to this RFP, as accepted by the State.

Director – The Director or Acting Director of the State Division of Purchase and Property, Department of the Treasury.

DOBI – The New Jersey Department of Banking and Insurance.

Evaluation Committee – A committee established, or Division staff member assigned to review and evaluate proposals submitted in response to this RFP and to recommend a contract award to the Director.

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. No additional fees or costs shall be paid by the State unless there is a change in the scope of work.

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

May – Denotes that which is permissible, not mandatory.

Project – The undertaking or services that are the subject of this RFP.

Project Manager – The designated HEPMO representative contracted by DOBI that will facilitate access to DOBI staff, State documents and experts, and approve all deliverables (i.e. projects, tasks, or other work elements in the scope of work).

Request for Proposal (RFP) – This document which establishes the bidding and contract requirements and solicits proposals to meet the purchase needs of the using Agencies as identified herein.

Service Level Agreements (SLA) – The standard by which the system shall perform and the services and deliverables will meet as described in Exhibit 4.

Shall or Must – Denotes that which is a mandatory requirement. Failure to meet a mandatory material requirement will result in the rejection of a proposal as non-responsive.

Should – Denotes that which is recommended, not mandatory.

State – State of New Jersey.

State Contract Manager (SCM) – The State employee responsible for the overall management and administration of the contract.

Subcontractor – An entity having an arrangement with a State Contractor, where by the State 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 of its [the 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 unit of work to be performed.

Vendor(s) – Bidder(s) awarded contract(s) resulting from this RFP.

2.1 DEFINITIONS/ACRONYMS HEALTH EXCHANGE

Affordable Care Act or ACA - The federal "Patient Protection and Affordable Care Act," Pub.L.111-148, as amended by the federal "Health Care and Education Reconciliation Act of 2010," Pub.L.111-152, and any federal rules and regulations adopted pursuant thereto.

Base configuration – Refers to the existing state of the technology vendor's platform as most recently deployed to support at least one SBE, prior to the issue of this RFP, exclusive of any alteration, customization, re-configuration, or extension of the platform's features, capabilities, or architecture necessary to fulfill the requirements of this RFP.

Exchange law – N.J.S.A.17B:27A-57 through N.J.S.A. 17B:27A-59. (P.L.2019, c.141)

Go Live Date – As described in the Part 1 and Part 2 Project Plans, the event(s) that occur(s) after the approval of a function or system, in whole or in part, by the State Contract Manager and the State Contract Manager decides to put the function or system, in whole or in part, into production.

Health Insurance Portability and Accountability Act of 1996 or HIPAA – The Health Insurance Portability and Accountability Act of 1996, Pub.L.104-191, and any regulations promulgated thereunder by the Secretary of the U.S. Department of Health and Human Services.

Insurance Affordability Programs – Includes NJ FamilyCare and subsidies available for qualified health plans purchased through the exchange.

Medicaid/CHIP or Medicaid -- The Medicaid program established pursuant to N.J.S.A. 30:4D-1 et seq.

NJ FamilyCare –The program established pursuant N.J.S.A. 30:4J-10 – through 30:4J-12

Acronyms:

ACA – Affordable Care Act

APTC – Advance Premium Tax Credit

CHIP – Children's Health Insurance Program

CMS – Centers for Medicare and Medicaid Services

CRM – Customer relations management

CSR – Cost-Sharing Reduction

DDI – Design, Development, and Implementation

DHS – New Jersey Department of Human Services

DMI – Data Matching Issues

DOBI – New Jersey Department of Banking and Insurance

EDI – Electronic Data Interchange

FDSH – Federal Data Services Hub

FFM – Federally Facilitated Marketplace

FTI – Federal Tax Information

FTI – Federal Tax Information

HEPMO – Heath Exchange Project Management Officer

HIPAA – Health Insurance Portability and Accountability Act of 1996

HIX – Health Insurance exchange

IRS – Internal Revenue Service

IVR – Interactive Voice Response

M&O – Maintenance and Operations

MAGI – Modified Adjusted Gross Income

MITC- MAGI in the cloud

MARS-E – Minimum Acceptable Risk Standards for Exchanges 2.0 (https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/3-MARS-E-v2-0-Catalog-of-Security-and-Privacy-Controls-11102015.pdf)

OEP – Open Enrollment Period

PCI SSC – Payment Card Industry Security Standards Council.

PII – Personally Identifying Information

PMBOK – Project Management Body of Knowledge

GDPR – General Data Protection Regulation

QHP – Qualified Health Plan

QLE – Qualifying Life Event

SADP – Stand-alone dental plan

SBE – State Based Exchange

SEP – Special Enrollment Period

SERFF – System for Electronic Rates & Forms Filing

SHOP – Small business health options plan

SISM – Statewide Information Security Manual (https://www.nj.gov/it/docs/ps/NJ_Statewide_Information_Security_Manual.pdf)

SMS – Short message service

UAT – User Acceptance Testing

WCAG – Web Content Accessibility Guidelines Version 2.0.

3.0 SCOPE OF WORK (SOW)

3.1 PROJECT OVERVIEW AND OBJECTIVES

The New Jersey Department of Banking and Insurance ("DOBI") is seeking proposals from qualified Vendors to provide: A hosted integrated online health insurance exchange technology platform **(Part 1)** and an associated consumer assistance center **(Part 2)** to support DOBI's anticipated operation of a State Based Exchange (SBE).

Part 1 – the integrated online health insurance exchange technology platform is further divided into three phases: (1) design, development, and implementation (DDI); (2) transition towards operation as an SBE (Transition); and (3) autonomous, ongoing maintenance and operations as an SBE (M&O). Phases one and two are further divided into distinct stages.

Part 2 – the consumer assistance center is divided into three phases: (1) implementation of the consumer assistance center (Implementation); (2) transition support and consumer assistance during Plan Year 2020 OEP (Consumer Assistance Transition); and (3) autonomous, ongoing maintenance and operations of the consumer assistance center (M&O). Phases one and two are further divided into distinct stages.

The State may award one or more contracts in conjunction with this RFP, as determined in the best interest of the State.

SOW Part 1 Contract
DOBI will administer the contract resulting from Part 1 of this RFP. The resulting contract will specify an initial contract term of 5 years and 4 months, anticipated to begin September 30, 2019 with an option to renew for two (2) one-year extensions, if agreed upon by Vendor and DOBI.

SOW Part 2 Contract
DOBI will administer the contract resulting from Part 2 of this RFP. The resulting contract will specify an initial contract term of 3 years, anticipated to begin September 30, 2019 with an option to renew for two (2) one-year extensions, if agreed upon by Vendor and DOBI.

DOBI has two primary objectives pursuant to the enabling legislation: (1) to achieve CMS approval for an SBE for the 2021 OEP; and (2) to achieve coordination and integration across Insurance Affordability Programs. With regard to this second objective, DOBI envisions an SBE that provides a high quality, accessible, and consumer-focused experience for New Jerseyans to explore information about Insurance Affordability Programs and health coverage options, apply for, and quickly and accurately enroll in health coverage, including Medicaid and CHIP.

DOBI recognizes that the second objective will not be fully ready for implementation for the 2021 OEP and therefore seeks a Vendor or Vendors capable of achieving the first objective in a timely fashion, while also offering the flexibility to adapt to New Jersey's evolving vision of how best to achieve the second objective.

3.2 PART 1 – TECHNOLOGY PLATFORM FOR STATE BASED EXCHANGE

The awarded Vendor's Base configuration of the platform shall be a hosted, logically separated technology environment that has successfully supported some portion of the operations of at least one Affordable Care Act (ACA)-compliant health insurance exchange over the course of at least

one complete Plan Year which should have supported all of the following functions for a single SBE within a single Plan Year. DOBI desires a Vendor with direct experience supporting an SBE, but any relevant experience supporting an ACA-compliant exchange will be considered. The solution should be capable of concurrently supporting each of the following functions:

A. User authentication/authorization administered from a remote system, for example using secure web services.
B. Anonymous pre-screening of eligibility
C. Anonymous plan comparison
D. Eligibility determination, including determination and verification advance premium tax credit (APTC) eligibility; calculation of APTC cost-sharing reduction (CSR) subsidies; and renewal, including auto reenrollment.
E. Coordinated and integrated Insurance Affordability Program eligibility and enrollment functionality, consistent with detailed requirements in 3.2.1 Detailed Requirements for Coordinated and Integrated Insurance Affordability Program Eligibility and Enrollment in the Part 1 Technology Platform.
F. Plan comparison/consumer decision support
G. Individual QHP and SADP enrollment during open enrollment period (OEP) and special enrollment period (SEP)
H. Small business health options plan (SHOP) functionality to the extent it is required for SBEs opting for direct enrollment through agents and brokers
I. SHOP premium aggregation functionality to the extent it is required for SBEs opting for direct enrollment through agents and brokers
J. Periodic testing of SBE Consumer Portal transaction times by simulated transactions in accordance with SLA 1.4.
K. Verification of SEP/qualifying life event (QLE) eligibility
L. Data persistence
M. Electronic, telephonic and paper (if required) applications with document attachment capability
N. Document Management system with electronic data interchange (EDI) enabling document exchange with State agencies and vendors and document imaging capabilities that is NJ DORES certified
O. EDI with the State Department of Treasury, Department of Labor, Bureau of Vital Statistics
P. EDI with vendors including United State Postal Service, National Change of Address, Center for Medicare and Medicaid Services, Third Party Liability Vendor
Q. EDI with New Jersey Health Information Network
R. EDI with insurance carriers
S. EDI with Federal Data Services Hub (FDSH) or EDI with state Medicaid agency using existing state Federal Data Services Hub webservices (discussed further in 3.2.1 Detailed Requirements for Coordinated and Integrated Insurance Affordability Program Eligibility and Enrollment in the Part 1 Technology Platform).
T. Plan preview for carriers during recurring data correction windows
U. Generate Consumer messaging to be delivered via U.S. mail, appropriately aligned with NJ FamilyCare member communication standards
V. Consumer messaging via email
W. Consumer messaging via short message service (SMS)
X. SBE Consumer Portal to allow consumers the ability to interact with the SBE, including but not limited to: (1) establish a password protected account; (2) save and edit unfinished application and view application status; (3) select mail, email, or SMS to receive notices; (4) select whether to receive letters by mail or electronically; (5) email and SMS to notify consumer of message available online; (6) change of circumstance reporting online; (7)

document upload online; (8) appeal online; (9) file complaints online; and set up an account; (10) complete redetermination online; (11) respond to request for information online; (12) re-apply online; (13) view, download, and print electronic notices; and, (14) update account settings: e.g., delivery preference for notices, email address, cell phone number, etc.

Y. Additional portal access for parties identified by DOBI which may include DOBI administrative staff; DHS administrative staff; consumer assisters; brokers, agents, and navigators; insurance carriers.

Z. Call center Interactive Voice Response (IVR) integration that automates: (1) application status lookup; (2) call back when operator becomes available functionality; (3) automatic routing of applicants to specialized agents as required; (4) integration with call center application so that the call center operator's screen auto-populates with case linked to linking phone number.

AA. Appeals processing

BB. Consumer complaint resolution

CC. Customer relations management (CRM)

DD. Accounting, including the compilation of enrollment and premium data, and as necessary the generation of carrier invoices and/or tools for reconciling carrier discrepancies.

EE. Carrier and individual payment calculation reconciliation

FF. 1095-A production

GG. 1095-A printing and delivery via U.S. Mail including standard inserts.

HH. Electronic reporting to IRS

II. Electronic reporting to CMS

JJ. Minimum Acceptable Risk Standards for Exchange 2.0 (Mars-E) certification and ongoing auditing/reporting and US Internal Revenue Service Publication 1075 security compliance

KK. Determine eligibility for exemptions from State shared responsibility tax, pursuant to P.L.2018, c.31.

LL. Communication with consumer through online chat function

MM. Optimization for mobile devices

NN. Reporting of benchmarks/performance indicators, including compliance and production reports to be provided to go live and monthly/quarterly/annually thereafter.

OO. Properly invoice enrollees for aggregated premiums due in accordance with SLA 1.13.

3.2.1 DETAILED REQUIREMENTS FOR COORDINATED AND INTEGRATED INSURANCE AFFORDABILITY PROGRAM ELIGIBILITY AND ENROLLMENT IN THE PART 1 TECHNOLOGY PLATFORM.

A. DOBI seeks a Vendor technology solution that will coordinate and integrate eligibility operations and systems across the SBE and New Jersey's NJ FamilyCare administering agency, DHS, to provide a seamless and streamlined consumer experience for New Jerseyans seeking to apply for and enroll in Insurance Affordability Programs. The proposed technology platform should be capable of delivering the following functionality – ***Eligibility and Enrollment Coordination and Integration Functionality for OEP 2021***:

1. Assess NJ FamilyCare eligibility based on Medicaid and CHIP MAGI-based income standards, consistent with 45 CFR 155.302, using a DHS provided webservice to New Jersey's "MAGI in the Cloud" eligibility rules engine. MAGI in the Cloud means an open-source software tool developed through the New England States Consortium Systems Organization (NESCSO), in concert with the CMS, that is solution for public entities to determine Medicaid Program and Children's Health Insurance Program income eligibility based on the modified adjusted gross income (MAGI) calculations

as defined by the Affordable Care Act. NJ has incorporated the tool, with state-specific configuration, into its eligibility determination procedure using the available Application Programing Interface.

2. Send and receive secure account transfers to and from DHS, including functionality to:
   a. Send NJ FamilyCare eligibility assessments to DHS via secure account transfer;
   b. Receive from DHS via secure account transfer accounts not eligible for NJ FamilyCare but potentially eligible for APTC/CSR or QHP.
   c. Bi-directionally transfer images between the SBE document management system and the DHS document management system.
   d. Bi-directionally transfer eligibility verification information obtained through FDSH and non-FDSH sources.

3. Coordinate with DHS to avoid duplication of any NJ FamilyCare eligibility findings already made in compliance with the federal regulations at 45 CFR 155.345 and conduct eligibility determinations for APTC/CSR and QHP enrollment.

4. Electronically verify eligibility for Insurance Affordability Programs, consistent with 45 CFR 155.320.

5. Connect to the FDSH through a direct FDSH connection, by means of a FDSH webservice provided by DHS, or both, to the extent CMS permits New Jersey to maintain two FDSH connections.

B. In addition, DOBI seeks the following items of additional high value functionality for ***Eligibility and Enrollment Coordination and Integration Functionality for OEP 2021*.** DOBI requests a timeline and plan for implementing this additional functionality in OEP 2021 or as soon thereafter as is practicable:

   1. Bi-directional application status updates between the SBE consumer portal and call center system and DHS's NJ FamilyCare consumer portal and call center system, so each call center can determine where the callers' applications are being processed and provide status updates.
   2. Bi-directional registered account transfer between SBE consumer portal and DHS's NJ FamilyCare consumer portal as applications are transferred.
   3. Bi-directional demographic and change in circumstance updates between the SBE and DHS.

C. No later than June 1, 2022, the successful Vendor shall deliver a ***Plan for Enhanced Eligibility and Enrollment Functionality and Services*** (the "Enhanced Plan") for further implementation of the State vision of a high quality, accessible, consumer-focused eligibility and enrollment experience. Within 180 days of contract award, Vendor shall meet with the State Contract Manager (SCM) to finalize development of the Enhanced Plan. This functionality may include, without limitation, enhanced features such as:
   1. A "virtual consumer portal" using shared design standards, a federated single sign on, and shared account demographics so consumer can move seamlessly between SBE and DHS consumer portals.

2. A single MAGI webservice to determine eligibility across Insurance Affordability Programs, which need not be one physical rules engine because NJ FamilyCare already has this with webservice to MITC.
3. Eligibility verification connections to federal and State data sources that could be provided by other state agencies, or if provided by SBE, that can be shared by other state agencies
4. Coordinated consumer eligibility notices across Insurance Affordability Programs; and
5. A "virtual consumer assistance center" where consumers are seamlessly routed to the SBE or NJ FamilyCare consumer assistance center as required

The Enhanced Plan should be informed by performance metrics, to be defined by DOBI, on SBE functionality and services described in Section 3.2 above. The Enhanced Plan should address design, development, and implementation, including a timeline and budget for execution of the Enhanced Plan. The State will make a determination on whether to proceed with the Enhanced Plan and DOBI may, in its sole discretion, direct changes to the design, development and implementation of the Enhanced Plan.

The Vendor may be asked to engage in additional tasks, hours, meetings, or provide additional work to develop the approved Enhanced Plan, in accordance with Section 4.5.1. The Vendor shall not begin any such work without first obtaining the SCM's approval.

In the event DOBI approves the Enhanced Plan, the Vendor must present a written Quote to perform the Plan work to the SCM. The Vendor's written Quote for Plan work must provide a detailed description of the work to be performed broken down by task and subtask. The written Quote must detail the cost necessary to complete the Plan work in a manner consistent with this Contract. Implementation of the Enhanced Plan is subject to recommendation of the SCM and approval by the State.

3.3 CONSTRAINTS TO PART 1 – TECHNOLOGY PLATFORM FOR STATE BASED EXCHANGE

A. Proposed solution and development methodologies for functionality described in Section 3.2.1 A. and B. shall comply with the applicable federal statutes and regulations – including but not limited to Social Security Act of 1943 (42 USC 1936w-3) and 45 CFR 155.302, 155.320 and 155.345, and 42 CFR 435.120 and 433.112. The proposed solution and development methodologies should also abide by the following principles and include the following features and activities:

1. Uses a modular, flexible approach to systems development, including the use of open interfaces and exposed application programming interfaces (APIs); the separation of business rules from core programming, available in both human and machine-readable formats. The proposed solution should be capable of modular integration of eligibility and enrollment functions with minimal changes to the solution's codebase.
2. Promotes sharing, leverage, and reuse of SBE and Medicaid technologies and systems within and among states, and DOBI specifically seeks to leverage existing DHS eligibility and enrollment system components to the greatest extent possible.
3. Considers strategies to minimize the costs and difficulty of operating the software on alternate hardware or operating systems, including leveraging commercial off-the-shelf (COTS) products and commercially available hosted solutions.

4. Includes documentation of components and procedures such that the systems could be operated by a variety of Vendors or other users.

B. The technology vendor shall assist the consumer assistance vendor with the import of migrated consumer data into the consumer assistance CRM system.

C. It is of critical importance to DOBI that delivery of the ***Eligibility and Enrollment Coordination and Integration Functionality for OEP 2021*** not be jeopardized by the delivery of ***Plan for Enhanced Eligibility and Enrollment Functionality and Services.*** Further, delivery of ***Eligibility and Enrollment Coordination and Integration Functionality for OEP 2021*** and the ***Plan for Enhanced Eligibility and Enrollment Functionality and Services*** must not disrupt the existing Exchange, Medicaid and NJ Family Care consumers and business processes of the FFM, DHS and DOBI.

3.4 PART 1 TIMELINE, ACTIVITIES, AND DELIVERABLES

The Vendor shall implement the Part 1 SOW articulated in Section 3.2, above and including Section 3.2.1, in three phases: (1) design, development, and implementation (DDI); (2) transition towards operation as an SBE (Transition); and (3) autonomous, ongoing maintenance and operations as an SBE (M&O). Phases one and two are further divided into distinct stages. A projected Go Live Date for all functions and systems shall be identified in the schedule submitted pursuant to Section 4.2.3, and will be subject to SCM approval. The Bidder's proposal shall describe the strategy for accomplishing the goals outlined in each phase.

3.4.1 TECHNOLOGY PLATFORM PHASE ONE

DDI. DDI is anticipated to last 11 months, shall commence upon execution of an approved contract, and will encompass five distinct stages.

A. DDI Stage One. DDI Stage One is anticipated to commence September 30, 2019 and conclude December 31, 2019, contingent upon HEPMO approval of deliverables.

1. The technology Vendor, in coordination with the HEPMO and the consumer assistance Vendor, shall develop a detailed Part 1 Project Plan for Technology Platform Phases One and Two.
2. The technology Vendor, in coordination with the HEPMO and the consumer assistance Vendor, shall develop a detailed Technology Platform Annual Work Cycle Plan for ongoing maintenance and operations, inclusive of procedural, compliance, and regulatory milestones (inspection, certification, carrier plan data correction, reporting, auditing, etc.).
3. Vendor, in coordination with the HEPMO, shall work with representatives of DHS, New Jersey's on-Exchange insurance carriers, CMS, Homeland Security, and the IRS to gather the technical and functional requirements for successful EDI with each external system. These requirements shall be used to create a detailed EDI Test Plan for each external system, to be furnished to the administrator(s) of each system. The test plan should include automated regression testing.
4. Vendor, in coordination with CMS, shall develop a detailed Data Migration Plan to ensure the successful migration of Plan Year 2020 consumers from the FFM to the proposed solution. The plan shall include technical requirements detailing the necessary format/data elements, to be furnished to CMS.

5. Vendor, in coordination with New Jersey's on-Exchange insurance carriers, shall develop a detailed Carrier Plan Certification Plan to ensure that carrier plan data is loaded from the SERFF system and made available for carrier review/correction during the limited data correction windows in July and September.
6. Vendor, in coordination with New Jersey's on-Exchange insurance carriers, shall develop a detailed consumer reconciliation plan to ensure that migrated consumer data from the FFM remains sufficiently in sync with subsequent enrollment, effectuation, and account maintenance transactions such that the migrated data can be utilized for eligibility re-verification and auto-reenrollment.
7. Vendor shall develop a detailed Insurance Affordability Program Assessment Plan to ensure the SBE is able to meet DOBI's requirements with regard to eligibility and enrollment coordination and integration functionality for OEP 2021, which must be submitted to the State Contract Manager for approval
8. All plans shall be developed in accordance with the recognized project management standards.
9. Deliverables:
    a. Part 1 Project Plan for Technology Platform Phases One and Two
    b. Technology Platform Annual Work Cycle Plan
    c. EDI Test Plans
    d. Data Migration Plan
    e. Carrier Plan Certification Plan
    f. Consumer Reconciliation Plan
    g. Insurance Affordability Program Assessment Plan

B. DDI Stage Two. DDI Stage Two is anticipated to commence January 1, 2020, and conclude February 15, 2020, contingent upon HEPMO approval of deliverables.

1. Vendor shall complete the initial customization and configuration of the technology platform, including: the configuration of electronic interfaces to external systems; the configuration of a fully functional, sandboxed Exchange Testing Environment for use in subsequent stages of DDI; the configuration of a fully functional, sandboxed Exchange Training Environment for ongoing use by DOBI and consumer assistance center personnel and others designated by DOBI; and the deployment of the customized codebase to the testing and training environments.
2. Vendor shall communicate the technical requirements for the EDI test plans to IT personnel from DHS and New Jersey's on-exchange insurance carriers; Vendor shall provide the necessary support and lead-time to ensure that those agencies have the information and resources required to re-configure their existing FFM interfaces for use with the proposed solution.
3. Deliverables:
    a. Exchange Testing Environment
    b. Exchange Training Environment

C. DDI Stage Three. DDI Stage Three is anticipated to commence February 16, 2020, and conclude March 31, 2020, contingent upon HEPMO approval of deliverables, Vendor, in coordination with the external stakeholders, shall execute the EDI Test Plans developed in DDI Stage One, which should include automated functionality and load testing. The HEPMO will approve the functional scenarios configured for automated functional regression testing. Load testing must simulate the peak loads from all system users during open enrollment period and be performed as part of each regression test. At the

conclusion of DDI Stage Three the Vendor shall have delivered documentation certifying the complete and successful execution of the EDI Test Plans.

1. During Stage Three the HEPMO will develop a User Acceptance Testing (UAT) plan, including scenarios for automated regression testing, for use during Stage Four; development of the UAT plan is mentioned for reference and is not intended to fall within the Vendor SOW.
2. Deliverables:
    a. Verified Execution of EDI Test Plan

D. DDI Stage Four. DDI Stage Four is anticipated to commence April 01, 2020 and conclude May 31, 2020, contingent upon the resolution of any defects discovered during UAT, and subsequent HEPMO approval of the deliverables. Vendor, in coordination with CMS, shall execute the Data Migration Plan developed during DDI Stage One, including the resolution of any data mismatches or outlier scenarios to the best of the Vendor's ability. Vendor shall migrate existing consumers from the FFM to the proposed solution while maintaining existing relationships between consumers, their respective insurance carrier and QHP/SADP IDs, their FFM-assigned HIX IDs, and, if applicable, their respective enrollment professionals, using the National Producer Number (NPN) code. At the conclusion of DDI Stage Four the Vendor shall have delivered documentation certifying the complete and successful execution of the approved Insurance Affordability Program Assessment Plan and the Data Migration Plan, including, if applicable, detailed status information for data mismatches/exceptions and their resolutions.

1. During Stage Four the HEPMO will execute the UAT plan developed by the HEPMO during Stage Three; execution of the UAT plan is mentioned for reference and is not intended to fall within the Vendor's SOW, however the Vendor shall be responsible for resolving any verified defects discovered during UAT. The Vendor will be responsible for configuring and successfully running automated regression testing scenarios and automated regression load testing prior to each scheduled UAT.
2. Deliverables:
    a. Verified Execution of Data Migration Plan
    b. Verified Execution of Insurance Affordability Assessment Plan

E. DDI Stage Five. Vendor, in coordination with New Jersey's on-Exchange insurance carriers, shall execute the Carrier Plan Certification Plan developed during DDI Stage One. At the conclusion of DDI Stage Five, the Vendor shall have delivered documentation certifying the complete and successful execution of the Carrier Plan Certification Plan.

1. Vendor, in coordination with New Jersey's on-Exchange insurance carriers, shall execute the Consumer Reconciliation Plan developed during DDI Stage One.
2. At the conclusion of DDI Stage Five, the Vendor shall have delivered documentation certifying the complete and successful execution of the Carrier Reconciliation Plan.
3. The technology Vendor, in coordination with the HEPMO and the consumer assistance Vendor, shall develop and execute a Consumer Assistance Center Technology Readiness Plan to ensure optimal technical integration between the technology platform and the consumer assistance center. Upon completion the technology Vendor shall deliver documentation certifying the complete and

successful execution of the Consumer Assistance Center Technology Readiness Plan.

4. The technology Vendor, in coordination with the HEPMO and the consumer assistance Vendor, shall develop a Consumer Messaging Plan for the purpose of educating migrated consumers on the actions required for re-verification of their migrated user accounts. At minimum, the technology Vendor should include in the Consumer Messaging Plan functionality for outgoing mail correspondence, including triggered messaging (such as enrollment confirmations, estimates of benefits, etc.) and scheduled messaging (such as 1095-As), in the plan.
5. Vendor shall develop a detailed Eligibility Re-Verification Plan to ensure a complete and accurate re-verification of migrated consumer eligibility.
6. Vendor shall develop a detailed Auto Re-Enrollment Plan to ensure a complete and accurate re-enrollment of migrated consumers without an active plan selection during Plan Year 2021 OEP.
7. Vendor shall configure and deploy a public-facing Exchange Production Environment, inclusive of any resolved defects identified during UAT, and populated with the resultant consumer data from the executed Data Migration Plan.
8. Vendor shall develop a detailed User Reference Manual describing the complete feature set of the technology platform, including detailed instructions for the business processes supported therein, for use by DOBI and consumer assistance center staff.
9. DDI Stage Five is anticipated to commence June 01, 2020 and conclude August 31, 2020, contingent upon HEPMO approval of deliverables and HEPMO certification of operational readiness for Phase Two.
10. Deliverables:
    a. Verified Execution of Carrier Plan Certification Plan
    b. Verified Execution of Consumer Reconciliation Plan
    c. Consumer Assistance Technology Readiness Plan (Technology Platform)
    d. Verified Execution of Consumer Assistance Technology Readiness Plan (Technology Platform)
    e. Consumer Messaging Plan (Technology Platform)
    f. Eligibility Re-Verification Plan
    g. Auto Re-Enrollment Plan
    h. Application Production Environment
    i. User Reference Manual

3.4.2 TECHNOLOGY PLATFORM PHASE TWO

Technology Transition. The Technology Transition phase is anticipated to last four months, commencing on September 01, 2020 and concluding 20 days after OEP 2021 and will encompass three distinct stages.

A. Technology Transition Stage One. Technology Transition Stage One is anticipated to commence September 01, 2020 and conclude September 30, 2020.

   Vendor shall ensure the continuous and ongoing availability and functionality of the Exchange Production Environment to support consumers and consumer assistance personnel with the re-verification of migrated user accounts, as defined in the Consumer Messaging Plan. Technology Transition Stage One is anticipated to commence September 01, 2020 and conclude September 30, 2020.

B. Technology Transition Stage Two. Technology Transition Stage Two is anticipated to commence October 01, 2020 and conclude October 31, 2020, contingent upon HEPMO approval of deliverables.

   At the earliest practical date, Vendor shall make certified plan data available in the Exchange Production Environment to facilitate anonymous plan comparison by consumers.

   1. Vendor shall execute the Eligibility Re-Verification Plan developed during DDI Stage Five.
   2. At the conclusion of Technology Transition Stage Two the Vendor shall have delivered documentation certifying the complete and successful execution of the Eligibility Re-Verification Plan.
   3. Deliverables:
      a. Verified Execution of Carrier Plan Certification Plan
      b. Anonymous plan comparison

C. Technology Transition Stage Three. Technology Transition Stage Three is anticipated to commence November 01, 2020 and conclude 20 days after OEP2021, contingent upon HEPMO approval of the deliverables.

   1. Vendor shall ensure the continuous and ongoing availability and functionality of the Exchange Production Environment to support Plan Year 2021 OEP.
   2. Vendor shall execute the Auto Re-Enrollment Plan developed during DDI Stage Five. At the conclusion of Technology Transition Stage Three the Vendor shall have delivered documentation certifying the complete and successful execution of the Auto Re-Enrollment Plan.
   3. Deliverables:
      a. Verified Execution of Auto Re-Enrollment Plan

3.4.3 TECHNOLOGY PLATFORM PHASE THREE: M&O

M&O is anticipated to last four years, commencing January 01, 2021 and concluding 20 days after OEP 2024.

A. Vendor shall ensure the continuous and ongoing availability and functionality of the Exchange Production Environment.
B. Vendor shall ensure the continuous and ongoing availability and functionality of the Exchange Training Environment.
C. Vendor shall ensure the availability of the Exchange Testing Environment, as needed to verify and approve changes to the technology platform's configuration (including change orders).
D. Vendor shall ensure ongoing compliance with the responsibilities outlined in the Technology Platform Annual Work Cycle Plan.

3.4.4 TECHNOLOGY PLATFORM ENHANCED PLAN

The Vendor shall deliver the Enhanced Plan no later than June 1, 2022.

3.5 PART 2 - CONSUMER ASSISTANCE CENTER

DOBI is seeking a proven consumer assistance center solution which has successfully supported the consumer assistance functions of at least one SBE over the course of at least one complete Plan Year. DOBI desires a Vendor with direct experience supporting an SBE, but any relevant experience supporting an ACA-compliant health insurance exchange will be considered. The solution must include both the technology and personnel required to provide the following functions to SBE consumers:

A. Consumer education for ACA requirements/eligibility
B. Consumer education for Medicaid/CHIP mixed household eligibility
C. Customer relations management
D. Direct enrollment of consumers, including taking applications by telephone
E. QLE/SEP eligibility verification, MAGI and CHIP eligibility verification
F. Resolution of Data Matching Issues (DMI)/FDSH exceptions to complete APTC/CSR eligibility determinations.
G. Account maintenance support
H. Ticketing
I. Ticket Escalation
J. Basic consumer complaint resolution (i.e. Tier 1 support)
K. Escalated consumer complaint resolution (i.e. Tier 2 support)
L. Call center solution that (1) allows for real time monitoring of phone conversations; (2) records all phone conversations; (3) makes recordings easily available to call center and DOBI staff; (4) allows for long-term archival of call recordings, for audit and other purposes. Long-term archiving refers to the retention requirements of the ACA and any other applicable state or federal regulations.
M. A Call center Interactive Voice Response that is continuously available and automates: (1) application status lookup; (2) call back when operator becomes available functionality; (3) automatic routing of applicants to specialized agents as required; (4) integration of SBE Technology Platform with call center application so that the call center operator's screen auto-populates with case linked to incoming phone number.
N. Communication with consumer through online chat function
O. Optimization for mobile devices
P. Imaging and document management system that will perform electronic document capture, management and distribution. The system will receive scanned, faxed, incoming mail or online information and associate them with an account and store the links to the appropriate data services. This will allow users to view and update their account information as well as any associated documents.
Q. Broker/Navigator support
R. Assister support
S. Insurance carrier support
T. Appeals processing
U. Informal appeals resolution
V. Representation at appeals hearings
W. Customer satisfaction surveys
X. Processing of incoming and outgoing mail.
Y. Outgoing correspondence shall have the ability to be generated as: printed media which shall be bundled for printing and sent through the mail or faxed; Email; text messages; or online account notifications.
Z. Print processing, which includes, but is not limited to, the printing of all notices, forms, letter, postcards, flyer, brochures, enrollment packages, and ad hoc mass mailings.

Printed documents shall include basic black printing on white paper to full-color glossy multifold brochures and presentation materials.

AA. Quality assurance
BB. Staffing, scheduling, and workforce management
CC. Staff training and retraining as needed and/or directed by the SCM
DD. Caseload forecasting
EE. Monitoring of benchmarks/performance indicators
FF. Reporting of benchmarks/performance indicators, including service compliance and production reports to be provided to go live and monthly/quarterly/annually thereafter
GG. Information Security/privacy oversight & monitoring

3.6 CONSTRAINTS TO PART II – CONSUMER ASSISTANCE CENTER IMPLEMENTATION

A. The proposed solution shall comply with all federal requirements related to the establishment and operation of consumer assistance center under the ACA, including but not limited to those requirements detailed in 45 CFR Part 155.

B. If integrated CRM functionality is not provided by the technology platform then the consumer assistance Vendor, with assistance from the technology Vendor, shall facilitate the import of migrated consumer data from the technology platform. The consumer assistance Vendor shall support crossover validation and reconciliation with the technology platform.

3.7 PART 2 TIMELINE, ACTIVITIES, AND DELIVERABLES

SOW Part Two will be divided into three phases: (1) implementation of the consumer assistance center (Implementation), (2) transition support and consumer assistance during Plan Year 2020 OEP (Consumer Assistance Transition), and (3) autonomous, ongoing maintenance and operations (M&O) of the consumer assistance center (Operations). Phases one and two are further divided into distinct stages. A projected Go Live Date for all functions and systems shall be identified in the timeline and will be subject to SCM approval. The Bidder's proposal shall describe the strategy for providing the services outlined in each phase, including a detailed timeline to implement each stage of the SOW.

3.7.1 CONSUMER ASSISTANCE CENTER PHASE ONE: IMPLEMENTATION

Implementation is anticipated to last 11 months, shall commence upon execution of an approved contract, and will encompass two distinct stages.

A. Implementation Stage One. The consumer assistance Vendor, in coordination with the HEPMO and the technology Vendor, shall develop a detailed Part 2 Project Plan for Consumer Assistance Center Phases One and Two. Implementation Stage One is anticipated to begin on September 30, 2019 and conclude on December 30, 2019, contingent upon HEPMO approval of deliverables.

    1. The consumer assistance Vendor, in coordination with the HEPMO and the technology Vendor, shall develop a detailed Consumer Assistance Annual Work Cycle Plan, inclusive of procedural, compliance, and regulatory milestones (inspection, certification, reporting, auditing, etc.).

2. Deliverables:
    a. All plans shall be developed in accordance with recognized project management standards.
    b. Part 2 Project Plan for Consumer Assistance Center Phases One and Two
    c. Consumer Assistance Annual Work Cycle Plan

B. Implementation Stage Two. The consumer assistance Vendor, in coordination with the HEPMO and the technology Vendor, shall cooperate in the development and execution of a Consumer Assistance Center Technology Readiness Plan to ensure optimal technical integration between the technology platform and the consumer assistance center. Upon completion, the technology Vendor will deliver documentation certifying the complete and successful execution of the Consumer Assistance Center Technology Readiness Plan.

1. The consumer assistance Vendor, in coordination with the HEPMO and the technology Vendor, shall develop a Consumer Messaging Plan for the purpose of educating migrated consumers on the actions required for re-verification of their migrated user accounts. The Consumer Messaging Plan shall include the consumer assistance Vendor's approach to ensuring that inquiries from FFM consumers for Plan Years 2020 and prior Plan Years are quickly identified and appropriately routed to the FFM call center.
2. The consumer assistance Vendor, in coordination with the HEPMO, shall codify standard operating procedures, as well as benchmarks and service-levels consistent with the SLAs and as approved by the SCM, in a Consumer Assistance Center Standard Operating Procedures Manual.
3. Vendor shall develop and execute an Open Ticket Migration Plan to ensure that open tickets from the FFM call center are successfully migrated to the consumer assistance CRM system in time for the consumer assistance center's anticipated go-live date of September 01, 2020. Upon completion the consumer assistance Vendor shall deliver documentation certifying the complete and successful execution of the Open Ticket Migration Plan.
4. Vendor shall prepare the consumer assistance center for operational readiness by September 01, 2020, including any required procurement, construction, hiring/training of staff, per the Part 2 Project Plan for Consumer Assistance Center Phases One and Two that was developed during Implementation Stage One.
5. Implementation Stage Two is anticipated to commence on June 01, 2020 and conclude on August 31, 2020, contingent upon HEPMO approval of deliverables.
6. Deliverables:
    a. Consumer Assistance Technology Readiness Plan (in cooperation with technology Vendor)
    b. Verified Execution of Consumer Assistance Technology Readiness Plan (in cooperation with technology Vendor)
    c. Consumer Messaging Plan (Consumer Assistance, and cooperation with technology Vendor's platform)
    d. Consumer Assistance Center Standard Operating Procedures Manual
    e. Open Ticket Migration Plan
    f. Verified Execution of Open Ticket Migration Plan
    g. Fully Staffed and Operational Call Center

3.7.2 CONSUMER ASSISTANCE CENTER PHASE TWO: CONSUMER ASSISTANCE TRANSITION.

The Consumer Assistance Transition phase is anticipated to last four months, commencing on September 01, 2020 and concluding 20 days after OEP 2021, and will encompass three distinct stages. DOBI anticipates peak consumer inquiries during this Phase.

A. Consumer Assistance Transition Stage One. Vendor shall provide full-capacity consumer support, including support for re-verification of migrated user accounts as defined in the Consumer Messaging Plan.
   1. Vendor shall begin complying with the terms of the Consumer Assistance Center Standard Operating Procedures Manual.
   2. Consumer Assistance Transition Stage One is anticipated to commence September 01, 2020 and conclude September 30, 2020.

B. Consumer Assistance Transition Stage Two. Vendor shall continue providing full-capacity consumer support, including consumer education to support the anonymous plan comparison process. Consumer Assistance Transition Stage Two is anticipated to commence October 01, 2020 and conclude October 31, 2020.

C. Consumer Assistance Transition Stage Three. Stage Three represents the open enrollment period. Vendor shall provide full-capacity consumer support for Plan Year 2021 OEP. Consumer Assistance Transition Stage Three is anticipated to commence November 01, 2020 and conclude 20 days after OEP 2021.

3.7.3 CONSUMER ASSISTANCE CENTER PHASE THREE: OPERATIONS.

Operations is anticipated to last four years, commencing 20 days after OEP 2021 and concluding 20 days after OEP 2024.

A. Vendor shall ensure the ongoing provision of consumer assistance in accordance with the terms of the Consumer Assistance Center Standard Operating Procedures Manual.

B. Vendor shall ensure ongoing compliance with the responsibilities outlined in the Consumer Assistance Annual Work Cycle Plan.

3.8 PROJECT SUPPORT

The State will provide to the Vendor(s) desktop workspace as determined by the SCM, and the Vendor(s)' personnel will have access to desktop telephones, web connectivity, office supplies, and copiers for black-and-white copying. The State will not provide the Vendor(s) with laptops and mobile technology. The Vendor(s)' personnel will have access to the workspace from 8:00 a.m. to 5:00 p.m. ET, unless approved otherwise, in advance, by the SCM.

The SCM will provide the Vendor(s) with access to all required locations and data necessary to perform the services. The State requires the Vendor(s)' participation in regular meetings as requested by the SCM during the contract term, as well as reporting as directed by the SCM.

3.9 TECHNICAL REQUIREMENTS - ASSESSMENTS AND PLANS

If data will be maintained outside of State managed infrastructure, describe the frequency and method by which that data shall be replicated back to the State so that it is available for reuse or in the event of a vendor disruption.

3.9.1 SECURITY PLAN

The Vendor(s) must provide security plan(s) that, at a minimum, conform(s) to the policies and standards contained in the New Jersey Statewide Information Security Manual, (https://www.nj.gov/it/docs/ps/NJ_Statewide_Information_Security_Manual.pdf). The security plan(s) shall address administrative, physical, and technical security controls, along with the privacy safeguards that are to be implemented as they relate to the scope of the engagement and the broader Vendor(s) information security program. The control areas to be addressed include:

The Vendor(s) shall provide detailed system design document(s) showing Security Plan, Disaster Recovery Plan and Contingency Plan. Logical and physical diagrams are required.

Vendor shall submit to the State for review and approval their Security Plan within 60 days of the Contract Award Date.

3.9.2 INFORMATION SECURITY PROGRAM MANAGEMENT

The Vendor(s)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 but is not limited to the following:

A. Establishment of a management structure and responsibility for information security;

B. Creation, maintenance, and communication of information security policies, standards, procedures, and guidelines to include the control areas listed 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 Vendor's information security program.

3.9.3 COMPLIANCE

The Vendor(s) shall develop and implement processes to ensure its compliance with all applicable statutory, regulatory, contractual, and internal policy obligations. Examples include but are not limited to GDPR, PCI SSCC, HIPAA, IRS-1075.

A. Within 10 days of award, the Vendor(s) shall designate an 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 development process, Vendor(s) should 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.

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

3.9.4 PERSONNEL SECURITY

The Vendor(s) shall implement processes to ensure all personnel have the appropriate background, skills, and training to perform their job responsibilities in a competent, professional, and secure manner. Workforce security controls shall include but are not limited to:

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. Vendor 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.

3.9.5 SECURITY AWARENESS AND TRAINING

The Vendor(s) should provide information security awareness and training to ensure employees 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 information from a loss of confidentiality, integrity, availability and privacy. Security awareness and training should include but is not limited to:

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

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

C. Role-based security training is provided to individuals 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.

3.9.6 RISK MANAGEMENT

The Vendor(s) 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 but are not limited to:

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

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

C. Risk assessments should 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 or risk.

3.9.7 PRIVACY

Personally Identifiable Information (PII)- refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual.

A. *Data Ownership.* The State is the data owner. Vendor does not obtain any right, title, or interest in any of the data furnished by the State.

B. Data usage, storage, and protection of PII and Confidential Information is subject to all applicable international, federal and state statutory and regulatory requirements, as amended from time to time, including, without limitation, those for Health Insurance Portability and Accountability Act of 1996 (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. Vendor shall also conform to Payment Card Industry (SSC) Security Standards Council.

C. Security: Vendor agrees to take appropriate administrative, technical and physical safeguards reasonably designed to protect the security, privacy, confidentiality, and

integrity of user information. Vendor shall ensure that PII and other Confidential Information is secured and encrypted during transmission or at rest.

D. Data Transmission: The Vendor must only transmit or exchange State of New Jersey data with other parties when expressly requested in writing and permitted by and in accordance with requirements of the State of New Jersey. The Vendor shall only transmit or exchange data with the State of New Jersey or other parties through secure means supported by current technologies. The Vendor must encrypt all data defined as personally identifiable or confidential by the State of New Jersey or applicable law, regulation or standard during any transmission or exchange of that data.

E. 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 Vendor. No State data of any kind 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.

F. Security 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 PII (each, a Security Breach) that may concern any State Confidential Information or PII, Vendor shall: (a) notify the State immediately following the Vendor's knowledge of such breach, (b) designate a single individual employed by Vendor who must be available to the State twenty-four (24) hours per day, seven (7) days per week as a contact regarding Vendor's obligations under this Section; (c) not provide any other notification or provide any disclosure to the public regarding such Security Breach 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 (Law) (in which case Vendor shall consult with the State and reasonably cooperate with the State to prevent any notification or disclosure concerning any PII, security breach or other Confidential Information); (d) assist the State in investigating, remedying and taking any other corrective action or mitigation the State deems necessary regarding any Security Breach and any dispute, inquiry or claim that concerns the Security Breach; (e) follow all reasonable instructions provided by the State relating to the Confidential Information affected or potentially affected by the Security Breach; (f) take such actions as necessary to prevent future Security Breaches; (g) unless prohibited by an applicable statute or court order notify the State of any third party legal process relating to any Security Breach, including, but not limited to, any legal process initiated by any governmental entity (foreign or domestic) (h) and provide a written Security Report as required by SLA 1.11.

G. Minimum Necessary. Vendor attests that the PII and/or Confidential Information requested represents the minimum necessary information for the services as described in the Agreement and, unless otherwise agreed to in writing by the State, that only necessary individuals or entities who are familiar with and bound by the Agreement will have access to the confidential information in order to perform the work.

H. End of Contract Data Handling: Upon termination/expiration of this Contract the Vendor shall first return all State data to the State in a usable format as defined in the Contract, or in an open standards machine-readable format if not. The Vendor shall then erase, destroy, and render unreadable all Vendor copies of State data according to the standards enumerated in accordance with the State's most recent Information Disposal and Media Sanitation policy, currently 09-10-NJOIT (http://www.nj.gov/it) and certify in writing that these actions have been completed within thirty (30) days after the termination/expiration of the Contract or within seven (7) days of the request of an agent of the State whichever shall come first.

I. 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 Vendor or any of its subcontractors or agents, the Vendor shall be responsible for recreating such lost data in the manner and on the schedule set by the Contract Manager. The Vendor shall ensure that all data is backed up and is recoverable by the Vendor. In accordance with prevailing federal or state law or regulations, the Vendor shall report the loss of non-public data.

3.9.8 ASSET MANAGEMENT

The Vendor(s) should 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 should include but are not limited to:

A. Information technology asset identification and inventory;

B. Assigning custodianship of assets; and

C. Restricting the use of non-authorized devices.

3.9.9 SECURITY CATEGORIZATION

The Vendor(s) 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 should there be a loss of confidentiality, integrity, availability, or privacy. Information classification and system categorization includes labeling and handling requirements. Security Categorization controls should include but are not limited to the following:

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.

3.9.10 MEDIA PROTECTION

The Vendor(s) 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 Vendor, business partners, or individuals. Media protections should include but are not limited to:

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.

3.9.11 CRYPTOGRAPHIC PROTECTIONS

The Vendor(s) 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 should include but are not limited to:

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.

3.9.12 ACCESS MANAGEMENT

The Vendor(s) shall establish security requirements and ensure appropriate mechanisms are provided for the control, administration, and tracking of access to, and the use of, the Vendor(s)' information systems. Access management plan should 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; and

F. Conduct periodic reviews of access authorizations and controls.

3.9.13 IDENTITY AND AUTHENTICATION

The Vendor(s) 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 Vendor(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 but are not limited to:

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 Vendor {Contractor}'s systems.

3.9.14 REMOTE ACCESS

The Vendor(s) shall strictly control remote access to the Vendor(s) internal networks, systems, applications, and services. Appropriate authorizations and technical security controls should be implemented prior to remote access being established. Remote access controls should include but are not limited to:

A. Establishing centralized management of the Vendor'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 Security Engineering and Architecture

The Vendor 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 should 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.

3.9.15 CONFIGURATION MANAGEMENT

The Vendor 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 includes but is not limited to:

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.

3.9.16 ENDPOINT SECURITY

The Vendor 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 includes but is not limited to:

A. Maintaining an accurate and updated inventory of endpoint devices;

B. Applying security categorizations and implementing commensurate safeguard 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.

3.9.17 ICS/SCADA/OT SECURITY

The Vendor should 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 included here in this document, including but not limited to:

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 Vendor {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.

3.9.18 INTERNET OF THINGS SECURITY

The Vendor should 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 includes but is not limited to 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 Vendor's networks; and

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

3.9.19 MOBILE DEVICE SECURITY

The Vendor 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 includes but is not limited to 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.

3.9.20 NETWORK SECURITY

The Vendor 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 Vendor must:

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 Vendor information systems (e.g. network segmentation, network intrusion detection and prevention systems, wireless restrictions, etc.

3.9.21 CLOUD SECURITY

The Vendor 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 includes but is not limited to ensuring 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 Vendor and the cloud provider are delineated and documented; and

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

3.9.22 CHANGE MANAGEMENT

The Vendor should 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 Vendor with the ability to handle changes in a controlled, predictable, and repeatable manner, and to identify, assess, and minimize the risks to operations and security. Change management controls include but are not limited to the following:

A. Notifying all stakeholder of changes;

B. Conducting a security impact analysis for changes; and

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

3.9.23 MAINTENANCE

The Vendor 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 includes but is not limited to 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.

3.9.24 THREAT MANAGEMENT

The Vendor shall establish a formalized mechanism 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.

3.9.25 VULNERABILITY AND PATCH MANAGEMENT

The Vendor 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 include but are not limited to 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 conduct Independent vulnerability scanning, penetration testing, and red-team exercises.

3.9.26 CONTINUOUS MONITORING

The Vendor 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 include but are not limited to 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.

3.9.27 SYSTEM DEVELOPMENT AND ACQUISITION

The Vendor shall establish security requirements necessary to ensure that systems and application software programs developed by the Vendor or third-parties (e.g. vendors, contractors, etc.) perform as intended to maintain information confidentiality, integrity, and availability, and the privacy and safety of individuals. System development and acquisition security practices include but are not limited to 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.

3.9.28 PROJECT AND RESOURCE MANAGEMENT

The Vendor should 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 include but are not limited to:

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.

3.9.29 CAPACITY AND PERFORMANCE MANAGEMENT

The Vendor 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 include but are not limited to the following:

A. Ensuring the availability, quality, and adequate capacity of compute, storage, memory and network resources are planned, prepared, and measured to deliver the required system performance and future capacity requirements; and

B. Implementing resource priority controls to prevent or limit Denial of Service (DoS) effectiveness.

3.9.30 THIRD PARTY MANAGEMENT

The Vendor 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 include but are not limited to:

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 Vendor's systems and sensitive information;

C. Third party interconnection security; and

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

3.9.31 PHYSICAL AND ENVIRONMENTAL SECURITY

The Vendor shall establish physical and environmental protection procedures that limit access to systems, equipment, and the respective operating environments, to only authorized individuals. The Vendor ensures appropriate environmental controls in facilities containing information systems and assets, to ensure sufficient environmental conditions exist to avoid preventable hardware failures

and service interruptions. Physical and environmental controls include but are not limited to 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.

3.9.32 CONTINGENCY PLANNING

The Vendor should develop, implements, tests, and maintains contingency plans to ensure continuity of operations for all information systems that deliver or support essential or critical business functions on behalf of the Vendor {Vendor}. Contingency planning includes but is not limited to:

A. Backup and recovery strategies;

B. Continuity of operations plans;

C. Disaster recovery plans; and

D. Crisis management plans.

3.9.33 INCIDENT RESPONSE

The Vendor shall maintain an information security incident response capability that includes adequate preparation, detection, analysis, containment, recovery, and reporting activities. Information security incident response activities includes 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.

The Vendor shall disclose to the State of New Jersey a description of their roles and responsibilities related to electronic discovery, litigation holds, discovery searches, and expert testimonies. The Vendor shall disclose its process for responding to subpoenas, service of process, and other legal requests.

4.0 PROPOSAL PREPARATION AND SUBMISSION

4.1 GENERAL

A Bidder may submit additional terms as part of its Proposal and Proposals including Bidder proposed terms and conditions may be accepted, but Bidder proposed terms or conditions that conflict with those contained in the RFP, as defined in Section 2.0 above, or that diminish the State's rights under any Contract resulting from the RFP, may render a Proposal non-responsive. It is incumbent upon the Bidder to identify and remove its conflicting proposed terms and conditions prior to Proposal submission. Where additional terms are submitted they may be accepted, rejected, or negotiated, in whole or in part, at the State's sole discretion where the terms do not conflict with material terms of the RFP or do not diminish the State's rights under the Contract resulting from the RFP.

In the event that a Bidder intends to propose terms and conditions that conflict with the RFP, those Bidder proposed terms and conditions shall only be considered if submitted and agreed to pursuant to the electronic question and answer procedure set forth in Section 1.3.1 of this RFP. Bidders shall not submit exceptions in the Proposal.

After award of the Contract, if a conflict arises between a Bidder's additional terms included in the Quote and a term or condition of the RFP, the term or condition of the RFP will prevail.

Use of URLs in a Proposal should be kept to a minimum and shall not be used to satisfy any material term of the RFP. If a preprinted or other document included as part of the Proposal contains a URL, a printed copy of the URL page shall be provided and will be considered as part of the Proposal.

4.2 PROPOSAL CONTENTS

Bidders may bid on the technology Vendor contract (SOW Part 1), or the consumer assistance Vendor contract (SOW Part 2), or both. Responses to each scope of work will be evaluated independently, therefore separate and self-contained proposals should be submitted for each scope of work.

The Bidder should set forth its overall technical approach and plans to meet the requirements of the RFP in a narrative format. This narrative should demonstrate to the State 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. This narrative should demonstrate to the State that the Bidder's general approach and plans to undertake and complete the contract are appropriate to the tasks and subtasks involved.

SOW Part 1 (Sections 3.2, 3.3., and 3.4) is divided into three phases: (1) design, development, and implementation (DDI); (2) transition towards operation as an SBE (Transition); and (3) autonomous, ongoing maintenance and operations as an SBE (M&O). Phases one and two are further divided into distinct stages. The Bidder's proposal shall describe the strategy for providing the services outlined in each phase.

SOW Part Two (Sections 3.5, 3.6, and 3.7) is divided into three phases: (1) implementation of the consumer assistance center (Implementation), (2) transition support and consumer assistance during Plan Year 2020 OEP (Consumer Assistance Transition), and (3) autonomous, ongoing

maintenance and operations of the consumer assistance center (M&O). Phases one and two are further divided into distinct stages. The Bidder's proposal shall describe the strategy for providing the services outlined in each phase. The Bidder's proposal shall describe the strategy for providing the services outlined in each phase, including a detailed timeline to implement each stage of the SOW.

For SOW Part 1, the Bidder's proposal should describe in detail how the proposed solution will perform the functions outlined in Section 3.2 PART 1– Technology Platform for State Based Exchange.

For SOW Part 2, the Bidder's proposal should describe in detail how the proposed solution will perform the functions outlined in Section 3.5 PART 2 – Consumer Assistance Center.

The Bidder's proposal must include the completed Appendix A accompanying this Request for Proposal.

Mere reiterations of RFP tasks and subtasks are not acceptable, as they do not provide insight into the Bidder's ability to complete the contract. The Bidder's response to this section should be designed to demonstrate to the State 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 proposal will lead to successful contract completion.

4.2.1 DETAILED PROPOSAL REQUIREMENTS FOR SECTION 3.2 PART 1 – TECHNOLOGY PLATFORM FOR STATE BASED EXCHANGE

A. Describe in detail the proposed solution's support for Part 1 technology functions articulated in Section 3.2. The Bidder's response should include the following information, without limitation:

- Provide a narrative for the Bidder's approach for delivering the functionality in 3.2, specifically:
  - The Bidder's response should describe the architecture and implementation of the solution's authentication and authorization system, including any existing support for standardized protocols (Auth0, Microsoft Identity, SAML 2.0, etc.) and any changes required to accommodate remote administration.
  - Address the dependencies and requirements for Data Migration from the FFM to the proposed solution, including any required consumer follow-up activities (such as re-verification of user accounts).
  - Address the strategy for ensuring the readiness of migrated user accounts for eligibility re-verification and auto re-enrollment, including any requirements or dependencies not defined in this RFP.

- Provide the strategy for addressing the constraints outlined in 3.3.

- For the ***Eligibility and Enrollment Coordination and Integration Functionality for OEP 2021***, articulated at 3.2.1(A), if available approaches include using open APIs or customized software, describe both approaches for DOBI consideration.

- For the high value functionality ***Eligibility and Enrollment Coordination and Integration Functionality for OEP 2021*****,** described at 3.2.1 (B), describe a timeline and plan for implementing this additional functionality.

- For the ***Plan for Enhanced Eligibility and Enrollment Functionality and Services,*** propose a scope of work, budget and timeline for developing the plan, which should address further development of the proposed solution to provide enhanced eligibility and enrollment functionality and integration between Medicaid and the SBE. The Bidder should describe the approach for engaging with DOBI, DHS and other stakeholders***.***

- Delineate any assumptions or constraints in the Bidder's proposal.

4.2.2 DETAILED PROPOSAL REQUIREMENTS FOR PART 2 – CONSUMER ASSISTANCE

A. Describe in detail the proposed solution's support for Part 2 consumer assistance functions articulated in Section 3.5. The Bidder's response should include the following information, without limitation:

- The Bidder's training and implementation plan to ensure that consumer assistance personnel utilize the Part 1 technology platform to support the functions defined in Section 3.5.

- A detailed summary and description of the software and hardware utilized to provide the functions listed in Section 3.5.

- The benchmarks and performance indicators, including SLAs, that Bidder proposes to ensure a consistent level of customer satisfaction throughout each Plan Year.

- The Bidder's approach to staffing the consumer assistance call center, including an approach to increase staffing levels as necessary to ensure that the proposed benchmarks and target performance levels are met during OEP.

- The Bidder's approach to screening, initial and ongoing training and any necessary certification(s) of all consumer assistance personnel, including for the secure handling and processing of sensitive information, including PII, FTI, and HIPAA data.

- The Bidder's approach to post-call audit reviews and re-training based on audit findings to ensure maximum quality and accuracy for consumers.

- How the proposed solution will be of servicing at least a 20% increase in caseload versus the figures presented in Section 1.2.2 – Caseload.

- The reporting functionality supported by the Bidder's proposed solution, including the service compliance and production reports to be provided to go live and monthly/quarterly/annually thereafter.

4.2.3 PROJECT PLAN AND CONTRACT SCHEDULE

The Bidder must include a draft Part 1 and/or Part 2 Project Plan and contract schedule. Timeframes are a part of this RFP and the Bidder's schedule should incorporate such timeframes, and identify the completion date for each task and sub-task required by the Scope of Work. Such schedule should include an initial Project Plan meeting with the SCM within 5 calendar days of Contract Award, or as requested by the State. Such schedule should also identify the associated deliverable item(s) to be submitted as evidence of completion of each task and/or subtask. A projected Go Live Date for all functions and systems should be identified in the schedule and will be subject to SCM approval.

The Bidder should identify the contract scheduling and control methodology to be used and should provide the rationale for choosing such methodology. The Bidder must display the Project Plan and Contract Schedule in Gantt, PERT and/or other charts.

4.2.4 ORGANIZATIONAL SUPPORT AND 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 RFP. This section of the proposal must minimally contain the information identified below:

4.2.4.1 LOCATION

The Bidder should include the address of the Bidder's office where responsibility for managing the contract will take place. The Bidder should include the telephone number and name of the individual to contact.

4.2.4.2 CONTRACT-SPECIFIC ORGANIZATION CHART

The Bidder should include a contract organization chart, with names showing management, supervisory and other key staff (including subcontractor management, supervisory or other key staff, if applicable) to be assigned to the contract. The chart should include the labor category and title of each such individual.

4.2.4.3 RESUMES

Detailed resumes should be submitted for all management, supervisory and key staff 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 RFP for creating a State Based Health Exchange. Resumes should include the following:

- The individual's previous experience in completing each similar contract.
- Beginning and ending dates for each similar contract.
- 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 RFP.
- 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 staff that demonstrate knowledge, ability and experience relevant to that part of the work which the Subcontractor is designated to perform. When a bidder submits resumes pursuant to this paragraph, the Bidder shall redact the social security numbers, home addresses, personal telephone numbers and any other personally identifying information other than the individual's name from the resume.

4.2.4.4 EXPERIENCE WITH CONTRACTS OF SIMILAR SIZE AND SCOPE FOR STATE BASED EXCHANGES

The Bidder should provide a comprehensive listing of contracts of similar size and scope that it has successfully completed, as evidence of the Bidder's ability to successfully complete the services required by this RFP. Emphasis should be placed on contracts that are similar in size and scope to the work required by this RFP. 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 RFP. For each such contract, the Bidder should provide two names and telephone numbers of individuals for the other contract party. Beginning and ending dates should also be given for each contract.

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 proposal. The Bidder must provide a detailed description of services to be provided by each Subcontractor.

4.2.3.5 CONTRACTS WITH THE STATE OF NJ

Please provide a list of current contracts with State of NJ as a prime contractor, joint venture or Subcontractor.

4.3 SUBCONTRACTOR UTILIZATION PLAN

All bidders intending to use a subcontractor must submit a completed Subcontractor Utilization Plan. Please see the Subcontractor Utilization Plan form in Section 1.4.8. Subcontracting is encouraged as this RFP has an ambitious schedule and broad scope of work.

4.4 PRICE SCHEDULE/SHEETS

The Bidder must submit its pricing using the format set forth in the State-supplied price sheet/schedule(s) accompanying this RFP (See *Exhibit 5*). Failure to submit all information required may result in the proposal being considered non-responsive. Each Bidder is required to hold its prices firm through issuance of contract.

4.4.1 HOURLY RATE SCHEDULE FOR CHANGE ORDERS

Prices quoted for change orders/regulatory changes shall remain in effect for the duration of the contract. Proposers shall provide All Inclusive Hourly Rates for change orders/regulatory changes. Proposers shall provide an All Inclusive Hourly Rate for each staff classification identified on the project. Proposers shall not provide a single compilation rate.

4.5 TECHNOLOGY PROJECT PLAN (TPP)

The Bidder shall provide its draft TPP to accomplish all work required by this RFP. The Technology Project Plan shall include:

A. The Technology Design and Development Plan: The Bidder should describe the methodology by which it will design and develop the required system functionality including the Software Development Lifecycle;

B. The Technology System Test Plan: The Bidder should describe its plans to complete system and user acceptance testing including its methodology for fixing bugs and defects and retesting;

C. The Technology Implementation Plan: The Bidder should describe its plans for system roll-out including System Pilot Testing and full deployment; and

D. Technology Operations and Maintenance Plans: The Bidder should describe its plans to support the operational system including application updates, new releases, bug and defect repairs, emergency maintenance/repairs of hardware and software and routine maintenance.

E. The TPP should also include draft plans for how the Bidder will address the plans located throughout Section 3:

1. The TPP should demonstrate to the Evaluation Committee that the Bidder understands the scope of work required for a successful implementation of the system, its operations and maintenance and support.

4.5.1 PLANS REQUIRED BY BID SOLICITATION SECTION 3.9.1 SECURITY PLAN AND STANDARDS

The Bidder shall provide a draft of the following plans:

A. Disaster Recovery Plan:
This plan shall define the steps the Vendor will take in reaction to a disaster (i.e. flooding, hurricane, etc.) in any portion of or throughout the State. The plan shall include considerations for participant benefit and card availability, vendor readiness and related assessments, as well as interface with all state systems.

B. Backup Plan:
The Vendor shall have in place a Continuation of Business (COB) Plan and procedures to ensure the continuation of operations in the event of a disruption in operations, which will allow benefit access when the Vendor's production computer systems, terminals, gateway, or communications are not operational. The Backup Plan must detail how the Vendor will ensure that data is backed up on a regular basis. If data contains PII, PCI, and FISMA – backups must be encrypted unless otherwise approved by NJWIC or USDA. Backups shall be verified on a regular basis to ensure that files are retrievable. Extra backups should be kept off-site in a secure location in the event of property damage at the main site. Backups must be sanitized or destroyed before discarding.

C. Security Plan:

a. Security of data exchange and interface between WOW and the e-WIC systems;
b. Encryption of PINs and secure maintenance of PIN data;
c. Security of all access points to the e-WIC systems (portals, ARU, etc.);
d. System roles;
e. Security of all phases of transaction processing and settlement; and
f. Physical Security of primary and secondary data processing, switching, and other support sites.

4.6 NON-COLLUSION

By submitting a proposal, the bidder certifies as follows:

A. The price(s) and amount of its proposal have been arrived at independently and without consultation, communication or agreement with any other Vendor, Bidder or potential Bidder;

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

C. No attempt has been made or will be made to induce any firm or person to refrain from bidding on this contract, or to submit a proposal higher than this proposal, or to submit any intentionally high or noncompetitive proposal or other form of complementary proposal;

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

E. The Bidder, its affiliates, subsidiaries, officers, directors, and employees are not currently under investigation by any governmental agency and have not in the last four (4) years been convicted or found liable for any act prohibited by state or federal law in any jurisdiction, involving conspiracy or collusion with respect to bidding on any public contract.

5.0 SPECIAL TERMS AND CONDITIONS

5.1 PRECEDENCE

The contract awarded as a result of this RFP shall consist of this RFP, addenda to this RFP, the Vendor's proposal, any best and final offer and the Notice of Award.

Unless specifically stated within this RFP, the Special Terms and Conditions of the RFP take precedence over the State of NJ Standard Terms and Conditions (4/15/19), and Waivered Contracts Supplement to The State of New Jersey Standard Terms and Conditions (6/14/2018) accompanying this RFP *(See Exhibits 2 and 3).*

In the event of a conflict between the provisions of this RFP, including the Special Terms and Conditions and the State of NJ Standard Terms and Conditions, and any addendum to this RFP, the addendum shall govern.

In the event of a conflict between the provisions of this RFP, including any addendum to this RFP, and the Bidder's proposal, the RFP and/or the addendum shall govern.

5.2 CHANGE IN LAW

Whenever a change in applicable law or regulation affects the scope of work, the Director shall provide written notice to the Vendor of the change and the Director's determination as to the corresponding adjusted change in the scope of work and corresponding adjusted contract price. Within five (5) business days of receipt of such written notice, if either is applicable:

A. If the Vendor does not agree with the adjusted contract price, the Vendor shall submit to the Director any additional information that the Vendor believes impacts the adjusted contract price with a request that the Director reconsider the adjusted contract price. The Director shall make a prompt decision taking all such information into account, and shall notify the Vendor of the final adjusted contract price; and

B. If the Vendor has undertaken any work effort toward a deliverable, task or subtask that is being changed or eliminated such that it would not be compensated under the adjusted contract, the Vendor shall be compensated for such work effort according to the applicable portions of its price schedule and the Vendor shall submit to the Director an itemization of the work effort already completed by deliverable, task or subtask within the scope of work, and any additional information the Director may request. The Director shall make a prompt decision taking all such information into account, and shall notify the Vendor of the compensation to be paid for such work effort.

5.3 DATA CONFIDENTIALITY

All financial, statistical, personnel, customer and/or technical data supplied by the State to the Vendor are confidential (State Confidential Information). The Vendor must secure all data from manipulation, sabotage, theft or breach of confidentiality. The Vendor is prohibited from releasing any financial, statistical, personnel, customer and/or technical data supplied by the State that is deemed confidential. Any use, sale, or offering of this data in any form by the Vendor, or any individual or entity in the Vendor's charge or employ, will be considered a violation of this Contract and may result in Contract termination and the Vendor's suspension or debarment from State contracting. In addition, such conduct may be reported to the State Attorney General for possible criminal prosecution.

The Vendor shall assume total financial liability incurred by the Vendor associated with any breach of confidentiality.

When requested, the Vendor and all project staff including its Subcontractor(s) must complete and sign confidentiality and non-disclosure agreements provided by the State. The Vendor may be required to view yearly security awareness and confidentiality training modules provided by the State. Where required, it shall be the Vendor's responsibility to ensure that any new staff sign the confidentiality agreement and complete the security awareness and confidentiality training modules within one month of the employees' start date.

The State reserves the right to obtain, or require the Vendor to obtain, criminal history background checks from the New Jersey State Police for all Vendor and project staff (to protect the State of New Jersey from losses resulting from Vendor employee theft, fraud or dishonesty). If the State exercises this right, the results of the background check(s) must be made available to the State for consideration before the employee is assigned to work on the State's project. Prospective employees with positive criminal backgrounds for cyber-crimes will not be approved to work on State Projects. Refer to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook, Section 10.1.3, Filling the Position – Screening and Selecting.

5.4 NEWS RELEASES

The Vendor is not permitted to issue news releases pertaining to any aspect of the services being provided under this contract without the prior written consent of DOBI.

5.5 ADDITIONAL WORK AND/OR PROJECTS

The Vendor may propose additional projects during the performance of this contract. The Vendor shall not begin performing any additional work or special projects without first obtaining written approval from both the SCM and the Director.

In the event of additional work and/or special projects, the Vendor must present a written proposal to perform the additional work to the SCM. The proposal should provide justification for the necessity of the additional work. The relationship between the additional work and the base contract work must be clearly established by the Vendor in its proposal.

The Vendor's written proposal must provide a detailed description of the work to be performed broken down by task and subtask. The proposal should also contain details on the level of effort, including hours, labor categories, etc., necessary to complete the additional work.

The written proposal must detail the cost necessary to complete the additional work in a manner consistent with the contract. The written price schedule must be based upon the hourly rates, unit costs or other cost elements submitted by the Vendor in the Vendor's original proposal submitted in response to this RFP. Whenever possible, the price schedule should be a firm, fixed price to perform the required work. The firm fixed price should specifically reference and be tied directly to costs submitted by the Vendor in its original price. A payment schedule, tied to successful completion of tasks and subtasks, must be included.

Upon receipt and approval of the Vendor's written proposal, the SCM shall forward same to the Director for the Director's written approval. Complete documentation from the Using Agency, confirming the need for the additional work, must be submitted. Documentation forwarded by the SCM to the Director must include all other required State approvals, such as those that may be required from the State of New Jersey's Office of Management and Budget and NJOIT.

No additional work and/ or special project may commence without the Director's written approval. In the event the Vendor proceeds with additional work and/ or projects without the Director's written approval, it shall be at the Vendor's sole risk. The State shall be under no obligation to pay for work performed without the Director's written approval.

5.6 CONTRACT TERM AND EXTENSION OPTIONS

The State may award one or more contracts in conjunction with this RFP, as determined in the best interest of the State.

SOW Part I Contract
DOBI shall administer the contract resulting from Part I of this RFP. The resulting contract shall specify an initial contract term of 5 years and 4 months, anticipated to begin September 30, 2019 with an option to renew for two (2) one (1) year extensions, if agreed upon by vendor and DOBI.

SOW Part II Contract
DOBI shall administer the contract resulting from Part II of this RFP. The resulting contract shall specify an initial contract term of 3 years, anticipated to begin September 30, 2019 with an option to renew for two (2) one (1) year extensions, if agreed upon by vendor and DOBI.

Any such extensions shall be made upon the same terms and conditions, and pricing at the rates in effect in the last year of the Contract, or at rates more favorable to the State

5.7 CONTRACT AMENDMENT

Any changes or modifications to the terms of the contract shall be valid only when they have been reduced to writing and signed by the Vendor and the Director.

5.8 LIQUIDATED DAMAGES

The Division of Purchase and Property and the Vendor ("the Parties") agree that it would be extremely difficult to determine actual damages which the State of New Jersey will sustain as the result of the Vendor's failure to meet the performance requirements. Any breach by the Vendor will negatively impact the State and deprive the State of the ability to timely provide services for government-funded individual assistance programs. Moreover, any breach by the Vendor may negatively impact New Jersey residents' access to affordable, quality healthcare and will affect the State's ability to provide certain services which are required under both State and Federal law. Access to health insurance for these eligible individuals and their families is of paramount importance, not only to these individuals but also the State. Therefore, the Parties agree that Liquidated Damages, as defined in *Exhibit 4,* are reasonable estimates of the damages the State of New Jersey may sustain from the Vendor's performance deficiencies set forth within this section and are not to be construed as penalties.

The State has the sole discretion to determine whether liquidated damages should be assessed.

Assessment of liquidated damages shall be in addition to, and not in lieu of, such other remedies as may be available to the State of New Jersey. Except and to the extent expressly provided herein, the Division shall be entitled to recover liquidated damages under each section applicable to any given incident.

Please refer to *Exhibit 4* for the list of Performance Standards and Liquidated Damages.

5.8.1 NOTIFICATION OF LIQUIDATED DAMAGES

Upon determination that Liquidated Damages are to be assessed, the State will notify the Vendor 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 Vendor 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 provision. Notwithstanding any provision of any Bid Solicitation to the contrary, should there be any conflict between this section and any provision of a Bid Solicitation, this section shall supersede such Bid Solicitation provision to the contrary.

5.8.2 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 Vendor corrects the condition(s) for which liquidated damages were imposed;

B. The Vendor notifies the State in writing that the condition(s) has (have) been corrected; and

C. The Director reviews and approves in writing the recommendation of State.

5.8.3 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.

5.8.4 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 to the State, 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.

5.8.5 PAYMENT OF LIQUIDATED DAMAGES

Once assessed pursuant to Section 5.14, liquidated damages will be deducted from any funds owed to the Vendor by the State, and in the event the amount due the Vendor is not sufficient to satisfy the amount of the liquidated damages, the Vendor 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 Vendor.

5.9 RETAINAGE

Ten percent (10%) retainage will be withheld from each invoice submitted. At the end of each three (3) month period, the State will review the Vendor's performance. If performance has been satisfactory, the State will release 90% of the retainage for the preceding three (3) month period. Following certification by the State Contract Manager that all services have been satisfactorily performed the balance of the retainage shall be released to the Vendor.

5.10 SERVICE LEVEL AGREEMENTS

5.10.1 VENDOR WARRENTS THAT IT SHALL MAINTAIN THE SYSTEM AND HOSTING SERVICES, IN WHOLE AND IN PART, TO MEET THE SERVICE LEVEL AGREEMENTS.

Vendor and DOBI will conduct tests for measuring and certifying the achievement of the Service Level Agreements as described in *Exhibit 4*. Vendor must implement all testing, measurement and monitoring tools and procedures required to measure and report Vendor's performance of the System against the applicable Service Level Agreements. Such testing, measurement and monitoring must permit reporting at a level of detail sufficient to verify compliance with the Service Level Agreements and will be subject to audit by DOBI. Vendor will provide DOBI with information and access to all information or work product produced by such tools and procedures upon request for purposes of verification.

If the System fails to meet all Service Level Agreements, Vendor shall modify, reconfigure, upgrade or replace Equipment, the Network, and/or Software at no cost to the Exchange in order to ensure that the System and Hosting Services comply with such Service Level Agreements.

5.11 DATA SECURITY STANDARDS

- Data Security: The Vendor at a minimum must protect and maintain the security of data in accordance with the policies and standards contained in the New Jersey Statewide Information Security Manual (https://www.nj.gov/it/docs/ps/NJ_Statewide_Information_Security_Manual.pdf), which is derived from applicable State and federal laws; industry best practices including the National Institute of Standards and Technology (NIST) Cybersecurity Framework for Improving Critical Infrastructure; NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations; NIST Special Publication 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations; the Center for Internet Security (CIS) Top 20 Critical Security Controls; and the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM).

- All information assets and information shall be classified according to their sensitivity and criticality. Protection mechanisms shall be implemented commensurate with the impact should there be a loss of confidentiality, integrity, and/or availability of the asset or information.

- Data Storage: All data provided by the State of New Jersey or State data obtained by the Vendor 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 Project Manager.

The Vendor shall encrypt all data at rest defined as personally identifiable information by the State of New Jersey or applicable law, regulation or standard. The Vendor shall not store or transfer State of New Jersey data outside of the United States.

- Data Scope: All provisions applicable to State data include data in any form of transmission or storage, including but not limited to: database files, text files, backup files, log files, XML files, and printed copies of the data.

5.12 FEDERAL TAX INFORMATON SECURITY (TAX INFORMATION SECURITY GUIDELINES FOR FEDERAL, STATE, AND LOCAL AGENCIES (IRS PUBLICATION 1075)

GENERAL SERVICES

I. PERFORMANCE

In performance of this contract, the Vendor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

(1) All work will be performed under the supervision of the Vendor or the Vendor's responsible employees.

(2) Any Federal tax returns or return information (hereafter referred to as returns or return information) made available 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 other than an officer or employee of the Vendor is prohibited.

(3) All returns and return information will be accounted for upon receipt and properly stored before, during, and after processing. In addition, all related output and products will be given the same level of protection as required for the source material.

(4) No work involving returns and return information furnished under this contract will be subcontracted without prior written approval of the IRS.

(5) The Vendor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

(6) The agency will have the right to void the contract if the Vendor fails to provide the safeguards described above.

II. CRIMINAL/CIVIL SANCTIONS

(1) 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 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 years, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized future 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 $1,000.00 or imprisonment for as long as 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 $1,000.00 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. The penalties are prescribed by IRC Sections 7213A and 7431.

(3) Additionally, it is incumbent upon the Vendor 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 Vendors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a Vendor, 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 so 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.

(4) Granting a Vendor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Vendors must maintain their 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, Vendors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (*IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and 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. (See Section 10) For both the initial certification and the annual certification, the Vendor should sign, with either ink or electronic

signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the Vendor 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 Vendor is found to be noncompliant with contract safeguards.

TECHNOLOGY SERVICES

I. PERFORMANCE

In performance of this contract, the Vendor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

(1) All work will be done under the supervision of the Vendor or the Vendor's employees.

(2) 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 Vendor will be prohibited.

(3) 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.

(4) The Vendor 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 Vendor will retain no output at the time the work is completed. If immediate purging of all data storage components is not possible, the Vendor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures.

(5) 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 Vendor 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.

(6) 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.

(7) No work involving Federal tax information furnished under this contract will be subcontracted without prior written approval of the IRS.

(8) The Vendor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office.

(9) The agency will have the right to void the contract if the Vendor fails to provide the safeguards described above.

II. 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 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 the 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 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 Vendor 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 Vendors by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a Vendor, 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.

(4) Granting a Vendor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Vendors must maintain their 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, Vendors should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (*IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and 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. (See Section 10) For both the initial certification and the annual certification, the Vendor should sign, either with ink or electronic signature, a confidentiality statement certifying their understanding of the security requirements.

III. INSPECTION:

The IRS and the Agency shall have the right to send its officers and employees into the offices and plants of the Vendor 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 Vendor is found to be noncompliant with contract safeguards.

6.0 PROPOSAL EVALUATION

6.1 RIGHT TO WAIVE

Pursuant to N.J.A.C. 17:12-2.7(d) the Director may waive minor irregularities or omissions in a proposal. The Director also reserves the right to waive a requirement provided that the requirement does not materially the procurement of the State's interest associated with the procurement.

6.2 STATE'S RIGHT OF FINAL PROPOSAL ACCEPTANCE

The Director reserves the right to reject any or all proposals, or to award in whole or in part if deemed to be in the best interest of the State to do so. The Director shall have authority to award orders or contracts to the Vendor or Vendors, best meeting all specifications and conditions in accordance with N.J.S.A. 52:34-12. Tie proposals will be awarded by the Director in accordance with N.J.A.C.17:12-2.10.

6.3 STATE'S RIGHT TO INSPECT BIDDER'S FACILITIES

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

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

6.4 STATE'S RIGHT TO REQUEST FURTHER INFORMATION

The State reserves the right to request all information which may assist it in making a contract award, including factors necessary to evaluate the Bidder's financial capabilities to perform the contract. Further, the State reserves the right to request a bidder to explain, in detail, how the proposal price was determined.

6.5 PROPOSAL EVALUATION COMMITTEE

Proposals may be evaluated by an Evaluation Committee composed of members of affected departments and agencies together with representative(s) that the State deems appropriate. Representatives from other governmental agencies may also serve on the Evaluation Committee. On occasion, the Evaluation Committee may choose to make use of the expertise of outside consultant(s) in an advisory role.

6.6 ORAL PRESENTATION AND/OR CLARIFICATION OF PROPOSAL

After the submission of proposals, unless requested by the State as noted below, Bidder contact with the State is still not permitted.

After the proposals are reviewed, one, some or all of the Bidders may be asked to clarify certain aspects of their proposals. A request for clarification may be made in order to resolve minor ambiguities, irregularities, informalities or clerical errors. Clarifications cannot correct any deficiencies or material omissions or revise or modify a proposal.

The Bidder may be required to give an oral presentation to the State concerning its proposal.

Bidders may not attend the oral presentations of their competitors.

It is within the State's discretion whether to require a Bidder to give an oral presentation or require the Bidder to submit written responses to questions regarding its proposal. Action by the State in this regard should not be construed to imply acceptance or rejection of a proposal. The Division will be the sole point of contact regarding any request for an oral presentation or clarification.

6.7 EVALUATION CRITERIA

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

6.7.1 TECHNICAL EVALUATION CRITERIA

a. Personnel: The qualifications and experience of the Bidder's management, supervisory, and key staff 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 contracts of a similar size and scope in relation to the work required by this RFP.

c. Ability of firm to complete the Scope of Work based on its Technical Proposal: The Bidder's demonstration in the proposal 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. If the State elects to have oral presentations, they will be a factor in scoring.

6.7.2 BIDDER'S PRICE SCHEDULE

For evaluation purposes, Bidders will be ranked according to the total proposal price located on the Price Sheet/Schedule accompanying this RFP (See *Exhibit 5).*

6.7.3 PROPOSAL DISCREPANCIES

In evaluating proposals, 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.

6.7.4 EVALUATION OF THE PROPOSALS

After the Evaluation Committee completes its evaluation, it recommends that the award be made to the most responsible Bidder(s) whose proposal, conforming to this RFP, is most advantageous to the State, price and other factors considered. The Evaluation Committee considers and assesses price, technical criteria, and other factors during the evaluation process and makes a recommendation. The Evaluation Committee's recommendation may be accepted, rejected or modified. Whether or not there has been a negotiation process as outlined in Section 6.8 below, the State reserves the right to negotiate price reductions with the selected Bidder.

6.8 NEGOTIATION AND BEST AND FINAL OFFER (BAFO)

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

Similarly, the Division may invite one 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 is not equal to or lower in price than the pricing offered in the Bidder's original proposal will be rejected as non-responsive and the State will revert to consideration and evaluation of the Bidder's original pricing.

If required, after review of the BAFO(s), clarification may be sought from the Bidder(s). The Division may conduct more than one round of negotiation and/or BAFO in order to attain the best value for the State.

After evaluation of proposals and as applicable, negotiation(s) and/or BAFO(s), the Division will recommend, to the Director, the responsible Bidder(s) whose proposal(s), conforming to the RFP, is/are most advantageous to the State, price and other factors considered. The Director may accept, reject or modify the recommendation of the Division. The Director may initiate additional negotiation or BAFO procedures with the selected Bidder(s).

Negotiations will be conducted only in those circumstances where they are deemed 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 proposal in response to this RFP since the State may, after evaluation, make a contract award based on the content of the initial submission, without further negotiation and/or BAFO with any bidder.

All contacts, records of initial evaluations, any correspondence with Bidders related to any request for clarification, negotiation or BAFO, any revised technical and/or price proposals, the Evaluation Committee Report and the Award Recommendation, will remain confidential until a Notice of Intent to Award a contract is issued.

6.9 COMPLAINTS

A Bidder with a history of performance problems as demonstrated by formal complaints and/ or contract cancellations for cause pursuant to the State of NJ Standard Terms and Conditions accompanying this RFP may be bypassed for an award issued as a result of this RFP *(See Exhibit 2).*

7.0 CONTRACT ADMINISTRATION

7.1 STATE CONTRACT MANAGER

The State Contract Manager (SCM) is the State employee responsible for the overall management and administration of the contract.

The SCM for this project will be identified at the time of execution of contract. At that time, the Vendor will be provided with the SCM's name, department, division, agency, address, telephone number, fax phone number, and e-mail address.

7.1.1 SCM RESPONSIBILITIES

In addition to responsibilities set forth in the RFP, the SCM will be responsible for engaging the Vendor, assuring that Purchase Orders are issued to the Vendor, directing the Vendor to perform the work of the contract, approving the deliverables and approving payment vouchers. The SCM is the person that the Vendor will contact after the contract is executed for answers to any questions and concerns about any aspect of the contract. The SCM is responsible for coordinating the use of the Contract and resolving minor disputes between the Vendor and any component part of the SCM's Department.

The SCM is also responsible for notifying Office of Information Technology (OIT) and other appropriate parties of security and privacy violations or incidents. The SCM cannot modify the Contract, direct or approve a Change Order.

APPENDIX A:

Vendor Experience in implementing Part 1 – Technology Platform for State Based Exchange

In providing its overall technical approach to SOW Part 1 –Technology Platform for State Based Exchange, the Bidder should provide the following information:

A. Using the following table, indicate which State exchanges, if any, have been supported by the Base configuration of the Bidder's platform (provide the two-letter state abbreviation and the exchange agency name); the Plan Years in which the SBE received support from the Bidder; and which, if any of the functions in Section 3.2 were NOT supported for each Agency/Plan Year (the list of unsupported functions should be identified using the Section 3.2 function numbering and labels (e.g. "3.2.B. Anonymous pre-screening of eligibility"), and separated with semicolons). Use separate rows for each Agency/Plan Year. Add additional rows as necessary.

State	Exchange Agency Name	Plan Year	Exchange Functions *NOT* Supported and Explanation

B. Using the following table, indicate which, if any of the State exchange functions that were supported by the Bidder for the SBEs listed above were provided in part or in full by sub-contractors Provide the exchange agency name, the Plan Year, the list of supported functions identified using the Section 3.2 function numbering and labels (e.g. "3.2.A. Anonymous pre-screening of eligibility"), and the name of the sub-contractor that provided the function. Use separate rows for each agency/Plan Year/function. Add additional rows as necessary.

Exchange Agency Name	Plan Year	Exchange Function	Sub-Contractor

C. Using the following table, indicate which State exchanges listed above required the Bidder's platform to support seamless collaboration with Medicaid. Describe the nature and extent of such collaboration, including how the platform supported such collaboration and any functional limitations or carve-outs. Use separate rows for each Agency/Plan Year. Add additional rows as necessary.

State	Exchange Agency Name	Plan Year	Explain Medicaid collaboration including limitations/carve-outs

Vendor Experience in Implementing Part 2 – Consumer Assistance Center

In providing its overall technical approach to fulfilling the requirements of Section 3.5, Part 2 –Consumer Assistance Center, the Bidder should provide the following information:

A. Using the following table, indicate which State exchanges, if any, have been supported by the Bidder's proposed solution (provide the two-letter state abbreviation and the exchange agency name); which Plan Years received support; and which, if any, of the above-mentioned functions were NOT supported for each Agency/Plan Year (the list of unsupported functions should be identified using the Section 3.5 function numbering and labels (e.g. "3.5.A. Consumer education for ACA requirements/eligibility"), and separated with semicolons). Use separate rows for each Agency/Plan Year. Add additional rows as necessary.

State	**Exchange Agency Name**	**Plan Year**	**Consumer Assistance Functions *NOT* Supported**

B. Using the following table, indicate which, if any, of the State exchange functions that were supported by the Bidder for the SBEs listed above were provided in part or in full by sub-contractors. Provide the exchange agency name, the Plan Year, the list of supported functions identified using the Section 3.5 function numbering and labels (e.g. "3.5.A. Consumer education for ACA requirements/eligibility"), and the name of the sub-contractor that provided the function. Use separate rows for each agency/Plan Year/function. Add additional rows as necessary.

Exchange Agency Name	Plan Year	Consumer Assistance Function	Sub-Contractor

C. Using the following table, indicate which, if any, of the consumer assistance functions listed in Section 3.5 would NOT be supported by the proposed solution. Provide the number of the exchange function (as listed in Section 3.5) and an explanation detailing the circumstances of the omission. Use separate rows for each function. Add additional rows as necessary.

Consumer Assistance Function that Will NOT be Supported	Explanation

D. Using the following table, indicate the State exchanges to which the Bidder has provided its proposed consumer assistance solution that have required integration and collaboration with Medicaid, and describe the nature and extent of such integration/collaboration, including any functional limitations or carve-outs. Use separate rows for each Agency/Plan Year. Add additional rows as necessary.

State	Exchange Agency Name	Plan Year	Explain Medicaid collaboration including limitations/carve-outs