Solicitation Information
May 2, 2017

RFP# 7551629

TITLE: RFP – Utility Bill Analysis and Management Platform

Submission Deadline: May 31, 2017 at 2:30 PM (ET)

PRE-BID/ PROPOSAL CONFERENCE: NO

Questions concerning this solicitation may be e-mailed to the Division of Purchases at gail.walsh@purchasing.ri.gov no later than Friday, May 12, 2017 at 5:00 PM (ET). Questions should be submitted in a Microsoft Word attachment. Please reference RFP #7551629 on all correspondence. Questions received, if any, will be posted on the Internet as an addendum to this solicitation. It is the responsibility of all interested parties to download this information.

SURETY REQUIRED: NO

BOND REQUIRED: NO

GAIL WALSH
CHIEF BUYER

Applicants must register on-line at the State Purchasing Website at www.purchasing.ri.gov

Note to Applicants:

Offers received without the entire completed three-page RIVIP Generated Bidder Certification Form attached may result in disqualification.

THIS PAGE IS NOT A BIDDER CERTIFICATION FORM
TABLE OF CONTENTS

SECTION 1: INTRODUCTION 3
    INSTRUCTIONS AND NOTIFICATIONS TO OFFERORS 3
SECTION 2: BACKGROUND 4
SECTION 3: REQUIREMENTS 5
SECTION 3: SCOPE OF WORK 9
SECTION 4: TECHNICAL PROPOSAL 10
SECTION 5: COST PROPOSAL 10
SECTION 6: EVALUATION AND SELECTION 11
SECTION 7: PROPOSAL SUBMISSION 12
SECTION 8: RESPONSE CONTENTS 13
SECTION 9: CONCLUDING STATEMENTS 13
ATTACHMENT A: COST PROPOSAL FORM 14
SECTION 1: INTRODUCTION AND INSTRUCTIONS AND NOTIFICATIONS TO OFFERORS

The Rhode Island Department of Administration (“Department”), Division of Purchases (“Division”), on behalf of the Office of Energy Resources (“OER”), is soliciting proposals from qualified Vendors to provide utility tracking software. OER is seeking a software package that can analyze billing data that may be utilized by several State of Rhode Island Agencies (“State”).

This contract will be awarded under the State’s General Conditions of Purchase which are available on the Internet at: http://www.purchasing.ri.gov

This is a Request for Proposals, not an invitation for Bid. Responses will be evaluated on the basis of the relative merits of the proposal, in addition to price; there will be no public opening and reading of responses received by the Division of Purchases pursuant to this Request, other than to name those offerors who have submitted proposals.

INSTRUCTIONS AND NOTIFICATIONS TO OFFERORS:

1. Potential vendors are advised to review all sections of this RFP carefully and to follow instructions completely, as failure to make a complete submission as described elsewhere herein may result in rejection of the proposal.

2. Alternative approaches and/or methodologies to accomplish the desired or intended results of this procurement are solicited. However, proposals which depart from or materially alter the terms, requirements, or scope of work defined by this RFP will be rejected as being non-responsive.

3. All costs associated with developing or submitting a proposal in response to this RFP, or to provide oral or written clarification of its content shall be borne by the vendor. The State assumes no responsibility for these costs.

4. Proposals are considered to be irrevocable for a period of not less than 120 days following the opening date, and may not be withdrawn, except with the express written permission of the State Purchasing Agent.

5. All pricing submitted will be considered to be firm and fixed unless otherwise indicated herein.

6. Proposals misdirected to other state locations, or which are otherwise not present in the Division at the time of opening for any cause will be determined to be late and will not be considered. For the purposes of this requirement, the official time and date shall be that of the time clock in the reception area of the Division.
7. It is intended that an award pursuant to this RFP will be made to a prime vendor who will assume responsibility for all aspects of the work. Joint venture and cooperative proposals will not be considered. All proposals should include the vendor’s FEIN or Social Security number as evidenced by a W9, downloadable from the Division’s website at [www.purchasing.ri.gov](http://www.purchasing.ri.gov).

8. The purchase of services under an award made pursuant to this RFP will be contingent on the availability of funds.

9. Vendors are advised that all materials submitted to the State for consideration in response to this RFP will be considered to be Public Records as defined in Title 38, Chapter 2 of the General Laws of Rhode Island, without exception, and will be released for inspection immediately upon request once an award has been made.

10. Interested parties are instructed to peruse the Division of Purchases website on a regular basis, as additional information relating to this solicitation may be released in the form of an addendum to this RFP.

11. Equal Employment Opportunity (G.L. 1956 § 28-5.1-1, et seq.) – § 28-5.1-1 Declaration of policy – (a) Equal opportunity and affirmative action toward its achievement is the policy of all units of Rhode Island state government, including all public and quasi-public agencies, commissions, boards and authorities, and in the classified, unclassified, and non-classified services of state employment. This policy applies to all areas where State dollars are spent, in employment, public services, grants and financial assistance, and in state licensing and regulation. For further information, contact (401) 222-3090 or krystal.waters@doa.ri.gov.

12. In accordance with Title 7, Chapter 1.2 of the General Laws of Rhode Island, no foreign corporation, a corporation without a Rhode Island business address, shall have the right to transact business in the State until it shall have procured a Certificate of Authority to do so from the Rhode Island Secretary of State (401-222-3040). This is a requirement only of the successful vendor(s).

13. The vendor should be aware of the State’s Minority Business Enterprise (MBE) requirements, which address the State’s goal of ten percent (10%) participation by MBE’s in all State procurements. For further information visit the website [www.mbe.ri.gov](http://www.mbe.ri.gov). For further information, call (401) 574-8670 or Dorinda.keene@doa.ri.gov. Visit the website at [www.mbe.ri.gov](http://www.mbe.ri.gov).

**SECTION 2: BACKGROUND**

OER currently operates a centralized business process to handle payment of electric, natural gas and delivered fuel bills for State agencies. The State receives approximately 3,000 monthly utility bills. OER is tasked with approving payment to the utilities and also supporting State agencies by making energy usage and cost data accessible online. Currently, OER manages the
central collection, analysis, and payment of all electric, gas and delivered fuels bills. In the future, OER may also manage State agency water and/or sewer bills.

Electric and Natural Gas utilities currently send a monthly consolidated electronic file that includes all energy consumption and charges for the previous month. Distribution charges for the State’s electric and natural gas accounts are billed from the local distribution company, National Grid. Commodity supplies for both electric and natural gas are currently billed from a third party (presently: Direct Energy). Approximately 2,200 of the utility bills received are electric accounts and, of those, 1,800 are related to street and traffic lights.

OER currently utilizes Microsoft Access to maintain and track utility data. Utility consumption and charges are imported to Microsoft Access using Microsoft Excel files that are submitted to the State by utilities and energy suppliers. Microsoft Access generates accounting entries that reconcile charges to State Agencies.

A centralized utility management system will assist in the collection and analysis of energy usage down to the individual meter (site level). It will also provide State agencies with a real-time enterprise-wide view of their energy costs, identifying both problem areas and possible energy-saving opportunities. Implementation of a centralized utility management system will reduce operating costs and late fees by streamlining the state’s invoice collection and payment system.

### SECTION 3: Requirements

OER is seeking proposals for a web-based, Commercial Off-The-Shelf, Software-As-A-Service (“SaaS”) application for utility bill management that will improve reporting capabilities, enhance expenditure tracking and auditing, and increase the understanding of energy consumption. The system should provide the following minimum requirements:

1. **Core Business Requirements**
   1.1. Benchmarking capability and ability to identify energy efficiency opportunities and connectivity with EPA Portfolio Manager.
   1.2. Maintain a bill database.
   1.3. Bill importing capability.
   1.4. Capability to perform budgeting and forecasting.
   1.5. Capability to provide contract management.
   1.6. Capability to provide cost and use reporting.
   1.7. Capability to perform energy price analysis.
   1.8. Capability to provide analysis on greenhouse gas emissions associated with energy supplies/consumption.
   1.9. Capability to provide load control (demand) analysis.
   1.10. Capability to provide weather normalization using “tried and true” degree day statistical techniques. Automatic daily download of weather data.
1.11. Provide a web interface with different user types that have different administrative/viewing capabilities.
1.12. Capability to provide Calendarization - to “smooth out” utility bill usage and cost data by allocating them to the appropriate calendar month.
1.13. Capability to normalize energy consumption data based on a user-selected baseline year to make “apples-to-apples” comparison across multiple years.
1.14. Capability to provide energy production data tracking from renewable energy systems and other power generation locations.

2. Preferred Business Requirements:
2.1. Flexible options for filtering data for reports.
2.2. Capability to export reports to different file formats such as CSV, PDF, Microsoft Excel, SQL, JSON, etc.
2.3. Capability to access data via a modern web-services Application Programming Interface (API).
2.4. Capability to email reports directly from the system without requiring an intermediate export step.
2.5. Capability to automatically distribute reports to lists of recipients per specific schedules and filter options.
2.6. Capability to provide rate/tariff analysis which compares current rates with alternatives.
2.7. Capability to provide production and occupancy tracking.
2.8. Capability to provide greenhouse gas emissions, renewable energy credits (RECs), tracking & reporting; include a complete web-based library of conversion factors for CO2 equivalencies.
2.9. Capability of the system to interface with ENERGY STAR Benchmarking. Have the capacity to store and distribute building attribute data to ENERGY STAR Portfolio Manager and receive energy efficiency ratings back.
2.10. Capability to provide energy supply contract tracking and related administration.
2.11. Capability to track and generate reports on the energy and cost savings from energy management or energy improvement projects.
2.12. Capability to provide budget reports using historical cost and consumption unit data to create any number of budgets on a detailed meter-by-meter and month-by-month basis. Reports should include budget vs. actual, indicating surplus/deficit.
2.13. Capability to provide a contract tracker to track and administer energy supply contracts.
2.14. Capability to provide Benchmarking Charts - create any number of ‘peer groups’ and instantly rank the buildings by cost/square foot, usage/square foot and peak watts/square foot. The system should also have the capability to Rank meters by usage, cost per day, and unit cost. It should also Indicate the group average and instantly highlight ‘outliers’ such as abnormal meters, buildings, and bills.
2.15. Capability to integrate data from “Internet of Things” (“IoT”) devices. Bidders should outline their product roadmap as it pertains to IoT. The State is in the early stages of exploring its strategy, so this shall not constitute a scored requirement.
2.16. Capability to integrate to the State’s Oracle E-Business Suite to create accounting/general ledger entries and reflect paid bills.

3. Usability and Accessibility Requirements
3.1. The overall user experience should be simple and intuitively designed for all users.
3.2. The system should give visual representation of users’ progress throughout a given workflow.
3.3. Users should have the ability to save their progress in a given workflow and return to it later.
3.4. The system must be in compliance with the accessibility principles of Section 508 of the Federal Rehabilitation Act and the standards documented in the World Wide Web Consortium’s Web Content Authoring Guidelines, Version 2, Level AA (WCAG2 Standards). In addition, bidders should submit an annual Voluntary Product Assessment Template OR “VPAT” (Version 2.0 preferred at the date of publication of this RFP and required when VPAT 2.0 leaves its Beta stage or when State enters into a contract with a chosen Vendor).
3.5. General and workflow or page-specific help resources, such as “walkthroughs,” should be available and easily accessible.

4. Architecture and Hosting
4.1. A shared, multi-tenant hosting solution is permissible. The State strongly prefers solutions that comply with the Federal Risk and Authorization Management Program (“FedRAMP”) requirements, as developed by the Federal Cloud Computing Initiative (“FCCI”) at the US General Services Administration (“GSA”) (https://www.fedramp.gov/). FedRAMP security controls and enhancements have been selected from the NIST SP 800-53 Revision 3 catalog of controls. FedRAMP requires that cloud computing services and systems offered by Cloud Service Providers (“CSPs”) meet specified security requirements. CSPs will be required to use qualified, accredited, Third-Party Assessment Organizations to perform independent assessments on their service and systems which results will be shared with the State. Data shall be hosted within the continental US (government-only shared hosting is preferable). The Vendor may provide hosting services itself, or use an approved sub-contractor; however, the Vendor is solely responsible for assuring that the requirements are met. The Vendor shall obtain prior written approval from the State before entering into an agreement for hosting services to be provided by another entity, including but not limited to a third-party data center or other subVendor, for purposes of providing this system.
4.2. Given the nature of the data to be hosted by the system, FedRAMP “Low” certification is an acceptable hosting level.
4.3. The Vendor shall provide the hardware, software, communications, and other infrastructure necessary to meet the requirements of this RFP, including any licenses that must be procured and maintained.
4.4. Regardless of provider, the State expects that the Vendor shall provide or cause to be provided a secure, Tier 3 data center to house equipment, with 24/7 system monitoring, managed firewall services, and managed backup services.
4.5. The data center shall meet the specifications of at a minimum a Tier 3 data center as per the Uptime Institute guidelines.
4.6. The Vendor main data center must utilize redundant components so that no single point of failure exists on any equipment supporting the Solution as specified for Uptime Institute Tier 3 data center classification.
4.7. The Vendor shall have an alternate secure hosting site available in the event that it is not possible to restore operations in the primary site within the Recovery Time Objective of four (4) hours.

4.8. The Vendor must provide separate Q&A and training environments similar in configuration to the one in production and such environment must be accessible by the State for testing, prototyping and training.

4.9. All Solution data will be retained during the Term of the contract with Vendor and for a period of two (2) years thereafter, and will be backed up, co-located and replicated to be in compliance with applicable FedRAMP requirements.

4.10. Policies and procedures for destruction of data must be in compliance with State policies.

4.11. The data center shall have a redundant, fault-tolerant network and connections to the Internet.

4.12. The Vendor shall maintain or cause to be maintained sufficient network bandwidth to support concurrent multiple users, maintaining acceptable performance with 97% of the executed transactions averaging 6.0 seconds or less, measured by real user monitoring (“RUM”) over a twenty-four (24) hour period. Failure to achieve this performance level will be subject to the “Problem” and “Incident” categorizations below, as well as the applicable credits as expressly set forth herein.

4.13. The Vendor shall not be responsible for issues on State networks or the public Internet.

4.14. The data center shall have fault tolerant, redundant environmental systems, including power, temperature and humidity control, and fire suppression as specified for Uptime Institute Tier 3 data center classification.

4.15. The data center shall be physically secured as specified for Uptime Institute Tier 3 data center classification.

4.16. Access to the data center shall be restricted to authorized personnel using multi-layered controls and procedures.

4.17. The Vendor must establish and follow policies for granting access to the data center. These policies must be reviewed and approved by the State.

4.18. Access shall only be granted to those with a need to perform tasks in the data center. The data center shall be physically secured as specified for Uptime Institute Tier 3 data center classification.

4.19. The data center network shall include robust firewall, intrusion prevention and intrusion detection systems intended to prevent and detect unauthorized access.

4.20. All software, including operating systems and middleware, used to host the System shall be patched no more than one month after patch availability to minimize security vulnerabilities.

4.21. Vendor shall perform vulnerability scans of the Solution prior to the release of new versions of the Solution. The software used to perform this scan must be approved by the State and the result of the scans must be provided to and approved by the State prior to releasing new systems or new versions of the application to production.

4.22. To ease security concerns and user account creation and maintenance, the State will give due consideration to solutions who allow for direct integration into the State’s existing Active Directory Federation Service (ADFS) infrastructure for authorized Department user
authentication into the solution. The State may, during the course of the contract with a
selected Vendor, implement a Single Sign On solution a la OneLogin or Okta. The State will also
give due deference to Vendors who support authentication via these systems with no
additional configuration necessary by the State.

4.23. All servers and devices supporting the Solution shall have currently-supported and hardened
operating systems, employing up to date anti-viral, anti-hacker, anti-spam, anti-spyware, and
anti-malware utilities.

4.24. Vendor must retain a history of all network and application accesses including a history of all
transactions performed while the user was logged on. This information must be retained for a
minimum of two (2) years.

4.25. The Vendor will notify the State about unscheduled downtime and complete required reports
as prescribed in the Maintenance and Support Requirements herein.

4.26. The Vendor shall notify the State about any breach of cyber or physical security within one (1)
hour of Vendor’s actual knowledge of the incident.

4.27. The Vendor shall sufficiently automate System performance monitoring such that State and
Vendor personnel are notified via email and/or text message/SMS of significant performance
or security issues.

4.28. The State expects that all interactions with the Solution will be transmitted securely, either via
the HTTPS protocol or, in the case of secure file transfers, SFTP, using at least 2048-bit
encryption, or such other highly-secure methods.

4.29. Data not in-flight during a transaction but stored for future access should be encrypted at rest
at the highest-feasible encryption level, with a minimum of 128-bit encryption required as per
the Rhode Island Identity Theft Act of 2015.

4.30.

SECTION 3: SCOPE OF SERVICES

In addition to providing Utility Tracking Software the Vendor shall provide the following
services:

Initial Setup: The Vendor is requested to provide implementation services that will make the
software ready to use for the end users (State employees). The initial setup includes project
management and installation of the existing business processes that are currently performed in
Microsoft Access in the new software. This process includes grouping accounts by Agency and
installing parameters that are necessary for the software to perform the analysis.

Training: The Vendor shall provide initial on-site training to State staff on the use of the
System. It is anticipated that this training shall include up to five (5) administrative users that are
responsible for System maintenance, up to five (5) State technical support staff, and five (5)
power users utilizing a train-the-trainer approach to address future State training needs.
Additional training shall be made available via on-line videos and resources on an ongoing basis
throughout the term of the resultant Contract. Vendor should provide a self-help manual that is
continually updated with new software version releases. The Vendor shall provide a yearly
addendum for the training manual that includes all processes and procedures for all updates provided within the last year.

**Maintenance and Support**: Maintenance and support contract shall be renewable on an annual basis. Contract price shall include the support and maintenance services outlined in Exhibit B. In addition, the contract shall include line item price per hour for staff positions. These line item charges will be used if OER requires additional features, functions, or interfaces to be developed that are not mentioned herein.

**Acceptance Testing**: Subsequent to final installation of all System components, the Vendor shall conduct a preliminary acceptance test plan created in consultation with OER that shall be based upon the software versions and configurations as proposed. Any failures found during the acceptance testing shall be immediately corrected by the Vendor. As the project develops and the System is purchased, OER reserves the right to coordinate final acceptance testing protocol with Vendor. A final acceptance test plan is required before placing the System into service. It is expected that final acceptance testing will commence immediately upon System cutover and proceed for 90 consecutive calendar days without any failures or to the OERs satisfaction.

**SECTION 4: TECHNICAL PROPOSAL**

Proposals shall contain the following information and be formatted as described below. Adherence to these instructions will be a factor in the evaluation of proposals.

A. **Organizational Background – Experience and Qualifications**
   Provide a brief description of your firm and information regarding governmental agencies and/or other large organizations that use your product and the services you have provided them.

B. **Capacity to provide the System Requirements**
   Provide a detailed listing and discussion of the services you will provide.

C. **Detailed Project implementation Plan**
   The proposal should include a detailed project implantation plan and associated timeline.

D. **Capacity to Provide Services**
   Provide a list of Principals (executive management) and project staff members who would be assigned to the project. Provide resumes/CV and describe qualifications and experience.

E. **References** – Provide a list of three references with whom you have worked within the last five (5) years who can provide insight regarding software, training, maintenance and support services. References from other public sector entities are encouraged.

**SECTION 5: COST PROPOSAL**

Costs must be itemized and indicated on the attached Cost Sheet in Exhibit A.
SECTION 6: EVALUATION AND SELECTION

Proposals will be reviewed by a Technical Review Committee comprised of staff from State agencies. To advance to the Cost Evaluation phase, the Technical Proposal must receive a minimum of 60 out of a maximum of 70 technical points. Any technical proposals scoring less than 60 points will not have the cost component opened and evaluated, and will be removed from further consideration. Proposals scoring 60 technical points or higher will be evaluated for cost and assigned up to a maximum of 30 points in the cost category, bringing the potential maximum score to 100 points.

The State reserves the exclusive right to select the individual(s) or firm (vendor) that it deems to be in its best interest to accomplish the project as specified herein; and conversely, reserves the right not to fund any proposal(s).

Proposals will be reviewed and scored based upon the following criteria:

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Possible Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organizational Background and Experience/Qualifications</td>
<td>10</td>
</tr>
<tr>
<td>Capability to provide the system requirements and additional features identified in the RFP</td>
<td>30</td>
</tr>
<tr>
<td>Detailed Project Implementation Plan – Timeline</td>
<td>10</td>
</tr>
<tr>
<td>Capacity to provide initial setup, training, maintenance and support and acceptance testing</td>
<td>10</td>
</tr>
<tr>
<td>References</td>
<td>10</td>
</tr>
<tr>
<td><strong>Total Possible Technical Points</strong></td>
<td><strong>70</strong></td>
</tr>
<tr>
<td>Cost Calculated as lowest responsive cost proposal divided by (this cost proposal) times 30 points *</td>
<td>30</td>
</tr>
<tr>
<td><strong>Total Possible points</strong></td>
<td><strong>100</strong></td>
</tr>
</tbody>
</table>

*The Low bidder will receive one hundred percent (100%) of the available points for cost. All other bidders will be awarded based upon the following formula:

\[
\text{(low bid / vendors bid) } \times \text{ available points}
\]

For example: If the low bidder (Vendor A) bids $65,000 and Vendor B bids $100,000 for monthly cost and service fee and the total points available are Thirty (30), vendor B’s cost points are calculated as follows:

\[
\frac{65,000}{100,000} \times 30 = 19.5
\]
Points will be assigned based on the offeror’s clear demonstration of his/her abilities to complete the work, apply appropriate methods to complete the work, create innovative solutions and quality of past performance in similar projects.

Applicants may be required to submit additional written information or be asked to make an oral presentation before the technical review committee to clarify statements made in their proposal.

SECTION 7: PROPOSAL SUBMISSION

Questions concerning this solicitation may be e-mailed to the Division of Purchases at gail.walsh@purchasing.ri.gov, no later than the date and time indicated on page one of this solicitation. Please reference RFP #7551629 Utility Management Software on all correspondence. Questions should be submitted in a Microsoft Word attachment. Answers to questions received, if any, will be posted on the Internet as an addendum to this solicitation. It is the responsibility of all interested parties to download this information. If technical assistance is required to download, call the Help Desk at (401) 222-3766 or lynda.moore@doit.ri.gov.

Offerors are encouraged to submit written questions to the Division of Purchases. No other contact with State parties will be permitted. Interested offerors may submit proposals to provide the services covered by this Request on or before the date and time listed on the cover page of this solicitation. Responses received after this date and time, as registered by the official time clock in the reception area of the Division of Purchases will not be considered.

Responses (an original plus four (4) copies) should be mailed or hand-delivered in a sealed envelope marked “RFP#7551629 – Utility Management Software” to.

RI Dept. of Administration
Division of Purchases, 2nd floor
One Capitol Hill
Providence, RI 02908-5855

NOTE: Proposals received after the above-referenced due date and time will not be considered. Proposals misdirected to other State locations or those not presented to the Division of Purchases by the scheduled due date and time will be determined to be late and will not be considered. Proposals faxed, or emailed, to the Division of Purchases will not be considered. The official time clock is in the reception area of the Division of Purchases.
SECTION 8: RESPONSE CONTENTS

Responses shall include the following:

1. A completed and signed three-page R.I.V.I.P generated bidder certification cover sheet downloaded from the RI Division of Purchases Internet home page at www.purchasing.ri.gov.

2. A completed and signed W-9 downloaded from the RI Division of Purchases Internet home page at www.purchasing.ri.gov.

3. A Technical Proposal in accordance with Section 4 of this solicitation. The Technical Proposal is limited to twenty (20) pages (this excludes any appendices).

4. A separate, signed and sealed Cost Proposal using Attachment A: Cost Proposal Form reflecting the hourly rate, or other fee structure, proposed to complete all of the requirements of this project.

5. In addition to the multiple hard copies of proposals required, Respondents are requested to provide their proposal in electronic format (CD-Rom, disc, or flash drive). Microsoft Word / Excel OR PDF format is preferable. Only 1 electronic copy is requested and it should be placed in the proposal marked “original”.

SECTION 9: CONCLUDING STATEMENTS

Notwithstanding the above, the State reserves the right not to award this contract or to award on the basis of cost alone, to accept or reject any or all proposals, and to award in its best interest.

Proposals found to be technically or substantially non-responsive at any point in the evaluation process will be rejected and not considered further.

The State may, at its sole option, elect to require presentation(s) by offerors clearly in consideration for award.

The State’s General Conditions of Purchase contain the specific contract terms, stipulations and affirmations to be utilized for the contract awarded to the RFP. The State’s General Conditions of Purchases/General Terms and Conditions can be found at the following URL: https://www.purchasing.ri.gov/RIVIP/publicdocuments/ATTA.pdf
**Exhibit A**

**Cost Proposal Form**

All-inclusive pricing to provide the OER with utility analysis and management software in accordance with the requirements set forth in this RFP.

In addition to the summaries below, bidders should break out any individual pricing components so the State can properly understand the dynamics of the cost proposal. I.E. If a bidder’s pricing is based on a per-user annual license cost, for example, the bidder should list the cost for one user and any tiered pricing based on number of users.

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>COST</th>
</tr>
</thead>
<tbody>
<tr>
<td>SaaS Licensing Cost – 5 Years</td>
<td>$</td>
</tr>
<tr>
<td>Configuration and setup, including acceptance testing</td>
<td>$</td>
</tr>
<tr>
<td>Training (40 hours)</td>
<td>$</td>
</tr>
<tr>
<td>Total Proposed Price for a Utility Tracking System</td>
<td>$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Personnel Types/Titles for Additional Work Outside of the Installation/Maintenance Contracts</th>
<th>Hourly Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>


Exhibit B
Maintenance and Support

This Exhibit B is a standard delineation of the State’s Maintenance and Support expectations for a selected Vendor.

Definitions - The definitions below shall apply to this Exhibit B:

1. “Agreement” means the eventual contract entered into by the State and a selected Vendor.

2. “Best Practices” means the industry standard as adopted in writing by RI DoIT for IT Service Management, ITIL v 3 (Information Technology Infrastructure Library) Service Level Management standard in effect as of the Effective Date and as may be updated from time to time during the Term; provided, however, that the State will provide Vendor with reasonable advance written notice of any update.

3. “Breach” means an actual or reasonably perceived event arising from a risk, threat, or vulnerability that may affect the confidentiality, integrity, or availability of information resources or data, cause damage to IT systems and/or network, or result in a significant loss of vital business assets or User Data as defined herein.

4. “Defect” means an error, flaw, mistake, failure, fault or “undocumented feature” in the Solution that causes a material deviation, which in the State’s reasonable discretion is detrimental, from its intended behavior or performance as specified in its written specifications provided herein.

5. “Designated Representatives” means the State’s administrative support and management staff who are designated by the State in writing and authorized to contact Vendor for the purpose of obtaining Call Center assistance pursuant to the Agreement.

6. “Incident” is an unplanned disruption or degradation of service capabilities that needs to be resolved to restore functionality of the Solution during Normal Business Hours. This can either be through a permanent fix or a workaround. An example of an Incident would be a disruption in the system services caused by a server crash (“Server Crash Incident”). If a server is used only during State business hours, a crash after State business hours is, not yet an Incident since no system service was affected. It becomes an incident only when the outage extends to the hours of use. If an outage is planned, for example, a scheduled maintenance, this is not an Incident and should not be counted as part of the system performance metrics. If the planned outage exceeds the scheduled time, then the over time for the outage becomes an incident if service capabilities are affected. Other examples would be if a system service becomes unusable, or service capabilities are degraded. (Note: Severity of the issue is determined by the impact. Incidents are addressed by severity first, then age, oldest being addressed first.)

7. “Incident Categorization” means classification of the Incident by severity level as further specified herein.

8. “Initial Response” means an email or other notification acknowledging receipt of the support ticket or request, which may be in the form of an automated email notification or other automated response.

9. “Maintenance Services” means the maintenance services to be provided by Vendor pursuant to the Agreement.
10. “Support Level” refers to the extent of technical assistance, which must be provided by Vendor for the Solution’s authorized users consistent with the Agreement. Vendor’s support level definitions are described as shown below:

<table>
<thead>
<tr>
<th>1st Level Support</th>
<th>The responsibility of 1st Level Support is to register and classify received Incidents and to undertake an immediate effort in order to restore a failed IT service as quickly as possible.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>If no ad-hoc solution can be achieved, 1st Level Support will transfer the Incident to expert technical support groups (2nd Level Support).</td>
</tr>
<tr>
<td></td>
<td>1st Level Support also processes Service Requests and keeps users informed about their Incidents’ status at agreed intervals.</td>
</tr>
<tr>
<td>2nd Level Support</td>
<td>2nd Level Support takes over Incidents which cannot be solved immediately with the means of 1st Level Support.</td>
</tr>
<tr>
<td></td>
<td>If necessary, 2nd Level Support will request external support, e.g. from software or hardware manufacturers.</td>
</tr>
<tr>
<td></td>
<td>The aim is to restore a failed IT Service as quickly as possible.</td>
</tr>
<tr>
<td></td>
<td>If no solution can be found, the 2nd Level Support passes on the Incident to Problem Management.</td>
</tr>
</tbody>
</table>

11. “Normal Business Hours” means and refers to the period of time starting at 7:00 a.m. EST and ending at 9:00 p.m. EST.

12. “Problem” is a cause of one or more Incidents. Problems are not Incidents. An Incident can expose a problem. You may raise a Problem in a support request ticket and reference it to a known Incident. The cause of the Problem may be known or not known.

13. “Support Services” means the support services to be provided by Vendor pursuant to the sections of this Exhibit.

14. “Term” has the meaning set forth in the body of the Agreement.

15. “Workaround” is a bypass of a recognized incident in the System. A Workaround is typically a temporary fix and indicates that a permanent solution to the underlying Problem is needed. Typically, Workarounds are considered ‘brittle’ because they are implemented before extensive testing can be completed and may not respond well to the expected range of system inputs. It is required that Workarounds are tracked and managed to address risk and that the development of a permanent solution is analyzed and designed. Furthermore, Vendor is required to schedule and complete the development of a permanent solution expeditiously.
16. “Service Capabilities” are the functional business related capabilities the Solution provides. An example of a Solution Service Capability is the ability to [INSERT COMMON TRANSACTION HERE]. The loss or degradation of a Service Capability may impact the business of [THE AGENCY OR 3RD PARTY].

17. “Service Level(s)” is/are the specific performance metrics and level of Support Service required in this Exhibit.

Support Service Objectives

To ensure reasonable, consistent, high quality delivery of Support and Maintenance Services for the System, Vendor shall apply Best Practices to provide the Maintenance and Support Services defined in the Agreement in accordance with the Service Objectives, Procedures, Service Levels and chargebacks defined in the Agreement.

1. Vendor shall diligently process, categorize and assess all changes to the Solution environment, validating that changes to the Solution are tested and controlled, and unplanned Services disruptions are resolved in the shortest time as is commercially reasonably.

2. Vendor shall oversee and maintain the Solution so that all software and hardware are current and supported technology, subject to changes requiring a Change Order.

3. Subject to the terms herein, Vendor shall provide Support Services via the Call Center, e-mail Support Services and Web-based Support Services during Normal Business Hours for the Term to Designated Representatives. Vendor shall provide access to Vendor’s Support Services for resolution, feedback, troubleshooting, and support consistent with the terms herein. All Vendor personnel providing the Support Services pursuant to the Agreement shall have expertise and be fully trained in issue (i.e., Incident and Problem) identification and resolution or escalation relating to the System. Vendor personnel shall, as necessary, refer the Incident and Problem to Vendor’s software engineering and technical resources for resolution, feedback, troubleshooting, and support consistent with the terms herein. All Incidents and Problems shall be logged in Vendor’s designated on-line support management software consistent with the terms herein. The reported Incidents and Problems shall be viewable in detail and summary format by Designated Representatives.

4. Vendor shall be responsible for implementing occasional updates to the Solution in response to changes in the legal or regulatory environment in the State affecting Vendor’s provision of the Services, with the cooperation of Designated Representatives; provided, however, the Parties shall follow the Change Order process to the extent such updates involve any material changes to the Solution.

5. Vendor shall provide or cause to be provided to the State monthly Maintenance and Support reports, in a mutually-agreed-upon format. The report(s) shall document past Support Services performance, future scheduled maintenance activities and anticipated System changes, as further discussed in Section 3 of this Exhibit, below.
General Responsibilities
The following are general Support Services for which the Vendor shall be responsible:

Security
Vendor’s data storage policies with respect to User Data will comply with the Agreement and applicable State law, and other security policies, regulations, and standards in effective as of the Effective Date and applicable to the Solution for information, information systems, and personnel, physical and logical security, each to the extent as set forth herein. See below for expectations on a Comprehensive Security Strategy.

Data Availability
Subject to the terms and conditions of the Agreement, upon the State’s reasonable request during the Term, or upon expiration or termination of the Agreement, Vendor will provide or make available an encrypted copy of the State Data or User Data to the State (as applicable), in a non-proprietary, easily-accessible format. Upon written acknowledgement of verified receipt and decryption of the applicable data by the State, and subject to the terms and conditions of the Agreement, including, without limitation, Vendor’s data retention obligations hereunder, the Vendor shall irreversibly erase all PII from its systems in accordance with Exhibit I.

Policies, Procedures and Standards
Subject to the terms and conditions of the Agreement, the Vendor is responsible for conforming to the policies and procedures of the State as outlined in the Agreement, including governance standards, each such policies, procedures and standards in effect as of the Effective Date. Vendor employees using the State resources shall adhere to all the State policies and procedures in effect as of the Effective Date as outlined herein, including, but not limited to, policies and procedures for security and code of conduct (e.g., Internet usage, passwords, access to the State production systems and intellectual property rights, etc.). The State will provide Vendor with reasonable advance written notice any time such policies, procedures and standards change during the Term. To the extent that any such change is material, the Parties shall follow the Change Order process described herein.

Maintenance Services
Subject to the terms and conditions of the Agreement, Vendor shall provide Maintenance Services for the System as set forth herein. Maintenance Services shall consist of the following:

(i) Solution Maintenance and Updates
   1. Vendor periodically deploys releases of the Solution into the Solution’s technical environments as defined in the Agreement.
2. Except in cases of emergency or a reasonably necessary update as determined by Vendor in its reasonable discretion, Vendor shall notify the State at least thirty (30) days prior to activating each update. If it is determined that additional time is necessary to address any impact on the integration of Solution with other system components of the overall Solution the update shall be rescheduled to a later date as mutually agreed upon by the Vendor and the State. Notification of each update shall include the following, at a minimum:
   a. Date of update activation;
   b. Notes describing the update content;
   c. Date, time, and duration of time required to deploy the update; and
   d. Results of tests that document satisfactory test run of the update in Pre-production (Staging) environment of Solution.
3. Vendor shall apply commercially reasonable efforts and resources to resolve any Defect in the Solution identified by the State, otherwise brought to Vendor’s attention, or a Defect of which Vendor should reasonably become aware.
4. All Vendor code developed for the System will be subject to automated unit testing and, where appropriate, manual regression testing by Vendor.
5. The State also expects that, at a minimum, only code that has passed all local and system-wide unit and automated regression tests will be cleared for an automatic deployment/continuous integration into the Vendor’s production environment. Vendor will apply Best Practices to standard deployment procedures.

(ii) Maintenance Schedule

Current and Supported
The Vendor shall assure fully-supported, current versions of all hardware and software components are used to support the system(s).

Scheduled Maintenance
Vendor shall perform routine maintenance on a regular basis to ensure proper operation. The maintenance shall be within the Service Levels defined in this Exhibit. The scheduled maintenance shall be performed between the hours of 11:00PM on Saturday and 6:00AM Sunday EST. The Vendor shall provide the State with seventy-two (72) hours advanced notice of scheduled maintenance, whenever and to the extent commercially reasonable.

Emergency Maintenance
Vendor may need to perform emergency maintenance, such as when a Service Capability cannot be met by a nonperforming application with no workaround, or caused by a security patch installation or hardware replacement. The Vendor shall provide the State with notice of emergency maintenance in accordance with the change management procedures outlined in the Agreement.

(iii) Update Management
Update Management activities include Services required to appropriately manage and document changes to the Solution (e.g., Hardware, Software, Hosting etc., excluding services related to implementation) and its components, which shall be subject to associated costs and fees only if outside of mutually agreed upon scope or if a Change Order is required.
(iv) Patching
The Vendor shall install all hardware and software patches, updates, and other utilities according to Vendor’s commercially reasonable discretion as required to maintain system operations and security. All critical patches shall be applied within thirty (30) days of general release, or sooner if mutually agreed to by the Parties.

(v) Version Control
The Vendor shall be responsible for the reasonable maintenance, tracking and auditing of modifications to the System’s components over time, facilitating the restoration or rollback of the System, or a component thereof, to prior development stages should a problem arise.

(vi) Turnover Management
The Vendor shall be responsible for promotion of software changes across different phases of the software deployment life cycle (e.g., development, unit test, systems test and production), including management of the approval process, production turnover and software migration control.

(vii) Platform Change
The Vendor will coordinate activities with the State prior to any requested or required changes to the Solution that may affect the Service Capability performance of any of the system environments. Any changes to the Solution must be managed consistent with the change management procedures defined in the Agreement.

(viii) Testing
All patches and updates shall be fully tested prior to implementation in the production environment. The Vendor will maintain a QA environment to be used for such testing.

Monitoring and Reporting Services
Vendor shall provide monitoring and reporting Services that include the activities associated with the ongoing surveillance, tracking, escalation, resolution and reporting of application development problems, each as expressly specified herein. These Problem Management activities require coordination with the designated Level 1 and Level 2 Support Services described herein. This monitoring shall include:

1. Monitoring the health of the System and notifying the authorized members of the State’s designated operations team of potential issues consistent with the Agreement.
2. Monitoring the connections between the different layers of the System and the public internet.
3. Monitoring for critical exceptions as mutually agreed to by the Parties in writing within the System consistent with the Agreement.
4. Monitoring the transaction and login rates for capacity and security.
5. The Monitoring Plan, as mutually agreed to by the Parties in writing, shall provide a list of all physical devices (if dedicated hardware is used to host the System), hosts, ports, URLs, Web sites and other components that are required to be actively monitored pursuant to such Monitoring Plan.
6. The Monitoring Plan, as mutually agreed to by the Parties in writing, shall include the provisions for the detection of actions that attempt to compromise the confidentiality, integrity or availability of resources or User Data.

The Vendor shall generate and provide to the State system usage and performance reports on a minimum of a monthly basis, including the following:

1. Server up-time and down-time
2. All critical outages, including issue and resolution
3. All changes, patches and upgrades implemented
4. System access by authorized users; and
5. Any other Incidents and resolution thereof

On a quarterly basis, Vendor shall provide to the State a consolidated list of major activities being performed on the Solution, their status and plans for the next reporting period.

In addition to internal testing and tools, the State expects Vendor to utilize tools to measure system performance akin to https://www.pingdom.com/ and https://www.librato.com/, as well as publish an availability dashboard in the fashion of services offered by https://www.statuspage.io/. At a minimum, the State expects secure, anonymized, aggregated performance data of this kind to be made available via an Application Programming Interface (API).

Support Services

Subject to the terms and conditions of the Agreement between the State and Vendor, Vendor shall provide Support Services as described herein for all components of the System, including hardware and third party supplied system software chosen by Vendor, if applicable. Support Services shall consist of the following:

Support Center

Standard customer care services are required to provide continued proper and effective use of the Solution by users throughout the Term of the Agreement. The primary mechanism for delivering this service is the Support Center. Support Center services are provided as follows:

1. The Vendor will provide Level One and Level Two support for the Solution, subject to the terms of the Agreement and as specified in the Support Levels chart in this Exhibit.
2. Support Center staff may be contacted by Solution end-users for support or the reporting of Defects via a toll-free telephone number provided by Vendor. The Support Center must also provide for E-Mail Support and Web based Support consistent with the terms herein.
3. Support Center staff provide assistance in the following areas:
   a. Assistance related to the use of the System;
   b. Advice on work-arounds for verified Defects;
   c. Information on verified Defects previously identified by the State and reported to Vendor.
   d. Advice on completion and authorization for submission of the Vendor Incident Report Form to report identified Incidents which may indicate a Problem in the Solution.
e. Vendor shall create and add appropriate documentation to the Solution help files or other mutually agreed upon tools.

**Escalation Procedures**

All Incidents shall be reported as follows:

1. Users record Incident in the designated help desk system (e.g. E-Mail, Web-based, Phone).
2. Vendor records Incident in the Support System with ticket number and specified severity level as determined by the Severity Level Table below.
3. Designated Representatives may escalate incidents in Support System via:
   a. Support Center (Phone);
   b. E-mail Support; or
   c. Web-based Support.
4. Vendor personnel shall respond to Designated Representative based on the State-assigned severity level in accordance with the Severity Levels herein. Vendor personnel shall resolve incidents as expeditiously as is commercially reasonable, consistent with Best Practices and industry standards.

**Complaints**

The State shall escalate to Vendor’s personnel manager upon unsatisfactory results not in compliance with Severity Level or if an issue is not resolved within a reasonable time for any Incident or Problem.

**Support Service Availability**

Vendor shall provide Support Services via phone during Normal Business Hours, as set forth above, with compliance to the Severity Levels defined in this Exhibit. Outside Normal Business Hours requests must be initiated through E-Mail, or Web-based support. The Initial Response time requirement begins at the next business hour during Normal Business Hours following the user’s report of the issue. The State, within its reasonable discretion, shall review the assigned Severity Level based on the above definitions and shall convey its designation to Vendor after the issue is reported. If Vendor does not agree with the State’s designation of the Severity Level for any issue, it shall indicate the Severity Level Vendor attributes to the issue as soon as possible but in any event by the end of the Initial Response time for the Severity Level originally designated for the Incident. The Parties shall work in good faith to agree upon the appropriate Severity Level provided that such determination shall not unreasonably delay the implementation of a solution to the issue. However, Vendor shall not be deemed in breach of the timing obligations herein if Vendor cannot fulfill its obligations within the applicable timeframes set forth herein because of delays caused by the State.

**Severity Table – Incident Resolution Times**

The scope of Incident Management includes any event that materially disrupts, or could materially disrupt, a Service Capability. This includes Incidents that are communicated by authorized users, as well as Incidents detected and reported by technical staff or monitoring tools to the extent specified herein. Incident models can help ensure that standard approaches are followed and timescales are met - for example, for managing security Incidents, or using well-defined solutions for common types of Incidents.
<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Title</th>
<th>Description</th>
<th>Initial Response</th>
<th>Incident Categorization</th>
<th>Incident Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Critical</td>
<td>Production System undergoes a Server Crash Incident. If there is no reasonable work-around available, a patch may be produced. When an acceptable workaround is provided the Incident shall be downgraded to a lower priority.</td>
<td>Normal Business Hours: 05 minutes</td>
<td>1 hour</td>
<td>If Workaround is available in 4 hours or less, Incident closes and Problem is opened to evaluate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Outside of Normal Business Hours: 20 minutes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>High</td>
<td>Incidents render a feature inoperable and/or data has been corrupted without a work-around. They do not cause the production System to be inoperative, but they disrupt the normal business operations.</td>
<td>Normal Business Hours: 15 minutes</td>
<td>2 hours</td>
<td>If Workaround is available in 8 hours or less Incident closes and Problem is opened to evaluate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Outside of Normal Business Hours: 2 hours</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Medium</td>
<td>Incidents render a feature inoperable and/or data has been corrupted with acceptable work around to be used on an interim basis until incident addressed with a more effective work around and/or fix.</td>
<td>Normal Business Hours: 20 minutes</td>
<td>12 hours</td>
<td>If the Incident cannot be resolved in 24 hours, it leads to a Problem. The Incident is closed and a Problem is opened to evaluate further.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Outside of Normal Business Hours: 4 hours</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Low</td>
<td>Incidents have little impact on the business and application including questions not answered in the Vendor documentation and documentation errors. Incidents may be addressed in a future release.</td>
<td>Normal Business Hours: 30 minutes</td>
<td>24 hours</td>
<td>If the Incident cannot be resolved with a bug fix or patch in the next release, it leads to a Problem. The Incident is closed and a Problem is opened to evaluate further.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Outside of Normal Business Hours: 8 hours</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Severity Table – Problem Resolution Times

The scope of Problem Management includes diagnosing causes of Incidents, determining the resolution and ensuring that this is implemented. Problem Management uses the same tools as Incident Management, and similar categorization, impact and severity levels. Problem models can be used to help ensure consistent handling of similar types of Problems. Reactive Problem Management is part of Service Operation; proactive Problem Management is the activity in Continual Service Improvement that identifies Problems based on analysis of Incident data.

<table>
<thead>
<tr>
<th>Severity Level</th>
<th>Description</th>
<th>Root-Cause Analysis</th>
<th>Root-Cause Report</th>
<th>Problem Remediation Plan</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - Critical</td>
<td>Production System undergoes a Server Crash Incident. An emergency hotfix or patch must be produced.</td>
<td>24 hours</td>
<td>36 hours</td>
<td>48 hours</td>
</tr>
<tr>
<td>2 - High</td>
<td>Problem renders a feature inoperable and/or data is corrupted and a workaround is available. Production System is operative, but there may be disruptions in normal business operations.</td>
<td>36 hours</td>
<td>48 hours</td>
<td>72 hours</td>
</tr>
<tr>
<td>3 - Medium</td>
<td>Problem renders a feature inoperable and/or data is corrupted and no workaround is available.</td>
<td>14 days</td>
<td>5 days</td>
<td>15 days</td>
</tr>
<tr>
<td>4 - Low</td>
<td>Problem has little impact on the business and application including questions not answered in the Vendor documentation and documentation errors. Problem may be addressed in a future release.</td>
<td>4 months</td>
<td>5 months</td>
<td>6 months</td>
</tr>
</tbody>
</table>

Problem Resolution Steps

<table>
<thead>
<tr>
<th>Problem Resolution Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A – Categorization</td>
<td>Acknowledgement the Problem has been logged</td>
</tr>
<tr>
<td></td>
<td>Provides reassurance that the Problem is going to be dealt with accordingly.</td>
</tr>
<tr>
<td></td>
<td>Adopt Incident severity initially</td>
</tr>
</tbody>
</table>
| B – Root Cause Analysis | Incident management may have resulted in a temporary fix  
Problem management works out the root cause  
This is an operational level process (“OLP”) about identifying and not resolving the root cause  
The outcome that is being measured by the OLP is going to be the production of a deliverable Policy will determine what that deliverable might contain  
The OLP measures the time between the formal closure of the Incident and the formal delivery of the root cause analysis Re-evaluate severity (increase or decrease) |
| C – Root Cause Report | This OLP ensures that a formal document is delivered in a timely fashion  
The document describes the timeline of events that caused the Problem and actions taken to provide a workaround  
It lists all of the actions and recommendations with identified owners and realistic dates in order to fix the Problem |
| D – Remediation Plan | The root cause analysis identifies actions that need to affect a permanent fix to the original issue  
All resolutions will not be equal in complexity, effort and duration  
There will be an initial estimation of a target date for live implementation of a permanent fix  
Moving the target completion date is allowed, however this OLP limits how often this can occur |

**Failure to Meet Performance Requirements**

Subject to the terms and conditions herein, Vendor’s material failure to satisfy performance standards or other requirements expressly set forth herein, may result in a chargeback in the amount as articulated below and/or an Event of Default under the Agreement. The chargeback shall be paid to the State in the form of a credit against the Vendor’s invoice submitted to the State immediately following the month in which the Vendor failed to satisfy the standard or requirement. For the avoidance of doubt, each of the following chargeback amounts is based on Vendor failures for cause by an Event of Default only. Vendor shall not be penalized with a chargeback or otherwise liable to the State for any failures (whether listed below or otherwise) caused by or attributable to the State, users of the Services or Solution, or a third party, including any causes beyond the reasonable control of Vendor.

1. Failure to meet Incident or Problem Resolution Times as listed in the above sections respectively, shall result in a credit to the State per Incident based on the following scale: Critical = $500; High = $400; Medium = $300; and Low = $200.
2. Failure to provide Incident or Problem Resolution for any Incident or Problem beyond thirty days of the listed resolution times in the above sections shall result in a credit to the State, based on the following scale: Critical = $250; High = $200; Medium = $150; and Low = $100 which will be imposed per Incident for each month until such issue is resolved as mutually agreed upon by the Parties.
3. Failure to provide customer service Support Services during the Normal Business Hours as defined in this section shall result in a $50 credit per hour to the State for the first eight (8) hours per month and $100 credit per hour thereafter for every hour after that per month, for each hour of failure.

4. Failure to resume operation after scheduled maintenance hours as defined in this Exhibit shall result in a $100 credit per hour to the State for the first 24 hours and $200 credit per hour, thereafter, for each hour of failure.

5. Failure to ensure that all elements of the Solution are operational and available 24 hours a day, seven (7) days a week, except for the scheduled maintenance hours defined in the Agreement or as otherwise provided herein, shall result in a $100 credit per hour to the State for the first 24 hours and $200 credit per hour, thereafter, for each hour of failure.

6. Failure to maintain sufficient network bandwidth to support concurrent multiple users shall result in a $50 credit per hour to the State for the first eight (8) hours per month and $100 credit per hour thereafter for every hour after that per month, or any portion thereof, that response time does not meet the times designated.

7. Failure to implement the approved disaster recovery plan, as defined by the Parties herein, by the agreed upon implementation date as set forth in Exhibit B shall result in a $500 credit per day credit to the State.

Data Migration Into Solution
Vendor will assist the State Division of Information Technology to migrate applicable data from the State’s legacy system or systems into the new System. The Vendor will clearly delineate which aspects of Extraction, Transformation, and Loading (“ETL”), if any, will be performed by State resources and which will be performed by Vendor staff.

Data Redundancy Policy
Vendor, or its data hosting vendor, must have a defined policy in place in the event of catastrophic data loss.

Comprehensive Security Strategy
All software and processes related to the Solution must comply with all Applicable Data Protection Laws. The Vendor, and any associated subVendors, may be required to have all employees with access to the Solution data center or data to sign a data confidentiality statement attesting that they will keep any Solution information viewed during the course of their employment, private and safe.

The solutions and processes developed as part of the Services provided under the Agreement must comply with or exceed all State technology policies and standards effective as of the Effective Date and provided by State to Vendor in writing, including any updates thereto as may be provided by State to Vendor in writing during the Term; provided, however, that the State will provide Vendor with reasonable advance written notice of any update and, to the extent any such update is reasonably determined to be material, the Parties shall follow the Change Order process described in the Agreement. A risk assessment
and risk management plan for the proposed solutions should follow an industry-standard format, such as those developed by the US National Institute of Standards and Technology ("NIST").

The Vendor will be expected to perform risk assessments including 3rd-party penetration testing at least annually and prior to any proposed significant updates. The Vendor shall be reasonable available to review risk management efforts with the DoIT Information Security Officer ("CISO") or its designee at least monthly.

Where technically feasible, security solutions such as auditing; logging and continuous monitoring; and authentication systems should integrate with existing State solutions.

In the event of a security breach, the Vendor must follow the procedures outlined as part of DoIT Incident Handling and Response policy effective as of the Effective Date and Exhibit I ("Breach of PII"). Any costs associated with the resolution of such security breach including, but not limited to, a forensic audit acceptable to the State, call centers, penalties, credit monitoring and insurance, and all notifications that must be issued as required by law, and shall be paid by and are the responsibility of the Vendor.