Request for Quotation-RFQ

for

NJ Temporary Disability and Family Leave Insurance Claims Management System

Version 2.0
Dated: December 18, 2020

RFQ Issued on: December 1, 2020 (Version 1.0)

Submission of Questions - Due Date and time:
December 15, 2020 4:00 PM
Proposal Due Date and Time: Extended to January 29, 2021 at 2:00PM

- **NOTE: All proposals are to be submitted to the following: NJDOLTDIFLIMOD@dol.nj.gov**

Table of Contents

PLEASE READ THIS DOCUMENT IN ITS ENTIRETY.

ALL QUESTIONS MUST BE SUBMITTED IN ONE DOCUMENT. PLEASE DO NOT SUBMIT MULTIPLE EMAILS/SEPARATE DOCUMENTS. ALL QUESTIONS MUST REFERENCE THE SECTION OF THE RFQ TO WHICH IT PERTAINS. ALL QUESTIONS MUST BE SUBMITTED VIA EMAIL TO THE FOLLOWING EMAIL ADDRESS:

NJDOLTDIFLIMOD@dol.nj.gov

THE EMAIL NOTED ABOVE SHALL BE FOR RFQ SPECIFIC QUESTIONS ONLY.

1.0 PURPOSE AND INTENT

This Request for Quotation (RFQ) is issued by the New Jersey Department of Labor and Workforce Development Division of Temporary Disability and Family Leave Insurance. The purpose of this RFQ is to solicit Quotations for a business specific Claims Management System in order to process Temporary Disability Claims and Family Leave Insurance claims. This system shall replace the existing legacy mainframe case management system known as the Disability Automated Benefits Processing (DABS) system. The Division is requesting multiple pricing quotes to include the following:

1) Quote for software licensing, configurations, integration and hosting based on a Software as a Service (SaaS) pricing model

1.1 Current System Background

TDI/FLI processes claims via the DABS legacy mainframe, implemented in 1988. Although it has been periodically modified since that time, the DABS system and others that interface with it, no longer provide the functionality required to deliver services in the most cost-efficient manner possible. DABS is a COBOL based mainframe system that utilizes two databases. The databases are the Information Management System (IMS) and DB2. There are 16 Virtual Storage Access Method (VSAM) files used to maintain the data within the system. DABS contain Customer Information Control System (CICS) applications for entry, maintenance and determinations of claims. The batch portion of DABS deals with the benefit payments, forms, and reporting requirements of the system.
The DABS system in its current architecture does not allow TDI/FLI the required flexibility with regard to workflow changes, is not user friendly for claim and call center personnel, requires frequent re-entry of data to navigate, and requires a programming skill set that is on the decline. Since reporting is handled within the batch process, real-time management reporting is not available.

Due to batch processing, real-time claim processing and user access is also not available with the DABS system. The system is available for 12 hours each weekday, with overnight updates and other access limitations existing on weekends and during maintenance.

In 2009, the introduction of the new Family Leave Insurance program resulted in TDI's DABS system being "retro-fitted" to pay FLI claims. This adaptation was found to rely on inefficient manual processing by claim staff due to a number of unique FLI program requirements.

In 2016, a web-based application was implemented to increase the efficiency of filing and processing initial applications, changes of address, claim inquiries, and annual tax statements. A separate Oracle database

was also constructed, not only to house the online data, but to also capture new data elements outside of DABS. A subsequent automated processing application was created for filing claim extensions, which is also dependent upon DABS to complete the operation

Table 1: Existing DABS Environment

Environment	Users
DABS User Base	
Customer Service	*44*
Temporary Disability Insurance	*93*
Family Leave Insurance	*36*
Total Number of Users	*173*
Current Web Application User Base	
Temporary Disability Insurance	*55,000 (annual avg.)*
Family Leave Insurance	*20,000 (annual avg.)*
Other Systems/Tools Related	
Claims Intake (Imaging)	*19*
Disability During Unemployment (DDU)	*17*
Private Plan	*15*
Browsers Used	
Internet Explorer	
Firefox	
Chrome	
Safari	
Other	

1.2 Current System Infrastructure

The following systems are leveraged to support the operations of the TDI/FLI Program:

- DABS (Disability Automated Benefits System) that runs on a mainframe whose hardware is maintained by the Office of Information Technology (OIT) and whose application is maintained by NJ Dept of Labor Division of Information Technology (DIT). This system is an NJDOL system that the TDI/FLI program uses for data validation, benefit payment, and a variety of workflow needs.

- A web-based user interface application written in the programming language ASP.net and JAVA with an Oracle backend supported by NJDOL's internal Division of Information Technology (DIT). This infrastructure exists in the NJDOL DIT Data Center.

- The LOOPS mainframe, whose hardware is maintained by the Office of Information Technology (OIT) and whose application is maintained by NJ Dept of Labor Division of Information Technology (DIT).

- Interfaces to Federal, State, and other vendors who support the validation and payment processing.

- Avaya phone and Interactive Voice Response (IVR) system, which provides claim status information.

- Bank of America distributes debit cards upon initial claim entry. At the present time also adding direct deposit capability.

- The Document Imaging System (P8) hosted by the Division of Revenue Enterprise Services (DORES).

1.3 Current Business Process

The daily operations of the TDI/FLI programs are divided into five separate sections: Claims Intake, Initial Determinations, Reconsiderations, Customer Service, and Private Plan. Each section has their own functional scope and different levels of interaction with outside users. Utilizing the aforementioned infrastructure systems, these sectional elements operate under the effects of the established law to provide coherent and consistent processes.

Claims Intake

The Claims Intake section handles all documents that are received by the division. These documents can include new applications for benefits, any subsequent system-generated forms that are completed by the recipient, and any non-standard correspondence.

New applications for benefits are received by paper and/or electronically. Paper applications are sent to a scanning room with a batch cover sheet, used to identify the program area. New applications received via fax are processed by a legacy fax server and imported directly into a legacy optical character recognition (OCR) system. Claims Intake staff process these applications page by page, categorizing and indexing the types of batches to process values against the document image. Once appropriate values and assignment occurs in DABS, the images and values are exported to the document repository for storage. This same process occurs for any other correspondence and/or system-generated forms that are received by paper and/or electronically.

The other option for the receipt of new applications is through the TDI/FLI online application. These electronic applications are submitted by the claimant after they complete and certify the claimant section of the application. At that time, all rules validations and system interfaces have been triggered or executed, creating a summary of the claimant section elements. Additionally, a Form ID is generated on subsequent forms that the claimant can print and give to their medical provider for completion and certification of their sections of the claim. During regular business hours, the certified claimant section will become part of the scheduled job that runs every 5 minutes to process the files into the legacy claims system. Electronic applications that are completed and certified after regular business hours are added to a queued batch file to be transferred to the legacy claims system for processing at the start of the next business day.

Initial Determinations

For both Temporary Disability and Family Leave Insurance programs, all applications that have gone through the Claims Intake process are assigned to staff consisting of claims examiners. Claims are reviewed in the order of which they are received as there are no other indicators to advise staff on what actions may be taken until the claim is individually reviewed. Claims are first evaluated by Initial Determinations and then may be found to belong to other scopes or jurisdictions, such as the Private Plan section or the Workers' Compensation Unit. In these cases, each claim must be manually transferred to the respective scope or jurisdiction by designated staff.

If the claim is determined to be under State Plan jurisdiction, staff will review the claim for eligibility based on current procedures and laws. If additional information is needed, forms and/or phone calls may be used to contact the claimant, medical provider, or employers to resolve conflicts or obtain missing information. Most forms are generated in the legacy claims system and are given a Form ID which is used to track the form. Forms are mailed by regular postal service and phone conversations are documented via system memos, entered manually by each claims examiner.

When forms are returned to the Division, they are individually viewed on the P8 imaging system to determine if the missing information has been provided and/or the conflict resolved. If the claim is unable to be determined eligible, a decision of ineligibility is made and identifies the required resolution.

Online applications are processed by a unit of staff within Initial Determinations. Claimants may begin a claim application online, with information becoming available to staff during the operational DABS hours: between 7AM to 7PM, Monday through Friday and 8AM to 1PM on Saturday. As DABS is limited in its ability to differentiate workloads by functional roles, both online applications and paper applications are assigned at random to any active Determinations examiner workload. The online application tasks must then be recognized and manually transferred to the correct workloads of examiners who exclusively process online applications.

Online applications are processed by staff who have access to view several decentralized screens: DABS, LOOPS, SIDI, P8, and uniquely TDI/FLI Online Claims Status. COURTS-Online may also be used by staff for claims with liens, an exclusive characteristic of claims associated with Workers' Compensation benefits.

Reconsiderations/Redeterminations – Appeals Claim Processing

After the determination of a claim, any subsequent information that is received by the Division is routed to the Reconsiderations section, a process that applies to both the Temporary Disability and Family Leave Insurance programs. The Reconsiderations staff's responsibilities are to review, update, and correct claims that have been previously determined.
Reconsiderations staff have the ability and authority to redetermine previously denied claims or to adjust benefit entitlement rate and duration. To do so, the examiners in Reconsiderations must examine any claimant, medical, and/or employer information that has been received. The examiners look for items such as address changes, overlapping claims, medical extensions, additional wage information, etc.

Extensions of leave benefits impact approximately 90 percent of all approved TDI/FLI claims. After a claimant receives correspondence about a possible extension of their claim, the claimant will typically complete a web-based, online extension application. At this point, if the claim does not require manual intervention, the extension is auto-processed. This operation of auto-processing extensions affects approximately 2,800 claims per month, or 60 percent of submitted extensions. Any discrepancies detected by the legacy system are reviewed by Reconsiderations staff to resolve issues.

Other functions handled by the Reconsiderations staff include managing appeals, investigations, and refunds. The Reconsiderations unit also handles various efforts on irregular claims, including issues to covered employment, gross misconduct, wage record request, potential fraud, escalation to an independent medical examiner, and returned paper checks and documentation.

Customer Service

The Customer Service Section (CSS), operating from 2 locations, utilizes a centralized call system. This system transfers calls to the CSS staff based on availability. CSS staff are responsible for answering customer inquiries by claimants, medical providers, employers, attorneys, and the general public. This unit received nearly 2.8 million incoming calls in 2017. On average there are 50,000 inbound calls per week, with 100 outbound calls per week. On a weekly basis, there are approximately 300 calls that are abandoned by callers or disconnected by the IVR system based upon wait time. The bulk of the incoming calls are handled via the IVR system, which has programmed prompts to assist in directing callers and to answer the caller's questions without human intervention. The IVR handles nearly four times the volume of calls in comparison to a customer service representative.

A subunit of CSS is the Correspondence Unit. This unit responds to both paper and e-mail inquiries. Most of these requests are regarding specific claim inquiries and general information. Although this subunit utilizes approximately 200 pre-written correspondence letters, the Correspondence Unit staff has to populate claims-specific information and oftentimes manually rewrite letters to better suit claims-specific questions.

Private Plan

The Temporary Disability Benefits law allows employers to elect coverage through an approved private plan instead of the state's plan for benefits. Employers can opt to have this private plan coverage for TDI and/or FLI programs. The plan may be administered by an insurance company, by a union welfare fund, or by the employer directly. By law, private plans must offer at least the same amount of benefits, eligibility requirements, and duration of payments as the state plan.

The Private Plan section differs from the Initial Determinations and Reconsiderations units in the fact that the Private Plan staff does not process any claims. Instead, the Private Plan section is divided into two subunits: The Approval Unit and the Claims Review Unit.

The Approval Unit focuses on overseeing the administration of private plans. The staff in this unit has the responsibilities of approving, modifying, or terminating private plans. Additionally, this unit will also provide guidance to private plan carriers as to how to resolve or pay claims or how to act in accordance with the law. Presently, there are approximately 6,100 private plans operating in New Jersey covering approximately 905,000 workers. Meanwhile, the Claims Review Unit has two main responsibilities: to review all private plan denials and to resolve any disputed claims.

1.4 Business Process Interface

The Division of Temporary Disability and Family Leave Insurance is state supervised by the NJDOL. Currently, all division administration and staff are located in the centralized location of the Department's Trenton building and a satellite office in Freehold, NJ, which solely accommodates a portion of Customer Service staff. The Division interacts with other departments and private entities in the capacities listed below.

New Jersey Bureau of Benefit Payment Control (BPC)

The Division works in conjunction with New Jersey's BPC to process payments to eligible claimants of the TDI/FLI programs. BPC also collects overpayments which occur when a claimant has returned to work sooner than expected, for example.
TDI may receive checks intended as reimbursement to the agency for an overpayment, such as from a lien, but cannot cash or apply these amounts directly. Checks are received and reviewed by multiple sections of TDI, but are ultimately hand-walked to BPC staff when they are ready to be applied. These separate divisions seek to work in tandem; however, the risk of human error exists for either division. One example of a timing issue is if a check is not immediately deposited by BPC. This delay may result in financial notifications being mailed in error by BPC's system to claimants. Claimants are inclined to contact TDI representatives for an explanation as they are unaware of the distinction between benefit administration (TDI) and refunds (BPC).

New Jersey Department of the Treasury

Following the process between the Division of TDI/FLI and BPC, if the Division is over-reimbursed by check, BPC will contact the Department of Treasury to initiate the return of the over-reimbursed amount(s). Neither TDI nor BPC can monitor or provide updates to claimants regarding the status of these Treasury reimbursements. Treasury has their own timetable for this process, with reimbursements typically reaching claimants within 1 to 2 months.

Bank of America

Currently, the majority of benefit payments are available to claimants through a Bank of America prepaid debit card. NJDOL processes benefit payments and sends data to the private enterprise of Bank of America to disburse onto a debit card. Although a toll-free number exists to contact Bank of America for any debit card related issues, claimants are still inclined to contact TDI representatives for an explanation.

New Jersey Division of Unemployment Insurance

The TDI/FLI Division may contact designated Unemployment Insurance staff by e-mail to resolve conflicts arising between the benefit programs. Unemployment Insurance may adjust some of their payments to allow TDI or FLI benefits.

New Jersey Division of Employer Accounts

The Division also works with New Jersey's Division of Employer Accounts. Employer Accounts' duties, in relation to the TDI/FLI programs, include: determining if an employer is subject to Temporary Disability laws, assigning contribution tax rates, collecting the taxes used to fund the TDI/FLI programs, conducting periodic audits to ensure compliance with related laws, etc.

TDI/FLI may forward a recommendation that an audit be conducted to the Division of Employer Account's Audits & Field Services. These claims are initially investigated by TDI/FLI for issues arising from incorrectly reported wages or an employee being misclassified. The Division will seek to first determine eligibility and then forward a recommendation to Audits & Field Services by paper memorandum.

New Jersey Division of Workers' Compensation

Lien information is entered by staff of the Workers' Compensation Unit (WCU) onto COURTS-Online, the system used by the Division of Workers' Compensation to monitor court proceedings. All TDI lien amounts must be verified at the time of case disposition, and there is an established procedure of Workers' Compensation staff contacting the WCU by phone or e-mail to verify each lien.

Workers' Compensation Insurance Carriers / Private Insurance Carriers

Staff of the WCU contact workers' compensation insurance carriers by phone or e-mail to verify the receipt of any existing payments by that carrier. These payments may be a complete bar or a reduction to benefit entitlement by the TDI program.

The Private Plan Section also contacts private insurance carriers to answer inquiries or to ensure compliance with NJ laws.

Appeals Tribunal

The Appeals Tribunal is the first formal appellate level within NJDOL for deciding Unemployment, Disability During Unemployment, Temporary Disability Insurance, and Family Leave Insurance benefit disputes. Hearings are scheduled with notice to the interested parties. The Appeals Tribunal is most familiar with Unemployment Insurance laws, and their appeals examiners will conduct telephone or in-person hearings directly with appellants.
Appeals are received directly by the Division of TDI/FLI from claimants and employers for TDI/FLI claims. Staff will review these requests and notify the Appeals Tribunal by a specific paper form if an appeal hearing should be initiated. The Appeals Tribunal will schedule a telephone hearing and notify the Division of the hearing by written correspondence. Limited, read-only/non-print information can be viewed by a designated Reconsiderations staff member via a separate application known as NJLWDUI Appeal. Due to the limited information available, staff may e-mail the Appeals Tribunal for additional questions.

For appeals arising from TDI/FLI disputes, a designated representative of the Division is required to participate on behalf of the agency due to their expertise with the law. The agency can be notified of scheduled hearings in as few as 24 hours, but typically notifications are provided two weeks prior. The appeals examiner will conduct the hearing and provide a written decision of their conclusions after receiving testimony from TDI/FLI staff, appellants, and other parties such as attorneys. These telephone calls are recorded for additional review or escalation to the Board of Review. Since most appeals to the Board of Review are decided based on a call record created at the Appeal Tribunal hearing, if the call recording quality is poor, the hearing must be re-conducted.

New Jersey Department of Human Services – Office of Child Support Services

The Division is required by Federal Law to withhold a portion of TDI/FLI benefits for the purpose of satisfying court order child support obligations. The amount to be withheld is decided by a superior court judge in accordance with the Federal Social Security Act, Title IV-D. County personnel enter court ordered

information into their system which interfaces with LOOPS. LOOPS then interface with DABS and may garnish up to 65 percent of the weekly benefit rate of a TDI or FLI claim.

New Jersey Division of Pensions and Benefits

As TDI/FLI benefits are open to employees who work in NJ, this also includes NJ state workers. In certain rare cases, these claimants may be collecting pensions, which may reduce the benefits by a dollar-for-dollar amount. In order to determine and confirm information related to NJ administered pensions, a Reconsiderations staff member will have to contact the NJ Division of Pensions and Benefits, a division under the Department of the Treasury. On a weekly basis, this confirmation is requested through e-mail with a designated staff member of the Division of Pensions and Benefits.

Social Security Administration

The TDI/FLI (DABS) and UI (LOOPS) systems interface with the Social Security Administration for Social Security Number verification.

1.5 System Limitations

The current business processes and infrastructure systems have many limitations, circumstantial restrictions, and procedural restraints which the Division is seeking to improve upon and obsolete with the success of the modernization effort.

System Availability

As previously mentioned, the DABS mainframe legacy system does not have a 24/7 availability. The current mainframe availability is between the hours of 7AM and 7PM weekdays and between 8AM and 1PM Saturday, with no availability on Sunday. As a result of the downtime, applications that come through the web are pulled in a batch at the start of the next business day.

Legislative Inflexibility

DABS, as a COBOL-based legacy system, does not provide the flexibility needed when the Division is dependent and accountable to any new legislation effected. Implemented in 1988, and periodically "retro-fitted" since that time, DABS is a mainframe system that utilizes two databases: IMS and DB2. As of February 19, 2019, with the passing of A3975, procedures and protocols on the examiner level have been put into temporary effect to manipulate DABS to process and pay claims under new legislative definitions.

Data-capturing Information

The TDI/FLI staff are reliant upon many different systems (see Current Workflow- Appendix A) which do not interact with each other. Due to this absence of interaction, issues can arise with the process of manually entering relevant information. Although there can be no guarantee to eliminate human error after

modernization occurs, current business processes can be shown to effect more of a risk on the human error level. Claims Intake staff may have to manually lookup and scan documents if the OCR and legacy fax systems do not read the barcodes and/or Social Security Numbers (SSN). On the human error level, the Claims Intake staff may enter these images under an incorrect SSN or may accidentally include a page of a separate document, which would then be attached to a completely different claim.

Initial Determinations and Reconsiderations staff, reliant upon the images of these documents in the P8 imaging system, have to subsequently enter information from these images manually into the DABS segments, which may itself result in human error. Following the above example, the Determinations staff may not realize that an application is being processed under an incorrect SSN, or they may not alert appropriate management that an irrelevant document may be attached to the image they are viewing in P8. If a claim is processed and paid under an incorrect SSN—or with an incorrect applicant's name, date of birth, or address—the process to correct the mistake will impact the claimant. TDI/FLI staff will need to intervene with Bank of America to have the institution send another debit card, delaying the issuance of benefits to the claimants.

Medical Standard Changes

As the DABS system remains inflexible, certain fields that examiners need to enter no longer match with how outside guidelines have changed. For example, medical standards such as the nationwide adoption of International Classification of Diseases-10 (ICD-10) from ICD-9 and the inclusion of an extra digit to NJ medical license numbers could not be implemented in the mainframe.

Web-based User Interface Application

Initial Determinations examiners and other staff who work with claims prepopulated by the web-based user interface application still have to review every prepopulated field in the DABS mainframe. Not only are these examiners looking for inconsistencies made by the claimants, medical practitioners, and employers, but many fields in the DABS mainframe do not provide for the same number of characters as the web-application does, resulting in fields such as addresses, disability descriptions, diagnoses, and others to be truncated. As previously described, the process to fix any of these mistakes can be a detriment to claimants and result in delayed processing.

Contested Workers' Compensation Claims

Although Temporary Disability Insurance is for non-work-related injuries and illnesses, there is a provision that allows TDI benefits to be paid for a contested workers' compensation claim. This provision requires that a claimant sign a subrogation agreement to pursue the claim in Workers' Compensation Court and to repay the TDI benefits out of any award he or she may receive. These claims not only undergo the same processes and are evaluated under the same requirements as any other TDI claim, but are also supported with a more extensive process involving lien assessment and the contact of workers' compensation insurance carriers.

The WCU of TDI specializes in administering benefits for these work-related claims using COURTS-Online, New Jersey's Workers' Compensation automated system. Filing liens requires a subscription to COURTS-

Online and the interaction between this system and DABS is extremely specific and limited. Liens do not automatically apply or update information, necessitating manual lien verification by phone or e-mail. As there is no cross-reference feature between DABS and COURTS-Online, this agency may be unaware that a lien should exist and may discover this information several years after-the-fact, if at all.

Unique DABS limitations more readily observed by WCU include but are not limited to: an inability to pay claims that span multiple years or to adjust benefit rate entitlement within a single claim. Claims must be manually adjusted to bypass these limitations.

Refunds/Reimbursement Processing

DABS cannot create a refund for a specific dollar amount at will, and refund information is visible 12 hours later on the separate financial legacy system, LOOPS. Reimbursement checks derived from workers' compensation cases may be for a very specific amount, not the entire claim balance. These checks require staff to calculate payments, manipulate DABS into creating a refund of a similar amount on the first day, and then manually adjust the refund amount on LOOPS the next day.

When reimbursement checks are ready to be applied to a refund amount, they are hand-walked to BPC, separate division within NJDOL. DABS cannot directly process checks or other payment due back to the division. DABS is limited to only showing a history of payments and adjustments; it cannot directly accept reimbursement. The role of cashing reimbursements and applying them to refund segments on LOOPS is done by BPC.

NJDOL Program Conflicts

DABS is limited in its capacity to cross-reference the LOOPS system as a whole. Should a conflict arise between a TDI or FLI benefit and an existing Unemployment Insurance (UI) or Disability During Unemployment (DDU) benefit, this information will not be detected until the next day, after the claim has already been determined eligible. This limitation confuses claimants since they are receiving an eligibility notice generated by DABS, but payment cannot be released due to a UI/DI conflict. Although DABS can detect that a conflict exists, it cannot recognize specific information or provide a solution. Resolution of a conflict is done manually, by a Reconsiderations staff member evaluating UI payments on LOOPS and by contacting designated UI staff by e-mail before updating the claim once more on DABS.

1.6 Assumptions

The context of this RFQ and all attachments revolves around a compendium of defined assumptions.

Estimations will be used in the evaluation process. The rationale of each will be defined and supported to document each estimation's feasibility based on the limited information made available through the RFQ response.

As the claims processing landscape is vast with ever developing technologies, the assumption exists that this document is not exhaustive. Although the modernization team evaluated all public state Disability Insurance and Family Leave Insurance programs, in terms of insurance programs in the private sector, the scope has been limited to responses to the Department's RFQ. In a concerted effort for time management

and progress, the alternatives discussed in this RFQ are those of these public state programs and the RFQ responses.

All alternatives will be evaluated under the assumption that the constraints, as outlined below, shall be adhered to in full. These constraints include New Jersey state laws and regulations, organizational structures, staffing, and budget restraints.

1.7 Constraints

The TDI/FLI Modernization effort must adhere to certain defined boundaries and limitations under which the Division must operate. The system's functionality and management must comply with associated New Jersey state legislation, regulation, and budgetary restraints.

2.0 DEFINITIONS

TDI - Temporary Disability Insurance

FLI - Family Leave Insurance

DABS – Disability Automated Benefit System

DOL - New Jersey Department of Labor and Workforce Development

SFY - State Fiscal Year

PMBOK – Project Management Body of Knowledge

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.

SaaS - Software as a Service

3.0 SCOPE OF WORK

3.1 General

The scope of this project is for a Vendor {Bidder} to provide a fully-functional Software as a Service (SaaS) solution for an Electronic Temporary Disability and Family Leave Insurance Claims Management System. The system shall replace and modernize the current system that supports the business functions of claims processing within the Division of Temporary Disability and Family Leave Insurance. Through a single application that utilizes a common interface and business specific features, the new comprehensive system shall process and track all temporary disability and family leave insurance applications.

3.1.1 Claims Management System Options

The Vendor {Bidder} must provide and maintain a leading edge, fully integrated, business specific solution capable of meeting or exceeding all requirements specified within this RFQ for the term of the contract.

3.1.2 Customer & Employee Role-Base System

The Contractor shall assign a full time (Monday – Friday 8:00 AM ET– 5:00 PM ET) Project Manager to manage the implementation of the project and to manage resources in order to satisfy all requirements specified within this RFQ. The Contractor's Project Manager shall report directly to the State's Project Manager and shall serve as the liaison between the Contractor and the State. The State reserves the right to perform background checks on all Contractor staff assigned to this project.

3.2 Required Features and Functions

As part of the discovery phase, the Vendor Partner shall conduct requirements gathering sessions in order to understand the current systems and processes in use. The sessions shall be used to ensure that in addition to the required features and functions listed in this section, all desired current as-is business functionality is incorporated into the system.
The Vendor Partner must provide a system that shall include the core features and functions

The system shall have an integrated context-based "help utility" to assist users with narrative descriptions and instructions on searchable topics. The system shall have integrated document creation and management capabilities that support the creation of letter and form templates that are populated with system data.

The system shall utilize a document management solution and the State will consult with the Contractors on a proposed document management solution.

The system must have the ability to utilize current interfaces, APIs, web services, etc. The system must have the ability to interface with the legacy system, updated/more efficient systems, APIs web services, etc. or the creation of new ones as a result of the implementation of the Contractor's system.

The system shall be available to the public 24 hours a day 7 days a week. e system shall have the ability to retain data on a schedule determined by the State. The system shall have the ability to import/export data using secure File Transfer Protocol (FTP) methodology.

3.2.1 System Requirements

The TDI/FLI solution must meet the following requirements:

- Security - The Contractor is required to maintain a secure environment in compliance with State Security Standards identified under RFQ Section 5.2 Security and Confidentiality
- Testing/Production Environments - The Contractor shall have in place a testing and production environment for all enhancements and bug fixes. All enhancements and/or fixes must be tested and proven reliable before being placed into production;
- Sizing - The Contractor must ensure that the sizing of the system is adequate to support all concurrent users; (LWD estimates public access to the system will be ~35,000-40,000people)

- Performance - For individual transactions on a PC, the system shall respond to the user in three (3) seconds or less under full load during peak use time;
- Scalability - The system shall provide the ability for the environment to scale for growth as required by claims volume at a minimum rate of three (3) percent per year for the term of the contract;
- Availability - The system shall be available for use 24/7, 365 days per year and shall have an uptime of 99.99%. All regular maintenance and system upgrades shall be performed utilizing the same failover process as Disaster Recovery (below) to negate the possibility of service interruption. In the event that unscheduled system maintenance becomes necessary, the State's Project Manager must be notified at least 24 hours in advance, and there shall be a message generated to users indicating that the system is currently unavailable with a timeframe for its return to use;
- Disaster Recovery - The Contractor must ensure that in the event of a disaster the necessary steps are taken so that the system utilizes a hot failover process with at least 2 mirrored servers (a total of 3) that does not interrupt availability for internal and external users. The State's Project Manager must be notified immediately in the event that this process fails with the corrective actions to be taken by the Contractor and the estimated timeframe for the system to be fully recovered;
- Network Vulnerability - The Contractor must maintain a secure network environment at both the primary hosting facility as well as disaster recovery sites. In the event that it is determined that the network is vulnerable, the Contractor shall be responsible to remedy the problem within fifteen (15) business days, or as approved by the State; and
- Requirements for Computing Devices– The system shall be optimized to run efficiently on personal computers, Laptops, Tablets, Smart Phones, Touchscreen Enabled Devices, and be compatible with operating system software such as MS Windows 10, or later, Android, and iOS. The Contractor ~~s~~hould ensure that the system supports a minimum of three (3) previous versions of generally used web browsers such as Internet Explorer, Firefox, Google Chrome and Apple Safari. The system must comply with all state and federal ADA requirements.

3.2.2 Data Cleansing/Conversion/Migration

There are four (4) legacy databases that the Contractor shall be responsible to cleanse, convert, and migrate, as appropriate to ensure the full delivery of the system. These databases are as follows:

Legacy Databases Table

Business Area	Type of Database	Size	# of Records	Location
DABS	IMS	~2.8 GB	~33Ml segments	Office of Information Technology (OIT) - see ** below
TDI/FLI Webapp	Oracle	~20 GB	~15 K	LWD– Oracle Server
TDI/FLI 24/7	DB2	~7 GB	~800 K	Office of Information Technology (OIT)
DABS	VSAM	~1.5 MB plus	~20 M	~20+ files
VASM-** "Z13, but we will be moving to IBM hosted machine in 6-7 months. Most likely a z14"				

The Contractor shall plan and coordinate all conversion activities. The State shall provide a copy of the as-is legacy databases in a format which is accessible to the Contractor), along with data documentation, data schema and lookup domains for any data values that are coded. The Contractor shall work with the State to validate the data, and develop a data conversion plan and implementation plan which shall include a data map, data extraction process, impact if any on existing systems and procedures for handling problem data such as missing data, data exceptions and default values. The Contractor shall design, develop and test the Extract, Transform and Load (ETL) procedures to ensure data integrity.

3.2.3 User Roles

The application will be accessed by external users and internal State agency staff. The system shall be capable of creating and managing user access privileges based on standard user roles defined by the State. The system shall restrict public access to individual license and/or application data. The system must also allow the State Administrator to create IDs and modify user permissions as well as track usage. The system must have the ability to incorporate user accounts authorized by a 3rd party access and identity manager. Security Assertion Markup Language (SAML) is an open standard to securely exchange authentication and authorization data between an enterprise identity provider and a service provider. The state's identity management service, myNJ, is compliant with SAML 2.0 and integrates with service providers that support SAML 2 Web Single Sign On. Please ensure your solution supports SAML 2 Web Single Sign On.

3.2.4 Reports

The Contractor shall deliver a reporting suite to extract data and shall furnish ad-hoc and bulk reporting capabilities in addition to standard reports, such as workload reports, staff performance, aging claims and user audits necessary for ongoing operations. The Contractor shall also create reports based on existing State templates or as needed at no additional cost to the State.
The following is a list of required standard reports and their frequency. Frequency is On-Demand (O), Weekly (W), Monthly (M), Quarterly (Q), and Annually (A). The Contractor shall validate and expand this list of reports as necessary.

Standard Reports Table

Business Area	Name	Frequency
TDI/FLI	Claim Intake	W, M
	Claim Processing	W, M
	Fiscal	W, M
	Claim Disposition	W, M, O
	Claim Summary	W, M, O
	User Audit	W, M, O
	Demographic	W, M

	Aging	W, M, O
ORI	TDI Summary	A
	FLI Summary	A
	FLI Time to Adjudication	A
	FLI Reason for Denial	A
	FLI Bonding	A
	FLI Caring (Aggregate)	A
	FLI Newborn Caring	A
	FLI Adopted Child Caring	A
	FLI Sick Child Caring	A
	FLI Sick Spouse Caring	A
	FLI Sick Family Caring	A
	TDI Time to Adjudication	A
	TDI Reason for Denial	A
	TDI Morbidity Summary	A
	TDI Pregnancy Stats	A

3.2.5 Payments

The Contractor must create functions that allow the State to create, modify/edit payments, refunds via automation and manually. The solution must also provide the ability to modify payment parameters in order to create claim specific outcomes (e.g., adjustments - refunds, underpays, enrollments, deductions, garnishments, check payments, bankruptcy, offset percentage etc.). The solution must automatically calculate payments for claims based on state mandated payment deductions, formulas and calculations. It must also be able to maintain the original claim process parameters indefinitely (e.g., payment calculations, changes in legislative mandates, rates, etc.). The solution will issue automated real-time and historical reports as well as offer the ability to create ad-hoc fiscal reports. The solution will have the ability to generate payments and accept reimbursements using all generally accepted platforms. (e.g. PayPal, Venmo, etc.). Direct Deposit should only be created/modified by the claimant and will provide the ability to add/modify financial transaction information (e.g. bank info, account info, etc.). The State will provide the Contractor with the specific parameters necessary to fulfill this requirement.

Estimated Claim Numbers by Calendar Year (January 1 – December 31)

Program Area	2017	2018	2019
Temporary Disability	131,607	103,791	139,276
Family Leave	34,050	35,214	44,128

Information regarding program statistics is available via the Division's website at: https://myleavebenefits.nj.gov/labor/myleavebenefits/about/stats/

3.2.6 Interfaces

The State will need to interface with 39 different systems in a variety of ways (Web Services, APIs, batch processing etc.) Currently, most of the data processing for existing interfaces with the DABS system occurs when it is taken down each night for overnight batch processing. Requests are batched during normal operating hours, but are not submitted until the mainframe goes down at night. This means that it can sometimes take more than a day to get responses since most of the other systems that DABS interfaces with are also mainframe systems.

TDI/FLI also emulates a 24/7 live environment for the efficacy of its web applications by copying relevant data to DB2 tables so they can be accessed by users after DABS is taken down for the day. It is important to note however, that these DB2 tables only reflect data from the DABS system collected earlier that day and cannot be written to with any updated data from external users. It simply presents enough data that allows external users to access web applications after normal business hours.

The closest that TDI/FLI applications come to real-time interfacing occurs during the day when the mainframe systems are up. Requests from web applications are batched and submitted via MQ Series in five-minute intervals. The data from the responses is processed when it is received as long as the DABS system is up. If DABS has been taken down for overnight batch processing, the data is held until the following morning and processed when DABS comes back up for the day.

Overall these are convoluted and outdated processes that result in delays of application processing. It can also result in system conflicts because of the delays in data sharing. As part of the modernization effort, TDI/FLI is requiring the Contractor to analyze the current integrations and apply the most updated and efficient methods to create these integrations with the solution. The State will provide the Contractor with a list of current and desired integrations.

3.3 Tasks and Deliverables

A list of the minimum tasks/deliverables is included in this section. The Contractor shall propose a methodology and a schedule for delivering all tasks associated with the completion of these deliverables. The Contractor shall expand the list of tasks/deliverables as necessary to ensure the complete delivery of the system.

Discovery Stage:

During the Discovery Phase, the Contractor shall:

- Conduct an on-site project kickoff meeting;
- Provide an updated Project Plan to be approved by the State's Project Manager describing the activities for each phase;
- Review and validate LWD's functional, technical, data, security, performance, and training requirements;
- Review and validate desktop requirements;
- Provide an updated Requirements Matrix to be approved by the State's Project Manager that includes high level business processes and functional requirements. This matrix shall also be used as a basis for acceptance testing criteria;
- Define any custom functionality;
- Develop an End User Training Plan to be approved by the State's Project Manager that identifies the training to be provided;
- Provide an updated Data Conversion Plan and updated Implementation Plan showing how LWD requirements will be fully met. These plans should include all data models, business processes and reports and must be approved by the State's Project Manager;
- In conjunction with the State's Project Manager, create an Acceptance Test Plan to be approved by the State's Project Manager to determine the testing criteria the system must meet before acceptance.

Conversion/Configuration/Testing/Validation Stage:

During the Conversion/Configuration/Testing/Validation Stage, the Contractor shall:

- Perform data conversion and testing in compliance with the updated Data Conversion Plan developed in Phase 1;
- Customize and configure the system, and prepare LWD for production and on-going support of the solution;
- Conduct user sessions in order to refine the system to best meet all project requirements;
- Establish a Test Environment to ensure that the system is loaded and running properly, and databases are built completely and correctly;
- Perform System Testing as the system is being developed;
- Develop a Cutover Plan outlining the steps that must be taken to aid the move from the test environment to the fully functional production environment; and
- Execute the Acceptance Test Plan developed during the Discovery Phase.

Production Stage:

During the Production Stage, the Contractor shall:

- Bring all elements of the implementation together to successfully transition to full production;
- Provide all end user training as detailed in the Training Plan developed in Phase 1;
- Resolve any production issues to ensure System Acceptance; and
- Provide a 60-day follow-up on-site meeting.

3.3.1 System Test Plan and Testing

The Contractor shall develop and submit for State review and approval a comprehensive System Test Plan. The test plan shall include at a minimum:

- End-to-End Application Testing (including Unit and System testing);
- Business Requirements Testing;

- Stress Testing;
- Performance Testing; and
- Backup and Recovery Testing.
- Regression Testing
- Integration & Interface Testing
- Assistance with User Acceptance Testing

The Contractor shall be responsible for performing system testing and tracking and resolving all system test problems. The testing process shall be utilized by the Contractor and the State to determine whether the system is fully operational and is functioning in accordance with all requirements specified within this RFQ.

3.3.2 Documentation

The Contractor shall be responsible to provide the following documentation in printed and electronic format at the appropriate phase of the project:

- Operational Documentation - The Contractor shall provide documentation (user manual) which details the operational procedures of the system. The user manual shall be updated by the Contractor at each phase of the project to reflect system upgrades. Release of the manual should be in advance of any training.
- Database Documentation - The Contractor shall provide database documentation detailing the physical data model, data elements, platform specific Data Definition Language (DDL), and logical models. These include both informational and navigational metadata. The database documentation shall provide a common foundation of knowledge on which to communicate with the Contractor and system users regarding proposed enhancements and improved functionality.

The Contractor must grant the State authority to make additional copies for its own use of these documents as were developed or authorized by the Contractor. The documentation must be approved by the State's Project Manager.

3.3.3 Training

The Contractor shall train staff members in all aspects of the system and in such detail that the staff shall be able to operate and manage the system efficiently and effectively. All training shall be hands-on training completely supported by the Contractor. The training shall be conducted on-site and virtually at the Department of Labor and Workforce Development (LWD) building located at 1 John Fitch Plaza, Trenton, NJ. LWD will supply computers and internet access for the trainees. The Contractor shall supply all software, training manuals, and other documentation and materials online/electronically needed to conduct the training. All training materials shall become the property of the State. A detailed training plan will be developed by Contractor in coordination with the State Project Manager.

3.3.4 Assessments/Plans

The Contractor shall provide a detailed system design document showing the proposed solution's Security Plan, Disaster Recovery Plan and Contingency Plan to the State's Project Manager. Logical and physical diagrams are also required. The plans must be submitted to the State's Project Manager for approval within one (1) month after the contract start date.

3.3.5 Deliverable Acceptance and Payment

Deliverables Acceptance:

The Contractor will submit a Deliverable Acceptance Notice (DAN) to the State's Project Manager that includes the deliverables encompassed by the particular DAN, the amount of payment requested by the Contractor and signatures of approval by both the Contractor's Project Manager and the State's Project Manager.

The State requires a minimum of 10 business days to review and approve deliverables. In the event that a deliverable has been determined unacceptable by the State, the Contractor shall have 20 calendar days to correct and resubmit the deliverable for review and approval. The 10 business / 20 calendar day process shall continue until the Contractor submits a deliverable which is acceptable to the State.

Payment:

Deliverables

Payment for the tasks/deliverables required under this contract shall be made at the end of phases within each iteration outlined in Tasks and Deliverables. The completion of each phase shall be determined by the State's Project Manager once all required tasks/deliverables have been provided and accepted.

3.4 Project Management

The Contractor shall perform the following tasks and/or comply with the following deliverables:

- The Contractor shall utilize a project management methodology throughout the project life cycle in accordance with the standards outlined by the NJ Department of Labor Project Portfolio Management Office. Use of these processes and tools shall be in compliance with industry standards such as those employed under the Project Management Body of Knowledge (PMBOK) developed and maintained by the Project Management Institute (www.pmi.org);
- The Contractor shall participate in the State's System Architecture Review process at appropriate stages of the project as referred to in https://tech.nj.gov/services/governance.shtml#architecture
- The Contractor must provide and utilize project management templates for the duration of the project;
- The Contractor must assign a Project Manager who is responsible for submitting the updated project plans, status reports and other relevant deliverables and reports on an as needed basis for State Contractor Manager approval;
- The Contractor's Project Manager and the project team must attend all meetings that are required onsite. If any of the meetings requires a full work week's attendance excluding State holidays, the Contractor must ensure that the project manager and the project team are present for the entire duration; All meetings shall have an agenda and meeting minutes
- The Contractor's Project Manager must provide weekly progress reports to the State's Project Manager that documents the Contractor's progress during the current reporting period, including deliverables status (percent complete), potential risks and risk mitigation strategies, slippages to the schedule and progress planned during the upcoming reporting period;
- The Contractor's Project Manager is responsible for conducting bi-weekly status meetings with the State's Project Manager. The Contractor's Project Manager is responsible for providing the agenda for the status meetings;

- The Contractor shall document and distribute minutes to State agency staff after every meeting to document all the discussions and decisions that were made at the meeting including risk issues and slippages to the schedule;
- Subsequent to the project kick-off meeting the Contractor shall schedule and conduct regular business requirements meetings;
- The Contractor shall facilitate the meetings between respective parties and document the functional requirements while being on-site during functional requirements meetings and any other pertinent meetings identified by the State's Project Manager;
- The Contractor shall be responsible for updating the functional requirements document on as needed to basis. The document must then be submitted to the State's Project Manager for approval;
- The Contractor shall utilize a project management software program for reporting and tracking progress of the project. The Contractor shall procure license(s) for use by State employees. The State prefers to use MS Project;
- The Contractor shall be responsible for updating the functional requirements document and providing updates to State Agency staff once the document is approved by the State's Project Manager;

3.5 Project Initiation

Project initiation shall begin within ten (10) business days after contract award. The Contractor shall hold an on-site kickoff meeting within this time period. The kickoff meeting shall include but is not limited to: A review of the project schedule, all tasks and deliverables, Contractor resources assigned to the tasks, hours to complete the tasks, milestones, dependencies, stakeholders, and the payment process.

3.6 Implementation

The system must be fully functional as specified in the Statement of Work (SOW) and put into production within 9 months of contract award, or as agreed upon by both the Contractor and the State. The SOW will also detail the requirements for knowledge transfer based on support responsibility. After the system is put into production, there shall be a 90-day period of post implementation support. Maintenance shall occur after post implementation support. The Contractor shall remain responsible for maintenance and support of the system for the remainder of the contract period as described in the maintenance and support section of this RFQ.

3.7 Post Implementation Support/Help Desk Support/Maintenance

Post implementation support help desk support and maintenance shall be the responsibility of the Contractor.

Post Implementation Support shall occur for a 90-day period after the system has been put into production and accepted by the State. The Contractor shall be responsible for defect tracking, debugging and the resolution of all system problems that occur during this period of time.

Help Desk Support shall occur when the system is put into production and shall run for the remainder of the contract. The Contractor shall provide toll-free telephone support available between the hours of 8:00AM and 5:00PM EST, Monday - Friday, to provide technical assistance to LWD staff. The Contractor

must respond to technical problems within 2 hours of notification by LWD staff and resolve these problems within 24 hours. The Contractor must make every effort to respond to emergency requests, such as major system failure, within 1 hour. An escalation policy shall be developed by the Contractor and approved by the State for any support issues that cannot be resolved within 24 hours.

Maintenance shall occur after the Post Implementation Support phase and for the remaining term of the contract. It shall be the responsibility of the Contractor to ensure proper maintenance so that the system remains current, is fully functional and is free from defects, bugs and other imperfections.

3.8 System Acceptance

The State will agree to accept the system when the following criteria have been met:

- The system is customized, configured, implemented, passes system testing and is fully functional with no errors and no warnings for a period of 30 days;
- All data cleansing, conversion and migration have been successfully completed and installed;
- All plans are considered acceptable to the State;
- Documentation and training manuals are considered acceptable to the State;
- The Contractor has successfully completed all training; and
- All system related deliverables have been satisfactorily accepted by the State.

3.9 Project Closeout

The Contractor shall be responsible for generating a Project Closeout Report at the end of the contract term. The report shall define compliance with all requirements specified within this RFQ as well as all project related issues and lessons learned.

3.10 System Upgrades/Enhancements

The Contractor shall be responsible for post-production upgrades/enhancements to the system in order to comply with State and/or Federal rules, regulations and reporting requirements. Any system enhancements/upgrades proposed by the Contractor or by the State, must be approved by the Office of Information Technology through the Procurement Office, Department of Labor and Workforce Development prior to being implemented.

4.0 TECHNICAL PROPOSAL

In this section, the Vendor {Bidder} shall describe its approach and plans for accomplishing the work outlined in the Scope of Work section, i.e., Section 3.0. The Vendor {Bidder} must set forth its understanding of the requirements of this RFQ and its ability to successfully complete the contract. The Bidder must address the following topics with sufficient information to demonstrate the Contractor understands the scope of work required by the RFQ:

- Project Management;
- Design/Requirements Matrix;
- Data Conversion;
- Testing;

- Integration;
- Interfaces;
- Implementation;
- Disaster Recovery;
- Contingency Plan;
- Customization/Configuration;

The Vendor {Bidder} must complete and submit with its Proposal the attached "Requirements Matrix" (Appendix A).

4.1 Management Overview

The Vendor {Bidder} shall set forth its overall technical approach and plans to meet the requirements of the RFQ in a narrative format. This narrative should convince the State that the Vendor {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 convince the State that the Contractor's general approach and plans to undertake and complete the contract are appropriate to the tasks and subtasks involved.

Mere reiterations of RFQ tasks and subtasks are strongly discouraged, as they do not provide insight into the Vendor {Bidder}'s ability to complete the contract. The Vendor {Bidder}'s response to this section should be designed to convince the State that the Vendor {Bidder}'s detailed plans and approach proposed to complete the Scope of Work are realistic, attainable and appropriate and that the Vendor {Bidder}'s proposal will lead to successful contract completion.

4.2 Contract Management

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

4.3 Project Plan/Schedule

The Vendor {Bidder} must include a project plan/schedule. If key dates are a part of this RFQ, the Vendor {Bidder}'s project plan/schedule should incorporate such key dates and should identify the completion date for each task and sub-task required by the Scope of Work. Such schedule should also identify the associated deliverable item(s) to be submitted as evidence of completion of each task and/or subtask.
The Vendor {Bidder} should identify the contract scheduling and control methodology to be used and should provide the rationale for choosing such methodology. The use of Gantt, PERT or other charts is at the option of the Contractor.

4.4 Potential Problems

The Vendor {Bidder} must set forth a summary of any and all problems that the Vendor {Bidder} anticipates during the term of the contract. For each problem identified, the Contractor should provide its proposed solution.

4.5 Vendor {Bidder} Hardware and Software

The Vendor {Bidder} must include in its proposal a list of all hardware and software that shall be used in support of the SaaS environment including a diagram depicting the system architecture and how this architecture meets or exceeds the technical standards of the State as indicated in Section 5.2 Security and Confidentiality.

4.6 Compatibility with Barcode/Smartphones/Photo-Imaged Equipment

The Vendor {Bidder} should include in its proposal a list of all barcode formats, Smartphone & photo-imaged equipment that the system is compatible with.

4.7 State Data Format

The Vendor {Bidder} must include in its proposal the format that the State data should be provided in for the purpose of data cleansing, conversion and migration.

4.8 Service Level Requirements

The Vendor {Bidder} must include in its proposal a plan to meet the service level requirements listed in the RFQ.

4.9 Security

The Vendor {Bidder} must provide a summary overview of the security document and describe how it has been incorporated into a larger security program for automated data processing. In the plan the Contractor shall highlight security features of the systems and how they shall meet the requirements of the RFQ as outlined in section 5.2 in accordance with the State Information Security Manual (SISM).

The Vendor {Bidder} shall complete and submit the State of New Jersey Security Due Diligence Third-Party Information Security Questionnaire (Questionnaire) with its Quote. This Questionnaire is designed to provide the State with an overview of the Vendor's {Bidder's} security and privacy controls to meet the State of New Jersey's objectives as outlined and documented in the Statewide Information Security Manual and compliance with the State's security requirements

The State has executed a Confidentiality/Non-Disclosure Agreement which is attached to the Questionnaire. The Vendor {Bidder} must countersign the Confidentiality/Non-Disclosure Agreement and include it with its submitted Questionnaire. No amendments to Confidentiality/Non-Disclosure Agreement are permitted.

To the extent permissible under the New Jersey Open Public Records Act ("OPRA"), N.J.S.A. 47:1A-1.1 , the New Jersey common law right to know, and any other lawful document request or subpoena, the completed Questionnaire and supplemental documentation provided by the Vendor {Bidder} will be kept confidential and not shared with the public or other Vendors {Bidders}.

4.10 Environments

The Vendor {Bidder} must include in its proposal a list of all development, testing, training and production environments that will be used in support of the SaaS solution.

4.11 Sizing

The Vendor {Bidder}must indicate in its proposal the maximum number of concurrent users the SaaS solution will support without affecting the response time of the system.

4.12 Recoverability

THE VENDOR {BIDDER} MUST INDICATE IN ITS PROPOSAL THE RECOVERY PROCESS IN THE EVENT THAT THE SYSTEM SHOULD FAIL. THIS PROCESS SHOULD CLEARLY INDICATE THE STEPS THAT WILL BE TAKEN IN ORDER TO BRING THE SYSTEM BACK UP AS WELL AS A TIMEFRAME FOR THE SYSTEM TO BECOME FULLY FUNCTIONAL.

4.13 Adherence to State of New Jersey Shared Architecture

The Vendor {Bidder} must indicate in its proposal if its SaaS solution adheres to both the State of New Jersey Shared IT Architecture and State Information Security Manual (SISM) and all Security requirements outlined in section 5.2.

4.14 Business Continuity and Disaster Recovery

The Vendor {Bidder} must include in its proposal a description of redundancies in place to protect against the loss of database records and a failover/recovery plan in the event of catastrophic failure.

4.15 Shared vs. Dedicated Environment

The Vendor {Bidder} must indicate in its proposal whether the proposed SaaS solution will operate under a shared or dedicated hosting model environment and how this environment best meets the requirements of the State.

4.16 Organizational Support and Experience

The Vendor {Bidder} must include information relating to its organization, personnel, and experience, including but not limited to: references, together with contact names and telephone numbers, evidencing the Vendor {Bidder}'s qualifications, and capability to perform the services required by this RFQ. This section of the proposal shall minimally contain the information identified below:

4.17 Organization Charts

A. Contract-Specific Chart. The Vendor {Bidder} shall include a contract organization chart, with names showing management, supervisory and other key personnel (including Vendor {Bidder} management, supervisory or other key personnel) to be assigned to the contract. The chart should include the labor category and title of each such individual.

B. Chart for Entire Firm. The Vendor {Bidder} should include an organization chart showing the Contractor's entire organizational structure. This chart should show the relationship of the individuals assigned to the contract to the Vendor {Bidder}'s overall organizational structure.

4.18 Resumes

Detailed resumes must be submitted for all management, supervisory and key personnel to be assigned to the contract. Resumes must emphasize relevant qualifications and experience of these individuals in successfully completing contracts of a similar size and scope to those required by this RFQ. State project manager approval is required. Resumes must 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 RFQ.
- 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.

4.19 Backup Staff

The Vendor {Bidder} must include a list of backup staff that may be called upon to assist or replace primary individuals assigned. Backup staff must be clearly identified as backup staff.

In the event the Vendor {Bidder} must hire management, supervisory and/or key personnel if awarded the contract, the Contractor should include, as part of its recruitment plan, a plan to secure backup staff in the event personnel initially recruited need assistance or need to be replaced during the contract term. State project manager approval is required.

4.20 Experience with Contracts of Similar Size and Scope

The Vendor {Bidder} must have a minimum of five (5) years' experience in the Paid Family Medical Leave arena and must have successfully implemented at least one (1) similar system. This experience must be of similar size and scope of that required by this RFQ. A description of all such contracts must be included in the proposal and demonstrate how such contracts relate to the ability of the firm to complete the services required by this RFQ. For each such contract, the Vendor {Bidder} shall provide names and telephone numbers of individuals for the other contract party. Failure to provide this information in the proposal may result in the proposal being deemed non-responsive. Beginning and ending dates should also be given for each contract.

5.0 CONTRACT

5.1 Ownership of Material

All data, technical information, materials gathered, originated, developed, prepared, used or obtained in the performance of the contract, including, but not limited to, all reports, surveys, plans, charts, literature,

brochures, mailings, recordings (video and/or audio), pictures, drawings, analyses, graphic representations, software computer programs and accompanying documentation and print-outs, notes and memoranda, written procedures and documents, regardless of the state of completion, which are prepared for or are a result of the services required under this contract shall be and remain the property of the State of New Jersey and shall be delivered to the State of New Jersey upon thirty (30) Days' notice by the State. With respect to software computer programs and/or source codes developed for the State, except those modifications or adaptations made to Contractor's Background IP as defined below, the work shall be considered "work for hire", i.e., the State, not the Contractor, shall have full and complete ownership of all software computer programs and/or source codes developed. To the extent that any of such materials may not, by operation of the law, be a work made for hire in accordance with the terms of this Contract, Contractor hereby assigns to the State all right, title and interest in and to any such material, and the State shall have the right to obtain and hold in its own name and copyrights, registrations and any other proprietary rights that may be available.

Should the Contractor anticipate bringing pre-existing intellectual property into the project, the intellectual property must be identified in the proposal. Otherwise, the language in the first paragraph of this section prevails. If the Contractor identifies such intellectual property ("Background IP") in its proposal, then the Background IP owned by the Contractor on the date of the contract, as well as any modifications or adaptations thereto, remain the property of the Contractor. Upon contract award, the Contractor or Contractor shall grant the State a nonexclusive, perpetual royalty free license to use any of the Contractor/Contractor's Background IP delivered to the State for the purposes contemplated by the contract.

The Contractor shall deliver to the State or to a State approved escrow agent a complete set of the Contractor's software source programs, program object code, operations manuals, service manuals, written procedures, and any such other materials necessary for the State to operate the System. The software source and object programs, and documentation, can be delivered on mutually agreeable media. Installation packages for third party software products licensed by the Contractor must be included. These materials must allow the State to:

A. Continue operations in the event the Contractor becomes unable to perform.

B. Confirm that only authorized software and procedures are employed with the System. In this regard, access by the State to the escrow (if escrowed) shall be at the State's discretion for auditing its contents, or for preparation to assume operations of the System, or for purposes of the State's administration of its applications.

As System changes are implemented, both the change and change documentation shall be provided to the State (or escrow) to continue the State's protection. Changes to the State's (escrow's) copy of these materials must occur within one (1) week of installation in production operations.

5.2 Security and Confidentiality

The Contractor must provide a Security Plan that, at a minimum, conforms 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). The Security Plan 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 {Contractor's} information security program. The control areas to be addressed include:

5.2.1 Security Plan

The Contractor shall submit a detailed Security Plan that addresses the Vendor's {Contractor's} approach to meeting each applicable security requirement outlined below, to the State, no later than 30 days after the award of the Blanket P.O. The State approval of the Security Plan shall be set forth in writing. In the event that the State reasonably rejects the Security Plan after providing the Contractor an opportunity to cure, the Director may terminate the Blanket P.O. pursuant to the SSTC.

The Vendor {Bidder} shall complete and submit the State of New Jersey Security Due Diligence Third-Party Information Security Questionnaire (Questionnaire) with this quote. This Questionnaire is designed to provide the State with an overview of the Vendor's {Bidder's} compliance with the State's security requirements as outlined in Section 5.2.

The Vendor {Bidder} should submit the following supplemental documentation with the its Quote as described in Section V of the Questionnaire:

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

To the extent permissible under the New Jersey Open Public Records Act ("OPRA"), N.J.S.A. 47:1A-1.1 , the New Jersey common law right to know, and any other lawful document request or subpoena, the completed Questionnaire and supplemental documentation provided under this section will be kept confidential and not shared with the public or other Vendors {Bidders}.

5.2.2 Information Security Program Management

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

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

B. Creation, maintenance, and communication of information security policies, standards, procedures, and guidelines to include the control areas listed in sections below;
C. Development and maintenance of relationships with external organizations to stay abreast of current and emerging security issues and for assistance, when applicable; and
D. Independent review of the effectiveness of the Vendor's {Contractor's} information security program.

5.2.3 Compliance

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

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

5.2.4 Personnel Security

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

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

5.2.5 Security Awareness and Training

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

A. Personnel are provided with security awareness training upon hire and at least annually, thereafter;
B. Security awareness training records are maintained as part of the personnel record;
C. Role-based security training is provided to personnel with respect to their duties or responsibilities (e.g. network and systems administrators require specific security training in accordance with their job functions); and
D. Individuals are provided with timely information regarding emerging threats, best practices, and new policies, laws, and regulations related to information security.

5.2.6 Risk Management

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

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

5.2.7 Privacy

If the State data associated with the Contract includes PII or State Confidential Information, this section is applicable.

Data Ownership. The State is the data owner. Contractor shall not obtain any right, title, or interest in any of the data furnished by the State, or information derived from or based on State data.

Data usage, storage, and protection of PII and State Confidential Information, as defined in Section 5.9.1 are subject to all applicable international, federal and state statutory and regulatory requirements, as amended from time to time, including, without limitation, those for HIPAA, Tax Information Security Guidelines for Federal, State, and Local Agencies (IRS Publication 1075), New Jersey State tax confidentiality statute, the New Jersey Privacy Notice found at NJ.gov, N.J.S.A. § 54:50-8, New Jersey Identity Theft Prevention Act, N.J.S.A. § 56:11-44 et. seq., the federal Drivers' Privacy Protection Act of 1994, Pub.L.103-322, and the confidentiality requirements of N.J.S.A. § 39:2-3.4. Contractor shall also conform to PCI DSS, where applicable.

Security: Contractor agrees to take appropriate administrative, technical and physical safeguards reasonably designed to protect the security, privacy, confidentiality, and integrity of user information.

Contractor shall ensure that PII and other confidential information is secured and encrypted during transmission or at rest.

Data Transmission: The Contractor shall 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 Blanket P.O. or the State of New Jersey. The Contractor shall only transmit or exchange data with the State of New Jersey or other parties through secure means supported by current technologies. The Contractor shall encrypt all PII and other confidential information as defined by the State of New Jersey or applicable law, regulation or standard during any transmission or exchange of that data.

Data Re-Use: All State data shall be used expressly and solely for the purposes enumerated in the Blanket P.O. Data shall not be distributed, repurposed or shared across other applications, environments, or business units of the Contractor. 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.

Data Breach: In the event of any actual, probable or reasonably suspected breach of security, or any unauthorized access to or acquisition, use, loss, destruction, compromise, alteration or disclosure of any PII (each, a Security Breach) that may concern any State confidential information or PII, Contractor shall: (a) notify the State immediately of such breach, and otherwise take no less than its best efforts to notify the State of a Security Breach (but in no event later than 24 hours after such Security Breach); (b) designate a single individual employed by Contractor who shall be available to the State 24 hours per day, seven (7) days per week as a contact regarding Vendor's {Contractor's} obligations under Incident Response; (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 (in which case Contractor shall consult with the State and reasonably cooperate with the State to prevent any notification or disclosure concerning any PII, security breach, or other State Confidential Information); (d) assist the State in investigating, remedying and taking any other action the State deems necessary regarding any Security Breach and any dispute, inquiry, or claim that concerns the Security Breach; (e) follow all instructions provided by the State relating to the State Confidential Information affected or potentially affected by the Security Breach; (f) take such actions as necessary to prevent future Security Breaches; and (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, at a minimum, any legal process initiated by any governmental entity (foreign or domestic).

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

A. End of Contract Data Handling: Upon termination/expiration of this Blanket P.O. the Contractor shall first return all State data to the State in a usable format as defined in the Blanket P.O., or in an open standards machine-readable format if not. The Contractor shall then erase, destroy, and render unreadable all Contractor back up copies of State data according to the standards enumerated in accordance with the State's most recent Media Protection Policy, https://www.nj.gov/it/docs/ps/NJ_Statewide_Information_Security_Manual.pdf and certify in writing that these actions have been completed within 30 days after the termination/expiration of the Blanket P.O. or within seven (7) days of the request of an agent of the State whichever should come first.

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

5.2.8 Asset Management

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

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

5.2.9 Security Categorization

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

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

5.2.10 Media Protection

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

A. Media storage/access/transportation;

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

5.2.11 Cryptographic Protections

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

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

5.2.12 Access Management

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

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

5.2.13 Identity and Authentication

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

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

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

5.2.14 Remote Access

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

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

5.2.15 Security Engineering and Architecture

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

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

5.2.16 Configuration Management

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

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

5.2.17 Endpoint Security

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

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

5.2.18 ICS/SCADA/OT Security

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

A. Conducting risk assessments prior to implementation and throughout the lifecycles of ICS/SCADA/OT assets;
B. Developing policies and standards specific to ICS/SCADA/OT assets;
C. Ensuring the secure configuration of ICS/SCADA/OT assets;
D. Segmenting ICS/SCADA/OT networks from the rest of the Vendor's {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.

5.2.19 Internet of Things Security

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

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

5.2.20 Mobile Device Security

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

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

5.2.21 Network Security

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

A. Include protection mechanisms for network communications and infrastructure (e.g. layered defenses, denial of service protection, encryption for data in transit, etc.);
B. Include protection mechanisms for network boundaries (e.g. limit network access points, implement firewalls, use Internet proxies, restrict split tunneling, etc.);
C. Control the flow of information (e.g. deny traffic by default/allow by exception, implement Access Control Lists, etc.); and
D. Control access to the Vendor's {Contractor's} information systems (e.g. network segmentation, network intrusion detection and prevention systems, wireless restrictions, etc.).

5.2.22 Cloud Security

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

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

5.2.23 Change Management

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

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

5.2.24 Maintenance

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

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

5.2.25 Threat Management

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

5.2.26 Vulnerability and Patch Management (VU)

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

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

5.2.27 Continuous Monitoring

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

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

5.2.28 System Development and Acquisition

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

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

5.2.29 Project and Resource Management

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

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

5.2.30 Capacity and Performance Management

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

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

5.2.31 Third Party Management

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

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

5.2.32 Physical and Environmental Security

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

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

5.2.33 Contingency Planning

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

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

5.2.34 Incident Response

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

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

5.2.35 Tax Return Data Security

I. PERFORMANCE

A. In performance of this Blanket P.O., the Contractor agrees to comply with and assume responsibility for compliance by his or her employees with the following requirements:

B. All work will be done under the supervision of the Contractor or the Vendor's {Contractor's} employees;
C. Any return or return information made available in any format shall be used only for the purpose of carrying out the provisions of this Blanket P.O. 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 Blanket P.O. Disclosure to anyone other than an officer or employee of the Contractor will be prohibited;

D. 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;

E. The Contractor certifies that the data processed during the performance of this Blanket P.O. will be completely purged from all data storage components of his or her computer facility, and the Contractor will retain no output at the time the work is completed. If immediate purging of all data storage components is not possible, the Contractor certifies that any IRS data remaining in any storage component will be safeguarded to prevent unauthorized disclosures;

F. Any spoilage or any intermediate hard copy printout that may result during the processing of IRS data will be given to the agency or his or her designee. When this is not possible, the Contractor will be responsible for the destruction of the spoilage or any intermediate hard copy printouts, and will provide the agency or his or her designee with a statement containing the date of destruction, description of material destroyed, and the method used;

G. 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.

H. No work involving federal tax information furnished under this Blanket P.O. will be subcontracted without prior written approval of the IRS;

I. The Contractor will maintain a list of employees authorized access. Such list will be provided to the agency and, upon request, to the IRS reviewing office; and

J. The agency will have the right to void this Blanket P.O. if the Contractor fails to provide the safeguards described above.

II. CRIMINAL/CIVIL SANCTIONS:

A. Each officer or employee of any person to whom returns or return information is or may be disclosed will be notified in writing by such person that returns or return information disclosed to such officer or employee can be used only for a purpose and to the extent authorized herein, and that further disclosure of any such returns or return information for a purpose or to an extent unauthorized herein constitutes a felony punishable upon conviction by a fine of as much as $5,000 or imprisonment for as long as five (5) years', or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized further disclosure of returns or return information may also result in an award of civil damages against the officer or employee in an amount not less than $1,000 with respect to each instance of unauthorized disclosure. These penalties are prescribed by IRC sections 7213 and 7431 and set forth at 26 CFR 301.6103(n)-1;

B. 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 Blanket P.O. 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 Blanket P.O. Inspection by or disclosure to anyone without an official need to know constitutes a criminal misdemeanor punishable upon conviction by a fine of as much as $1,000 or imprisonment for as long as one (1) year, or both, together with the costs of prosecution. Such person shall also notify each such officer and employee that any such unauthorized inspection or disclosure of returns or return information may also result in an award of civil damages against the officer or employee [United States for federal employees] in an amount equal to the sum of the greater of $1,000 for each act of unauthorized inspection or disclosure with respect to which such defendant is found liable or the sum of the actual damages sustained by the plaintiff as a result of such unauthorized inspection or disclosure plus in the case of a willful inspection or disclosure which is the result of gross negligence, punitive damages, plus the costs of the action. These penalties are prescribed by IRC section 7213A and 7431;

C. Additionally, it is incumbent upon the Contractor to inform its officers and employees of the penalties for improper disclosure imposed by the Privacy Act of 1974, 5 U.S.C. 552a. Specifically, 5 U.S.C. 552a(i)(1), which is made applicable to Vendors {Contractors} by 5 U.S.C. 552a(m)(1), provides that any officer or employee of a Contractor, who by virtue of his/her employment or official position, has possession of or access to agency records which contain individually identifiable information, the disclosure of which is prohibited by the Privacy Act or regulations established thereunder, and who knowing that disclosure of the specific material is prohibited,

willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000; and

D. Granting a Contractor access to FTI must be preceded by certifying that each individual understands the agency's security policy and procedures for safeguarding IRS information. Vendors {Contractors} must maintain its authorization to access FTI through annual recertification. The initial certification and recertification must be documented and placed in the agency's files for review. As part of the certification and at least annually afterwards, Vendors {Contractors} should be advised of the provisions of IRC Sections 7431, 7213, and 7213A (see Exhibit 6, IRC Sec. 7431 Civil Damages for Unauthorized Disclosure of Returns and Return Information and Exhibit 5, IRC Sec. 7213 Unauthorized Disclosure of Information). The training provided before the initial certification and annually thereafter must also cover the incident response policy and procedure for reporting unauthorized disclosures and data breaches. (See Section 10) For both the initial certification and the annual certification, the Contractor should sign, either with ink or electronic signature, a confidentiality statement certifying its understanding of the security requirements.

III. INSPECTION:

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

5.3 Confidentiality

A. The obligations of the State under this provision are subject to the New Jersey Open Public Records Act ("OPRA"), N.J.S.A. 47:1A-1 et seq., the New Jersey common law right to know, and any other lawful document request or subpoena;

B. By virtue of this Blanket P.O., the parties may have access to information that is confidential to one another. The parties agree to disclose to each other only information that is required for the performance of their obligations under this Blanket P.O. Vendor's {Contractor's} Confidential Information, to the extent not expressly prohibited by law, shall consist of all information clearly identified as confidential at the time of disclosure and anything identified in Vendor's {Contractor's} Quote as Background IP ("Contractor Confidential Information"). Notwithstanding the previous sentence, the terms and pricing of this Blanket P.O. are subject to disclosure under OPRA, the common law right to know, and any other lawful document request or subpoena;

C. The State's Confidential Information shall consist of all information or data contained in documents supplied by the State, any information or data gathered by the Contractor in fulfillment of the contract and any analysis thereof (whether in fulfillment of the contract or not).

D. A party's Confidential Information shall not include information that: (a) is or becomes a part of the public domain through no act or omission of the other party; (b) was in the other party's lawful possession prior to the disclosure and had not been obtained by the other party either directly or

indirectly from the disclosing party; (c) is lawfully disclosed to the other party by a third party without restriction on the disclosure; or (d) is independently developed by the other party;

E. The State agrees to hold Vendor's {Contractor's} Confidential Information in confidence, using at least the same degree of care used to protect its own Confidential Information;

F. In the event that the State receives a request for Contractor Confidential Information related to this Blanket P.O. pursuant to a court order, subpoena, or other operation of law, the State agrees, if permitted by law, to provide Contractor with as much notice, in writing, as is reasonably practicable and the State's intended response to such order of law. Contractor shall take any action it deems appropriate to protect its documents and/or information;

G. In addition, in the event Contractor receives a request for State Confidential Information pursuant to a court order, subpoena, or other operation of law, Contractor shall, if permitted by law, provide the State with as much notice, in writing, as is reasonably practicable and Vendor's {Contractor's} intended response to such order of law. The State shall take any action it deems appropriate to protect its documents and/or information; and

H. Notwithstanding the requirements of nondisclosure described in these Sections 5.2 and 5.3, either party may release the other party's Confidential Information:

(i) if directed to do so by a court or arbitrator of competent jurisdiction; or
(ii) pursuant to a lawfully issued subpoena or other lawful document request:
(a) in the case of the State, if the State determines the documents or information are subject to disclosure and Contractor does not exercise its rights as described in Section 5.3(F), or if Contractor is unsuccessful in defending its rights as described in Section 5.3(F); or
(b) in the case of Contractor, if Contractor determines the documents or information are subject to disclosure and the State does not exercise its rights described in Section 5.3(G), or if the State is unsuccessful in defending its rights as described in Section 5.3(G).

6.0 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 RFQ. The evaluation criteria categories may be used to develop more detailed evaluation criteria to be used in the evaluation process:

6.1 Technical Evaluation Criteria

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

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

C. Ability of firm to complete the Scope of Work based on its Technical Proposal: The overall ability of the

Vendor {Bidder} to undertake and successfully complete the technical requirements of the contract in a timely manner.

6.2 Vendor {Bidder}'s Price Schedule

All proposals submitted for consideration must include the submittal of the State's Price schedule. Failure to do so will result in the proposal being considered non-responsive and therefore, not eligible for consideration for contract award.

For evaluation purposes, Vendor {Bidder}s will be ranked according to the total application cost located on the Price Schedule accompanying this RFQ. The Price Schedule has formulas imbedded to calculate the total application cost. The total application cost will be calculated as follows: Subtotal of Tasks & Deliverables + (monthly price for maintenance multiplied by 60 months) + (monthly price for SaaS/Hosting multiplied by 60.

7.0 CONTRACT AWARD

Contract award will be made with reasonable promptness by written notice to that responsible vendor {bidder}, whose quotation, conforming to this RFQ is most advantageous to the state, price, and other factors considered. The State reserves the right to award in whole or part, whichever is determined by the State to be in its best interest to do so. Any or all quotes may be rejected when the State Treasurer or the Director determines that it is in the public interest to do so.

All Bidder's must agree to the State of New Jersey Standard Terms and Conditions and Waivered Contracts Supplement to the State of New Jersey Standard Terms and Conditions. Both documents are located on the Waiver and DPA Contract Checklist, which is attached. Bidder's must also complete all of the State's required forms and certifications as listed on the Waiver and DPA Contract Checklist and submit with its proposal on the proposal submission date including Appendix A (Requirements Matrix), Appendix B (RFQ Price Sheet), and the State of New Jersey Third Party Information Security Questionnaire. **Failure to do so will result in the Bidder's proposal being deemed non-responsive and not eligible for further consideration or award.**

7.1 Contract Term

The term of the contract shall be for a period of five (5) years, with a possible five (5) years extension. The extensions may be one year at a time.

Appendix A- Requirements Matrix

See Attached

Appendix B- RFQ Price Sheet

See Attached