HOWARD COUNTY PUBLIC SCHOOLS
PURCHASING DEPARTMENT
10910 Clarksville Pike
Ellicott City, MD 21042
(410) 313-6644

ADDENDUM NO. 2
(Total Pages - 11)

October 4, 2021

Bid No. 064.21.B5

Amazon Web Services

Opening Date: October 12, 2021 Time: 3:00 P.M.

The following shall be incorporated into the captioned solicitation as though included in the original documents issued.

The Board of Education authorizes the following changes, clarifications and or attachments to the solicitation documents; however, such changes shall not relieve the firm of their responsibilities as otherwise required by the solicitation documents.

The bid due date has been extended from **October 5, 2021** at 3:00 P.M to **October 12, 2021** at 3:00 P.M.

Please add the attached six pages titled **Network/Data Security** as 3.4.5 Network/ Data Security to the original solicitation.

The attached four pages title **ATTACHMENT B REVISED INSURANCE REQUIREMENTS** replaces PART III, SUBMITTAL AND CONTRACT REQUIREMENTS, 3.7 Insurance in its entirety.

Questions:

1. Can you elaborate on what size m5's the Dedicated Hosts are on?
   Response: M5.4xlarge 730 hr per month.
2. Are the following documents: Appendix F: Data Sharing Agreement and Exhibit B: Contractor Performance/Evaluation Scorecard to be signed and submitted and included with bid response? Or will they be signed post-award at contract negotiation/signing?
   Response: Appendix F should be signed and included. Exhibit B is will be done at renewal time.
3. Please confirm there is no Exhibit A.
   Response: There is no Exhibit A.
4. Does Howard County need migration assistance services to facilitate the move to AWS?
   Response: No, that should be included in the web hosting service.
5. We are register under SAM.gov as a 100% Minority owned small business. However, we are not registered under MDOT as a certified MBE.
   Do we still qualify enough to submit and be awarded this RFP?
   Response: Yes.

There are no other changes.

10/4/21

ATTACHMENT B
REVISED INSURANCE REQUIRMENTS

3.7 General Insurance Requirements

1.1 - The Vendor shall not commence any operations or services on behalf of the Board of Education of Howard County (the “Board”) under this Contract until the Vendor has obtained at the Vendor’s own expense all of the insurance as required hereunder and such insurance has been approved by the Board. Approval of insurance required of the Vendor will be granted only after submission to the Board of original certificates of insurance signed by authorized representatives of the insurers or, at the Board's request, certified copies of the required insurance policies.

1.2 - Insurance as required hereunder shall be in force throughout the term of the Contract. Original certificates signed by authorized representatives of the insurers or, at the Board's request, certified copies of insurance policies, evidencing that the required insurance is in effect, shall be maintained with the Board throughout the term of the Contract.

1.3 - The Vendor shall require all Subcontractors to maintain during the term of the Contract insurance to the same extent required of the Vendor herein unless any such requirement is expressly waived or amended by the Board in writing. The Vendor shall furnish Subcontractors' certificates of insurance to the Board immediately upon request.

1.4 - All insurance policies required hereunder shall be endorsed to provide that the policy is not subject to cancellation, non-renewal or material reduction in coverage until thirty (30) days prior written notice has been given to the Board

1.5 - No acceptance and/or approval of any insurance by the Board shall be construed as relieving or excusing the Vendor from any liability or obligation imposed upon the Vendor by the provisions of this Contract.

1.6 - If the Vendor does not meet the insurance requirements of this Contract, the Vendor shall forward a written request to the Board for a waiver in writing of the insurance requirement(s) not met or approval in writing of alternate insurance coverage, self-insurance, or group self-insurance arrangements. If the Board denies the request, the Vendor must comply with the insurance requirements as specified in this Contract.

1.7 - All required insurance coverages must be underwritten by insurers allowed to do business in the State of Maryland and acceptable to the Board. The insurers must also have a policyholders' rating of "A-" or better, and a financial size of "Class VII" or better in the latest evaluation by A. M. Best Company, unless the Board grants specific approval for an exception.

1.8 - Any deductibles or retentions in excess of $10,000 shall be disclosed by the Vendor, and are subject to the Board's written approval. Any deductible or retention amounts elected by the Vendor or imposed by the Vendor's insurer(s) shall be the sole responsibility of the Vendor.

1.9 - If the Board is damaged by the failure or neglect of the Vendor to purchase and maintain insurance as described and required herein, without so notifying the Board, then the Vendor shall bear all reasonable costs properly attributable thereto.

2 - Vendor's Insurance

2.1 - The Vendor shall purchase and maintain the following insurance coverages at not less than the limits specified below or required by law, whichever is greater:

ATTACHMENT B
REVISED INSURANCE REQUIRMENTS

2.1.1 - Commercial general liability insurance or its equivalent for bodily injury, personal injury and property damage including loss of use, with minimum limits of:

$	1,000,000	each occurrence;
$	1,000,000	personal and advertising injury;
$	2,000,000	general aggregate; and
$	1,000,000	products/completed operations aggregate.

This insurance shall include coverage for all of the following:

i. Liability arising from premises and operations;
ii. Liability arising from the actions of independent contractors; and
iii. Contractual liability including protection for the Vendor from bodily injury and property damage claims arising out of liability assumed under this Contract.

2.1.2 - Business auto liability insurance or its equivalent with a minimum limit of $1,000,000 per accident and including coverage for all of the following:

i. Liability arising out of the ownership, maintenance or use of any auto (if no owned autos, then hired and non-owned autos only); and
ii. Automobile contractual liability.

2.1.3 Errors or omissions liability (or Professional Liability) insurance or its equivalent for the Service Provider firm or organization and its employees with limits totaling at a minimum:

$	1,000,000	each person or claim; and
$	2,000,000	annual aggregate.

Cyber Liability for both first-party liability coverage and third-party liability coverage

$1,000,000	Network Security and Privacy Liability
$1,000,000	Media Communications / Brand or Reputation Liability
$1,000,000	Data Breach
$1,000,000	Data Loss /Interruption of Computer Operations
$1,000,000	Regulatory Response
$1,000,000	Systems Damage
$1,000,000	Threats or Extortion
$2,000,000	Annual Aggregate for all Cyber Liability

2.1.4 - <u>If the Vendor has any employees</u>, workers compensation insurance or its equivalent with statutory benefits as required by any state or Federal law, including standard "other states" coverage; employers liability insurance or its equivalent with minimum limits of:

$	100,000	each accident for bodily injury by accident;
$	100,000	each employee for bodily injury by disease; and
$	500,000	policy limit for bodily injury by disease.

2.1.6 - Professional liability (or errors or omissions liability) insurance or its equivalent with minimum limits of:

$ 1,000,000	each claim or wrongful act; and
$ 2,000,000	annual aggregate.

2.1.5 - If the Vendor is an individual or sole proprietor operating without workers compensation coverage, personal health insurance or its equivalent.

2.1.5 - Umbrella excess liability or excess liability insurance or its equivalent with minimum limits of:

$ 1,000,000	per occurrence;
$ 1,000,000	aggregate for other than products/completed operations and auto liability; and
$ 1,000,000	products/completed operations aggregate

and including all of the following coverages on the applicable schedule of underlying insurance:

i. Commercial general liability;
ii. Business auto liability; and
iii. Employers liability.

2.2 - The Board of Education of Howard County and its elected and appointed officials, officers, employees and authorized volunteers shall be named as additional insureds on the Vendor's commercial general liability insurance with respect to liability arising out of the services provided under this Contract by Vendor.

2.3 - Insurance or self-insurance provided to the Board and its elected and appointed officials, officers, employees and authorized volunteers under any Vendor's liability insurance or self-insurance required herein shall apply separately to each insured against whom claim is made or suit is brought, except with respect to the limits of insurance or self-insurance. (Any cross suits or cross liability exclusion shall be deleted from Vendor's liability insurance policies required herein.)

2.4 - Insurance or self-insurance provided to the Board and its elected and appointed officials, officers, employees and authorized volunteers as specified herein shall be primary, and any other insurance, self-insurance, coverage or indemnity available to the Board and Board's elected and appointed officials, officers, employees and authorized volunteers shall be excess of and non-contributory with insurance or self-insurance provided to the Board and its elected and appointed officials, officers, employees and authorized volunteers as specified herein.

2.5 - If any liability insurance purchased by the Vendor has been issued on a "claims made" basis, the Vendor must comply with the following additional conditions:

2.5.1 - The Vendor shall agree to provide certificates of insurance evidencing such claims made coverages for a period of one year after final payment by the Board for Vendor’s services under this Contract. Such certificates shall evidence a retroactive date no later than the earlier of the date of this Contract or the commencement of Vendor’s services under this Contract; or

ATTACHMENT B
REVISED INSURANCE REQUIRMENTS

2.5.2 - The Vendor shall purchase an extended (minimum one year) reporting period endorsement for each such "claims made" policy in force as of the date of final payment by the Board for Vendor's services under this Contract and evidence the purchase of this extended reporting period endorsement by means of a certificate of insurance or a copy of the endorsement itself. Such certificate or copy of the endorsement shall evidence a retroactive date no later than the earlier of the date of this Contract or the commencement of Vendor's services under this Contract.

Indemnification

To the fullest extent permitted by law, Vendor agrees to defend, indemnify, pay on behalf of, and save harmless the Board of Education of Howard County, its elected and appointed officials, agents, employees, and authorized volunteers against any and all claims, losses, damages, expenses, including reasonable attorneys' fees and all other costs connected therewith, cause of action or liability arising out of or connected to the services provided by Vendor under this Contract, provided that any such claim, loss, damage, expense, cause of action or liability is caused in whole or in part by any negligent act or omission of the Vendor or any of the Vendor's employees, agents, officials or volunteers or anyone for whose acts the Vendor may be liable, regardless of whether or not it is caused in part by a party indemnified hereunder. This obligation to indemnify, defend and hold Board of Education of Howard County, its elected and appointed officials, agents, employees, and authorized volunteers harmless shall survive the termination of this Agreement.

Waiver of Subrogation

To the fullest extent permitted by law, the Vendor and its invitees, employees, officials, volunteers, agents and representatives waive any right of recovery against the Board of Education of Howard County for any and all claims, liability, loss, damage, costs or expense (including attorneys' fees) arising out of the services provided by Vendor under this Contract. Such waiver shall apply regardless of the cause of origin of the injury, loss or damage, including the negligence of the Board and its elected and appointed officials, officers, volunteers, Vendors, agents and employees. The Vendor shall advise its insurers of the foregoing.

Acknowledgment of Vendor's Independent Contractor Status and No Coverage for Vendor under Board's Workers Compensation Coverage

Vendor hereby acknowledges its status as an independent contractor while performing services on behalf on the Board and that the Board's workers compensation coverage or self-insurance is not intended to and will not respond to cover any medical or indemnity loss arising out of injury to the Vendor or its employees during the Vendor's performance of services for the Board.

Damage to Property of the Vendor and its Invitees

To the fullest extent permitted by law, the Vendor shall be solely responsible for any loss or damage to property of the Vendor or its invitees, employees, officials, volunteers, agents and representatives while such property is on, at or adjacent to the premises of the Board.

3.4.5 Network/Data Security

(1) Information Technology Security

(A) Contractors shall comply with and adhere to all federal, State, and local laws, and the Board of Education of Howard County Maryland policies and regulations applicable to its activities. The Howard County Public School System (HCPSS) Board of Education sets policy consistent with state and federal laws governing public education. At the direction of the Board, the Superintendent and the school system administrative staff develop policies and administrative procedures to support the HCPSS Information Technology procurement process. The State of Maryland Information Technology (DoIT) IT Security Manual policies are leveraged to align with federal and state government standards and procedures published by the National Institute of Standards and Technology (NIST). 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: www.doit.maryland.gov – keyword: Security Policy.

The Contractor shall:

1) Implement administrative, physical, and technical safeguards to protect HCPSS data that are no less rigorous than accepted industry best practices for information security such as those outlined in this document;

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

3) The Contractor, and Contractor Personnel, shall (i) abide by all applicable federal, State and local laws, rules and regulations concerning security of Information Systems and Information Technology and (ii) comply with and adhere to the HCPSS and State IT Security Policy and Standards as each may be amended or revised from time to time. Updated and revised versions of the HCPSS Policy and Standards are available online at: https://policy.hcpss.org/. Updated and revised versions of the Maryland State IT Policy and Standards are available online at: www.doit.maryland.gov – keyword: Security Policy.

(1) Data Protection and Controls

(A) Contractor shall ensure a secure environment for all HCPSS 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 and shall apply or cause application of appropriate controls so as to maintain such a secure environment (“Security Best Practices”). Such Security Best Practices shall comply with an accepted industry standard, such as the NIST cybersecurity framework that the Maryland State IT Policy and Standards utilize.

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

1. Establish separate production, test, and/or training environments for systems supporting the services provided under the Contract and ensure that production data is not replicated in test or training environment(s) unless it has been previously anonymized or otherwise modified to protect the confidentiality of Sensitive Data elements. The Contractor shall ensure the appropriate separation of production and non-production environments by applying the data protection and control requirements listed in Section **(Data Protection and Controls).**

2. Apply hardware and software hardening procedures as recommended by Center for Internet Security (CIS) guides https://www.cisecurity.org/, Security Technical Implementation Guides (STIG) http://iase.disa.mil/Pages/index.aspx, 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 HCPSS data is not comingled with non-HCPSS 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. For all HCPSS data the Contractor manages or controls, data encryption shall be applied to such data in transit over untrusted networks.

6. Encryption algorithms which are utilized for encrypting data shall comply with current Federal Information Processing Standards (FIPS), "Security Requirements for Cryptographic Modules", FIPS PUB 140-3: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-3.pdf

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 Maryland Department of Information Technology's Information Security Policy.

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. HCPSS shall have the right to inspect these policies and procedures 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 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, 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 vulnerability testing of operating system, application, and network devices. 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. HCPSS shall have the right to inspect the Contractor's policies and procedures and the results of 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 Policy (http://doit.maryland.gov/support/Pages/SecurityPolicies.aspx).

15. Ensure HCPSS data is not processed, transferred, or stored outside of the United States ("U.S."). The Contractor shall provide its services to HCPSS and the HCPSS end users solely from data centers in the U.S. Unless granted an exception in writing by HCPSS, the Contractor shall not allow Contractor Personnel to store HCPSS data on portable devices, including personal computers, unless authorized by the HCPSS designee. The Contractor shall permit its Contractor Personnel to access HCPSS data remotely only as required to provide technical support.

16. Ensure Contractor's Personnel shall not connect any of its own equipment to a HCPSS LAN/WAN without prior written approval by the HCPSS designee, which may be revoked at any time for any reason. The Contractor shall complete any necessary paperwork as directed and coordinated with the HCPSS contract designee to obtain approval by HCPSS to connect Contractor-owned equipment to a HCPSS LAN/WAN.

17. Ensure that anti-virus and anti-malware software is installed and maintained on all systems 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 vulnerability scans and take corrective actions for any findings.

(2) Security Logs and Reports Access

(A) For non-HCPSS hosted solutions, the Contractor shall provide reports to HCPSS in a mutually agreeable format.

(B) Reports shall include latency statistics, user access, user access IP address, user access history and security logs for all HCPSS files related to the Contract.

(3) Security Plan

(A) The Contractor shall protect HCPSS data according to a written security policy ("Security Plan") no less rigorous than that of the State of Maryland Information Technology Security Manual and shall supply a copy of such policy to HCPSS for validation, with any appropriate updates, on an annual basis.

(B) 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.

(C) The Security Plan shall address compliance with the NIST Risk Management Framework (RMF) that is used as guidance for the State of Maryland Information Technology Security Manual.

(4) Security Incident Response

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

1. notify in writing as soon as commercially practicable, however no later than forty-eight (48) hours of the discovery of a Security Incident by providing notice via written or electronic correspondence to the HCPSS contract designee, and HCPSS Department of Information Technology designee;

2. notify HCPSS within two (2) hours if there is a threat to Contractor's Solution as it pertains to the use, disclosure, and security of HCPSS data; and
3. provide written notice to HCPSS within one (1) Business Day after Contractor's discovery of unauthorized use or disclosure of HCPSS data and thereafter all information that HCPSS requests concerning such unauthorized use or disclosure.

(B) Contractor's notice shall identify:

1. the nature of the unauthorized use or disclosure;
2. the 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 HCPSS.

(C) The Contractor may need to communicate with outside parties regarding a Security Incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the Contract. Discussing Security Incidents with HCPSS 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.

(D) The Contractor shall comply with all applicable laws that require the notification of individuals in the event of unauthorized release of HCPSS data or other event requiring notification, and, where notification is required, assume responsibility for informing all such individuals in accordance with applicable law and to indemnify and hold harmless HCPSS and its officials from and against any claims, damages, and actions related to the event requiring notification.

(5) 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 HCPSS-identified contact within 48 hours by telephone in accordance with the agreed upon security plan or security procedures unless a shorter time is required by applicable law;
2. Cooperate with HCPSS 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) If a Data Breach is a direct result of the Contractor's breach of its Contract obligation to encrypt HCPSS data or otherwise prevent its release, 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.

1. Additional security requirements may be established in a Task Order and/or a Work Order.
2. HCPSS 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.
3. Provisions shall survive expiration or termination of the Contract. Additionally, the Contractor shall flow down all provisions (or the substance thereof) in all subcontracts.

(6) Problem Escalation Procedure

(A) The Contractor must provide and maintain escalation procedures for both routine and emergency situations. The procedures must state how the Contractor will address problem situations as they occur during the performance of the Contract, especially problems that are not resolved to the satisfaction of HCPSS within appropriate timeframes.

(B) The Contractor shall provide contact information to the HCPSS contract designee, as well as to other HCPSS officials as directed.

(C) The Contractor must provide the escalation procedures no later than fifteen (15) Business Days after notice of recommended award. The procedures, including any revisions thereto, must also be provided within fifteen (15) Business Days after the start of each Contract year and within fifteen (15) Business Days after any change in circumstance which changes the procedures. The procedures shall detail how problems with work under the Contract will be escalated to resolve any issues in a timely manner. The escalation procedures shall include:

1. The process for establishing the existence of a problem;
2. Names, titles, and contact information for progressively higher levels of personnel in the Contractor's organization who would become involved in resolving a problem;
3. For each individual listed in the Contractor's escalation procedures, the maximum amount of time a problem will remain unresolved with that individual before the problem escalates to the next contact person listed in the Contractor's escalation procedures;
4. Expedited escalation procedures and any circumstances that would trigger expediting them;
5. The method of providing feedback on resolution progress, including the frequency of feedback to be provided to HCPSS;
6. Contact information for persons responsible for resolving issues after normal business hours (e.g., evenings, weekends, holidays) and on an emergency basis; and
7. A process for updating and notifying the HCPSS contract designee of any changes to the escalation procedures.

(D) Nothing in this section shall be construed to limit any rights of HCPSS which may be allowed by the Contract or applicable law.

(7) SOC 2 Audit Report

(A) Contractors providing services for identified critical functions, handles Sensitive Data, or hosts any related implemented system for HCPSS under the Contract, the Contractor shall have an annual audit performed by an independent audit firm of the Contractor's handling of Sensitive Data or HCPSS critical functions. Critical functions are identified as all aspects and functionality of the solution including any add-on modules and shall address all areas relating to Information Technology security and operational processes. These services provided by the Contractor that shall be covered by the audit will collectively be referred to as the "Information Functions and Processes." Such audits shall be performed in accordance with audit guidance: Reporting on 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, or according to the most current audit guidance promulgated by the AICPA or similarly-recognized professional organization, as agreed to by the HCPSS, to assess the security of outsourced client functions or data (collectively, the "Guidance") as follows:

1. The type of audit to be performed in accordance with the Guidance is a SOC 2 Type 2 Audit (referred to as the "SOC 2 Audit" or "SOC 2 Report"). All SOC2 Audit Reports shall be submitted to the Contract Monitor as specified in Section F below. The initial SOC 2 Audit shall be completed within a timeframe to be specified by HCPSS. The audit period covered by the initial SOC 2 Audit shall start with the Contract Effective Date unless otherwise agreed to in writing by the HCPSS Contract designee. All subsequent SOC 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.

2. The SOC 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.
3. The audit scope of each year's SOC 2 Report may need to be adjusted (including the inclusion or omission of the relevant trust services principles of Security, Availability, Processing Integrity, Confidentiality, and Privacy) to accommodate any changes to the environment since the last SOC 2 Report. Such changes may include but are not limited to the addition of Information Functions and 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 Report engagement shall accommodate these changes by including in the SOC 2 Report all appropriate controls related to the current environment supporting the Information Functions and/or Processes, including those controls required by the Contract.
4. The scope of the SOC 2 Report shall include work performed by any subcontractors that provide essential support to the Contractor or essential support to the information functions and processes provided to HCPSS under the Contract. The Contractor shall ensure the audit includes all such subcontractors operating in performance of the Contract.
5. All SOC 2 Audits, including those of the Contractor, shall be performed at no additional expense to HCPSS
6. The Contractor shall provide to the HCPSS contract designee, within 30 calendar days of the issuance of each SOC 2 Report, a complete copy of the final SOC 2 Report(s) and a documented corrective action plan addressing each audit finding or exception contained in the SOC 2 Report. The corrective action plan shall identify in detail the remedial action to be taken by the Contractor along with the date(s) when each remedial action is to be implemented.
7. If the Contractor currently has an annual, independent information security assessment performed that includes the operations, systems, and repositories of the Information Functions and Processes being provided to HCPSS under the Contract, and if that assessment generally conforms to the content and objective of the guidance, HCPSS will determine in consultation with appropriate technology and audit authorities whether the Contractor's current information security assessments are acceptable in lieu of the SOC 2 Report(s).
8. If the Contractor fails during the Contract term to provide an annual SOC 2 Report by the date specified, HCPSS shall have the right to retain an independent audit firm to perform an audit engagement of a SOC 2 Report of the Information Functions and Processes utilized or provided by the Contractor and under the Contract. The Contractor agrees to allow the independent audit firm to access its facility/is for purposes of conducting this audit engagement(s) and will provide the necessary support and cooperation to the independent audit firm that is required to perform the audit engagement of the SOC 2 Report. HCPSS will invoice the Contractor for the expense of the SOC 2 Report(s), or deduct the cost from future payments to the Contractor.
9. Provisions in **Section (SOC2 Audit Report)** shall survive expiration or termination of the Contract. Additionally, the Contractor shall flow down the provisions of **Section (SOC 2 Audit Report)** or the substance thereof in all subcontracts.