Information Technology (IT) Supplemental

This supplemental contains additional requirements under Section 2 of the solicitation.

1.1 Deliverables

Not applicable to this procurement

1.2 Optional Features or Services, Future Work

Not applicable to this procurement

1.3 Contractor-Supplied Hardware, Software, and Materials

A. The Contractor is responsible for the acquisition and operation of all hardware, software and network support related to the services being provided. However, the State has the right to purchase hardware, software, and hosting services from a source other than the Contractor if it is determined to be in the best interest of the State based on value and price.

B. Cloud based applications shall be accessible from various client devices through a thin client interface such as a Web browser or a program interface.

C. For projects that require Contractor supplied materials, the costs for the materials shall be passed through to the State with no mark-up by the Contractor.

1.4 Product Requirements

A. Open-source software may be proposed; however, operational support for the proposed software must also be proposed. Operational support shall include maintenance and updating of code to address software dependencies, software updates and security vulnerabilities.

B. Bidders/Offerors proposing to resell services of another entity must be authorized by such other entity.

C. No international storage or processing for State Data: As described in **Section 1.6.5.B 15., Data Protection and Controls**, Bidders/Offerors are advised that any processing or storage of data outside of the continental U.S. is strictly prohibited.

D. Consistent expiration dates: Licenses/services purchased under the Contract shall expire coterminously with the earliest licenses/services delivered. As appropriate, charges shall be prorated.

E. Any terms of use or other agreement applicable to the Bidder's/Offeror's proposed services must be contained in the Bidder's/Offeror's Technical Proposal. The State is not subject to any terms of use or other agreement applicable to the Bidder's/Offeror's proposed services unless the same are explicitly agreed to by the State during the Proposal evaluation process.

F. The State does not recognize and is not subject to any auto-renewal of services provision that may be contained or provided for in any Contractor agreements.

1.5 Maintenance

Maintenance and support, and Contractor's ongoing maintenance and support obligations, are defined as follows:

A. Maintenance commences at the Go- - Live Date. Billing for such maintenance and support shall commence after Go-Live.

B. Software maintenance includes all software changes, modifications, updates, patching, bug fixes, vulnerability fixes, and enhancements applicable to all system modules licensed without further charge to all licensed users maintaining a renewable software support contract.

C. Maintenance shall be provided for superseded releases and back releases still in use by the State.

D. For the first year and all subsequent Contract years, the following services shall be provided for the current version:

1) Error Correction. Upon notice by the State of a problem with the Software (which problem can be verified), reasonable efforts to correct or provide a working solution for the problem.

2) Material Defects. Contractor shall notify the State of any material errors or defects in the Deliverables known, or made known to Contractor from any source during the life of the Contract that could cause the production of inaccurate or otherwise materially incorrect results. The Contractor shall initiate actions as may be commercially necessary or proper to effect corrections of any such errors or defects.

3) Vulnerabilities. Contractor shall notify the State of any vulnerabilities of which it is or becomes aware, that could allow unauthorized access, disclosure, or modification of data, applications, or systems. The Contractor shall fix all vulnerabilities in accordance with the State's IT Security Manual in Reference B of the Table in Section 1.2.

4) Updates. Contractor will provide to the State at no additional charge all new releases and bug fixes (collectively referred to as "Updates") for any software Deliverable developed or published by the Contractor and made available to its other customers.

E. Activity reporting

Information Technology (IT) Supplemental

1.5.1 Technical Support

A. “Technical Support” means Contractor-provided assistance for the services or Solution furnished under the Contract, after initial end-user support confirms a technical issue that requires additional troubleshooting capabilities; sometimes referenced as Tier II – IV support.

B. Technical Support shall be available during Normal State Business Hours.

C. The State shall be able to contact a Technical Support team member 24 hours per day, 7 days per week, 365 days per year, based on the Tier defined in the Service Level Agreement.

D. Contractor Personnel providing technical support shall be familiar with the State’s account (i.e., calls shall not be sent to a general queue).

E. Contractor shall return calls for service of emergency system issues within one (1) hour or per the Service Level Agreement.

F. Calls for non-emergency IT service requests will be returned within three (3) hours or immediately the following day if after Normal State Business Hours.

G. The State shall be provided with information on software problems encountered at other locations, along with the solution to those problems, when relevant to State software.

H. User support (Help Desk)

1) Contractor shall furnish Help Desk services for

2) Help Desk services are available during Normal State Business Hours.

3) Contractor shall utilize a help desk ticketing system to record and track all help desk calls. The ticketing system shall record with a date and timestamp when the ticket was opened and when the ticket was closed as well as which personnel at the organization handled and resolved the ticket with a full audit trail of activity as well as which personnel at the organization handled and resolved the ticket with a full audit trail of activity.

1.5.2 Backup

The Contractor shall:

A. Provide backups of the State created data libraries, and State user created data on a regular basis.. Contractor shall describe backup services offered.

B. Meet the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) metrics defined in Section 1.6 Service Level Agreement.

C. Backups shall consist of at least:

1) Incremental daily backups, retained for one (1) month,

2) Full weekly backups, retained for three (3) months, and

3) Last weekly backup for each month maintained for two (2) years;

D. Maintain one annual backup for at least **10** years;

E. Send the weekly backup electronically to a facility designated by the State;

F. Encrypt the backups using a pre-shared key;

G. Perform a backup recovery at least semi-annually; and

H. Provide on demand support for the State's recovery of a backup set.

1.6 Service Level Agreement (SLA)

1.6.1 Definitions

A. A "Problem" is defined as any situation or issue or breach or potential breach related to the system operation and is not an enhancement request that is reported to the Contractor. The Contractor shall utilize a tracking system, e.g. help desk ticket system, to track, update, and report the status of all reported problems.

B. "Problem resolution time" is defined as the period of time from when the issue was reported to the Contractor to when it is resolved to the satisfaction of the State.

C. Monthly Charges: for purposes of SLA credit calculation, Monthly Charges are defined as the charges set forth in **Attachment B, Financial Proposal Form**, invoiced during the month of the Problem for the monthly fixed services, or, in the event of annual billing, 1/12 of the annual invoice amount **Financial Proposal Form**.

1.6.2 SLA Requirements

The Contractor shall:

A. Be responsible for complying with all performance measurements, and shall also ensure compliance by all subcontractors.

B. Meet the Problem Response Time and the Problem Resolution Time requirements as defined in **Section 1.6.7.**

C. Provide a monthly report to monitor and detail response times and resolution times.

D. Log Problems into the Contractor-supplied tracking tool or other help desk software and assign an initial severity level (i.e., Emergency, High, Normal, or Low as defined in **Section 1.6.8**).

E. Respond to and update all Problems, including recording when a Problem is resolved and its resolution. Appropriate State of Maryland personnel shall be notified when a Problem is resolved.

F. The State of Maryland shall make the final determination regarding Problem severity as defined in **Section 1.6.8**.

G. Contractor shall review any Problem with the State of Maryland to establish the remediation plan and relevant target dates.

1.6.3 SLA Effective Date (SLA Activation Date)

SLAs set forth herein shall be in effect beginning with the commencement of services as of the completion of the Transition-In Period.

1.6.4 Service Level Reporting

A. Contractor performance will be monitored by the State of Maryland.

B. The Contractor shall, upon request, provide summarized SLA performance and detailed monthly reports evidencing the attained level for each SLA. All reports shall highlight any SLA performance criteria that did not meet the compliance requirement designated in the SLA provided in **Section 2.6.7**. The Contractor shall provide an explanation of why any SLA was not met. For any problems not resolved the Contractor shall provide an explanation of how and when it will be met in the future.

C. Reports shall be delivered via e-mail to the Contract Monitor by the 15th of the following month.

1.6.5 SLA Service Credits

Beginning on the SLA Activation Date, for any performance measurement not met during the monthly reporting period, the SLA credit for that individual measurement shall be applied to the Monthly Charges.

Service credits will be cumulative for each missed service requirement. The State, at its option for amounts due to the State as service credits, may deduct such from any money payable to the Contractor or may bill the Contractor as a separate item. In the event of a catastrophic failure affecting all services , in addition to all other rights and remedies available to the State, all affected SLAs shall be credited to the State.

Example: If the Monthly Charges were $100,000 and one SLA were missed, with an applicable 4% credit, the credit to the monthly invoice would be $4,000, and the State would pay a net Monthly Charge of $96,000.

The parties agree that any assessment of service credits shall be construed and treated by the parties not as imposing a penalty upon the Contractor, but as compensation to the State for the Contractor's failure to satisfy its service level obligations.

1.6.6 Root Cause Analysis

The State has the right, at its sole discretion, to direct the Contractor to perform and deliver a root cause analysis in connection with any SLA measurement that yields an SLA credit. Such root cause analysis shall be provided within 30 days of the request.

In addition, for each 'Emergency' or 'High' priority Problem, the affected parties will perform a root cause analysis and institute a process of problem management to prevent recurrence of the issue.

1.6.7 Service Level Measurements Table (System performance)

Offeror shall complete the table below with its proposed service level metrics and SLA credits.

No.	Service Requirement	Measurement	Service Level Agreement	SLA Credit
1	Problem Response Time Emergency (example)	(Example) Average Response Time for High Priority Problems.	98% <15 minutes (example)	1%

1.6.8 Problem Response Definitions and Times

Below are the State's basic expectations without metrics or SLA credits.

Service Priority	**Response Time**	**Resolution Time**	**Response Availability**	**Work Outage**	**Users Affected**

Emergency	Less than 15 minutes	Within 2 hours of first report	24 hours per day, seven days per week	Major portions of the System are inaccessible Systems or users are unable to work, or to perform some portion of their job.	Users or internal System functionalities are impaired. To include <<Claimants and Employers>>
High	Less than 30 minutes	Within 4 hours after first report	24 hours per day, seven days per week	Major portions of the System are inaccessible Systems or users are unable to work, or to perform some portion of their job.	Affects the majority of users to include public facing users <<Claimants & Employers>> Affects high profile users (i.e. executive management)
Normal	Within 2 hours	Within 1 day (24 hours) after the first report. If the outage is not resolved a resolution plan must be in place.	Mon-Fri, 7AM-7PM	Specific non-critical features are not operating as specified Systems or users are unable to perform a small portion of their job, but are able to complete most tasks.	Affects a number of users

Low	Within 2 hours	Within 3 days (72 hours) after the first report. If the outage is not resolved a resolution plan must be in place.	Mon-Fri, 7AM-7PM	Lower priority features that can be done manually are not operating as specified Often a request for service with ample lead time.	Affects a number of users

1.7 Required Project Policies, Guidelines and Methodologies

The Contractor must comply with all applicable laws, regulations, policies, standards and guidelines affecting Information Technology projects, which may be created or changed periodically. These include, but are not limited to:

Reference	Regulations, Policies, Guidelines and Methodologies
A	The State of Maryland System Development Life Cycle (SDLC) methodology https://doit.maryland.gov/SDLC/Pages/agile-sdlc.aspx
B	The State of Maryland Information Technology Security Policy and Standards at: https://doit.maryland.gov/policies/Pages/ContractPolicies.aspx
C	The State of Maryland Information Technology Non-Visual Standards at: https://doit.maryland.gov/policies/Pages/nva.asp
D	The State of Maryland Information Technology Project Oversight at: https://doit.maryland.gov/epmo/Pages/ProjectOversight.aspx
E	The Contractor shall follow project management methodologies consistent with the most recent edition of the Project Management Institute's Project Management Body of Knowledge Guide.
F	Hardware and Software hardening procedures by Center for Internet Security (CIS) guides https://www.cisecurity.org/ or Security Requirements Guides (SRG) http://www.nist.gov
G	Federal Information Processing Standards (FIPS), "Security Requirements for Cryptographic Modules", FIPS PUB 140-3:

Reference	Regulations, Policies, Guidelines and Methodologies
	https://csrc.nist.gov/publications/detail/fips/140/3/final https://csrc.nist.gov/Projects/cryptographic-module-validation-program/fips-140-3-standards
H	Purchasing and Recycling Electronic Products https://dgs.maryland.gov/Pages/GreenPurchasing/Resources/Electronics.aspx

1.8 Disaster Recovery and Data

1.8.1 Redundancy, Data Backup and Disaster Recovery

a) Unless specified otherwise, throughout the Contract term, the Contractor shall maintain or cause to be maintained disaster avoidance procedures designed to safeguard State data and other confidential information, Contractor’s processing capability and the availability of hosted services. Any force majeure provisions of the Contract do not limit the Contractor’s obligations under this provision.

b) The Contractor shall have robust contingency and disaster recovery (DR) plans in place to ensure that the services provided under the Contract will be maintained in the event of disruption to the Contractor/subcontractor’s operations (including, but not limited to, disruption to information technology systems), however caused.

   1) The Contractor shall furnish a DR site.

   2) The DR site shall be at least 100 miles from the primary operations site, and have the capacity to take over complete production volume in case the primary site becomes unresponsive.

c) The contingency and DR plans must be designed to ensure that services under the Contract are restored after a disruption within 24 hours from notification, with a recovery point objective of one hour or less prior to the outage in order to avoid unacceptable consequences due to the unavailability of services.

d) The Contractor shall test the contingency/DR plans at least twice annually to identify any changes that need to be made to the plan(s) to ensure a minimum interruption of service. Coordination shall be made with the State to ensure limited system downtime when testing is conducted. At least one annual test shall include backup media restoration and failover/fallback operations at the DR location. The Contractor shall send the Contract Monitor a notice of completion following completion of DR testing.

e) Such contingency and DR plans shall be available for the State to inspect and practically test at any reasonable time, and subject to regular updating, revising, and testing throughout the term of the Contract.

1.8.2 Data Export/Import

a) The Contractor shall, at no additional cost or charge to the State, in an industry standard/non-proprietary format:

1) perform a full or partial import/export of State data within 24 hours of a request; or

2) provide to the State the ability to import/export data at will and provide the State with any access and instructions which are needed for the State to import or export data.

b) Any import or export shall be in a secure format per the Security Requirements.

1.8.3 Data Ownership and Access

As set forth in the Contract, data, databases and derived data products created, collected, manipulated, or directly purchased as part of the solicitation are the property of the State. The purchasing State agency is considered the custodian of all State data. The use, access, and distribution of all data shall comply with the requirements of the **Data Use Agreement (Attachment Y)**.

The Contractor may not access State data other than as necessary to perform the services under this Contract.

The Contractor shall limit access to and use of State data to Contractor Personnel whose responsibilities require such access or use and shall train such Contractor Personnel on the confidentiality obligations set forth herein.

At no time shall any data or processes – that either belong to or are intended for the use of the State or its officers, agents or employees – be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the State.

The Contractor shall not use any information collected in connection with the services furnished under the Contract for any purpose other than fulfilling such services.

Provisions in **Sections 1.8.1 - 1.8.3** shall survive expiration or termination of the Contract. Additionally, the Contractor shall flow down the provisions of **Sections 1.8.1 - 1.8.3** (or the substance thereof) in all subcontracts.

1.9 Security Requirements

1.9.1 Employee Identification

This section is inapplicable to this RFP

1.92 Security Clearance / Criminal Background Check

A criminal background check is not required for Contractor Personnel.

A security clearance is not required for Contractor Personnel.

Contractor Personnel that would have **access to systems supporting the State or to State data** who have been **convicted of a felony** or **convicted of a crime involving telecommunications and**

electronics or **convicted within the past five (5) years of a misdemeanor from the above list of crimes** shall not be permitted to work on the Contract.

1.9.3 On-Site Security Requirement(s)

This section is inapplicable to this RFP.

1.9.4 Information Technology Security

A. Contractors shall comply with and adhere to the State IT Security Manual, Policies and Standards. These policies may be revised from time to time and the Contractor shall comply with all such revisions. Updated and revised versions of the State IT Policy and Standards are available online at: Policies, Standards, and Guidelines.

B. The Contractor shall not connect any of its own equipment to a State LAN/WAN without prior written approval by the State as directed and coordinated with the Contract Monitor.

The Contractor shall:

1) For IT Security Policies and Standards that are no covered by the State IT Security Manual, the Contract shall Implement administrative, physical, and technical safeguards to protect State data that are no less rigorous than accepted industry best practices for information security such as those listed below (see **Section 1.6.5**)

2) Ensure that all such safeguards, including the manner in which State data is collected, accessed, used, stored, processed, disposed of and disclosed, comply with applicable data protection and privacy laws as well as the terms and conditions of the Contract; and

3) Ensure compliance with all applicable federal, State, and local laws, rules and regulations concerning security of Information Systems and Information Technology.

1.9.5. Data Protection and Controls

A. Contractor shall ensure a secure environment for all State data and any hardware and software (including but not limited to servers, network and data components) provided or used in connection with the performance of the Contract according to a written security policy (“Security Plan”) no less rigorous than that of the State and using best practices that comply with an accepted industry standard, such as the NIST cybersecurity framework.

1) The Security Plan shall detail the steps and processes employed by the Contractor as well as the features and characteristics which will ensure compliance with the security requirements of the Contract. Such Security Plan shall be provided to the State for its review with solicitation response. If awarded a contract, the Security Plan shall be provided on an annual basis or whenever updates are made.

2) The Contractor shall supply a copy of such policy to the State for validation, with any appropriate updates, on an annual basis.

3) If any Security Plan information, including procedures, are different based on a Task Order, Contractor shall furnish such differences to the respective TO Manager.

B. To ensure appropriate data protection safeguards are in place, the Contractor shall implement and maintain the following controls during the Contract Term (the Contractor may augment this list with additional controls):

1) Establish separate production, test, and training environments for systems supporting the services provided under the Contract and ensure that production data is not utilized in test or training environment(s).

2) Apply hardware and software hardening procedures as recommended by Center for Internet Security (CIS) guides, Security Technical Implementation Guides (STIG), or similar industry best practices to reduce the systems' surface of vulnerability, eliminating as many security risks as possible and documenting what is not feasible or not performed according to best practices. Any hardening practices not implemented shall be documented with a plan of action and milestones including any compensating control. These procedures may include but are not limited to removal of unnecessary software, disabling or removing unnecessary services, removal of unnecessary usernames or logins, and the deactivation of unneeded features in the Contractor's system configuration files.

3) Ensure that State data is not commingled with non-State data through the proper application of compartmentalization Security Measures.

4) Apply data encryption to protect Sensitive Data at all times, including in transit, at rest, and also when archived for backup purposes. Unless otherwise directed, the Contractor is responsible for the encryption of all Sensitive Data.

5) Apply data encryption to all Contractor managed or controlled State data when the data is in transit over untrusted network segments.

6) Utilize encryption algorithms for encrypting data that comply with current Federal Information Processing Standards (FIPS), "Security Requirements for Cryptographic Modules."

7) Enable appropriate logging parameters to monitor user access activities, authorized and failed access attempts, system exceptions, and critical information security events as recommended by the operating system and application manufacturers and information security standards, including the Maryland Department of Information Technology's Information Security Manual.

8) Retain the aforementioned logs and review them at least daily to identify suspicious or questionable activity for investigation and documentation as to their cause and remediation, if required. The State shall have the right to inspect the logs and the Contractor or subcontractor's performance to confirm the

effectiveness of these measures for the services being provided under the Contract.

9) Ensure system and network environments are separated by properly configured and updated layer seven firewalls.

10) Restrict network connections between trusted and untrusted networks by physically or logically isolating systems from unsolicited and unauthenticated network traffic.

11) By default "deny all" and only allow access by exception.

12) Review, at least annually and after changes, the aforementioned network connections, documenting and confirming the business justification for the use of all service, protocols, and ports allowed, including the rationale or compensating controls implemented for those protocols considered insecure but necessary.

13) Perform regular internal and external vulnerability testing of operating system, applications, and all network devices utilized in this Contract. Such testing is expected to identify outdated software versions; missing software patches; device or software misconfigurations; and to validate compliance with or deviations from the security policies applicable to the Contract. Contractor shall evaluate all identified vulnerabilities for potential adverse effect on security and integrity and remediate the vulnerability no later than 30 days following the earlier of vulnerability's identification or public disclosure, or document why remediation action is unnecessary or unsuitable. The State shall have the right to conduct vulnerability testing and inspect the results of similar Contractor performed vulnerability testing to confirm the effectiveness of these measures for the services being provided under the Contract.

14) Enforce strong user authentication and password control measures to minimize the opportunity for unauthorized access through compromise of the user access controls. At a minimum, the implemented measures should be consistent with the most current Maryland Department of Information Technology's Information Security Policies, including specific requirements for password length, complexity, history, and account lockout.

15) Ensure State data is not processed, transferred, or stored outside of the continental United States ("U.S."). The Contractor shall provide its services to the State and the State's end users solely from data centers in the U.S. Unless granted an exception in writing by the State, the Contractor shall not allow Contractor Personnel to store State data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. Contractor Personnel may access State data remotely only as required to provide technical support and with the prior approval of the State.

16) Ensure Contractor Personnel shall not connect any of their own equipment to State IT assets without prior written approval by the State. Any such approval may be revoked, rescinded, or curtailed at any time for any reason. The Contractor shall coordinate requests for approval with the Contract Monitor and is subject to all State approval processes as they may be revised from time to time.

17) Ensure that anti-virus and anti-malware software is installed and maintained on all systems and end points supporting the services provided under the Contract; that the anti-virus and anti-malware software is automatically updated; and that the software is configured to actively scan and detect threats to the system for remediation. The Contractor shall perform routine weekly vulnerability scans and take corrective actions for any findings.

18) Conduct regular external vulnerability testing designed to examine the service provider's security profile from the Internet without benefit of access to internal systems and networks behind the external security perimeter. Evaluate all identified vulnerabilities on Internet-facing devices for potential adverse effect on the service's security and integrity and remediate the vulnerability promptly or document why remediation action is unnecessary or unsuitable. The State shall have the right to inspect the Contractor's processes and the performance of vulnerability testing to confirm the effectiveness of these measures for the services being provided under the Contract.

1.9.6 Security Logs and Reports Access For any cloud hosted, or Contractor, or third party hosted solution, the Contractor shall provide security logs and reports to the State in a mutually agreeable format.

a) Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all State data, systems, and software data, systems, and software related to the Contract.

1.9.7 Payment Card Industry Compliance

This section is not applicable to this RFP.

1.9.8 Security Incident Response

A. The Contractor shall notify the State when any Contractor system that may access, process, or store State data or State systems experiences a Security Incident or a Data Breach as follows:

1) notify the State within twenty-four (24) hours of the discovery of a Security Incident by providing notice via written or electronic correspondence to the Contract Monitor, State Chief Information Security Officer and Maryland Security Operations Center (MD-SOC);

2) notify the State within seventy-two (72) hours if there is a threat to Contractor's solution as it pertains to the use, disclosure, and security of State data; and

3) provide written notice to the State within one (1) Business Day after Contractor's discovery of unauthorized use or disclosure of State data and thereafter all information the State requests concerning such unauthorized use or disclosure.

B. Contractor's notice shall identify:

1) the nature of the unauthorized use or disclosure;

2) the State data used or disclosed,

3) who made the unauthorized use or received the unauthorized disclosure;

4) what the Contractor has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure; and

5) what corrective action the Contractor has taken or shall take to prevent future similar unauthorized use or disclosure.

6) The Contractor shall provide such other information, including a written report, as reasonably requested by the State.

C. Discussing Security Incidents with the State should be handled on an urgent as-needed basis, as part of Contractor communication and mitigation processes as mutually agreed upon, defined by law or contained in the Contract. The Contractor shall obtain approval from the State prior to communicating with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise.

D. The Contractor shall comply with all applicable system security breach laws.

1.9.9 Data Breach Responsibilities

A. If the Contractor reasonably believes or has actual knowledge of a Data Breach, the Contractor shall, unless otherwise directed:

1) Notify the appropriate State-identified contact within 24 hours by telephone and email to the Maryland Security Operations Center (MD-SOC) in accordance with the agreed upon security plan or security procedures unless a shorter time is required by applicable law;

2) Cooperate with the State to investigate and resolve the data breach;

3) Promptly implement commercially reasonable remedial measures to remedy the Data Breach; and

4) Document responsive actions taken related to the Data Breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services.

B. With respect to State data within the possession or control of the Contractor, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by State law; (3) a credit monitoring service required by State or federal law; (4) a website or a toll-free number and call center for affected individuals required by State law; and (5) complete all corrective actions as reasonably determined by Contractor based on root cause; all [(1) through (5)] subject to the Contract's limitation of liability.

C. The public disclosure of a cybersecurity incident shall be pursuant to Guidelines for the Public Disclosure of Cybersecurity Incidents or any successor thereto..

1.9.10 The State shall, at its discretion, have the right to review and assess the Contractor's compliance to the security requirements and standards defined in the Contract.

1.9.12 Provisions in **Sections 1.9.1 – 1.9.9** shall survive expiration or termination of the Contract. Additionally, the Contractor shall flow down the provisions of **Sections 1.9.4 - 1.9.9** (or the substance thereof) in all subcontracts.

1.10 SOC 2 Type 2 Audit Report

A SOC 2 Type 2 Audit Report applies to the Contract. The Contractor shall cause an SOC 2 Type 2 audit report to be conducted annually covering the previous 12- month period of the contract.

Such audits shall be performed in accordance with audit guidance: Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2) as published by the American Institute of Certified Public Accountants (AICPA) and as updated from time to time.

a) The Contractor shall provide to the Contract Monitor, within thirty (30) calendar days of the issuance of the final SOC 2 Type 2 Audit Report, the audit results and a documented corrective action plan that addresses each audit finding or exception contained in the SOC 2 Type 2 Audit Report, identifying in detail the remedial action to be taken by the Contractor along with the date(s) when each remedial action is to be implemented. The scope of the SOC 2 Type 2 Audit Report shall include work performed by any subcontractors that handles, store or process Sensitive Data or are responsible for security controls and provide essential support to the TO Contractor for or essential support to the Information Functions and Processes for the services provided to the State under the Contract. The Contractor shall ensure the audit includes all such subcontractors operating in performance of the Contract or, in the case the subcontractor's services are covered by a separate SOC 2 Type 2 Audit, that separate SOC 2 Type 2 Audit reports are obtained from all subcontractors and submitted to the Contract Monitor via the Contractor's primary point of contact.

b) All SOC 2 Type 2 Audit Reports shall be submitted to the Contract Monitor as specified in Section a above. The initial SOC 2 Type 2 Audit shall be completed within a timeframe to be specified by the State. The audit period covered by the initial SOC 2 Type 2 Audit shall start with the Contract Effective Date unless otherwise agreed to in writing by the Contract Monitor. All subsequent SOC 2 Type 2 Audits after this initial audit shall be performed at a minimum on an annual basis throughout the Term of the Contract, and shall cover a 12-month audit period or such portion of the year that the Contractor furnished services.

c) The SOC 2 Type 2 Audit shall report on the suitability of the design and operating effectiveness of controls over the Information Functions and Processes to meet the requirements of the Contract, including the Security Requirements identified in **Section 1.6**, relevant to the trust services criteria identified in Section 1.7.1: as defined in the aforementioned Guidance.

d) The audit scope of each year's SOC 2 Type 2 Audit Report may need to be adjusted (including the inclusion or omission of the relevant trust services criteria of Security, Availability, Processing Integrity, Confidentiality, and Privacy) to accommodate any changes to the environment since the last SOC 2 Type 2 Audit Report. Such changes may include but are not limited to the addition of Information Functions and/or Processes through modifications to the Contract or due to changes in Information Technology or the operational infrastructure. The Contractor shall ensure that the audit scope of each year's SOC 2 Type 2 Audit Report engagement shall accommodate these changes by including in the SOC 2 Type 2 Audit Report all appropriate controls related to the current environment supporting the Information Functions and/or Processes, including those controls required by the Contract.

e) The scope of the SOC 2 Type 2 Audit Report shall include work performed by any subcontractors that handle, store or process Sensitive Data and provide essential support to the TO Contractor for or essential support to the Information Functions and Processes for the services provided to the State under the Contract. The Contractor shall ensure the audit includes all such subcontractors operating in performance of the Contract or shall ensure their subcontractors obtain a SOC 2 Type 2 Audit Report as described in this Section.

f) All SOC 2 Type 2 Audits shall be completed at the Contractor's expense, including those of the Contractor, shall be performed at no additional expense to the State.

g) If the Contractor fails during the Contract term to obtain an annual SOC 2 Type 2 Audit Report by the date specified in **Section 1.7.2.A**, the State shall have the right to retain an independent audit firm to perform an audit engagement to issue of a SOC 2 Type 2 Audit Report of the Information Functions and/or Processes utilized or provided by the Contractor and under the Contract. The Contractor agrees to allow the independent audit firm to access its facility/ies for purposes of conducting this audit engagement(s), and will provide the necessary support and cooperation to the independent audit firm in the performance of the engagement.that is required to perform the audit engagement of the SOC 2 Type 2 Audit Report. The State, at its option, will invoice the Contractor for the expense of the SOC 2 Type 2 Audit Report(s), or deduct the cost from future payments to the Contractor.

h) Provisions in **Section 1.7.1-2** shall survive expiration or termination of the Contract. Additionally, the Contractor shall flow down the provisions of **Section 1.7.1-2** (or the substance thereof) in all subcontracts.

1.11 Nonvisual Access

1.11.1 The bidder or offeror warrants that the information technology offered under this bid or proposal (1) provides equivalent access for effective use by both visual and non-visual means consistent with the standards of § 508 of the federal Rehabilitation Act of 1973 and Code of Maryland Regulations 14.33.02; (2) provides an individual with disabilities with non-visual access in a way that is fully and equally accessible to and independently usable by the individual with disabilities so that the individual is able to acquire the same information, engage in the same interactions, and enjoy the same services as users without disabilities, with substantially equivalent ease of use; (3) will present information, including prompts used for interactive communications, in formats intended for both visual and nonvisual use; (4) if intended for use in a network, can be integrated into networks for obtaining, retrieving, and disseminating information used by individuals who are not blind or visually impaired; and (5) is available, whenever possible, without modification for compatibility with software and hardware for nonvisual access. The bidder or offeror further warrants that the cost, if any, of modifying the information technology for compatibility with software and hardware used for nonvisual access will not increase the cost of the information technology by more than 15 percent.

1.11.2 If the information technology procured under this solicitation does not meet the non-visual access standards set forth in the Code of Maryland Regulations 14.33.02, the State will notify the bidder or offeror in writing that the bidder or offeror, at its own expense, has 12 months after the date of the notification to modify the information technology in order to meet the non-visual access standards. If the bidder or offeror fails to modify the information technology to meet the nonvisual access standards within 12 months after the date of the notification, the bidder or offeror may be subject to a civil penalty of a fine not exceeding $5,000 for a first offense, and a fine not exceeding $10,000 for a subsequent offense.

1.11.3 The bidder or offeror shall indemnify, defend and hold harmless the State for liability resulting from the use of information technology that does not meet the applicable non-visual access standards.

1.11.4 For purposes of this provision, the phrase ‘equivalent access' means the ability to receive, use, and manipulate information and operate controls necessary to access and use information technology by nonvisual means. Examples of equivalent access include keyboard controls used for input and synthesized speech, Braille, or other audible or tactile means used for output.

1.11.5 Prior to any IT solution being pushed to production or going live, the Contractor shall provide DoIT with a comprehensive accessibility audit report demonstrating conformance with Web Content Accessibility Guidelines (WCAG) 2.1 that includes the results from automated and manual testing tools, such as the use of Job Access With Speech (JAWS), VoiceOver and Non-Visual Desktop Access (NVDA). The Contractor shall leverage a variety of commonly used accessibility testing procedures, including accessing the site through mainstream web browsers and evaluating accessibility, and performing comprehensive mobile accessibility testing using physical iOS and Android devices (not mobile emulators) to ensure the native accessibility features work with the respective IT solution. The report shall include a detailed timeline for the remediation of all identified accessibility issues. The Contractor may use an independent third-party accessibility testing company to conduct this work. Vendors may submit the comprehensive accessibility audit report through the Maryland OneStop system. Vendors who do not have an account should register for a OneStop account. Once registered, Vendors should go to Vendor Digital Accessibility Compliance Form to complete the form and attach the documents.

1.11.6 A testing and remediation plan must be provided for accessibility issues discovered with respect to information technology provided under the Contract. A testing and remediation plan must include items identified in paragraphs 4.33.3 and 4.33.3.1. If the Contractor will use any subcontractors as part of its plan, the Contractor must name the subcontractors in this plan. The Contractor shall remediate any accessibility issues identified in the accessibility audit, by DoIT, or any other state agency. The Contractor must conduct validation testing on all remediated accessibility issues and provide a copy of the validation testing results as an Excel or Word file. Vendors may submit the comprehensive testing and remediation plan, validation testing results through the Maryland OneStop system. Vendors who do not have an account should register for a OneStop account. Once registered, Vendors should go to Vendor Digital Accessibility Compliance Form to complete the form and attach the documents.

1.11.7 The Contractor agrees that the use of out-of-the-box or third-party source code does not waive a Contractor's obligation to ensure that a product complies with the requirements of this Section. Furthermore, the Contractor agrees that it bears sole responsibility to determine if any out-of-the-box source code or third-party code is accessible and to remediate any noncompliance with the State's nonvisual access requirements or cause any noncompliance to be remediated to ensure compliance with such requirements.

1.11.8 Ten percent (10%) of all invoiced amounts shall be held back from each payment (the "Retention Amount"), as retention money to guarantee Contractor's performance of the obligations set forth in this clause. Contractor may invoice the State for release of the Retention Amount upon DoIT's written approval to place the IT solution into production. DoIT reserves the right to use the Retention Amount to pay for third-party solutions to remediate WCAG 2.1 Level A and AA accessibility issues if the Contractor is unable to remediate after 90 days following launch of the website or application.

1.12 Mercury and Products That Contain Mercury

This solicitation does not include the procurement of products known to likely include mercury as a component.

1.13 Location of the Performance of Services Disclosure

This solicitation does not require a Location of the Performance of Services Disclosure.

1.14 HIPAA - Business Associate Agreement

A HIPAA Business Associate Agreement is not required for this procurement.

1.15 Additional Clauses

The Contractor is subject to the requirements in this section and shall flow down the provisions of **Sections 1.15.1 – 1.15.5** (or the substance thereof) in all subcontracts.

1.15.5 The State of Maryland's Commitment to Purchasing Environmentally Preferred Products and Services (EPPs)

Maryland's State Finance & Procurement Article §14-410 defines environmentally preferable purchasing as "the procurement or acquisition of goods and services that have a lesser or reduced effect on human health and the environment when compared with competing goods or services that serve the same purpose." Accordingly, Bidders/Offerors are strongly encouraged to offer EPPs to fulfill this contract, to the greatest extent practicable.

Change Control and Advance Notice

A. Unless otherwise specified in an applicable Service Level Agreement, the Contractor shall give seven (7) days advance notice to the State of any upgrades or modifications that may impact service availability and performance.

B. Contractor may not modify the functionality or features of any SaaS provided hereunder if such modification materially degrades the functionality of the SaaS.

1.16 Considerations for IT Technical Proposals

1.16.1 As part of the Offeror's Technical Proposal under the **Offeror Technical Response to RFP Requirements and Proposed Work Plan**, submit under **TAB F** the following information:

1) The Offeror shall provide a Voluntary Product Accessibility Template (VPAT) or an Accessibility Conformance Report (ACR) for any pre-existing digital technology, software, or source code proposed to be provided under the Contract containing a comprehensive analysis of the Offeror's conformance to accessibility standards in Code of Maryland Regulations 14.33.02 (See RFP §4.33). The completed VPAT (VPAT 2.5 WCAG or most recent) must adhere to the current published standards. Failure to supply a VPAT or ACR for any pre-existing coded solution may result in the Offeror's Proposal being deemed not reasonably susceptible for award.[1] [2]
2) The Offeror shall provide a Backup solution/ strategy recommendation as part of its Proposal.
3) Disaster Recovery and Security Model description - For hosted services, the Offeror shall include its DR strategy, and for on premise, a description of a recommended DR strategy.
4) The Offeror shall include a deliverable description and schedule describing the proposed Deliverables as mapped to the State SDLC and the **Deliverables Summary Table** in **Section 1.1.4**. The schedule shall also detail proposed submission due date/frequency of each recommended Deliverable.
5) The Offeror shall include an SLA as identified in **Section 1.6 of this Supplemental**, including service level metrics offered and a description how the metrics are measured, any SLA credits should the service level metrics not be met, and how the State can verify the service level. The Offeror shall describe how service level performance is reported to the State. 6) Description of technical risk of migrating from the existing system.
7) Product Requirements

a) Offerors may propose open source software; however, the Offeror must provide operational support for the proposed software.

b) Details for each offering: The Offeror shall provide the following information for each offering:

i) Offering Name;

ii) Offeror relationship with manufacturer (e.g., manufacturer, reseller, partner);

iii) Manufacturer;

iv) Short description of capability;

v) Version (and whether version updates are limited in any way);

vi) License type (e.g., user, CPU, node, transaction volume);

vii) Subscription term (e.g., annual);

viii) License restrictions, if any;

ix) Operational support offered (e.g., customer support, help desk, user manuals online or hardcopy), including description of multiple support levels (if offered), service level measures and reporting;

x) Continuity of operations and disaster recovery plans for providing service at 24/7/365 level;

xi) Ability of the offering to read and export data in existing State enterprise data stores. Offerors in their Proposals shall describe the interoperability of data that can be imported or exported from the Solution, including generating industry standard formats;

xii) Any processing or storage of data outside of the continental U.S;

xiii) Any limitations or constraints in the offering, including any terms or conditions, e.g., terms of service, ELA, AUP, professional services agreement, master agreement;

xiv) Compatibility with the State's existing single sign-on system, SecureAuth or other single sign-on approaches;

xv) APIs offered, and what type of content can be accessed and consumed;

xvi) Update / upgrade roadmap and procedures, to include: planned changes in the next 12 months, frequency of system update (updates to software applied) and process for updates/upgrades;

xvii) Frequency of updates to data services, including but not limited to, datasets provided as real-time feeds, and datasets updated on a regular basis (e.g., monthly, quarterly, annually, one-time);

xviii) What type of third party assessment (such as a SOC 2 Type II audit) is performed, the nature of the assessment (e.g., the trust services criteria and scope of assessment), and whether the results of the assessment pertinent to the State will be shared with the State. See also **Section 1.10**;

xix) Offeror shall describe its security model and procedures supporting handling of State data. If more than one level of service is offered, the Offeror shall describe such services. Include, at a minimum:

(1) procedures for and requirements for hiring staff (such as background checks),

(2) any non-disclosure agreement Contractor Personnel sign,

(3) whether the service is furnished out of the continental U.S. (see security requirements in **Section 1.9**),

(4) Certifications such as FedRAMP,

(5) Third party security auditing, including FISMA,

(6) Published Security Incident reporting policy, and

(7) Cybersecurity insurance maintained, if any.

1.16.3 As part of the Offeror’s Technical Proposal under the **Required Forms and Certifications**, in addition to the forms listed in **Table A**, submit under **TAB P** the following information:

1) Offerors shall furnish any and all agreements and terms and conditions the Offeror expects the State to sign or to be subject to in connection with or in order to use the Offeror’s services under this Contract. This includes physical copies of all agreements referenced and incorporated in primary documents, including but not limited to any software licensing agreement for any software proposed to be licensed to the State under this Contract (e.g., EULA, Enterprise License Agreements, Professional Service agreement, Master Agreement) and any AUP. The State does not agree to terms and conditions not provided in an Offeror’s Technical Proposal and no action of the State, including but not limited to the use of any such software, shall be deemed to constitute acceptance of any such terms and conditions. Failure to comply with this section renders any such agreement unenforceable against the State.
2) For each service, hardware or software proposed as furnished by a third-party entity, Offeror must identify the third-party provider and provide a letter of authorization or such other documentation demonstrating the authorization for such services. In the case of an open source license, authorization for the open source shall demonstrate compliance with the open source license.
3) A Letter of Authorization shall be on letterhead or through the provider’s e-mail. Further, each Letter of Authorization shall be less than twelve (12) months old and must provide the following information:

i) Third-party POC name and alternate for verification

ii) Third-party POC mailing address

iii) Third-party POC telephone number

iv) Third-party POC email address

v) If available, a Re-Seller Identifier